PROPUESTA DE MEJORA PARA LA GESTIÓN INTEGRAL DE RIESGOS EN UNA EMPRESA DE TECNOLOGÍAS DE LA INFORMACIÓN EN BOGOTÁ

NATALIA ANDREA BUITRAGO DIAZ
JULIAN FELIPE CAHO RODRIGUEZ

PROYECTO INTEGRAL DE GRADO PARA OPTAR EL TÍTULO DE
MAGÍSTER EN GERENCIA INTEGRAL DE LA CALIDAD Y PRODUCTIVIDAD

DIRECTOR
NASLI MIRANDA ARANDIA
INGENIERA INDUSTRIAL
MSC. SISTEMAS INTEGRADOS DE GESTIÓN

FUNDACIÓN UNIVERSIDAD DE AMÉRICA
FACULTAD DE INGENIERÍAS
PROGRAMA DE MAGÍSTER EN GERENCIA INTEGRAL DE LA CALIDAD Y PRODUCTIVIDAD
BOGOTÁ D.C
2024

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____

_____

_____ _____

Nombre del director Nombre

Firma del Director Firma del presidente Jurado

_____

Nombre

Firma del Jurado

_____

Nombre

Firma del Jurado

Bogotá, D.C. agosto de 2024

DIRECTIVAS DE LA UNIVERSIDAD

Presidente de la Universidad y Rector del Claustro
Dr. Mario Posada García - Peña

Consejero Institucional
Dr. Luis Jaime Posada García - Peña

Vicerrectora Académica
Dra. María Fernanda Vega de Mendoza

Vicerrector Administrativo y Financiero
Dr. Ricardo Alfonso Peñaranda Castro

Vicerrectora de Investigaciones y de Extensión
Dra. Susan Margarita Benavides Trujillo

Secretario General
Dr. José Luis Macías Rodríguez

Decana Facultad de Ingenierías
Dr. Naliny Patricia Guerra Prieto

Director Programa de Magíster en Gerencia Integral de la Calidad y Productividad
Msc. Mónica Yennith Suárez Serrano

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

DEDICATORIA

A mi querida mamá: Quiero agradecerte de corazón por ser mi inspiración y apoyo incondicional. Este logro de mi maestría lleva tu amor y aliento en cada página. Tu influencia ha sido mi guía y motivación. Gracias por ser la mejor mamá y celebrar conmigo en cada paso en este camino.

Con todo mi amor,

Natalia Buitrago Diaz

Dedico este proyecto de maestría a ustedes mamá y papá, quienes han sido mi fuente de inspiración, apoyo y aliento incondicional a lo largo de mi vida.

Con sabiduría, paciencia y amor infinito han sido mi mayor motivación para alcanzar mis metas y perseguir mis sueños con determinación.

¡Gracias!

Julián Felipe Caho Rodríguez

AGRADECIMIENTOS

Quiero expresar mi agradecimiento a todas las personas que han contribuido a la realización de esta tesis de maestría en Gerencia Integral de la Calidad y Productividad. En particular, deseo destacar y agradecer profundamente a mi guía y confidente, por su apoyo incondicional y su acompañamiento constante a lo largo de todo el proceso; todo su acompañamiento y aliento fueron fundamentales para no renunciar en momentos difíciles. También quiero agradecer a mi compañero y mejor amigo, Julián Caho, por su apoyo y motivación en este camino que decidimos emprender juntos. A mi familia y amigos, gracias por su comprensión y respaldo. Este logro no habría sido posible sin ustedes. ¡Muchas gracias a todos por ser parte de este importante logro!

Natalia Buitrago Diaz

Agradezco a todas las personas participaron en el desarrollo y culminación de este proyecto. En primer lugar, quiero agradecer a mi familia por su apoyo constante y su comprensión durante todo este proceso. A mamá y papá, su guía y aliento han sido un soporte en todo momento. A mi apoyo incondicional de estos últimos años por acompañarme, aconsejarme y escucharme. A mis amigos, quienes han estado a mi lado brindándome ánimos. Y entre ellos a Natalia Buitrago, pilar fundamental en todo momento desde el inicio hasta la culminación de esta etapa. A nuestra guía de proyecto por su celeridad, aportes y agilidad. A todas las personas que han participado en entrevistas, o que han brindado su tiempo y conocimientos para enriquecer este estudio.

Finalmente, quiero expresar mi gratitud a todas aquellas personas cuyas contribuciones, grandes o pequeñas, han dejado una marca en este trabajo. A todos ustedes, mi más sincero agradecimiento por formar parte de este importante logro en mi vida.

Con gratitud,

Julián Felipe Caho Rodríguez

TABLA DE CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

pág.

RESUMEN

El propósito principal de este proyecto es construir una metodología de gestión de riesgos que facilite la integración de los marcos de referencia aplicables en una empresa tecnológica de la información ubicada en Bogotá. Este enfoque se desarrolla a lo largo de cinco fases secuenciales. La primera fase, conocida como diagnóstico, tiene como objetivo evaluar la situación actual de la empresa, logrando recopilar información y analizar el contexto organizacional, lo que permite una comprensión sobre el cómo se encuentra actualmente la gestión de riesgos. La segunda fase se enfoca en la selección de la metodología, marco o método más adecuado para la empresa, considerando criterios para una gestión del riesgo eficaz. En la tercera fase, se diseña la metodología, basándose en la elección previamente realizada. Esta fase implica la definición de aspectos clave, criterios relevantes, responsabilidades y los actores involucrados en el proceso de gestión de riesgos. Una vez que se ha generado la propuesta metodológica, se avanza a la cuarta fase, que se centra en su aplicación en el contexto real de la empresa. Esto abarca la identificación, análisis y valoración de los riesgos, así como la formulación de controles y planes de tratamiento adecuados. Finalmente, en la quinta y última fase se aplica la evaluación de la propuesta. Su objetivo es determinar la viabilidad y aceptabilidad de la metodología desarrollada en comparación con la que se aplica actualmente en la empresa.

Al aplicar las fases mencionadas, se encontró que la empresa de tecnología gestiona alrededor de 32 matrices de gestión del riesgo, que en conjunto identificaban más de 600 riesgos. Estas matrices se manejaban de manera independiente en los diferentes sistemas de gestión de la empresa.

A partir de esto, se identificaron las metodologías aplicables, de las cuales se seleccionó una metodología y dos marcos de referencia que se alineaban con el Core del negocio de la empresa tecnológica. Luego, se diseñó una nueva metodología que incorpora un artefacto de recolección de datos y unifica las matrices, reduciendo en más de 500 riesgos debido a que le logra una unificación de riesgos que afectan a más de un proceso

y así facilita su gestión de manera optimizada, sin impactar a la correcta identificación de los riesgos que ya estaban definidos y logrando oportunidad en corrección de aquellos que presentaban oportunidades en su identificación. Además, esta metodología permite la integración de los procesos relacionados con el marco ITIL y procesos internos, aplicables a los sistemas de gestión de servicio, calidad y seguridad de la información.

La evaluación comparativa entre la metodología actual y la propuesta reveló que el 80% de los evaluadores, que incluyen gerentes, líderes y responsables de la gestión del riesgo con autoridad de decisión, aprobaron directamente la nueva metodología. Para el 10% de los ítems evaluados, la metodología actual se consideró superior, mientras que para otro 10% de los ítems, no hubo una preferencia clara entre ambas metodologías.

Palabras clave: Gestión del riesgo, sistemas de gestión, tecnologías de la información, integración de sistemas

INTRODUCCIÓN

El presente trabajo de grado se enfoca en la formulación de una propuesta metodológica destinada a la gestión integral de riesgos en una empresa del sector tecnológico con sede en Bogotá. La esencia de esta propuesta radica en la integración de la gestión de riesgos en los diversos Sistemas de Gestión previamente establecidos en la organización.

Como antecedentes para este proyecto, se ha realizado un análisis de proyectos previos desarrollados en organizaciones del mismo sector. Estos proyectos compartían la premisa de diseñar una metodología que incorpora la gestión de riesgos dentro de los marcos de los Sistemas de Gestión existentes. Los resultados de dichos proyectos indicaron mejoras significativas en la eficiencia de la gestión de riesgos y en la formulación de controles y planes de tratamiento debido a la perspectiva holística con la que se abordaron los riesgos en estas organizaciones se tradujo en beneficios notables. Uno de los proyectos representativos dentro de la presente investigación fue el desarrollado por Ávila y Caloggero (2022), en donde demostraron el impacto positivo que tiene la gestión de riesgos dentro de los procesos de tecnologías de la información de la empresa Labe Corporation S.A.C a través de una disminución del 28.94% en el incumplimientos en estándares de TI, teniendo una influencia positiva con la implementación de normas como la ISO 27001 e ISO 31000, los cuales fueron base fundamental de este proyecto (p 50).

Inicialmente se realizó un diagnóstico de la situación actual de la organización con respecto a la gestión de riesgos. Este diagnóstico reveló que, aunque se contaba con una metodología fundamentada en la norma ISO 31000, la gestión de riesgos se efectuaba de forma fragmentada, abordando por separado los riesgos de proceso y los riesgos relacionados con la seguridad de la información. Además, la gestión se dividía en matrices específicas según los procesos, sistemas o clientes, generando una duplicidad en la definición de riesgos y una variación en su gestión, dependiendo del propietario de cada proceso.

Después de considerar varios marcos metodológicos para la gestión de riesgos, se optó por seleccionar aquel que mejor se ajustaba a los criterios preestablecidos dentro de la organización. Basándonos en este marco elegido, desarrollamos una propuesta metodológica que tenía como objetivo centralizar la evaluación de los diferentes sistemas de gestión, tales como Gestión de Calidad, Gestión de Seguridad de la Información y Gestión de los Servicios de TI, en una única matriz.

Esta metodología fue diseñada siguiendo las directrices de la norma ISO 31000 y las pautas definidas por el marco de referencia ITIL, que ofrece un enfoque específico para el sector de tecnologías de la información. En la aplicación de esta metodología, logramos optimizar la gestión de riesgos de manera notable. Consolidamos las diversas matrices en una sola y estandarizamos la gestión de riesgos que anteriormente se realizaba de forma fragmentada. Además, involucramos a los responsables de cada proceso relacionado, centralizando así los esfuerzos con el fin de lograr una mitigación del riesgo más efectiva. Una vez evaluada la metodología por los interesados con poder de decisión, se identifica que la metodología propuesta genera valor significativo dentro de la organización.

OBJETIVOS

Objetivo general

Diseñar una propuesta integral de mejora para fortalecer la gestión del riesgo que permita la integración de las normas de referencia aplicables a la Empresa de Tecnologías de la Información de Bogotá ampliando la oportunidad en toma de decisiones, seguimiento y control dentro de sus operaciones.

Objetivos específicos

- Realizar un diagnóstico inicial de la gestión del riesgo implementado en la empresa de tecnología de Bogotá de la presente investigación identificando las normas de referencia y metodologías aplicadas.

- Determinar los modelos y metodologías aplicables a la empresa de tecnología teniendo en cuenta lo expuesto en el marco teórico y las restricciones de cada una de acuerdo con la actividad económica.

- Proponer un modelo para la gestión del riesgo basados en las mejores prácticas o estándares internacionales adaptados a la operación de la empresa de tecnología.

- Aplicar la propuesta dentro de la organización, de acuerdo con los lineamientos definidos en el diseño para la determinación de resultados, centrándose en el análisis del cambio metodológico propuesto.

- Evaluar la funcionalidad de la propuesta mediante la verificación de requisitos y criterios definidos que permitan validar el funcionamiento y adaptación de esta dentro de la empresa de tecnología.

1. MARCO TEÓRICO

Para Perano et al., (2018) A través del tiempo las organizaciones han evolucionado adoptando diferentes metodologías para hacerse más eficientes y competitivas, así mismo adoptando la gestión del riesgo posiblemente impulsando a su desarrollo y generando una mejor reputación generando valor hacia sus clientes (p.17). Teniendo en cuenta esto, dentro de las organizaciones y proyectos se empezó a emplear los conceptos de gestión del riesgo y control interno pues los pilares fundamentales para el logro de las metas trazadas por la administración, al mismo tiempo que diagnostica la institución y establece planes de intervención estratégica (Hernandez, 2018, p.2).

De la misma forma según lo propuesto por Soler et al. (2018) se ha identificado que el riesgo cero no existe, dado que el riesgo es algo inherente a casi toda actividad empresarial y por esto es necesario contar con un equipo que sea capaz de identificar, evaluar y controlar realizando un tratamiento adecuado de lo que se va identificando (p 53). Adicionalmente, se tiene en cuenta que la gestión del riesgo no solamente se cierra a la reducción de los riesgos identificados, sino también a la interacción y participación de diferentes actores lo que dificulta la toma de decisiones asertivas pudiendo disminuir a cero cualquier tipo de beneficio, significa un proceso de control sobre la construcción o persistencia de amenazas y vulnerabilidad (Lavell y Argüello, 2003, p 14).

Teniendo en cuenta lo anterior, existen diversas metodologías para la gestión del riesgo organizacional, estas metodologías para implementar y gestionar riesgos de tecnologías de información pueden variar en formas, mecanismos de evaluación y presentación de resultados, dado que a partir de lo investigado por Llauce, (2022), algunas son difíciles de implementar y cuantificar, tanto en sus resultados como en sus logros, asimismo, existen otras que se prestan para un diagnóstico numérico (p 29). A partir de esto, a continuación, se relacionan diversas aplicaciones de estas metodologías, en donde se encuentran metodología por mapa de riesgos indagada (Rosales, 2022, p 17) los cuales son una parte fundamental dentro de la gestión correctiva del mismo y con esto, se deben establecer las amenazas teniendo como orígenes diferentes fuentes las cuales pueden

ser asociadas a condiciones humanas o materiales que sean transformados o trabajados por estos, con algún nivel de vulnerabilidad.

Por otro lado, se encuentran el marco de referencia para la gestión del riesgo Magerit la cual implementa el proceso de gestión de riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones, teniendo en cuenta, los riesgos derivados del uso de tecnologías de la información (Becerra et al. 2022, p 7). Adicionalmente, se tiene la metodología Octave, la cual según explican Pedro y Rodríguez, (2022) aporta en gran medida a la definición de criterios y un rango de participación para que se pueda efectuar como exitosa entre los que se pueden encontrar financieros, jurídicos, de renombre, cliente, entre otros (p 74).

A partir de la investigación de Jaspal et al. (2022), Además de las metodologías relacionadas anteriormente, existe la llamada CORAS diseñada para ofrecer un índice de evaluación del riesgo que incluye elementos tanto analíticos (p 791). Según lo que evidenciaron Park et al. (2022), a nivel de marcos de referencia que nos son certificables se cuenta con el estándar asociado a la norma ISO 31000:2018, en donde se tienen diferentes parámetros para la gestión del riesgo, presentando oportunidades a nivel estratégico, metodológico y procedimental tanto cualitativo como cuantitativo aplicable a cualquier ámbito de negocio (p 2).

Así como existen marcos de referencia asociados a ISO para la gestión del riesgo, existen marcos que se asocian como buenas prácticas para el ámbito tecnológico, destacándose ITIL el cual es desarrollado por la oficina de comercio gubernamental (OGC) en el reino unido, aceptado a nivel mundial no solo porque es adaptable al entorno tecnológico sino todos los sectores del mercado (Rusman et al. 2022, p 800).

Todo lo anterior se proyecta para lograr el desarrollo de la propuesta que pretende unificar cada uno de los sistemas de gestión organizacional los cuales están asociados al sistema de gestión de servicios el cual según la Norma NTC-ISO/IEC 20000-1 “Se especifican los requisitos para que un prestador del servicio planifique, establezca,

implemente, opere, monitoree, revise, mantenga y mejore un SGS. Los requisitos incluyen el diseño, transición, prestación y mejora de los servicios para cumplir con los requisitos de servicio" (Instituto colombiano de normas técnicas – NTC ISO/IEC 20000-1:2018 Sistema de gestión del servicio, numeral 1).

Este asociado inicialmente a los servicios de TI pero ampliando alcance a otro tipo de servicios, por otro lado, continuando con el ámbito tecnológico se cuenta con el sistema de gestión de seguridad de la información asociado y acotando la importancia (Instituto colombiano de normas técnicas – NTC ISO/IEC 20000-1:2018 Sistema de gestión del servicio, numeral 1) como el factor clave para decidir sobre la implementación de un sistema de gestión de la seguridad de la información radica en la importancia que los activos de información tienen dentro de una organización como elementos críticos para lograr o no un cumplimiento de las metas y objetivos establecidos.

Adicionalmente, la empresa de la presente investigación cuenta con un sistema que está direccionado para el cumplimiento de la seguridad en importación y exportación de productos de tecnología nombrado OEA (Operador Económico Autorizado) el cual está regulado por la DIAN establecido en el decreto 103 de 2015 se define como los lineamientos propuestos por la Organización Mundial de Aduanas, cualquier organización que garantice que se encuentra alineada con los parámetros de seguridad en toda la cadena de suministro (desde la adquisición de materias primas o productos, hasta la entrega al cliente final) teniendo en cuenta sus aliados, proveedores, contratistas, clientes, empleados mediante el cumplimiento de requisitos en materia de seguridad e historial satisfactorio de obligaciones aduaneras y fiscales. Decreto 103 de 2015 [Presidencia de la República]. Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones. 20 de enero de 2015.

1.1. Antecedentes

En el artículo formulado por Figueroa et al. (2013) se menciona como una adecuada gestión del riesgo, en este caso enfocada en las condiciones laborales, aporta a la dignificación del trabajo de las personas y en cómo pueden mejorar sus condiciones a partir de un correcto estudio de los riesgos y el seguimiento a los controles, aportando a la maximización de la gestión del recurso humano y el logro del aumento de la productividad (p 12). Para Martinez y Blanco, (2017) en su estudio proponen ver la gestión del riesgo desde un enfoque integral en donde evalúan desde diferentes estudios a partir de revisión literaria el impacto que se ha tenido en este tipo de gestiones a nivel de avances tecnológicos y cómo afectan las condiciones externas para potencializar una gestión de riesgos que permita ver los riesgos de manera integral en las organizaciones (p 73).

En la guía “Gestión de riesgos: Una guía de aproximación para el empresario” publicada por el Instituto Nacional de Ciberseguridad (2015) se encuentra de manera fácil y práctica conceptos que son de importancia para tener presente en la implementación de una metodología de gestión de riesgos en una organización, teniendo un enfoque en la importancia que debe tener con respecto al cumplimiento de requisitos sobre la seguridad de la información (p 4). También con respecto a este tipo de literatura, la “Guía de gestión de riesgos: Seguridad y Prevención de la información” publicado por el Ministerio de Tecnologías de la Información de Colombia – MINTIC, (2015) presenta un marco de referencia para la implementación de un sistema de gestión de riesgos en donde enuncia las prioridades y criterios relevantes que se deben tener en cuenta, sobre todo para la definición de los criterios y/o escala de valoración de los riesgos e implementación y seguimiento de controles para la mitigación de los mismos (p 10). Ambas guías tienen como punto en particular que resaltan de manera especial lo contemplados por estándares enfocados en la seguridad de la información. Este tipo de literatura permite tener presente algunos puntos relevantes que pueden definir el éxito de un buen sistema de gestión de riesgos y cómo de manera sencilla se puede relacionar dentro del desarrollo del trabajo de grado.

Ya de manera práctica, se revisaron algunos estudios o experiencias que se han desarrollado en la implementación de este tipo de metodologías o sistemas de gestión, en donde se resalta el publicado por Ochoa (2015) quien hace el diseño de una metodología de gestión de riesgos en una institución de Salud en donde como resultado proponen un método de cinco pasos para organizar la gestión de riesgos en este tipo de organizaciones el cual tiene un nivel aceptable de validez, confiabilidad y objetividad debido a que fue aplicado en tres procesos de manera exitosa (p 5). Otro estudio de referencia fue el presentado por Argüelles et al. (2019) en donde se buscaba analizar la importancia que tiene la gestión de riesgo, en este caso enfocado a desastres, dentro del desarrollo local; en donde se tomó una muestra de los Consejos Populares en Cuba y que como resultados se obtuvieron aportes de información oportuna que aportaba al desarrollo local teniendo aportes teóricos mediante la profundización de conocimientos (p 2).

Dentro del desarrollo del sistema de gestión de riesgo implementado en la Sección de Dermatología de la Universidad de Antioquia realizado por Velásquez et al. (2017) en donde tiene un enfoque basado en la norma NTC-ISO 31000:2011 definieron una metodología de riesgos para gestionar los riesgos clínicos que se podían encontrar, teniendo así un aporte a la implementación de un Sistema de Gestión de Calidad con un marco de referencia como lo es la norma ISO 9001. (p 82)

Por otro lado, se cuenta con la aplicación realizada sobre la gestión del riesgo tomando aspectos de tecnologías de la información, en donde se verifican y se tienen en cuenta diferentes aspectos que se adapten a la secretaría donde se realiza el estudio para adoptar todo lo referente a la gestión del riesgo en activos de información, pero adaptados bajo el estándar de la ISO 31000:2018 (Ayuningtyas y Tanaem, 2022, p 96).

Aterrizando al sector económico en el que se encuentra la empresa en estudio, se encontró el artículo publicado por Correa et al. (2016) en donde se busca articular el uso de estándares para la gestión con una metodología y el gobierno de procesos de TI para asegurar el éxito de iniciativas que puedan afectar la reputación u operatividad de las

empresas demostrando que el éxito de un sistema de gestión de riesgos está en lograr la sinergia entre los estándares, lineamientos o fundamentación teórica con una metodología adecuada a la cultura organizacional y con un gobierno de TI que lidere y defina estrategias a aplicar dentro de la organización. (p 27)

Por otro lado, se identifica que existen metodologías que integran varios marcos como el de continuidad de negocio al que normalmente se asocian los riesgos bajo el esquema presentado de organización integral, permite su inclusión en la gestión de continuidad de negocios como fase de apoyo, en lo respectivo a la identificación de dependencias claves, activos y procesos críticos, amenazas existentes y futuras. Dicha metodología que se estructuró en la investigación consultada tiene su base en los estándares internacional ISO 31000 e ISO 27005, dado su enfoque en gestión de riesgos y siendo parte de los estándares de la familia ISO fue posible establecer una alineación entre los dos y ajustarlos a la metodología diseñada junto al modelo PHVA. (Ramírez y Ortíz, 2011, p 64).

Adicionalmente, Contreras realiza la investigación sobre la comparación entre dos de las principales metodologías para la gestión de riesgos de seguridad las cuales son MAGERIT y OCTAVE, indicando que sus parámetros fueron recopilados durante el desarrollo de las mismas, mediante conceptualizaciones, fases y procesos que permitan identificar cuál metodología cumple con parámetros completos y genere mayor confianza para la reducción de los riesgos. MAGERIT en cierta medida, se considera como la metodología principal para el análisis de riesgos más detallado, teniendo en cuenta los principales objetivos de seguridad para la misión de una organización, así como algunos detalles adicionales en cuanto a su funcionamiento y que no permite ilegalidad del personal analista (Contreras, 2022, p 19).

A partir de la revisión descrita anteriormente, se seleccionaron tres artículos como referencia teniendo en cuenta la afinidad con la definición de metodologías similares a las que se quiere proponer dentro del desarrollo del presente trabajo.

Tabla 1.
Resumen Antecedentes

	Referente 1	***Referente 2***	***Referente 3***
Título	Implementación de la gestión de riesgo en los procesos misionales de la Sección de Dermatología de la Universidad de Antioquia (Medellín, Colombia) siguiendo las directrices de la norma ISO 9001:2015	Information Technology Asset Security Risk Management at the Secretariat of the Salatiga City DPRD Using ISO 31000	Análisis comparativo de metodologías de gestión de riesgos de tecnologías de la Información en el marco de la NTP - ISO/IEC 27001:2014
Autor(es)	Paula Andrea Velásquez-Restrepo Sandra Milena Velásquez-Restrepo Margarita Velásquez-Lopera Jhon Villa-Galeano	Ayuningtyas y Tanaem	Luciano Llauce Valdera
Año	2017	2022	2022
Objetivo	En este trabajo se presenta un procedimiento para la gestión de riesgos de los procesos misionales de la Sección de Dermatología de la Universidad de Antioquia, que busca influir en la calidad y la seguridad del paciente durante el proceso de atención, adoptando a este efecto las directrices de la norma NTC-ISO 31000:2011 (11) y siguiendo la metodología de investigación-acción.	Realizar la identificación y evaluación de riesgos asociados a tecnologías de la información bajo el marco de referencia ISO 31000	Determinar una metodología de gestión de riesgos de tecnología de información que mejor se relacione con la Norma Técnica Peruana NTP - ISO/IEC 27001:2014.
Tipo de investigación	Cualitativa	Cualitativa	Cualitativa
Metodología	1. Identificación del proceso y su contexto. 2. Identificación de los riesgos potenciales 3. Evaluación y valoración de los riesgos 4. Control de los riesgos A partir de esto, se plantea la integración de los riesgos de seguridad y salud en el paciente al sistema de gestión de calidad implementando y manteniendo controles (Velásquez et al, 2017, p 81)	A partir de la identificación de necesidades y partes interesadas se establece: ● Establecer contexto ● Gestión del riesgo basados en la identificación, análisis y evaluación. Luego de esto manejar un monitoreo y análisis continuo (Ayuningtyas y Tanaem, 2022, p 94)	1. Identificación del problema 2. Análisis de la Norma Técnica Peruana NTP-ISO 27001/IEC:2014 y factores de riesgos. 3. Elección del método comparativo. 4. Adaptación de método comparativo 5. Categorización de la información. 6. Desarrollo de los pasos del método comparativo seleccionado 7. Discusión de resultados.

Tabla 2. (Continuación)

	Referente 1	***Referente 2***	***Referente 3***
			El estudio se aplica como referencia metodológica para la identificación de herramientas aplicables de acuerdo con un marco de referencia común con el presente estudio como lo es la ISO 27001 (Llauce, 2022, p 59)
Principales resultados	La gestión del riesgo es un esfuerzo anticipado para reducir las pérdidas que se pueden presentar en el futuro, porque es un proceso de identificación, análisis y cuantificación de las vías adecuadas para emprender acciones preventivas, correctivas y de reducción del riesgo. (Velásquez et al. 2017, p 89). Luego del análisis de los resultados de esta investigación, recomendamos a la Sección de Dermatología mantener la certificación bajo la ISO 9001 e integrarla con el Sistema de Gestión del riesgo, bajo la nueva actualización de la ISO 9001:2015, ya que las estrategias que la sección tiene implementadas dentro de su sistema de gestión son un soporte importante para el desarrollo de una gestión del riesgo proactiva (Velásquez et al. 2017, p 89).	Se llevó a cabo en varias etapas, que incluyen la identificación de riesgos, el análisis de riesgos, la evaluación de riesgos y el tratamiento de riesgos. A partir de estas etapas, en el presente análisis de riesgos identificaron 20 posibles riesgos que podrían interferir con los procesos comerciales en la Secretaría de la DPRD de la ciudad de Salatiga. Adicionalmente, hay 3 posibles riesgos de alto nivel, 12 posibles riesgos de nivel medio y 5 posibles riesgos de bajo nivel. (Ayuningtyas y Tanaem, 2022, p 96)	Se realizó un análisis de las metodologías de gestión de riesgos de tecnologías de información más importantes en el mercado, conforme a seis criterios de selección diseñados para este trabajo investigativo, y se obtuvo como resultado que, de un total de siete (7) metodologías analizadas, solo cuatro (4) cumplieron el 100% los criterios de selección; metodologías que finalmente fueron comparadas con la Norma Técnica Peruana NTP - ISO/IEC 27001:2014. Se determinó que la metodología Magerit V3, es la metodología de gestión de riesgos de tecnologías de información que más se relaciona con la Norma Técnica Peruana NTP-ISO/IEC 27001:2014, al presentar un 96% de similitud (Llauce, 2022, p 134)

Nota. En la tabla se mencionan tres estudios relevantes que comparten similitudes con la presente investigación, contribuyendo así al marco de referencia utilizado.

2. PLANTEAMIENTO DEL PROBLEMA

Actualmente en las organizaciones ha cobrado mayor importancia el tener una adecuada gestión de riesgos que permita de alguna forma visualizar los posibles escenarios de riesgos a los que se puede enfrentar y sobre todo la importancia de verlos de manera holística para diferentes estándares o criterios , por ejemplo con respecto a los riesgos tecnológicos presentados por Gomez et al. (2010) mencionan que las organizaciones son cada vez más conscientes de lo que significan los riesgos informáticos y, sobre todo, han aprendido que en la mayoría de los casos deberán coexistir con ellos pero en forma controlada (p 115).

En particular, la gestión de riesgos para las organizaciones colombianas según Correa et al. (2016) ha permitido que generen un gran conocimiento en medio de un mejoramiento continuo el cual ha contribuido en los últimos años a elevar la productividad consiguiendo aportar en la eficiencia y eficacia de los procesos de la organización y en la definición de estrategias de mejoramiento (p 28).

De acuerdo con lo anterior, es importante mantener definida una gestión del riesgo óptimo y eficiente, en este caso de estudio en la empresa de tecnología del presente proyecto se identificó que se cuentan con varias fuentes de información para el manejo de la gestión del riesgo, cada una enfocada hacia las normas de referencia, entre los que se pueden encontrar ISO 9001:2015 – NTC-ISO/IEC 20000-1: 2018, ISO 27001:2013 y OEA. Adicionalmente, para cada línea de negocio se pueden encontrar diferentes matrices de gestión del riesgo, ya que por cada cliente que tenga un contrato superior a un año, se genera una, lo que aumenta la gestión y la identificación de riesgos en una escala exponencial dependiendo de la variación de clientes dificultando el seguimiento, control y análisis de resultados de la información presentada por cada uno de los sistemas en cuanto a controles efectivos, seguimiento de tratamientos, riesgos materializados.

Si bien la gestión del riesgo de la compañía tiene un marco de referencia bajo la norma ISO 31000, no todos los sistemas están estandarizados dado que en seguridad de la información se deben asociar aspectos como los activos de la información lo que no se relacionan desde los otros sistemas de gestión.

Con base en lo anterior, a continuación, se relacionan las cantidades de matrices de gestión del riesgo por cada sistema de gestión de la compañía:

Tabla 3.

Cantidad de riesgos y matrices por sistema

SISTEMA DE GESTIÓN	NÚMERO DE MATRICES	NÚMERO DE RIESGOS
ISO 27001:2013	1	109
OEA	1	38
ISO 9001:2015 – ISO 20000-1:2018	30	515

Nota. La tabla resume la cantidad de riegos y matrices que se tienen para cada uno de los sistemas de gestión.

De acuerdo con lo anterior, se puede observar que principalmente en las normas de Calidad y Gestión del servicio, se encuentran la mayor cantidad de matrices dado que existe una por cliente, y en estas pueden existir riesgos que ya se encuentren identificados con diferente redacción lo que aumenta la cantidad de riesgos identificados por la línea de negocio.

2.1. Pregunta de investigación

¿Cómo integrar la gestión del riesgo según diferentes estándares para la generación de una propuesta integral de mejora adaptada a las necesidades y operación de una empresa de tecnologías de la información?

3. JUSTIFICACIÓN

Actualmente, debido a la globalización y la transformación digital a raíz de la pandemia, la tecnología ha tenido un desarrollo acelerado y su participación ha aumentado a nivel de las organizaciones (Dellepiane, 2021, p 23). Adicionalmente, Gálvez et at. (2013) indican que este impacto se refleja también en Colombia, donde se marca relación directa entre su uso y el rendimiento de las empresas, presentando las TICs como facilitadores para que la gestión y el desarrollo de actividades sean más eficaces y la interacción entre los procesos pueda ser óptima aplicándose a cualquier sector del mercado (p 357).

Teniendo en cuenta lo anterior, según lo planteado por Gómez et at. (2010), el nivel de participación de la tecnología en las organizaciones ha venido en aumento y con esto, es importante realizar una gestión adecuada del riesgo, pues probablemente se generaron nuevos riesgos que no se contemplaban con la implementación de la práctica tecnológica y es necesario gestionarlos adecuadamente pues de no hacerse, puede generar pérdidas económicas y de otra índole para la organización (p 114).

Adicionalmente, a nivel LATAM también se han venido incorporando metodologías para la evaluación del riesgo, las cuales han demostrado algunos beneficios obtenidos como la preparación corporativa ante la materialización de posibles situaciones identificadas, herramientas de medición, identificación y control lo cual ha llevado a generar beneficios como el aumento de confianza en los clientes dado que al demostrar una gestión del riesgo adecuada, disminuye la incertidumbre hacia la prestación de servicios o compra de productos (Jaramillo y Anzulez, 2020, p 2).

Según lo planteado anteriormente, se realiza un diagnóstico a pequeña escala en donde se identifica que se cuentan con dos metodologías para la identificación y tratamiento de riesgos dentro de los cuatro sistemas implementados en la empresa de tecnología de Bogotá, analizando que se realiza la identificación de riesgos con múltiples tratamientos de acuerdo a lo que se plantea por cada uno de los clientes en donde hay planteamientos

efectivos y otros no efectivos; adicionalmente salvo a documentos con lecciones aprendidas y socializaciones, no se cuenta con un registro que permita evidenciar el nivel de materialización de riesgos, efectividad de controles y las consecuencias generadas por cada uno de estos en los sistemas de gestión asociados a la ISO 9001:2015, NTC-ISO/IEC 20000-1:2015 y OEA; por parte de la metodología de gestión de riesgo asociada a la ISO 27001:2013 se encuentran evidencias parciales sobre la efectividad de controles asociados a los planes de continuidad de negocio cuando los solicitan los clientes.

En el presente proyecto de investigación, se pretende identificar la manera óptima y que reflejen resultados positivos en la gestión del riesgo adoptando dentro de la organización alguna de las metodologías que mejor se adapte a la actividad, partiendo de una evaluación entre estas, definidas de acuerdo a criterios establecidos hasta llegar a la propuesta que permita mejorar la gestión del riesgo que también presente el menor impacto de adaptación, siendo fácilmente replicable en empresas del mismo sector.

Por motivos de confidencialidad, no es posible la relación comercial de la empresa en la cual se aplicará el desarrollo del proyecto, sin embargo, se informa que pertenece al sector tecnológico, ubicada en Bogotá y con sede principal de operaciones en Bogotá.

4. DISEÑO METODOLÓGICO

4.1. Metodología

Durante el desarrollo de este trabajo de investigación tendrá un enfoque mixto y con un alcance descriptivo, en donde buscará establecer una metodología que permita la integración de diferentes estándares haciendo un análisis de riesgos a los procesos o al funcionamiento adecuado del negocio o fin último que tiene la organización.

Lo anterior a través de una investigación basada en la información obtenida dentro de una empresa prestadora de servicios de tecnología en donde se cuenta con un sistema de gestión que busca integrar de manera adecuada la gestión de riesgos teniendo en cuenta las definiciones de diferentes estándares; para la recolección de información se tiene definido hacer un diagnóstico dentro de los procesos actuales en donde a través de la observación e inspección de datos poder determinar la propuesta de mejora dentro del Sistema Integrado de Gestión que tiene actualmente la empresa. A continuación, se exponen las fases que se aplicarán para dar cumplimiento al proyecto:

Figura 1.

Metodología del proyecto

Nota. La Figura resume las fases planteadas dentro de la metodología.

Fase 1: Aplicar instrumento con partes responsables en la empresa, obteniendo el análisis que permita indicar el estado actual de la empresa

Fase 2: Definir los parámetros y criterios para la selección de metodología de gestión del riesgo a aplicar

Fase 3: A partir de lo seleccionado en la fase 2, diseñar la propuesta de adaptación de metodología en empresa

Fase 4: Generar el artefacto de la matriz de riesgos a partir de la metodología propuesta

Fase 5: Seleccionar al grupo evaluador y a partir de los criterios de evaluación, evaluar la propuesta definida

A continuación, se detallan las actividades a realizar y los entregables esperados para lograr el cumplimiento de los objetivos específicos:

Tabla 4.
Metodología

O1	**Diagnosticar (Fase 1)**	
	Actividad	**Registro de cumplimiento**
A1	**Entrevistas por procesos:** A partir del mapa de procesos, definir agendas con los responsables de cada uno y/o de los sistemas de gestión, así se realizan entrevistas 1 a 1 con los actores definidos basados en una lista de chequeo de aspectos verificables sobre la gestión del riesgo	Cronograma de entrevista Aspectos verificables (lista de chequeo)
A2	**Análisis del contexto de la organización:** Recopilar la información y junto con la gerencia realizar el análisis de contexto necesario para el desarrollo de la gestión del riesgo.	Matriz DOFA
A3	**Recolección de información de riesgos por proceso**: Tomar la información documentada por proceso y por sistema tales como registros, formatos, evidencias, manuales y procedimientos de acuerdo con el listado maestro de documentos, identificando cómo se plantea la gestión del riesgo a nivel corporativo.	Relación de información consultada
A4	**Análisis de información recolectada:** Analizar los resultados de las entrevistas e información documentada de la gestión del riesgo corporativa.	Diagnóstico
O2	**Determinar (FASE 2)**	
A1	**Definición de criterios para la selección de la metodología:** Plantear matriz de definición y evaluación de criterios	Criterios de evaluación
A2	**Identificación de modelos y/o metodologías aplicables**: De acuerdo con la actividad empresarial, se estipulan las metodologías que se pueden adoptar para la gestión del riesgo	Estudio aplicado

Tabla 5. (Continuación)

A3	**Evaluación y selección de la metodología a aplicar:** De acuerdo con el análisis de los resultados se selecciona la metodología para realizar la adopción	Cuadro comparativo entre metodologías aplicables y los criterios
O3	**Diseñar (FASE 3)**	
A1	**Definir los criterios de la propuesta de gestión del riesgo seleccionada aplicables a la empresa:** Basados en la metodología seleccionada, se plantean los aspectos, criterios, responsables y actores ajustados para la gestión del riesgo	Propuesta
O4	**Aplicar (FASE 4)**	
A1	**Identificación de riesgos:** A partir del diseño de la propuesta y junto con la metodología se procede con la identificación de riesgos	Matriz de riesgos
A2	**Análisis y valoración de riesgos:** Aplicar la evaluación de riesgos identificados.	
A3	**Definir planes de tratamiento y/o control:** Teniendo en cuenta la evaluación de riesgos, se procede con el planteamiento de tratamiento procedente de cada responsable	
O5	**Evaluar (FASE 5)**	
A1	**Selección de instrumentos:** Definir el instrumento por el cual se va a evaluar la propuesta por parte de los responsables de procesos y/ o sistemas de gestión	Análisis de resultados de la evaluación
A2	**Definición de criterios:** Definir los aspectos evaluables que permitan comparar la gestión del riesgo actual y la gestión propuesta	
A3	**Aplicación de evaluación:** Los responsables de los procesos y sistemas efectúan la evaluación	

Nota. La tabla resume las actividades planteadas para el cumplimiento de cada uno de los objetivos específicos del proyecto.

5. RESULTADOS, ANÁLISIS Y DISCUSIÓN

5.1. Diagnóstico de situación actual

5.1.1. Entrevistas a los procesos

Dentro de la organización, existen 14 procesos dentro del mapa de procesos, de los cuales; 2 son definidos como procesos estratégicos, 7 como procesos misionales y 5 como procesos de apoyo; adicional, la empresa dentro de sus mejores prácticas tiene implementado como referencia el marco de ITIL, el referencia 34 procesos enfocados en la prestación de servicios de TI, de estos actualmente se encuentran definidos dentro de la metodología de gestión del riesgo organizacional 7 procesos (Seguridad de la Información, Gestión de Eventos, Gestión de Cambios, Gestión de Incidentes, Gestión de Acuerdos de Niveles de Servicio, Gestión de Disponibilidad, Gestión de Problemas)

Teniendo en cuenta lo anterior, se realizó una programación de entrevista con los responsables de cada uno de los procesos con el fin de poder conocer los lineamientos o propiedad adquirida con respecto a la gestión de riesgos. Se realizaron 19 entrevistas con los responsables de los diferentes procesos desde los roles tácticos y estratégicos, teniendo como modalidad de los espacios de manera presencial, virtual o en casos particulares que se realizó de modo híbrido, contando con el 100% de la asistencia de acuerdo con lo programado, generando 8 sesiones con el equipo táctico y 11 sesiones con el equipo estratégico. En resumen, las entrevistas realizadas se pueden ver en la siguiente tabla:

Tabla 6.

Entrevistas por proceso

Cargo	Estado	Tipo	Proceso
Gerente Calidad	Ejecutada	Virtual	Calidad
Líder Calidad	Ejecutada	Presencial	Calidad
Líder Calidad	Ejecutada	Virtual	Calidad
Gerente Comunicaciones	Ejecutada	Presencial	Plataforma
Director de comunicaciones	Ejecutada	Presencial	Plataforma

Tabla 4. (Continuación)

Cargo	Estado	Tipo	Proceso
Gerente de servicios de comunicaciones	Ejecutada	Presencial	Plataforma
Gerente Proyectos	Ejecutada	Híbrida	Consultoría
Directora Operaciones Colombia	Ejecutada	Híbrida	Dirección Operaciones
Gerente Automatización	Ejecutada	Presencial	Automatización
Gerente de servicios de operaciones	Ejecutada	Presencial	Automatización
Gerente TI	Ejecutada	Híbrida	Gestión TI
Directora Finanzas	Ejecutada	Híbrida	Finanzas
Gerente de Compras	Ejecutada	Presencial	Compras
Líder de control financiero	Ejecutada	Presencial	Control Financiero
Líder Nómina	Ejecutada	Virtual	Nómina
Líder SST	Ejecutada	Presencial	HSE
Líder de bienestar y desarrollo	Ejecutada	Presencial	Desarrollo de Personas
Director Comercial	Ejecutada	Virtual	Comercial
Gerente de experiencia de cliente	Ejecutada	Virtual	Clientes

Nota. Resumen de las entrevistas realizadas para cada proceso de la organización

Los espacios agendados para cada proceso varían entre 2 a 4 horas teniendo en cuenta la criticidad de este con respecto a la responsabilidad sobre la gestión de riesgos dentro de la organización, lo anterior fue evaluado por parte de los autores de la siguiente manera:

Tabla 7.

Priorización de entrevistas

	NIVEL DE CARGO			NIVEL DE INFLUENCIA		
Proceso	**Operativo**	**Táctico**	**Estratégico**	**Bajo**	**Medio**	**Alto**
Calidad			1			1
Comunicaciones			1		1	
Proyectos			1		1	
Dirección Operaciones			1			1
Operaciones			1		1	
Gestión TI			1		1	

Tabla 5. (Continuación)

Finanzas			1			1
Compras			1		1	
Control Financiero		1			1	
Nómina		1		1		
SST		1		1		
Bienestar y desarrollo		1		1		
Comercial			1			1
Clientes			1		1	

Nota. Priorización de las entrevistas realizadas de acuerdo al tipo del proceso y la influencia dentro de la investigación.

La metodología para el desarrollo de la entrevista fue a través de un grupo focal en donde el objetivo era identificar los conocimientos que tenían las personas entrevistadas para cada uno de los procesos y que sirviera como entrada en el diagnóstico inicial en donde las preguntas guía para el desarrollo de los espacios fueron:

- ¿Cuál es su comprensión actual de la gestión de riesgos de la organización?
- ¿Existen políticas o procedimientos establecidos para la gestión de riesgos?
- ¿Cuáles son los principales desafíos que enfrenta la organización en términos de gestión de riesgos?
- ¿Qué medidas se toman en función de los resultados de las matrices de riesgo?
- ¿Existe alguna área o aspecto específico en la gestión de matrices de riesgo que consideren que necesita mejoras o atención especial?

5.1.2. Análisis del contexto de la organización

A partir de los grupos focales realizados, en conjunto con los responsables de procesos y gerencias, se identifican aspectos asociados a fortalezas, debilidades, oportunidades y amenazas en donde se comentaba a los asistentes qué consistía la herramienta, para algunas personas una breve explicación, para otros informando objetivo, contexto e importancia de la recolección de datos para el desarrollo de la presente investigación, pues el resultado del ejercicio es un insumo importante para la gestión del riesgo que se generaría más adelante. Según esto, los resultados obtenidos por cada vertical se relacionan a continuación de forma general.

Tabla 8.

Matriz DOFA

FORTALEZAS	
1	Experiencia y conocimiento en el modelo de servicios recurrentes
2	Alto volumen de servicios
3	Tomas de decisiones oportunas a partir de analítica de datos
4	Fuerza laboral económica con respecto a región
5	Servicio basado en buenas prácticas de ITIL y aplicación coherente de los sistemas de gestión.
6	Procesos con presencia nacional en todo Colombia para apoyo de soportes
7	Conocimiento multimarca
8	Portafolio competitivo
9	Efecto (Fiscal -económico-financiero) de las políticas de Ingresos
10	Alianzas fortalecidas con partner robustos y reconocidos en el mercado
11	Flexibilidad operativa y funcional remota y presencial
12	Rapidez y asertividad en implementación de automatizaciones reutilizables
OPORTUNIDADES	
1	Demanda creciente de servicios con automatizaciones
2	Generar cross selling basados en la analítica de datos
3	Implementación de Metodologías para el mejoramiento de los sistemas del SIG
4	Mayor aprovechamiento de las plataformas tecnológicas
5	Fortalecimiento del portafolio de servicios a través de nuevas soluciones de innovación.
6	Uso de relaciones comerciales con plataformas y entes que permitan capacitar al personal sobre nuevas tecnologías y certificaciones requeridas. Soluciones multipráctica
7	Mejorar/ mantener alianzas estratégicas con partners que permitan manejar precios competitivos a los clientes y la implementación e integración de nuevas tecnologías

Tabla 6. (Continuación)

DEBILIDADES	
1	Falta de actitud para la prestación servicio
2	Falta de calidad y excelencia de servicio
3	Desconocimiento y falta de implementación de iniciativas de transformación
4	Atender oportunidades de negocio en países latinos donde la capacidad operativa es nula o muy limitada
5	Costos elevados para la dimensión de nuevos negocios
6	Baja usabilidad de los canales para el reporte de peticiones realizadas por los clientes
7	Débil relacionamiento con clientes estratégicos
8	Demora en la atención de requerimientos sobre propuestas comerciales expresadas por los clientes
9	Limitaciones de gestión por autorizaciones regionales
AMENAZAS	
1	Precios y márgenes de la competencia más bajos
2	Alta rotación y salarios del mercado
3	Competidores con altos niveles de automatización
4	Las nuevas generaciones no culminan sus estudios formales
5	Reformas tributarias y políticas, variables macroeconómicas
6	Situaciones imprevistas que no permitan el normal funcionamiento de la compañía (Pandemias – COVID 19 y/o desastres naturales)
7	Inflación de precios e intereses en el mercado.
8	Ataques cibernéticos que superen la capacidad de infraestructura actual

Nota. La tabla relaciona las debilidades, fortalezas. Oportunidades y amenazas de la organización

Ya contando con el resultado por cada vertical a nivel de DOFA, se procede con la recolección de información por cada proceso en la misma sesión programada.

5.1.3. Recolección de información de riesgos por proceso

Teniendo en cuenta los espacios gestionados con los responsables en cada uno de los procesos entrevistados se hizo un análisis de las respuestas obtenidas con el fin de identificar patrones, tendencias y temas recurrentes relacionados con los conocimientos en gestión de riesgos dentro de la organización. De acuerdo con lo anterior, a continuación, se dará respuesta a cada una de las preguntas formuladas de manera consolidada.

- ***¿Cuál es su comprensión actual de la gestión de riesgos de la organización?***

De manera general se evidencia que se reconoce entre los responsables que en la organización actualmente se gestionan los riesgos, pero es evidente que el conocimiento específico sobre la metodología tiene mayor manejo por parte del proceso responsable de los Sistemas de Gestión, debido a que los procesos Misionales consideran que es una gestión transversal en donde se involucran únicamente sí desde Calidad los involucran

- ***¿Existen políticas o procedimientos establecidos para la gestión de riesgos?***

Esta respuesta fue mucho más clara por parte de los responsables del Proceso de Calidad, se pudo evidenciar que se cuenta con una metodología de gestión de riesgos para los procesos y otra para seguridad de la información. En general ambas metodologías están basadas en ISO 31000 pero se tienen la segmentación debido a que los riesgos de seguridad de la información deben contemplar criterios específicos, como lo son el activo de información impacto; lo cual consideran que no es estándar al momento de evaluar los riesgos de proceso.

Definen dentro de la organización a los riesgos de proceso, como los que afectan la ejecución de los procesos específicos dentro de la organización o los que afectan los procesos dentro de la gestión de los servicios de TI, según los estándares de la norma ISO 20000-1 (Gestión de incidentes, requerimientos, etc.). Con respecto a los riesgos de Seguridad de la Información, los ven como riesgos transversales que pueden comprometer la continuidad de los servicios o la fuga de información.

- ***¿Cuáles son los principales desafíos que enfrenta la organización en términos de gestión de riesgos?***

En general, para la organización el reto es la unificación de la gestión de estos dos tipos de riesgos mencionados anteriormente. Debido a que se presenta duplicidad en los riesgos y existe la oportunidad en la optimización de esfuerzos para la gestión de estos.

Consideran importante que se tenga mayor conocimiento y apropiación por parte de la gestión de riesgos en cada uno de los procesos y que se rompa el paradigma que es responsabilidad únicamente del proceso de Calidad.

Adicionalmente, debido a que los servicios contratados se gestionan con cada uno de los clientes de acuerdo con las prácticas ofrecidas, existen matrices de riesgos para cada uno de los proyectos en donde también existen riesgos similares que pueden ser optimizados en su gestión.

- **¿Qué medidas se toman en función de los resultados de las matrices de riesgo?**

De acuerdo con lo definido dentro de del Sistema de Gestión de Calidad y dentro de la Metodología de Gestión de Riesgos para los procesos los resultados obtenidos sobre la gestión de riesgos son presentados a la Alta Dirección y se tienen documentados los planes de tratamiento para cada uno de los riesgos, los cuales tienen seguimiento periódico por parte del Equipo de Calidad.

- **¿Existe alguna área o aspecto específico en la gestión de matrices de riesgo que consideren que necesita mejoras o atención especial?**

Algunos de los aspectos de mejora que se mencionaron por los entrevistados fueron:

- Facilidad en el diligenciamiento.

- Contar con algún método para que se diligencie una única matriz.

- La redacción de un riesgo al momento de la identificación es muy importante, por lo que sería valioso contar con capacitaciones que permitan mejorar estas habilidades.

- Poder identificar riesgos que ya han sido gestionados en otros procesos o proyectos y que podrían facilitar el proceso.

5.1.4. Análisis de información recolectada

Basado en la información recopilada durante el diagnóstico, se llega a la conclusión de que la organización emplea dos metodologías para la gestión de riesgos. Estas metodologías comparten el mismo fundamento en la norma ISO 31000:2018, pero cada una considera criterios específicos según sus respectivos objetivos.

Es importante resaltar que el concepto de riesgo es claro en la organización, pero se aborda desde dos perspectivas distintas:

- Riesgos de Seguridad de la Información: Estos riesgos son de naturaleza transversal y pueden poner en peligro la continuidad de los servicios ofrecidos a los clientes, así como provocar pérdidas o filtraciones de información. Estos riesgos se evalúan en función de los criterios establecidos en la norma ISO 27001:2013.

- Riesgos de Procesos: Estos riesgos están relacionados con la correcta ejecución de los procesos en la organización. Se evalúan de manera específica para cada proyecto o proceso, y se toman como marco de referencia las normas ISO 9001:2015 e NTC-ISO/IEC 20000-1:2018.

En cuanto a la documentación existente en la organización, se ha elaborado un resumen de los procesos con el objetivo de identificar los documentos o registros relacionados con la gestión de riesgos en cada uno de ellos.

Tabla 9.

Resumen de la información recolectada

Proceso	Tipo de Información	Contexto
Calidad	Metodología	Se cuenta con una metodología definida para la gestión del riesgo, el cual tiene las definiciones para la gestión de riesgos de procesos y de Seguridad de la Información. Cada uno de los tipos de riesgos (Procesos - SI) tienen criterios de evaluación específicos
Plataforma	Matrices	Se cuenta con una matriz de proceso general. Pero adicional se tienen matrices de procesos para clientes asociados a la práctica las cuales son gestionadas por parte del equipo de trabajo asignado a cada cliente
	Matrices	Se cuenta con matrices de riesgos asociadas a Seguridad de la Información para clientes dentro de la práctica
Consultoría	NA	Los riesgos de este proceso se encuentran gestionados de alguna manera dentro de las matrices de las otras prácticas. Para Consultoría se encuentra en proceso de construcción y modelamiento. Se puede encontrar matrices de riesgos en clientes donde se encuentren riesgos asociados a Consultoría debido a que anteriormente la práctica era constituida como transversal
Dirección Operaciones	NA	No se cuenta con información específica para el proceso. Es el proceso al cual se le rinde cuenta como Dirección General
Automatización	Matrices	Se cuenta con una matriz de proceso general. Pero adicional se tienen matrices de procesos para clientes asociados a la práctica las cuales son gestionadas por parte del equipo de trabajo asignado a cada cliente
	Matrices	Se cuenta con matrices de riesgos asociadas a Seguridad de la Información para clientes dentro de la práctica
Gestión TI	Matrices	Se cuenta con una matriz de proceso general. Pero adicional se tienen matrices de procesos para clientes asociados a la práctica las cuales son gestionadas por parte del equipo de trabajo asignado a cada cliente
		Se cuenta con matriz de riesgos asociadas a Seguridad de la Información donde se tiene una gestión de los riesgos asociados a la organización, la cual se enlaza con la Gestión de Continuidad del Negocio
Finanzas	Matrices	Se cuenta con una matriz para el proceso en donde se evalúan los riesgos de manera general para el proceso y subproceso

Tabla 10. (Continuación)

Comercial	Matrices	Se cuenta con una matriz para el proceso en donde se evalúan los riesgos de manera general para el proceso y subproceso
Clientes	Matrices	Se cuenta con una matriz para el proceso en donde se evalúan los riesgos de manera general para el proceso y subproceso
Capital Humano	Matrices	Se cuenta con una matriz para el proceso en donde se evalúan los riesgos de manera general para el proceso y subproceso

Nota. Resumen de los documentos recolectados para cada uno de los procesos de la organización.

Adicional, también se pudo identificar que existen varias matrices para la gestión de riesgos dentro de la organización, las cuales fueron resumidas de la siguiente manera:

Tabla 11.

Resumen riesgos

SISTEMA DE GESTIÓN	NÚMERO DE MATRICES	NÚMERO DE RIESGOS
Seguridad de la Información	1	109
Operador Económico Autorizado (OEA)	1	38
Procesos	30	515

Nota. Resumen de la cantidad de riesgos y matrices para cada uno de los sistemas de gestión dentro de la organización.

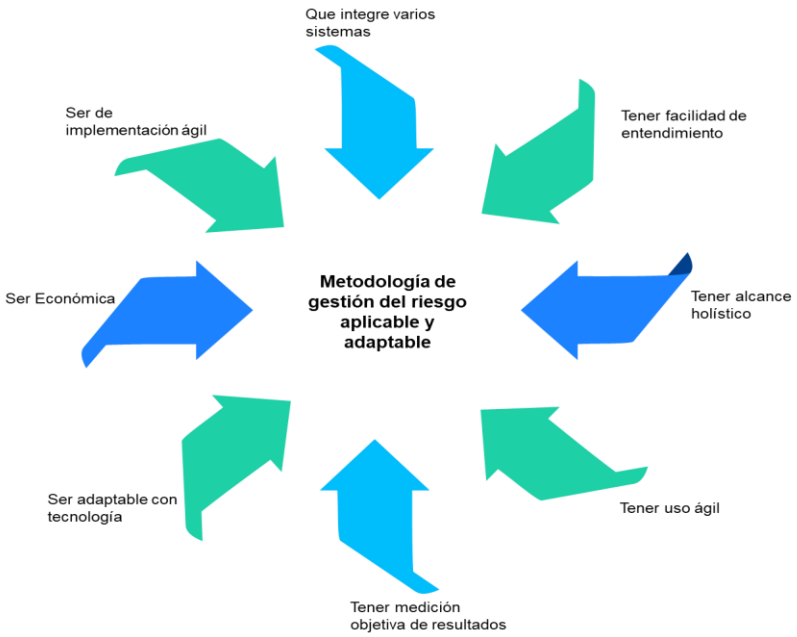
Finalmente, se puede inferir, en virtud del diagnóstico realizado, que la administración de los riesgos de la organización se encuentra centralizada en el ámbito del proceso de Calidad, dado que son ellos quienes ejercen el control de los Sistemas de Gestión implementados. No obstante, se vislumbra una oportunidad de mejora para que los responsables de los demás procesos adquieran un sentido de responsabilidad más arraigado en relación con el cumplimiento de la metodología establecida en cada uno de ellos, con el propósito de promover una cultura organizacional más sólida en torno a la gestión de riesgos.

5.2. Determinación de parámetros aplicables

5.2.1. Definición de criterios de selección

Con el propósito de discernir los aspectos esenciales por la gerencia y responsables de procesos que debe tener una metodología de gestión del riesgo efectiva y aplicable para la empresa de tecnología en Bogotá, se procede con la aplicación de una lluvia de ideas. Durante esta sesión, cada participante genera un insumo inicial, entregando un mínimo de ideas las cuales posteriormente se someten a un análisis por el grupo completo con el objetivo de llegar a un resultado final tras este debate. Una vez concluido el debate y análisis centrado en la selección de los aspectos relevantes, se procede con la identificación de los aspectos que se alinean y requiere la empresa de tecnología en Bogotá para determinar si una metodología es adaptable a la compañía o no obteniendo lo relacionado a continuación.

Figura 2.
Aspectos requeridos por la empresa en una metodología de gestión del riesgo



Nota. Criterios definidos por la organización como relevantes para la evaluación de la metodología

Considerando lo expuesto anteriormente, se procede a evaluar la importancia de cada aspecto a nivel organizacional, por lo que se definió la siguiente escala de evaluación:

Alto (5): El aspecto evaluado es importante para la organización.
Medio (3): El aspecto evaluado es medianamente importante para la organización.
Bajo (1): El aspecto evaluado no es relevante o no es importante para la organización.

A partir de las escalas asociadas y los aspectos relevantes, se genera la evaluación por cada uno en donde luego del consenso entre los asistentes, se obtienen los siguientes resultados:

Tabla 12.

Evaluación de aspectos importantes para la organización

ASPECTO /CRITERIO	BAJO	MEDIO	ALTO
1. Tener facilidad de entendimiento		X	
2. Tener alcance holístico			X
3. Ser de implementación ágil			X
4. Tener uso ágil		X	
5. Tener medición objetiva de resultados			X
6. Ser adaptable con la tecnología		X	
7. Ser económica			X
8. Que integre varios sistemas			X

Nota. Evaluación sobre la importancia de los criterios definidos

Tras analizar los aspectos identificados, se concluye que ninguno de estos se califica como no importante y la mayoría se califican como importantes o relevantes dentro de la organización. En consecuencia, se tomarán todos los aspectos como criterios de evaluación para las metodologías que sean seleccionadas posteriormente como aplicables a la empresa de acuerdo con su actividad.

5.2.2. Identificación de modelos y/o metodologías aplicables

Teniendo en cuenta los criterios definidos por las partes interesadas, se procede a realizar una evaluación para determinar qué métodos y metodologías pueden ser adecuados para la gestión del riesgo, dando como resultados la siguiente matriz:

Tabla 13.

Metodologías de riesgos posibles

Análisis de riesgos y puntos críticos de control (HACCP)	Análisis de modo y efecto de fallas (FMEA)	Análisis de riesgo operacional (ORA)	Análisis de seguridad de procesos (PHA)
ISRAM	Análisis de riesgo de seguridad informática	ISO 27001	Análisis de riesgo y seguridad en el diseño (HAZOP)
Bowtie	ISO 31000	COSO	COBIT
ITIL 4	NIST SP 800-30	OCTAVE	FAIR

Nota. Resumen de las metodologías de gestión de riesgos posibles a aplicar.

No obstante, al analizar cada una de las metodologías, se procedió a descartar varias de ellas debido a que no eran aplicables dentro del sector tecnológico, por lo que a continuación se relacionan las seleccionadas:

Tabla 14.

Metodologías de riesgos depuradas

Análisis de riesgo operacional (ORA)	ISRAM	Análisis de modo y efecto de fallas (FMEA)	ISO 31000
COSO	COBIT	ISO 27001	ITIL 4
Bowtie	NIST SP 800-30	OCTAVE	FAIR

Nota. Resumen de las metodologías depuradas de acuerdo a su aplicabilidad.

A partir de las 12 metodologías elegidas, se registra un detalle de información adicional para cada una, obteniendo la siguiente resultante:

Tabla 15.

Resumen conceptual de metodologías de riesgos posibles

Metodología	Creador	Descripción
Análisis de riesgo operacional (ORA)	Banqueros y reguladores financieros	Es una metodología para evaluar los riesgos operativos en una organización, incluyendo los riesgos asociados con los procesos, el personal, la tecnología y el entorno empresarial. Se utiliza en la gestión de riesgos en el sector financiero. Específicamente se encuentra en el sector financiero, sin embargo, al gestionar riesgos en diferentes frentes, especialmente el tecnológico, es probable que se pueda adaptar a la empresa de tecnología de la presente investigación. (Izhar et at, 2010, p 92).
ISRAM	Profesionales de la seguridad	Es una metodología para evaluar los riesgos asociados con la seguridad física y la protección de activos, incluyendo la identificación de amenazas y la evaluación de los riesgos asociados con cada amenaza. Se utiliza en la gestión de la seguridad en una variedad de sectores, desde la seguridad pública hasta la seguridad empresarial. (Gonzalez et al. 2021, p 3). Al igual que la anterior, aunque son aplicadas en otros sectores puede ser aplicable a una empresa de tecnología pues toca aspectos que se deben fortalecer a niveles de infraestructura o procesos
Análisis de modo y efecto de falla (FMEA)	Ingenieros de seguridad	Es una metodología para identificar y evaluar los riesgos de falla en un sistema complejo, con el objetivo de prevenir fallas y mejorar la confiabilidad del sistema. Se utiliza en la gestión de la seguridad en una variedad de sectores, desde la industria automotriz hasta la atención médica. (Sharma & Srivastava, 2018, p 2). Según lo analizado, aunque no es de producción la empresa de la presente investigación, esta metodología está enfocada también hacia la mejora asegurando procesos.
ISO 31000	Organización Internacional de Normalización (ISO)	Es una norma internacional que establece los principios y directrices para la gestión del riesgo en cualquier tipo de organización, incluyendo la identificación, análisis y evaluación de riesgos, así como la selección y aplicación de medidas de gestión del riesgo. (Instituto colombiano de normas técnicas – NTC ISO 31000:2018, Gestión del riesgo. Principios y directrices, p 3)
COSO	Committee of Sponsoring Organizations of the Treadway Commission	De acuerdo con Sousa et al, (2020) COSO es un marco de gestión de riesgos empresariales desarrollado por un grupo conjunto de organizaciones privadas sin fines de lucro. Se utiliza para ayudar a las organizaciones a identificar, evaluar y gestionar riesgos en todas las áreas de su operación. (p 6)

Tabla 16. (Continuación)

ITIL	Axelos	Es un marco de gestión de servicios de TI que se centra en la entrega de servicios de alta calidad y en la satisfacción del cliente. El enfoque de gestión del riesgo de ITIL 4 se centra en la identificación y evaluación de los riesgos asociados con los servicios de TI, así como en la selección y aplicación de medidas de gestión del riesgo (Gehrmann, 20212, 5)
ISO 27001	Organización Internacional de Normalización (ISO)	Según el (Instituto colombiano de normas técnicas – NTC ISO 27001, Seguridad de la Información). Es una norma internacional que establece los requisitos para un sistema de gestión de la seguridad de la información (SGSI) efectivo en cualquier tipo de organización (numeral 6.1.2). El enfoque de gestión del riesgo de ISO 27001 se centra en la identificación, evaluación y gestión de los riesgos de seguridad de la información.
Bowtie	Shell	El método Bowtie es una técnica de análisis de riesgos visuales que se utiliza para identificar y gestionar riesgos. El método se basa en una representación gráfica con posibles caminos de falla, donde los eventos tendrán una probabilidad de ocurrencia (Ruijter y Guldenmund, 2016)
NIST SP 800-30	National Institute of Standards and Technology (NIST)	A partir de la Guide for Conducting Risk Assessments es una guía del NIST de los Estados Unidos para la gestión de riesgos de tecnología de la información. Proporciona un enfoque detallado para la identificación, evaluación y mitigación de riesgos en los sistemas de TI. (NIST, 2012, p 4)
OCTAVE	Software Engineering Institute (SEI) de la Universidad Carnegie Mellon	Es un enfoque de evaluación y gestión de riesgos desarrollado específicamente para abordar los riesgos de seguridad de la información en las organizaciones de TI. Proporciona una metodología estructurada para identificar y mitigar los riesgos de seguridad (Alberts et at. 2005, p 3).
FAIR	Factor Analysis of Information Risk (FAIR) Institute	Es un modelo cuantitativo para evaluar y gestionar los riesgos de seguridad de la información. Proporciona un enfoque basado en datos y análisis para evaluar los riesgos en términos de pérdidas económicas, lo que permite tomar decisiones informadas sobre la asignación de recursos para mitigar los riesgos. (Pribadi y Ramli, 2023, p 675)
COBIT	ISACA y IT Governance Institute (ITGI)	Control Objectives for Information and Related Technologies (COBIT) es un marco de gobierno y gestión de TI que aborda la gestión de riesgos de TI en términos de alineación con los objetivos del negocio, la entrega de valor y la gestión de riesgos y recursos. (ISACA, 2012, p 13)

Nota. Resumen teórico sobre las metodologías que son aplicables dentro de la organización

5.2.3. Evaluación y selección de la metodología a aplicar

A partir de las metodologías seleccionadas para la aplicación de la evaluación, se procede con la verificación por cada una los criterios previamente definidos en conjunto con los líderes de procesos obteniendo la matriz presentada a continuación:

Tabla 17.
Matriz de metodologías y criterios de selección

Metodología /Criterio de selección	Facilidad de entendimiento	Alcance holístico	Implementación ágil	Uso ágil	Medición objetiva de resultados	Ser adaptable con la tecnología	Ser económica	Que integre varios sistemas
Análisis de modo y efecto de fallas (FMEA)		x			x	x		x
Análisis de riesgo operacional (ORA)				x	x	x		x
Análisis de riesgo de seguridad (SRA)			x	x	x	x		x
ISO 31000	x	x	x		x	x	x	x
COSO		x			x	x		x
ITIL 4	x	x			x	x	x	x
ISO 27001		x		x	x	x		x
Bowtie		x				x		x
Octave	x			x	x	x		x
FAIR					x	x		
COBIT		x						x
NIST SP 800-30					x	x		x

Nota. Resumen de la evaluación de cada una de las metodologías aplicables versus los criterios definidos dentro de la organización

De acuerdo con lo mencionado anteriormente, se observa que la metodología que mejor se adapta es la ISO 31000 con un cumplimiento de siete de los ocho ítems establecidos. Sin embargo, es importante destacar que tanto ITIL como la ISO 27001 obtuvieron un cumplimiento de seis ítems cada una. Por lo tanto, se efectuará la revisión de las tres con el propósito de generar la metodología que sea completamente aplicable a la empresa de tecnología de la información.

5.3. Diseño de propuesta metodológica

Teniendo en cuenta la metodología seleccionada, se ha desarrollado una propuesta aplicable a la organización con el objetivo fundamental de proporcionar una metodología integral que permita la identificación, análisis, valoración, definición de controles y planes de tratamiento de los riesgos que puedan afectar los procesos, servicios y activos de información, y que, a su vez, contribuya al cumplimiento de la misión y objetivos de la entidad dentro de su Sistema Integrado de Gestión. Esta metodología se fundamenta en los lineamientos establecidos por la norma ISO 31000 de Gestión del riesgo, abarcando criterios que satisfacen los estándares de la norma ISO 27001 y modelo ITIL, los cuales, a su vez, se basan en los principios fundamentales definidos dentro de la misma norma ISO 31000 de Gestión del riesgo.

5.3.1. Definir los criterios de la propuesta de gestión del riesgo seleccionada aplicables a la empresa

La metodología propuesta se diseñó con el propósito de integrar de manera cohesionada la gestión de riesgos en los sistemas de gestión previamente implementados dentro de la organización. Estos sistemas son: el Sistema de Gestión de Calidad (ISO 9001:2015), el Sistema de Gestión de Seguridad de la Información (ISO 27001:2013) y el Sistema de Gestión del Servicio (NTC-ISO/IEC 20000-1:2018). Mediante esta integración, se busca fortalecer la eficacia y eficiencia de la gestión de riesgos, logrando así una gestión organizacional más cohesionada y alineada con las mejores prácticas y estándares internacionales. Es importante mencionar que, en la metodología propuesta, se mantiene

la versión de la norma ISO 27001:2013, debido a que, en el momento de la ejecución del proyecto, la migración a la nueva versión no estaba dentro del mapa de ruta de la organización. La metodología se estructura en distintas fases para su implementación eficiente:

Fase 1 - Identificación del riesgo: En esta etapa se procede a identificar exhaustivamente las diversas fuentes, causas y posibles consecuencias que podrían afectar el cumplimiento de los objetivos establecidos para los procesos dentro del alcance definido. Para hacer una adecuada identificación del riesgo se deben considerar los siguientes parámetros:

Tabla 18.

Parámetros identificación de riesgos

Parámetro	Definición
Proceso al que pertenece el riesgo	Identificar el proceso específico al cual está asociado cada riesgo.
Riesgo	Describir detalladamente los riesgos identificados que podrían afectar el proceso en cuestión.
Causas	El responsable del riesgo debe determinar las causas que podrían generar cada riesgo.
Consecuencias	El responsable del riesgo debe identificar y describir las posibles consecuencias indeseadas que podrían surgir si el riesgo se materializa.
Objetivo que puede ser afectado	Identificar y relacionar los objetivos, ya sean procesos o estratégicos, que podrían ser impactados por la materialización del riesgo. Aplica para riesgos de gestión de calidad
Activos de información afectado	En el caso de los riesgos de seguridad de la información, se deben indicar los Activos de Información específicos que podrían verse afectados si el riesgo se hace realidad, tomando como referencia el Inventario de Activos de información.

Nota. Resumen de los parámetros definidos para le identificación de riesgos, los cuales están basados en la norma ISO 31000:2018

Fase 2 - Análisis de riesgos: En esta etapa, se lleva a cabo el desarrollo y la comprensión detallada de cada riesgo, proporcionando una base sólida para su posterior

evaluación. Además, se establecen criterios para determinar la necesidad de abordar los riesgos identificados y se definen estrategias adecuadas para su tratamiento.

Tabla 19.

Criterios según el sistema de gestión al que aplique el riesgo

Seguridad de la Información	**Confidencialidad:** Asegurar que la información solo sea accesible para quienes cuenten con la autorización correspondiente. Se refiere a datos cuya divulgación podría ocasionar desventajas competitivas, pérdidas económicas y afectar la reputación o imagen de la organización. **Integridad:** Proteger la precisión y la integridad completa de la información y los métodos de procesamiento. Se busca evitar errores o fraudes que puedan ocasionar pérdidas **Disponibilidad:** Asegurar que los usuarios autorizados tengan acceso a la información y a los activos asociados cuando lo necesiten. La información debe ser fácilmente accesible y recuperable incluso en situaciones de suspensión del procesamiento
Gestión de Calidad y Gestión del Servicio	**Satisfacción del cliente:** Evaluación de la percepción del cliente en cuanto al grado de cumplimiento de sus requisitos y expectativas **Efectividad del proceso:** Medición del logro de los objetivos del proceso en términos de tiempo y eficiencia de recursos empleados. **Oportunidad del servicio:** Cumplimiento de los términos y condiciones acordados desde el momento en que se realiza la prestación del servicio. **Calidad del servicio:** Se refiere a la satisfacción de las necesidades y expectativas de los clientes, asegurando un nivel óptimo de servicio y atención.

Nota. Criterios definidos para cada sistema de gestión abordado en la metodología propuesta

Para abordar los riesgos identificados, se procede a un análisis detallado que incluye una evaluación cuidadosa de la probabilidad de que cada riesgo se materialice y las posibles consecuencias que podrían derivar de su ocurrencia (conocido como impacto).

Al considerar tanto la probabilidad como el impacto, se obtiene una visión integral de la importancia y urgencia de cada riesgo, lo que facilita la priorización adecuada de las acciones y estrategias para su gestión. Así, el proceso de análisis se convierte en un componente crucial para la formulación de planes de tratamiento y en la adopción de medidas preventivas y correctivas, encaminadas a salvaguardar los intereses y objetivos de la organización.

Dentro de la propuesta, hemos desarrollado criterios que nos permiten asignar niveles de probabilidad adecuados a cada riesgo identificado. Estos criterios, que se detallan en el siguiente cuadro, nos brindan una visión clara y objetiva de la posibilidad de que un riesgo se materialice.

Tabla 20.

Matriz de probabilidad

Nivel	Frecuencia Cuantitativa	Frecuencia Cualitativa
Muy bajo (Excepcional)	Nunca se ha materializado el riesgo, pero no se descarta su ocurrencia.	Puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales).
Baja (Remoto)	La materialización del riesgo ocurre en periodo de 2 a 5 años.	Puede ocurrir en algún momento.
Moderada (Posible)	La materialización del riesgo ocurre una vez al año.	Se espera que ocurra en algún momento.
Alta (Frecuente)	La materialización del riesgo ocurre una vez al mes.	Es viable que ocurra en la mayoría de las circunstancias.
Muy alta (Inminente)	La materialización del riesgo ocurre diariamente.	Se espera que ocurra en la mayoría de las circunstancias.

Nota. Matriz de prioridad definido dentro de la metodología propuesta, el cual tiene como referencia la norma ISO 31000:2018

De igual forma, para cada riesgo se requiere una estimación del impacto potencial de sus consecuencias en caso de materializarse, teniendo en cuenta las consecuencias identificadas durante la etapa previa. Para asignar el nivel de impacto correspondiente a cada riesgo, se utilizará la siguiente tabla como referencia:

Tabla 21.

Matriz de impacto

Categoría	Operacional	Reputacional	Legal
1 - Insignificante	No afecta la operación de las actividades del Proceso.	La afectación de la imagen del proceso es insignificante y se puede resolver fácilmente.	No genera afectación legal.
2 - Leve	Genera reprocesos en las actividades cotidianas, pero no afecta significativamente la operación del Proceso.	La afectación de la imagen del proceso es leve y se puede resolver al interior de este.	Incumplimiento de políticas, procedimientos y lineamientos definidos como buenas prácticas.
3 - Moderado	Genera reprocesos y afecta parcialmente los procesos.	La afectación de la imagen involucra a varios procesos en la organización, afectando la reputación interna y transversalmente en la Organización.	Incumplimiento de políticas, procedimientos y lineamientos relacionados con el cumplimiento de requisitos legales.
4 - Severo	Afecta la operación de varios Procesos, incidiendo en el cumplimiento de Acuerdos de Nivel de Servicio (ANS) con los clientes.	Se afecta la imagen de la Organización, generando pérdida de credibilidad y opinión pública negativa (clientes, partes interesadas).	Acciones legales hacia la Organización por personas jurídicas o naturales debido a incumplimiento de obligaciones legales y contractuales (demandas, denuncias, sanciones, multas o inhabilidades).
5 - Catastrófico	Afecta la operación de toda la Organización.	Se ve gravemente afectada la imagen de la Organización, con pérdida de credibilidad y opinión pública negativa, con divulgación en medios de comunicación.	Acciones legales hacia la Organización por parte de entes de control, que podrían resultar en la cancelación de licencias de operación. Incumplimientos legales que lleven a la intervención por orden judicial o de autoridad competente.

Nota. Matriz de impacto definida dentro de la metodología propuesta, el cual tiene como referencia la norma ISO 31000:2018

Teniendo en cuenta la combinación entre impacto y probabilidad, se define la zona de riesgo la cual se describe dentro del siguiente mapa de calor:

Tabla 22.

Mapa de calor

5 muy alta (Casi certeza)	Zona Media	Zona Alta	Zona Extrema	Zona Extrema	Zona Extrema
4 alta (Frecuente)	Zona Baja	Zona Media	Zona Alta	Zona Extrema	Zona Extrema
3 moderada (Posible)	Zona Baja	Zona Media	Zona Media	Zona Alta	Zona Extrema
2 baja (Rara Vez)	Insignificante	Zona Baja	Zona Media	Zona Media	Zona Alta
1 muy baja (Excepcional)	Insignificante	Insignificante	Zona Baja	Zona Baja	Zona Media
PROBABILIDAD	**1-Insignificante**	**2 - Leve**	**3-Moderado**	**4 - Severo**	**5-Catastrófico**
	IMPACTO				

Nota. Mapa de calor de acuerdo con la combinación entre la probabilidad e impacto

De acuerdo con la zona en la que se defina el riesgo, en su valoración, se define un plan de tratamiento de la siguiente manera:

Tabla 23.

Tratamiento de riesgos

ZONA	TRATAMIENTO
Insignificante	Riesgos de baja exposición y severidad, para lo cual se recomienda monitoreo permanente. Los riesgos en esta zona pueden ser asumidos
Bajo	Riesgos de baja exposición y severidad, para lo cual se recomienda monitoreo permanente. Los riesgos en esta zona pueden ser asumidos.
Medio	Riesgos de mediana severidad, para los cuales se requiere de monitoreo permanente. Los riesgos en esta zona pueden ser asumidos, sin embargo, se recomienda plantear controles para llevarlos a la zona de riesgos baja.
Alto	Riesgos que requieren de controles y alertas permanentes que permitan su gestión constante. Los riesgos en esta zona no podrán ser asumidos.
Extremo	Riesgos de alta severidad y exposición, para los cuales se deben implementar sistemas de control para su adecuado tratamiento, los cuales por su importancia y criticidad son de máxima prioridad para la organización. Los riesgos en esta zona no podrán ser asumidos.

Nota. Matriz de tratamiento de riesgos basada en la norma ISO 31000:2018

Con base en esta primera evaluación de la probabilidad y el impacto, se determina el riesgo inherente, que se define como el riesgo intrínseco de una actividad o un conjunto

de ellas, sin considerar el efecto de medidas de tratamiento o controles que permitan llevarlo a los niveles aceptables por la organización.

En otras palabras, el riesgo inherente representa la exposición de la organización frente a los posibles riesgos identificados, sin tener en cuenta las acciones de mitigación que se puedan aplicar posteriormente. Esta evaluación del riesgo inherente es un punto de partida crucial, ya que proporciona una visión objetiva de la magnitud de los riesgos antes de implementar cualquier medida de tratamiento, permitiendo a la organización identificar áreas de mayor vulnerabilidad y tomar decisiones informadas para abordar los riesgos de manera efectiva y lograr niveles aceptables de riesgo para la organización.

Fase 3 – Evaluación de riesgos

Para tratar o gestionar los riesgos identificados, se deberán implementar los controles suficientes para disminuir su probabilidad o impacto. Ya sean controles preventivos, los cuales actúan sobre las causas del riesgo, con el fin de disminuir la probabilidad de ocurrencia, en general este tipo de controles son considerados como la primera barrera de seguridad que se establece para reducir un riesgo. O también pueden definirse, controles correctivos, que son aquellos que permiten corregir la desviación de los resultados en un proceso y prevenir de nuevo su ocurrencia; este tipo de control toma las acciones necesarias una vez se ha materializado el riesgo y busca mejorar los demás controles.

Fase 4 - Tratamiento de riesgos

Una vez calificados los controles y evaluado su nivel de incidencia en la mitigación de los riesgos, si el riesgo con controles se ubica en una zona de riesgo que requiera tratamiento, este se deberá realizar en función de las siguientes opciones:

Tabla 24.

Tratamiento de riesgo

Evitar el Riesgo	Implica tomar medidas encaminadas a prevenir su materialización, se logra cuando al interior de los procesos se generan cambios sustanciales por mejoramiento, rediseño o eliminación de la actividad o proceso que originan el riesgo.
Reducir el Riesgo	Implica tomar medidas encaminadas a disminuir tanto la probabilidad, como el impacto, a través de la optimización de los procedimientos y la implementación de controles.
Compartir o Transferir el Riesgo	Implica reducir su efecto a través del traspaso de posibles impactos a otras Institución, como por ejemplo el caso de los seguros o a través de otros medios que permitan distribuir una porción del riesgo a otra Organización.
Asumir el Riesgo	Una vez el riesgo ha sido reducido o transferido puede quedar un riesgo residual que se mantiene, en este caso la gerencia general, puede asumir el riesgo residual.

Nota. Opciones de tratamiento de riesgos basados en la norma ISO 31000:2018

El resultado del riesgo obtenido después de confrontar los controles como resultado de los planes de tratamiento de riesgos establecidos se denomina riesgo residual.

Los responsables de los riesgos deben formular los planes de tratamiento de riesgos o mejora de controles necesarios para el tratamiento de los riesgos residuales según su zona de criticidad. Los riesgos residuales después de la implementación de los planes de tratamiento deberán ser aceptados por los líderes de los procesos correspondientes.

Fase 5 - Monitoreo y seguimiento de los riesgos

Para el seguimiento a cada uno de los riesgos evaluados en zonas de riesgo severo y catastrófico, con el fin de validar la ejecución oportuna y eficacia de las acciones planificadas en los diferentes planes de tratamiento definidos por los responsables.

Todo lo anteriormente mencionado dentro de las fases propuestas, se encuentra plasmado dentro del formato de matriz de riesgos en el cual será aplicable la metodología dentro de la organización.

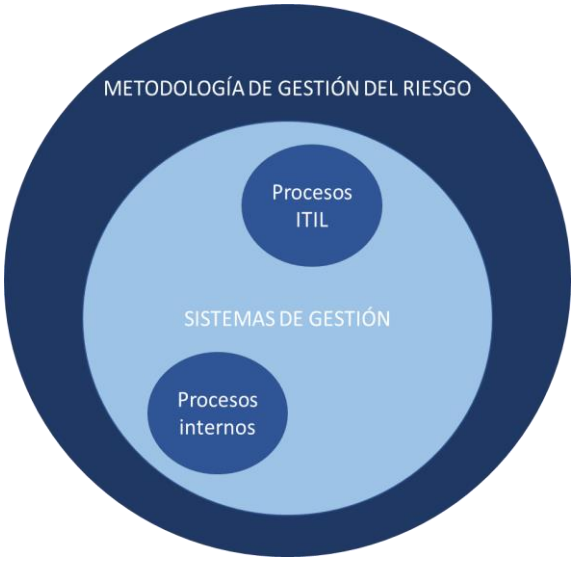
5.4. Aplicación de metodología de la gestión del riesgo

Debido a la naturaleza sensible de la información contenida en la matriz de riesgos de la empresa, por razones de seguridad de la información, no es posible proporcionar de manera completa. Es por esto, que se proporciona una versión genérica y representativa que permita evaluar la aplicación de la metodología propuesta. Esta muestra destaca los elementos clave del análisis de riesgos, preservando al mismo tiempo la confidencialidad de la información sensible.

Se introduce un artefacto de matriz de riesgos que abarca todos los criterios establecidos previamente. En las secciones subsiguientes, se proporcionará una explicación detallada de estos criterios, siguiendo la secuencia de fases dentro de la metodología. Este enfoque integrado permite la cobertura holística de diversos sistemas y procesos. Para una visión más detallada de la matriz, consultar el Anexo *Matriz de gestión de riesgo propuesta.*

Figura 3.

Alcance de la gestión de riesgo propuesta



Nota. El diagrama define el alcance de la gestión de riesgo propuesta

5.4.1. Identificación de riesgos

Para la identificación de riesgos se plantean los siguientes campos los cuales se deben diligenciar dentro de la matriz propuesta:

- Tipo de proceso: En este campo se debe seleccionar si son procesos internos de la compañía o procesos asociados al marco ITIL con el fin de desplegar la lista asociada a cada uno de estos frentes del siguiente campo.

- Proceso: Una vez seleccionado el campo anterior (dependiendo de cada campo) se desplegarán diferentes opciones ya sean todos los procesos internos o los 22 procesos asociados a ITIL, esto para poder agrupar tanto el marco ITIL como los procesos internos dentro de un solo artefacto que permita tener una visual completa sobre las operaciones de la empresa.

- ID Riesgo: Cada Riesgo debe tener su identificador con el fin de poder ubicarlo posteriormente en la matriz de calor para realizar los tratamientos respectivos según aplique de acuerdo con la metodología planteada

- Tipo de riesgo: Bajo este aspecto se dividen en tres opciones que están asociadas al sistema de seguridad de la información, sistema de gestión de la calidad y sistema de gestión del servicio, cada sistema tiene un campo que se debe marcar con X admitiendo marcar con todas las opciones posibles según necesidad, por ejemplo, el sistema de seguridad de la información y el sistema de gestión del servicio sin marcar el sistema de gestión de la calidad. Este campo permitirá facilitar el análisis de riesgo más adelante y adicionalmente, nos indica si el riesgo tiene transversalidad entre los sistemas o si le aplica a uno o uno específicamente.

- Riesgo: Se debe redactar claramente cuál es el riesgo identificado.

- Causa: Registrar cual o cuales son las causas que pueden efectuar la materialización del riesgo.

- Consecuencia: Identificar todas las consecuencias que se podrían generar por la materialización del riesgo.

- Objetivo que afecta: Teniendo en cuenta que la identificación de los riesgos se basa en todos estos escenarios que se pueden afectar al cumplimiento de objetivos propuestos, se incluye dentro del artefacto este campo para garantizar que los riesgos siempre tengan un criterio bien definido.

- Activo de la información (aplica solo para riesgos de la seguridad de la información): Este campo se registra siempre que se active en el campo del tipo de riesgo el sistema de seguridad de la información pues se debe relacionar el ID del activo asociado (listados en la pestaña de “inventario de activos”) y paralelamente el nombre del activo afectado, esta información se identifica de forma automática de acuerdo con el ID seleccionado.

De acuerdo con lo descrito anteriormente y como ejercicio práctico a continuación, se plantea en el **Ejemplo 1** un riesgo trabajado dentro de la organización con el fin de poder brindar mayor claridad en el manejo de la matriz propuesta:

Ejemplo 1:

Figura 4.

Sección identificación de procesos y tipo de riesgo

Tipo de proceso	Proceso	ID RIESGO	Tipo de Riesgo		
			Seguridad de la Informaci	Gestión de Calidad	Gestión del Servicio
PROCESOS INTERNOS	Compras y logística	RSI14	X		
PROCESOS INTERNOS	Juridica				
PROCESOS INTERNOS	Gestión TI				
PROCESOS INTERNOS	Nómina				
PROCESOS INTERNOS	Gestión TI				
PROCESOS INTERNOS	Gestión TI				

Nota. Matriz de riesgo caso aplicación

Figura 5.

Sección riesgo, causa y consecuencia

Riesgo	Causa	Consecuencia
Robo y/o pérdida de equipos. Medios de almacenamiento y documentos	*Ejecución de procedimientos inadecuados en temas de seguridad *Ausencia de un perfilamiento para el acceso de las herramientas de monitoreo y control *Falta de Backup de la plataforma tecnológica *Pérdida de integridad y disponibilidad de la información	*Acceso a información sensible / confidencial / propiedad intelectual que puede ser copiada / utilizada y/o robada *Corrupción de la información

Nota. Matriz de riesgo caso aplicación

Figura 6.

Sección de activos de información

Activos de Información (Aplica para riesgos de seguridad de la Información)	
Activos Afectados (ID)	Activos Afectados (Nombre)
1	Carpeta proveedor
3	Contratos y Anexos
17	Share point
8	Historias Laborales
10	Herramienta de monitoreo
5	Estaciones de trabajo (Equipos PC´s)

Nota. Matriz de riesgo caso aplicación

5.4.2. Análisis y valoración de riesgos

Una vez diligenciado el primer módulo de identificación de riesgos se debe continuar con el módulo de análisis de riesgos dentro de la matriz de riesgos, aquí se deben registrar los siguientes aspectos:

- Criterios de seguridad afectados: En caso de que en el tipo de riesgo se haya marcado seguridad de la información, este campo estará habilitado para identificar puntualmente si en uno, dos o los tres criterios se ve afectación en caso de materializarse el riesgo, refiriéndose a de los tres principios de la seguridad de la información confidencialidad, integridad y disponibilidad de la información.

- Criterios de calidad: Si en el campo del tipo de riesgo se marca sistema de calidad, se debe activar que afecta a satisfacción del cliente.

- Criterios de gestión del servicio: En caso de que el sistema marcado en el tipo de riesgo sea gestión del servicio se debe seleccionar según la materialización del riesgo si afecta en uno o varios de la calidad del servicio, efectividad del proceso u oportunidad del servicio.

- Riesgo Inherente: Este apartado se divide en varios registros los cuales se basan en lo que se definió previamente dentro de las escalas de valoración de la metodología pasando por la probabilidad y luego por el impacto del que se compone el impacto según la escala de valoración, el tipo de impacto de acuerdo con las opciones de despliegue previamente definidas en conjunto con los responsables de la gestión del riego y se debe seleccionar a la que más se afecte en caso de materialización. Teniendo en cuenta esto, la zona de riesgo es automáticamente calculada y se ubicará dentro del mapa de calor respectivo.

Continuando con el **Ejemplo 1**:

Figura 7.

Sección Análisis de riesgos

ANALISIS DE RIESGO										
Criterios de Seguridad Afectados			Criterios Gestión de Calidad	Criterio de Gestión del Servicio			Riesgo Inherente			
Confidencialidad	Integridad	Disponibilidad	Satisfacción del Cliente	Calidad del Servicio	Efectividad del Proceso	Oportunidad del Servicio	Probabilidad	Impacto		
								Impacto	Tipo de Impacto	Zona de Riesgo
X	X	X					5 – Inminente	5 – Catastrófico	Reputacional	Extremo

Nota. Matriz de riesgo caso aplicación

5.4.3. *Definir planes de tratamiento y/o control*

A partir de la valoración y teniendo en cuenta los criterios de aceptación del riesgo se hace una definición de controles. Dentro de la matriz, se evalúa a partir si es un control existente o si se va a definir como nuevo; estos controles, para el caso de los riesgos relacionados con Seguridad de la Información los controles se pueden relacionar con los que están definidos dentro del Anexo A de la norma ISO 27001:2013.

Cada uno de los controles definidos, deben contar con una descripción clara que permita vislumbrar el objetivo de este. Posteriormente, se hace una valoración al control a partir de los siguientes criterios:

- Documentación: Hace referencia a si el control está documentado y se aplica dentro de la organización.

- Efectividad: Si el control ha demostrado ser efectividad dentro de la ejecución. En caso de que sea un control que es nuevo, en la primera medición debe marcarse como No.

- Responsabilidad: Evalúa si se tiene claridad de los responsables de la ejecución del control.

- Monitoreo: Evalúa si se cuenta con medios para hacer seguimiento para la evaluación periódica de la efectividad.

- La frecuencia y/o el alcance: Evalúa que dentro de la ejecución del control se haya tenido un adecuado tiempo de frecuencia y/o alcance.

Siguiendo con el desarrollo del Ejemplo 1:

Figura 8.

Sección controles y valoración de controles

Controles				Valoración de los Controles					
				Valoración del Control					
Existe control (les)?	Control ISO 27001 Anexo A asociado	Descripción	Tipo	¿El control está documentado y se aplica?	¿El control ha demostrado ser efectivo?	Responsabilidad (están asignados responsables de su cumplimiento)	El control es monitoreado?	¿La frecuencia y/o el alcance de ejecución del control ha demostrado ser el adecuado?	Observaciones al Control
SI	A.8.2.1	Disposición de respositorio de información para	Correctivo:	0 No está	0 No	20 Si	0 No	0 No	
SI	A.9.1.1 Política de	Accesos restringidos de acuerdo al perfil	Correctivo:	20 Está	20 Si	20 Si	0 No	0 No	
SI	A.11.1.1 Perímetro	Adquisición de polizas y seguros por perdida de	Preventivo:	15 No está	0 No	20 Si	20 No Aplica	0 No Existe	

Nota. Matriz de riesgo caso aplicación

Cada uno de estos criterios se evalúa dependiendo del nivel de cumplimiento que se tenga. Esta evaluación del control permite cuantificar el nivel de reducción del riesgo el cual se ve reflejado en cada uno como el riesgo residual. Dependiendo del tipo de control, si es reactivo o preventivo, afectará la medición de la probabilidad o el impacto dentro del riesgo residual. Es decir, si el control es de tipo preventivo, se afectará la probabilidad y si de lo contrario es correctivo, afectará el impacto.

Figura 9.

Sección evaluación de riesgo residual

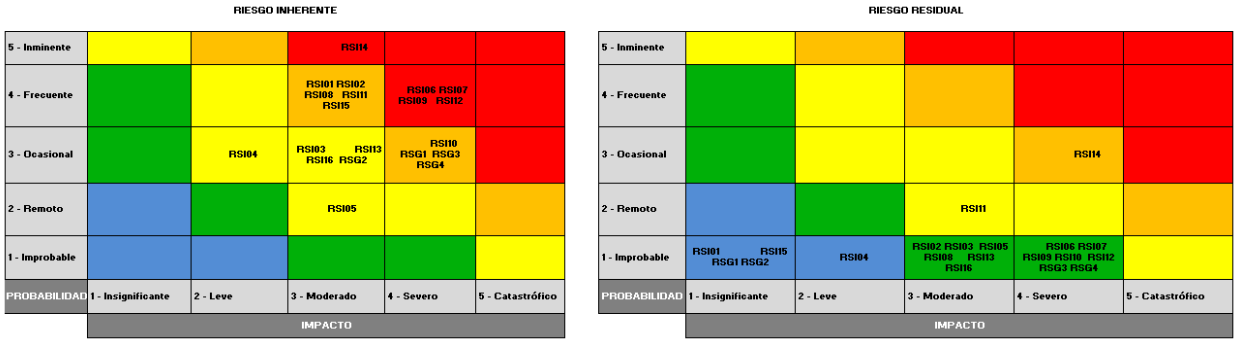
Disminución del Riesgo (# de niveles)		PROBABILIDAD	IMPACTO	Zona de Riesgo Residual	Opción de tratamiento
Probabilidad	Impacto				
2	1	3 - Moderado	4 - Severo	Alto	Riesgos que requieren de controles y alertas permanentes que permitan su gestión constante. Los riesgos en esta zona no podrán ser asumidos

Nota. Matriz de riesgo caso aplicación

Como resultado de este ejercicio, se podrá evaluar si el riesgo tuvo una disminución dentro del mapa de calor y demostrar la efectividad o no del control. Lo anterior se evidencia de la siguiente manera.

Figura 10.

Sección mapas de calor



Nota. Matriz de riesgo caso aplicación

Teniendo en cuenta las valoraciones del riesgo residual se debe revisar la zona dentro del mapa de calor. De acuerdo con la metodología propuesta, los riesgos que estén dentro de las zonas verdes y/o azules serán considerados mitigados y/o controlados, pero en el caso de los riesgos que se mantengan en las zonas amarilla, naranja o roja deberán tener la definición del plan de tratamiento. Estos planes de tratamiento deberán ser definidos con los responsables de cada riesgo según sea el proceso impactado, contemplando cada una de las actividades que se consideren necesarias para la mitigación del riesgo, estas actividades, de acuerdo con lo contemplado en cada riesgo pueden relacionar los controles definidos dentro del anexo A de la norma ISO 27001. Finalmente se debe definir el responsable de cada una, la fecha de implementación, fecha de seguimiento y las observaciones que se consideren necesarias dentro del proceso para dar trazabilidad al monitoreo realizado de manera periódica. Teniendo en cuenta el Ejemplo 1, los planes de tratamiento definidos fueron:

Figura 11.

Sección planes de tratamiento

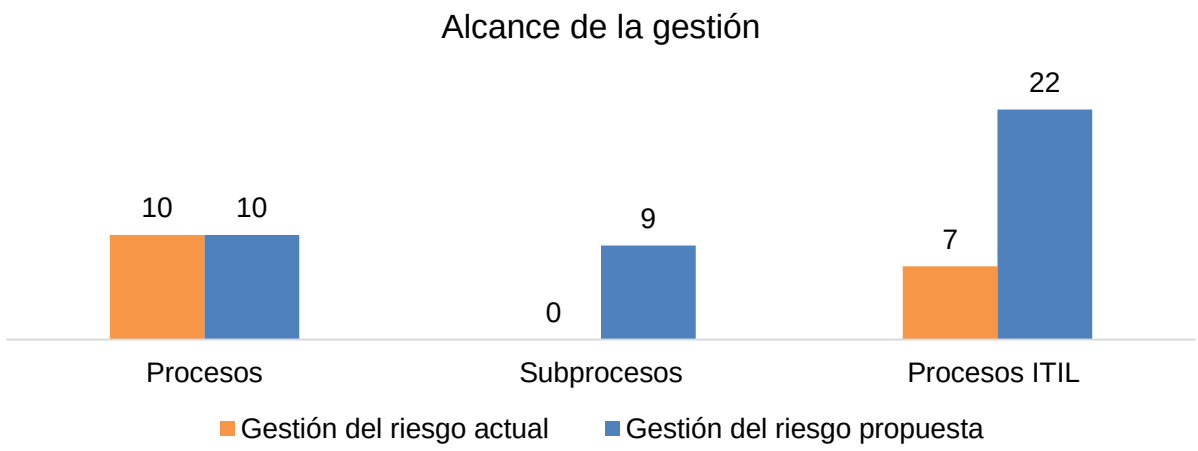
Actividades	Control ISO 27001 Anexo A asociado	Responsable	Fecha de Implementación	Fecha de Seguimiento	Observaciones
Definición de proceso de Borrado Seguro sobre los equipos entregados	A.11.2.7 Disposición s	Gestión de TI	15/07/2023		
Firma de acuerdo de niveles de servicio con el proveedor de Equipos con almacenamiento de información	A.15.1.2 Tratamiento d	Jurídica	15/07/2023		

Nota. Matriz de riesgo caso aplicación

Después de aplicar la metodología propuesta, se logra la ampliación de la cobertura a 41 procesos de la organización, lo que representa el 100% del alcance previsto. Del total de procesos mencionados, 22 están relacionados con ITIL y los 19 restantes están integrados en el mapa de procesos como procesos y subprocesos. A continuación, se presenta una comparativa entre el alcance propuesto y la situación actual:

Figura 12.

Alcance de la gestión del riesgo por metodología actual frente a la propuesta



Nota. El gráfico resume el alcance a través de la metodología de riesgos propuesta según los procesos y subprocesos definidos por la organización.

Lo expuesto anteriormente evidencia una estructura de alcance más amplia, ya que al incorporar los procesos de ITIL se asegura la identificación de riesgos que afectan de manera transversal a otros procesos, lo que facilita la toma de decisiones ante posibles escenarios de riesgo, ya sea debido a deudas tecnológicas o a la falta de estructura, permitiendo un análisis global más eficiente.

Por otro lado, en cuanto a la cantidad de riesgos definidos previamente a la intervención de la presente investigación y su gestión a través de varias matrices asociadas, se ha logrado una optimización del 97%, reduciendo la cantidad de matrices a solo una. Anteriormente, el proceso de revisión de cada matriz tomaba aproximadamente 2 horas, lo que requería alrededor de 8 días para completar el seguimiento de todos los riesgos definidos. Con la unificación de los riesgos y sus responsables en la matriz propuesta, este proceso se ha reducido a 2 días, lo que significa una mejora del 75% en la oportunidad de seguimiento de los riesgos en comparación con el tiempo asignado anteriormente para esta actividad.

A continuación, se presentan los datos que muestran la cantidad de matrices y los riesgos asociados, comparando la gestión actual del riesgo con la gestión propuesta, en esta se identifica la disminución de matrices y adicionalmente la reducción en riesgos, donde se evidencia que del total de riesgos identificados actualmente 52 se encuentran repetidos dos o más veces:

Tabla 25.

Volumetría de riesgos y matrices

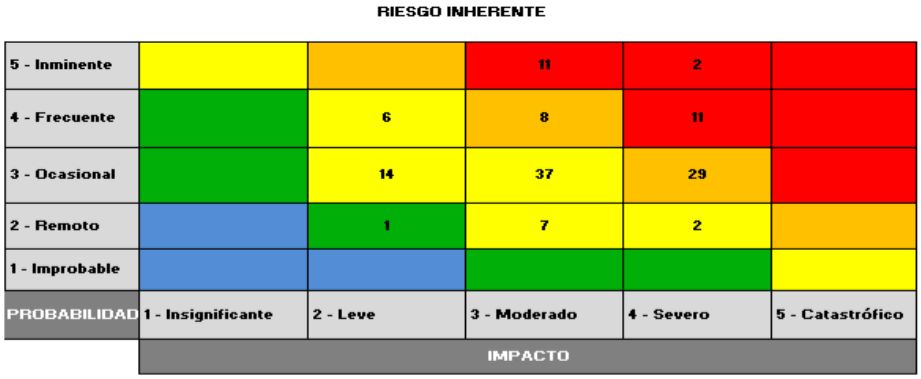
	Gestión del riesgo actual	Gestión del riesgo propuesta
Matrices	32	1
Riesgos asociados	662	128

Nota. Resumen de la cantidad de matrices y riesgos asociados

Al aplicar la metodología de gestión del riesgo, se obtienen los siguientes resultados en el mapa de calor, que representa el riesgo inherente para el 100% de los procesos incluidos:

Figura 13.

Mapa de calor riesgo inherente

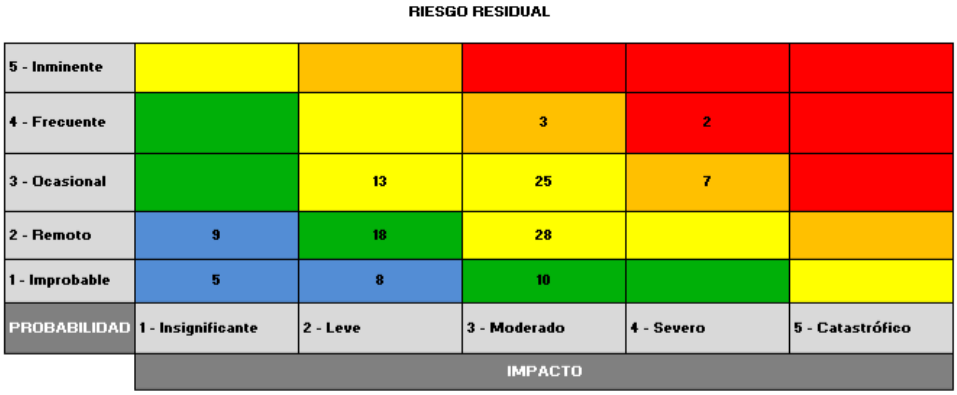


Nota. Resumen de la cantidad de riesgos para cada una de las zonas de tratamiento a partir de la evaluación del riesgo inherente

Después de definir los controles asociados a los riesgos identificados, se genera un nuevo mapa de calor que muestra el riesgo residual. Se recomienda a la organización aplicar los planes de tratamiento respectivos según lo establecido en la metodología propuesta.

Figura 14.

Mapa de calor riesgo residual



Nota. Cantidad de riesgos en cada una de las zonas de tratamiento de acuerdo a la evaluación del riesgo residual.

5.5. Evaluación de propuesta de para la gestión del riesgo

Teniendo en cuenta la propuesta realizada, se hizo un proceso de evaluación con la organización en donde a partir de los criterios tomados para la selección de la metodología, se hizo la valoración sobre la propuesta; con el fin de identificar oportunidades de mejora y el cumplimiento de los objetivos propuestos

5.5.1. Selección de instrumentos

Después de aplicar la metodología y generar el registro en la matriz de riesgos, se establece el medio por el cual se realizará la recopilación de datos. Para llevar a cabo este proceso, se aplica una de las herramientas colaborativas de office, forms dado que es el instrumento de recolección que facilita el análisis por cada ítem que se vaya a evaluar, obteniendo resultados directos y manteniendo la trazabilidad de cada comentario definido por cada uno de los evaluadores.

5.5.2. Selección de instrumentos

Con el objetivo de realizar las comparaciones de las dos metodologías (actual y propuesta) y basados en los criterios definidos previamente que fueron insumo para la construcción de la propuesta, se decide utilizar estos mismos y se procede con la construcción del formulario en web con método de evaluación por cada una y a continuación se asocian las preguntas:

Tabla 26.

Preguntas del instrumento de evaluación

ÍTEM	PREGUNTA
1	¿Cuál de las dos metodologías son más fáciles de entender?
2	¿Qué metodología presenta un mejor alcance?
3	¿En agilidad cuál metodología es la mejor opción?
4	A nivel de objetividad ¿Cuál cree usted que es la mejor opción?

Tabla 27.(Continuación)

5	¿Qué metodología tiene una mejor adaptación con el ámbito tecnológico?
6	¿Cuál metodología es la que genera mayor costo?
7	¿Qué metodología integra mejor los sistemas?
8	Comentarios u observaciones

Nota. Definición de las preguntadas utilizadas para la evaluación de la metodología.

Luego de la construcción de las preguntas se procede con el montaje del formulario en la web para realizar la evaluación y monitorear el nivel de respuestas a tiempo real generada por fuente propia con el objetivo de aplicarse a los mismos 19 entrevistados en la fase de diagnóstico.

5.5.3. Aplicación de evaluación

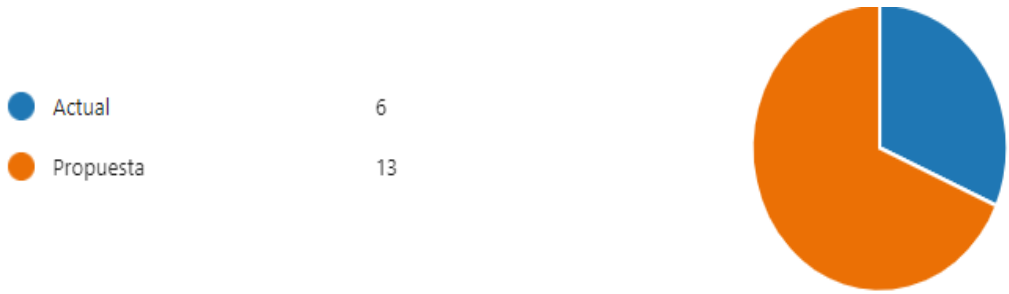
A partir del formulario en línea, se procede con la evaluación de las partes interesadas obteniendo la siguiente calificación para las preguntas mencionadas anteriormente:

- **¿Cuál de las dos metodologías son más fáciles de entender?**

Se obtuvieron del total de 19 respuestas, 13 personas indicaron que les pareció más fácil de entender la metodología propuesta, frente a seis respuestas que indicaron que era más entendible la metodología actual, obteniendo el 68% de aprobación.

Figura 15.

Resultados pregunta 1



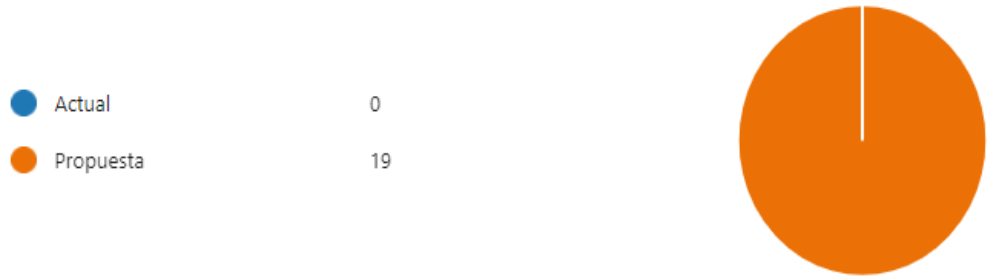
Nota. Evaluación resultados del caso aplicado.

- **¿Qué metodología presenta un mejor alcance?**

A nivel de alcance se presenta la calificación unánime del 100% de las 19 respuestas indicando que la metodología propuesta cuenta con un mayor alcance con respecto a la actual.

Figura 16.

Resultados pregunta 2



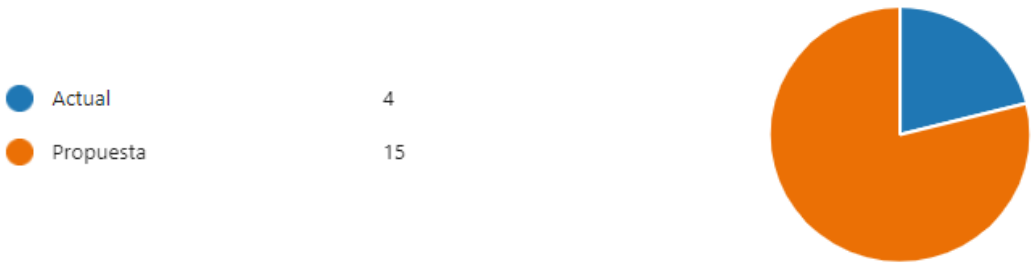
Nota. Evaluación resultados del caso aplicado.

- **¿En agilidad cuál metodología es la mejor opción?**

Del total de 19 respuestas, cuatro personas consideran que es mejor opción continuar con la metodología actual ya que presenta mayor agilidad, sin embargo, en contraste 15 personas indican que la metodología propuesta es mejor opción.

Figura 17.

Resultados pregunta 3



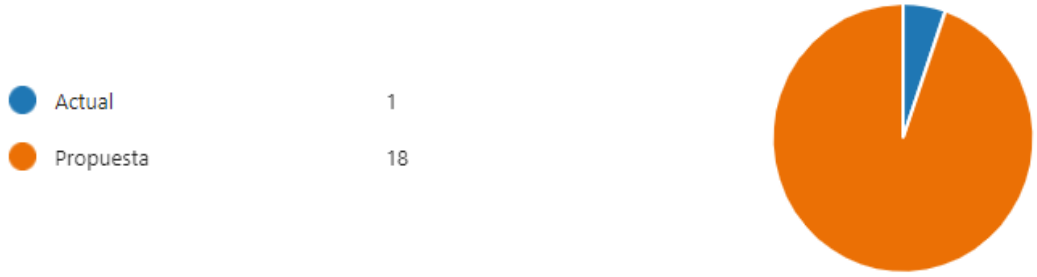
Nota. Evaluación resultados del caso aplicado.

- **A nivel de objetividad ¿Cuál cree usted que es la mejor opción?**

De acuerdo con lo analizado por los evaluadores se identifica que 18 personas opinan que la metodología propuesta es más objetiva que la actual.

Figura 18.

Resultados pregunta 4



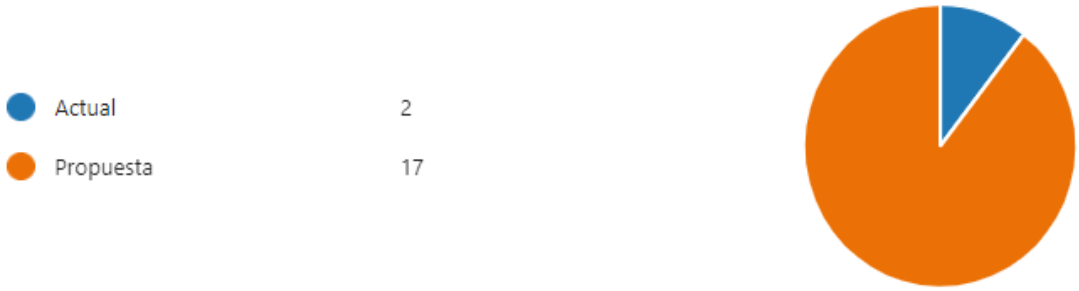
Nota. Evaluación resultados del caso aplicado.

- **¿Qué metodología tiene una mejor adaptación con el ámbito tecnológico?**

Teniendo en cuenta que la empresa es de tecnología, se hace la evaluación con respecto a qué metodología es más adaptable con el ámbito tecnológico a nivel de evolución que la empresa requiere, obteniendo 17 respuestas a favor de la metodología propuesta, a diferencia de dos personas que consideran la metodología actual como mejor adaptada

Figura 19.

Resultados pregunta 5



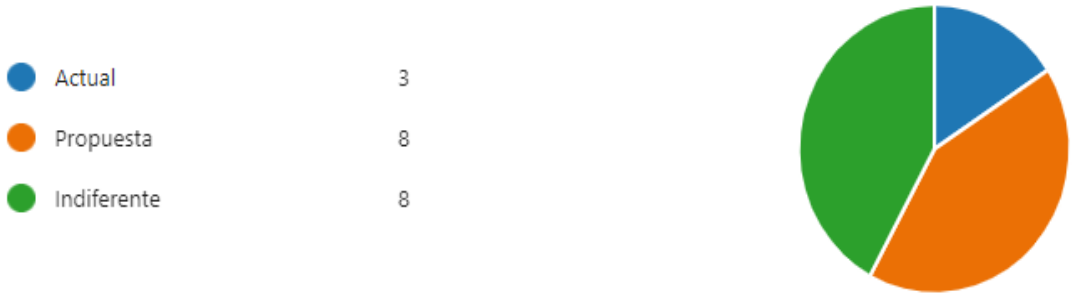
Nota. Evaluación resultados del caso aplicado.

- **¿Cuál metodología es la que genera mayor costo?**

A nivel de qué metodología consideran que genera mayor costo se incluye la opción de indiferente, obteniendo ocho respuestas para la metodología propuesta e indiferente y tres personas que mencionan la metodología actual como la más económica

Figura 20.

Resultados pregunta 5

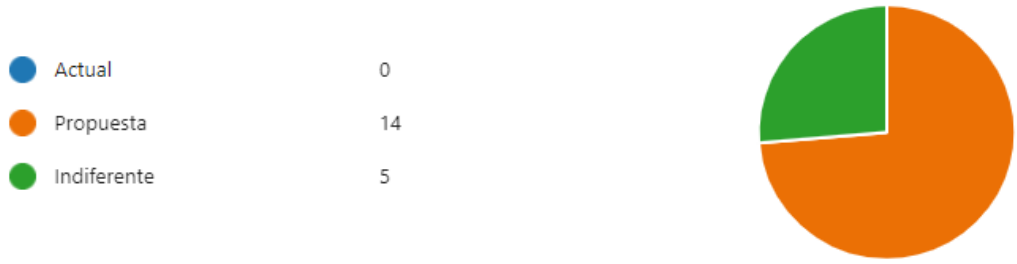


Nota. Evaluación resultados del caso aplicado.

- **¿Qué metodología integra mejor los sistemas?**

Entendiendo que en la empresa de tecnología se manejan varios sistemas y que la metodología actual no los recopila todos en un solo artefacto, al obtener los resultados de la evaluación se observa que ninguno de los evaluadores indica que la metodología actual es la mejor opción, 14 respuestas se inclinan hacia la propuesta como mejor integradora y cinco asistentes indican que les es indiferente cual integra mejor los sistemas.

Figura 21. *Resultados pregunta 6*

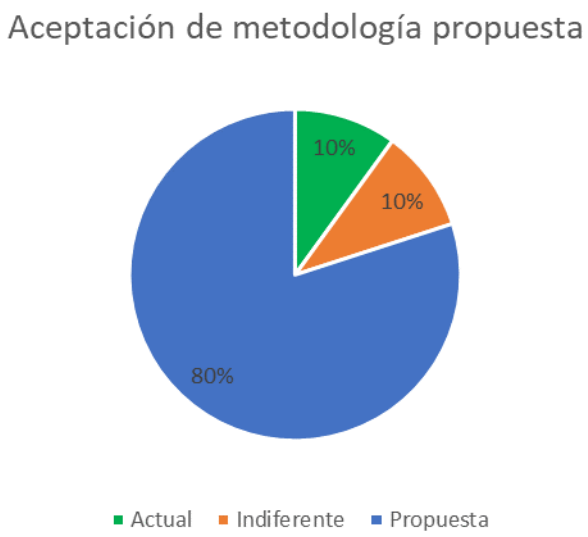


Nota. Evaluación resultados del caso aplicado.

Según estas respuestas y recopilando la cantidad total de la participación en preguntas y opciones de respuesta, a continuación, se representa de forma gráfica la percepción general de los evaluadores en donde se observa que el 80% de los aspectos evaluados favorecen a la metodología de gestión del riesgo propuesta, 10% le es indiferente la elección entre una y otra y el 10% restante opta por dar continuidad con la metodología de gestión del riesgo actual:

Figura 22.

Resultados pregunta 7



Nota. Evaluación resultados del caso aplicado.

Para reforzar lo mencionado anteriormente, se presentan los siguientes indicadores que permiten asociar la mejora observada en la metodología de gestión de riesgos propuesta con los resultados obtenidos:

Tabla 28.

Indicadores de evaluación

TIPO	OBJETIVO	MÉTRICA	RESULTADO	
			ACTUAL	PROPUESTA
Efectividad	Identificar la cantidad de matrices necesarias para la gestión del riesgo	# Matrices de riesgos definidas	32	1
Alcance	Identificar el número de procesos y subprocesos incluidos en la metodología de gestión del riesgo definidos por la organización	# Procesos incluidos en la metodología / # Total de procesos de la organización	41%	100%
Alcance	Identificar la cantidad de sistemas de gestión que se encuentran incluidos dentro de la metodología de gestión del riesgo	# Sistemas de gestión integrados en la metodología / #Total de sistemas de gestión implementados en la organización	50%	100%
Oportunidad	Identificar el tiempo dedicado para el seguimiento y control de los riesgos por parte del proceso de gestión de calidad	# Horas dedicadas para el seguimiento y control de riesgos por revisión programada	64	16

Nota. Resumen resultados de indicadores de evaluación de resultados.

6. CONCLUSIONES

A partir del análisis del contexto y el instrumento de recolección de información, se obtiene que la metodología de gestión del riesgo se encuentra centralizada en el proceso de gestión de calidad, sin embargo, no se aplica de la misma forma para todos los procesos de la empresa de tecnología, generando varias matrices de gestión del riesgo.

Se identifica que pese a tener definida la metodología de gestión del riesgo, en la organización no se encuentra interiorizada para quienes representan participación lo que dificulta tener resultados exactos y acordes a los procesos involucrados.

Se logran identificar los aspectos clave que para la organización deben tenerse en cuenta al momento de definir una metodología de gestión del riesgo que se adapte y genere valor para la actividad en la cual se desempeña, en consecuencia, de esto, se definen que se deben plantear bajo las normas ISO 31000:2018, ISO 27001:2013 y marco ITIL.

Una vez identificados los marcos de referencia para generar la metodología, se definen los criterios que permitan garantizar una implementación eficiente basándose en cinco fases integrando sistemas de gestión permitiendo incluir tanto procesos internos como procesos del marco ITIL aumentando el alcance a nivel de transversalidad en la compañía y reduciendo la posibilidad de manejo variado cerrando el alcance definitivo sobre su gestión al proceso de gestión de calidad como se encuentra definido actualmente como responsable.

Se logra la aplicación de la metodología en el ámbito real de la compañía con el fin de lograr a nivel demostrativo las ventajas de la propuesta con respecto a la metodología actual, identificando que existen varios riesgos definidos por diferentes proyectos y líderes que en ocasiones se asocian al mismo, redactados de forma diferente, con tratamientos diferentes, con controles definidos que no aplican debido a los alcances, etc. Adicionalmente, luego de la depuración e identificación de riesgos, se logró la definición de 128 riesgos centralizados en una sola matriz disminuyendo en 534 riesgos

definidos actualmente en más de 30 matrices de riesgos que tenían algún tipo de inconsistencia.

De acuerdo con la evaluación de las partes interesadas, se identifica que el nivel de aceptación de la metodología de gestión del riesgo es del 80%, 10% inclinado hacia la metodología actual y el 10% de las votaciones les es indiferente el uso de cualquiera de las dos metodologías.

Con base en las evaluaciones aplicadas, se identifica que la metodología propuesta representa un facilismo mayor en seguimiento y control de la gestión del riesgo; pudiendo aterrizar y tratar los riesgos oportunamente centralizadamente.

Basándose en los indicadores definidos para verificar la ampliación de la oportunidad en la toma de decisiones, se evidencia una reducción de 97% en la cantidad de matrices asociadas a la gestión.

En relación al tiempo dedicado al seguimiento y control de la gestión del riesgo, se logra una disminución del 75% del tiempo asignado para esta actividad por parte del proceso de Gestión de Calidad.

Se observa el incremento del alcance en el 59% sobre los procesos y subprocesos incluidos en el mapa de procesos y en un 50% en los sistemas de gestión implementados en la organización dentro de la metodología propuesta a comparación de la metodología de gestión del riesgo actual.

Se logró la integración de la gestión del riesgo en una metodología que abarca las normas ISO 27001:2013,9001:2015 y NTC-ISO/IEC 20000-1:2018 y los marcos de referencia ITIL y OEA

Para integrar eficazmente la gestión del riesgo conforme a los estándares ISO 27001:2013, ISO 9001:2015 y NTC-ISO/IEC 20000-1:2018, es crucial identificar y

establecer criterios pertinentes dentro de la organización. Esto implica considerar tanto el contexto organizacional como los requisitos específicos de cada sistema de gestión.

Es necesario generar artefactos que permitan articular estos criterios de manera óptima, facilitando así la toma de decisiones. Además, estos artefactos deben ser lo suficientemente dinámicos para adaptarse y evolucionar conforme a los nuevos desarrollos tecnológicos y a los cambios en el entorno empresarial.

Se recomienda la adopción de la metodología de la gestión de riesgos propuesta, dado que esta ofrece una ampliación sustancial del alcance, abarcando no solo los sistemas de gestión vigentes en la organización, sino también marcos de referencia relevantes mostrando un incremento del 59% en procesos y en 50% sobre los sistemas que abarca actualmente. Esta integración no solo simplifica la gestión, sino que también facilita el control y seguimiento de los riesgos en la organización teniendo la reducción de hasta el 75% del tiempo asignado para esta actividad, además de ser amigable para la migración de versiones posteriores de normas ISO como la norma ISO 27001:2022 y e implementaciones de herramientas tecnológicas.

Sin embargo, para asegurar una implementación exitosa, es crucial definir una ruta clara para la gestión del cambio. En este sentido, se sugiere que dicha ruta incorpore diversos aspectos, tales como planes de capacitación adecuados para todos los niveles de la organización basándose en las herramientas disponibles como e-learning, actividades de socialización para garantizar una comprensión común de los objetivos y beneficios de la nueva metodología, por medio de sesiones de refuerzos sobre el material ya generado, así como una evaluación y seguimiento continuo del uso de la metodología propuesta. Esto último es especialmente importante para identificar posibles desafíos y áreas de mejora en la implementación.

Por último, es fundamental analizar las observaciones presentadas durante la valoración de la metodología propuesta por parte de los evaluadores a fin de realizar los ajustes que tenga lugar. Este análisis puede ayudar a identificar oportunidades de mejora que

sean aplicables a la evolución de la metodología propuesta y se sugieren los ajustes previos al lanzamiento o en su defecto; trazar la ruta y plan de acción para la evolución posterior.

REFERENCIAS

Alberts C., Dorofee A., Stevens J. & Woody C. *OCTAVE-S Implementation Guide*. Pittsburgh, PA. Carnegie Mellon Software Engineering Institute, 2005.

Araujo S. L. E, Sousa e Silva D. E. L & Souza Campello L. O. (2020). Risk management the COSO methodology applied to manager an information unit. *Digital Journal of library and information Science.* 18, 1 – 21.

Ávila Irigoin J. W, & Caloggero Sangama C. T. (2022). Sistema de gestión de riesgos de TI usando las ISO 27001 y 31000 en la empresa LABE CORPORATION S.A.C. [Tesis de pregrado]. Universidad Cesar Vallejo.

Becerra Rozo Y. X, Betancourt Manjarres R. D. & Serrato Rodríguez Y. I. (2022). Propuesta para mejores prácticas en el proceso de gestión de infraestructura e interconexiones, alineado con la norma ISO 27001:2013, para la compañía sistemas satelitales de Colombia (SSC). http://hdl.handle.net/11371/5035.

Contreras Olea, G.A. (2022). Análisis comparativo entre las metodologías de gestión de riesgos de los sistemas de gestión de seguridad de la información (SGSI): Facultad de Administración Finanzas e Informática. [Tesis de Maestria]. Universidad Técnica de Babahoyo. http://dspace.utb.edu.ec/handle/49000/12551

Colombia. Presidencia de la República. Decreto 103 de 2015. por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones. D. O

Correa Henao, G.J. Ríos-González, E.M. y Acevedo-Moreno J.C. (2016). Evolución de la cultura de la gestión de riesgos en el entorno empresarial colombiano. *Journal of Engineering and Technology*. 6, (1), 23-45.

Dellepiane Hernández S. (2021). El desarrollo tecnológico en la Economía Mundial y la llegada de la pandemia COVID-19 a la Era de la Información. [Tesis de pregrado]. Universidad de la república Uruguay. https://hdl.handle.net/20.500.12008/31565

Figueroa Sierra N, Ribet Cuador M.J, Garrido Cervera M, Ramos Crespo M. E & Enrique Capote (2013). La gestión de riesgos laborales en las empresas forma parte de su responsabilidad social. *Revista Científica Avances*. 15, (1), 64 – 75.

Gálvez Albarracín E. J, Riascos Erazo S. C & Contreras Palacios F. (2013). Influencia de las tecnologías de la información y comunicación en el rendimiento de las micro,

pequeñas y medianas empresas colombianas. *Journal of Management and Economics for Iberoamerica*. 30, (1), p 355 – 364.

Gehrmann M. (2012). Combining ITIL, COBIT and ISO/IEC 27002 for structuring comprehensive information technology for management in organizations. *NAVUS – Revista de Gestão e Tecnologia.* 2, (2), 66 – 77.

Gomez R, Pérez D. H, Donoso Y & Herrera A. (2010). Metodología y gobierno de la gestión de riesgos de tecnologías de la información. *Revista de Ingeniería Universidad de Los Andes*. 31, 109 - 118.

Gonzázles Chacón J, H. Pacheco Fernández A, E & Suarez Santamaría L, I. (2021). Aplicar la Metodología OCTAVE de Identificación de Amenazas y Vulnerabilidades en una Entidad Bancaria. Universidad de Los Andes. [Archivo en pdf]. https://sistemas.uniandes.edu.co/maestrias/mesi/proyectos/proyecto.php?id=51

Hernandez D. F. (2018). Gestión del riesgo y control, una mirada tridimensional. *Revista Científica Hermes*. 22, (1), 449 - 465.

Instituto Colombiano de Normas Técnicas y Certificación Icontec – NTC ISO 9001:2015. Sistemas de gestión de calidad. El Instituto.

Instituto Colombiano de Normas Técnicas y Certificación Icontec – NTC ISO 27001:2022. Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de seguridad de la información. Requisitos. El Instituto.

Instituto Colombiano de Normas Técnicas y Certificación Icontec – NTC ISO 31000:2018. Gestión del riesgo. Principios y directrices. El Instituto.

Instituto Nacional de Ciberseguridad (2015). Gestión de riesgos: Una guía de aproximación para el empresario. Gobierno de España. [Archivo en pdf]. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_gestion_riesgos_metad.pdf

ISACA. *COBIT 5 for Information Security*. ISACA Journal. 2012.

Izhar H & Asutay M (2010). A theoretical analysis ofthe operational risk frameworkin islamic Banks. *IIUM Journal of Economics and Management.* 18, (1), 73-113.

Jaramillo Mosquera V., Anzulez Paredes J. (2020). Sistema web de gestión del riesgo con tecnología open source basado en la norma iso 31000 para la empresa

bitekso s.a. [Tesis de Pregrado]. Universidad de Guayaquil. http://repositorio.ug.edu.ec/handle/redug/52634

Jaspal R, Fino E & Breakwell G. M. (2022). The COVID-19 Own Risk Appraisal Scale (CORAS): Development and validation in two samples from the United Kingdom. *Journal of Health Psychology*. 27, (4), 790 – 804.

Lavell A. y Argüello Rodriguez M. (2003). Gestión de riesgo: un enfoque prospectivo*. Colección Cuadernos de Prospectiva 3*. 1, (1) p. 33.

Llauce Valdera L. (2022). Análisis comparativo de metodologías de gestión de riesgos de tecnologías de la Información en el marco de la NTP - ISO/IEC 27001:2014. [Tesis de Maestría] Universidad Nacional Pedro Ruiz Gallo

Martinez Hernandez R. y Blanco Dopico M. (2017). Gestión de riesgos: reflexiones desde un enfoque de gestión empresarial emergente*. Revista Venezolana de Gerencia*, 22, (80), 692 - 707.

Ministerio de Tecnologías de la Información de Colombia – MINTIC (2015) *Guía de gestión de riesgos: Seguridad y Prevención de la información". Gobierno de Colombia.* https://gobiernodigital.mintic.gov.co/692/articles 5482_G7_Gestion_Riesgos.pdf

National Institute of Standards and Technology, *Guide for Conducting Risk Assessments.* Gaithersburg: NIST, 2012

Ochoa Torres L. (2015). Diseño de una metodología para la gestión de riesgos de calidad, a partir de la norma ISO 31000:2011 numeral 5, ISO 9001:2015 requisito 6.1 y la normatividad del sector de alimentos, aplicado en la empresa Yod Buen Servicio. [Tesis de especialización]. Universidad Libre. https://repository.unilibre.edu.co/bitstream/handle/10901/10949/TRABAJO.pdf?sequence=1&isAllowed=y.

Park, Cho, Jun, Bang & Hong, 2022. Worker Protection Scenarios for General Analytical Testing Facility under Several Infection Propagation Risks: Scoping Review, Epidemiological Model, and ISO 31000. *International journal of environmental research and public health*. 19, (19). 1 – 16.

Pedro Huaman L. y Rodríguez Novoa F. Evaluación de riesgos en activos de tecnologías de información en una MIPYME. *Revista Ciencia y Tecnología*. 18, (3), 71 - 78.

Perano M., Della Piana B. y Casali G. (2018). Project and Risk Management in a Global Context: The Importance of Cultural Risk*. Information Resources Management Association*. 1, (1), 170 - 194.

Ramírez, A., Ortiz, Z. (2011). Gestión de riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios. *Ingeniería*, 16, (2), 56-66.

Reynaldo Argüelles, C. L, Guardado Lacaba, R. M., Sorhegui Ortega, R. A., & Rojas de la Cruz, R. (2019). Importancia de la gestión de riesgos para el desarrollo local. Caso de estudio Consejo Popular Caribe, Cuba. *Revista científica ecociencia*. 6, (5), 1 – 23.

Rosales Veitía J. (2022). Mapas comunitarios de riesgos, conceptualización y abordaje metodológico. Algunas consideraciones. *IPSA SCIENTIA*. 7, (1), 38 - 57.

Ruijter A., Guldenmund F (2016). The bowtie method: A review. *Safety Science*. 88, 211-218

Rusman A., Nadlifatin R. y Subriadi A. (2022). Analysis Factors Affect Information System Audit Using COBIT and ITIL Framework. *Sinkron: Jurnal dan Penelitian Teknik Informatika*. 7, (3), 799 – 810.

Sharma K. D & Srivastava S. (2018). Failure Mode and Effect Analysis (FMEA) Implementation: A Literature Review. *Journal of Advance Research in Aeronautics and Space Science.* 5, (1&2), 1 – 17.

Soler Gonzalez R., Varela Lorenzo P., Oñate Andino A. & Naranjo Silva E. (2018). La gestión de riesgo: el ausente recurrente de la administración de empresas. *Revista Ciencia UNEMI*. 11, (26), 51 - 62.

Sudarsana, I., & Ramli, K. (2023*).* Information security risk assessment using factor of analysis information risk (fair) in the healthcare sector: scoping review. *Journal Darma Agung*. 31, (4), 674 - 686.

Velásquez Restrepo P.A, Velásquez Restrepo S.M., Velásquez Lopera M. & Villa Galeano J. (2017). Implementación de la gestión de riesgo en los procesos misionales de la Sección de Dermatología de la Universidad de Antioquia (Medellín, Colombia) siguiendo las directrices de la norma ISO 9001:2015. *Revista Gerencia Política Salud*.16, (33), 78-101.

ANEXOS

ANEXO 1.
MATRIZ DE GESTIÓN DEL RIESGO PROPUESTA

El Anexo 1, Matriz de gestión del riesgo propuesta, se compone de tres aspectos importantes, el primero asociado al inventario de activos de la información que se tengan identificados en la compañía, el segundo aspecto, es el componente más amplio del anexo pues es el artefacto por el cual se recopila todos los datos de la gestión del riesgo desde la identificación hasta los planes de tratamiento y por último el aspecto donde se asocian los mapas de calor resultantes del ejercicio aplicado. (**Ver archivo adjunto)**