Escuela de Administración de Tecnologías de Información

Propuesta de Metodología para la Gestión de Riesgos de TI Basada en las Mejores Prácticas Internacionales para la Empresa Information Evolution Costa Rica

Trabajo Final de Graduación para optar al grado de Licenciatura en Administración de Tecnología de Información

Modalidad Proyecto de Graduación

Elaborado por: Fabiana Herrera Madriz

Prof. Tutor: Laura Alpízar Chaves

Cartago, Costa Rica

II semestre

Noviembre, 2024

Hoja de Aprobación

INSTITUTO TECNOLÓGICO DE COSTA RICA

ESCUELA DE ADMINISTRACIÓN DE TECNOLOGÍAS DE INFORMACIÓN

GRADO ACADÉMICO: LICENCIATURA

Los miembros del Tribunal Examinador de la Escuela de Administración de Tecnologías de Información, recomendamos que el siguiente informe del Trabajo Final de Graduación de la estudiante Fabiana Herrera Madriz sea aceptado como requisito parcial para obtener el grado académico de Licenciatura de Tecnología de Información.

Laura Alpízar Chaves

Firmado digitalmente por Laura Alpízar Chaves
Fecha: 2024.11.21 11:42:16 -06'00'

Laura Alpízar Chaves
Profesora Tutora

Dayana Vindas Sosa
Lectora externa

LUIS FELIPE PICADO VALVERDE (FIRMA)

Firmado digitalmente por LUIS FELIPE PICADO VALVERDE (FIRMA)
Fecha: 2024.11.20 13:45:27 -06'00'

Luis Felipe Picado Valverde
Lector académico

TEC | Tecnológico de Costa Rica

Firmado digitalmente por YARIMA TATIANA SANDOVAL SANCHEZ (FIRMA)
Fecha: 2024.11.20 23:37:01 -06'00'

Yarima Sandoval Sánchez
Coordinadora de Trabajo Final de Graduación

Dedicatoria

A mis papás, José y Marcela, por apoyarme y estar presentes, en cada momento, a lo largo de toda mi formación académica. Gracias por ser un apoyo incondicional y ejemplo a seguir, gracias por alentarme siempre a dar lo mejor de mí y no dejar nunca que me rindiera.

A mi hermanito, Marcel, por sacarme de la rutina, hacerme reír y motivarme siempre a ser mejor; y así servir de ejemplo e inspiración para su futuro.

A mi novio, Ernesto, por creer en mí incluso cuando ni yo lo hacía, por ser mi fuerza para salir adelante y ese rayito de luz que ilumina incluso los días más oscuros.

A la mejor amiga que el TEC me dejó, Fio Córdoba. Gracias a ella, por ser mi compañera de trasnochadas, lloradas, estrés y alegrías; desde el día uno de universidad me enseñó que nunca iba a estar sola en este proceso, en el cual formamos el equipo más lindo para todo.

Agradecimientos

A mi contraparte y mejor amigo, Carlos, por llegar a darle un giro de 180 grados a mi vida, por creer en mí y levantarme cuando sentía que no era capaz.

A mis amigos del TEC, en especial a Jairo, Andrés, Usiel y Randall, por formar junto con Fio y conmigo el mejor equipo de trabajo que se puede pedir y demostrarme siempre su amistad incondicional.

A mis abuelas, por apoyarme, cuidarme y celebrar conmigo cada pequeño logro obtenido desde que era apenas una niña.

A mi abuelo, porque sé que desde el cielo me está cuidando y celebra al lado de Tita y de mí lo bonito de la vida.

A mi profesora tutora, Laura Alpízar, por todo su apoyo, guía y palabras de aliento durante todo este proceso.

Al profesor Néstor Morales, por no permitir que me rindiera durante ese primer semestre de la carrera, y por su apoyo cada vez que me sentí incapaz y consideré abandonarlo todo.

Resumen

Herrera, F. (2024) *Propuesta de metodología para la gestión de riesgos de TI basada en las mejores prácticas internacionales para la empresa Information Evolution Costa Rica.* (Trabajo Final de Graduación). Escuela de Administración de Tecnologías de Información. Tecnológico de Costa Rica.

Este Trabajo Final de Graduación tiene como objetivo proponer una metodología de gestión de riesgos de Tecnologías de Información para Information Evolution Costa Rica, alineada con las mejores prácticas de la industria, con el fin de definir una estrategia y un proceso operativo para la gestión de riesgos de TI. La propuesta se fundamenta en la evaluación de las mejores prácticas de gestión de riesgos de TI de la industria para garantizar una implementación eficaz y sostenible en la empresa.

Para alcanzar este objetivo, se utilizó una metodología aplicada con un enfoque cualitativo y un diseño de investigación-acción, estructurada en tres fases. En la Fase 1, se evaluó la situación actual de la empresa y sus procesos de gestión de riesgos. En la Fase 2, se estudiaron las mejores prácticas de gestión de riesgos de TI de la industria y se evaluó su alineación con las necesidades de la empresa, seleccionando las más adecuadas. Finalmente, en la Fase 3, se desarrollaron los artefactos pertinentes para la metodología de gestión de riesgos de TI, tanto para el marco de gobierno de riesgos de TI como para el proceso de gestión de riesgos.

A partir del análisis de los resultados, se determinó que la empresa no contaba con un proceso formal para la gestión de riesgos de TI, lo que generaba una gestión reactiva ante los incidentes. Con base en esta evaluación, se desarrolló una propuesta metodológica estructurada de acuerdo con ISO 31000 y COBIT 2019, que permite implementar un proceso formalizado de gestión de riesgos de TI, con el objetivo de garantizar la continuidad operativa y minimizar los impactos adversos.

Palabras clave: metodología, gestión de riesgos, riesgos de TI, mejores prácticas, COBIT 2019, ISO 31000, gobierno de TI, proceso, estandarización

Abstract

Herrera, F. (2024) *Proposal for a methodology for IT risk management based on international best practices for the company Information Evolution Costa Rica.* (Final Graduation Project). School of Information Technology Management. Technological Institute of Costa Rica.

This Final Graduation Project aims to propose an IT risk management methodology for Information Evolution Costa Rica, aligned with industry best practices, to define a strategy and operational process for IT risk management. The proposal is based on an evaluation of industry best practices in IT risk management to ensure effective and sustainable implementation within the company.

To achieve this objective, an applied methodology with a qualitative approach and an action-research design was used, structured into three phases. In Phase 1, the company's current situation and risk management processes were evaluated. Phase 2 involved studying IT risk management best practices and assessing their alignment with the company's needs to select the most suitable ones. Finally, in Phase 3, the relevant artifacts for the IT risk management methodology were developed, covering both the IT Risk Governance framework and the risk management process.

The results analysis revealed that the company lacked a formal IT risk management process, leading to a reactive approach to incidents. Based on this evaluation, a structured methodological proposal was developed, aligned with ISO 31000 and COBIT 2019, enabling the implementation of a formalized IT risk management process aimed at ensuring operational continuity and minimizing adverse impacts.

Keywords: methodology, risk management, IT risk, best practices, COBIT 2019, ISO 31000, IT governance, process, standardization

Tabla de Contenidos

Índice de Figuras

Índice de Tablas

1. Introducción

1.1. Descripción General

En el entorno empresarial actual, caracterizado por una adaptación tecnológica exponencial y una dependencia creciente de los sistemas de información, la gestión eficiente y eficaz de los riesgos de las Tecnologías de Información se ha convertido en un requisito obligatorio. Este proyecto se centra en la empresa Information Evolution Costa Rica, una entidad dedicada al análisis de datos y al mantenimiento de bases de datos para el mercado de bienes raíces de Estados Unidos, donde la continuidad y la integridad de las operaciones dependen críticamente de la infraestructura de TI.

El rápido crecimiento de la empresa ha revelado vulnerabilidades significativas en su gestión de riesgos de TI, con incidentes técnicos que han impactado directamente su operatividad y productividad, y ha comprometido la seguridad de los datos de los clientes. A pesar de la importancia reconocida de la gestión de riesgos de TI por parte del departamento de TI, el contexto actual dentro de Information Evolution Costa Rica indica que no se ha implementado una metodología robusta y sistemática para abordar estos riesgos, resultando en desafíos operativos y estratégicos.

Asimismo, diversos proyectos previos y prácticas establecidas en la industria sugieren que la implementación de marcos de trabajo como COBIT 2019, junto con normativas como ISO/IEC 27005 e INTE/ISO 31000, fortalecen significativamente la gestión de riesgos, además de optimizar los recursos de TI y mejorar la resiliencia organizacional. Es por esto que, en este trabajo se postula que la adopción de una metodología estructurada de gestión de riesgos de TI, basada en estos estándares internacionales, incrementará la eficiencia operativa y la competitividad de Information Evolution Costa Rica. Se espera que la propuesta de un marco de trabajo adecuado no solo mitigue los riesgos identificados, sino que también prepare a la empresa para enfrentar nuevos desafíos en un entorno tecnológico y de mercado dinámico competitivo.

En este informe se abarca el contexto de la organización en la sección 2, el planteamiento del problema en la sección 3, los objetivos en la sección 4, los beneficios esperados del proyecto en la sección 5, el alcance esperado del proyecto en la sección 6 y la metodología de investigación utilizada en la sección 7. El alcance del proyecto abarca cuatro fases fundamentales: el análisis de la situación actual del proceso de gestión de riesgos de TI, la identificación de aspectos relevantes sobre gestión de riesgos, el desarrollo del ciclo de gestión de riesgos de TI y la mejora del proceso de gestión de riesgos de TI. Estas fases se orientan hacia el diseño y la propuesta de una metodología de gestión de riesgos específicamente adaptada a las necesidades de Information Evolution Costa Rica, alineada con las mejores prácticas de la industria y centrada en la optimización de la gestión de riesgos de TI.

1.2. Antecedentes

1.2.1. Descripción de la Organización

Information Evolution es una corporación multinacional fundada en el año 2007 en Austin, Texas, por Matt Manning. A lo largo de los años, la empresa ha expandido su presencia internacional, incluyendo una significativa expansión en la India bajo la dirección de Yasmin Imthiyas. Actualmente, emplea a un poco más de mil personas distribuidas en sus distintas sedes alrededor del mundo, ubicadas en Estados Unidos, India, Filipinas y Costa Rica.

Especializada en una diversidad de servicios en el ámbito del manejo de información, Information Evolution ofrece soluciones integrales a compañías, especialmente en el sector de bienes raíces, *FinTech*, *MarTech* y *CRE Enhancement.* Entre sus principales servicios se encuentran el análisis de datos, el diseño y la optimización de cadenas de suministro de información, la actualización de datos y el mantenimiento de bases de datos. Asimismo, la empresa se dedica a la integración de diversas fuentes de datos y al *crowdsourcing* gestionado, asegurando así un flujo de información eficiente y de alta calidad para todos sus clientes.

De acuerdo con la información disponible en su sitio web, cada una de las sedes de Information Evolution, incluyendo la de Costa Rica, opera como una entidad independiente y única ante la ley. Esto implica que cada sede país es responsable de sus acciones y omisiones, sin comprometer a las demás entidades miembro. Cada sede de Information Evolution cuenta con una estructura organizativa independiente que facilita la adaptación y la gestión de sus propios procesos y proyectos, atendiendo las necesidades específicas del mercado local. Aunque en ciertos proyectos se forman equipos multidisciplinarios que integran talentos de diferentes sedes, como, por ejemplo, proyectos que integran miembros tanto de Costa Rica como de Estados Unidos, cada entidad mantiene su propia autonomía, lo que significa que, desde un punto de vista organizacional y administrativo, las operaciones y la gestión de recursos se llevan a cabo de manera independiente, sin una dependencia directa entre los diferentes países.

En particular, Information Evolution Costa Rica, dirigida por Rodolfo Rojas desde su fundación en enero del 2023, es la única sede en Latinoamérica y la segunda en el continente americano tras la fundación de la sede principal en Estados Unidos. Gracias a su alta eficiencia operativa y a su mano de obra altamente calificada, la sede costarricense ha experimentado un rápido crecimiento, pasando de 20 a 168 empleados, con un equipo compuesto por un 45% de hombres y un 55% de mujeres, y una estructura organizacional que crece y se consolida de manera exponencial, esto significa que actualmente desempeña un papel crucial, al focalizar su trabajo exclusivamente en el análisis de datos y el mantenimiento de bases de datos para clientes del sector de bienes raíces de Estados Unidos.

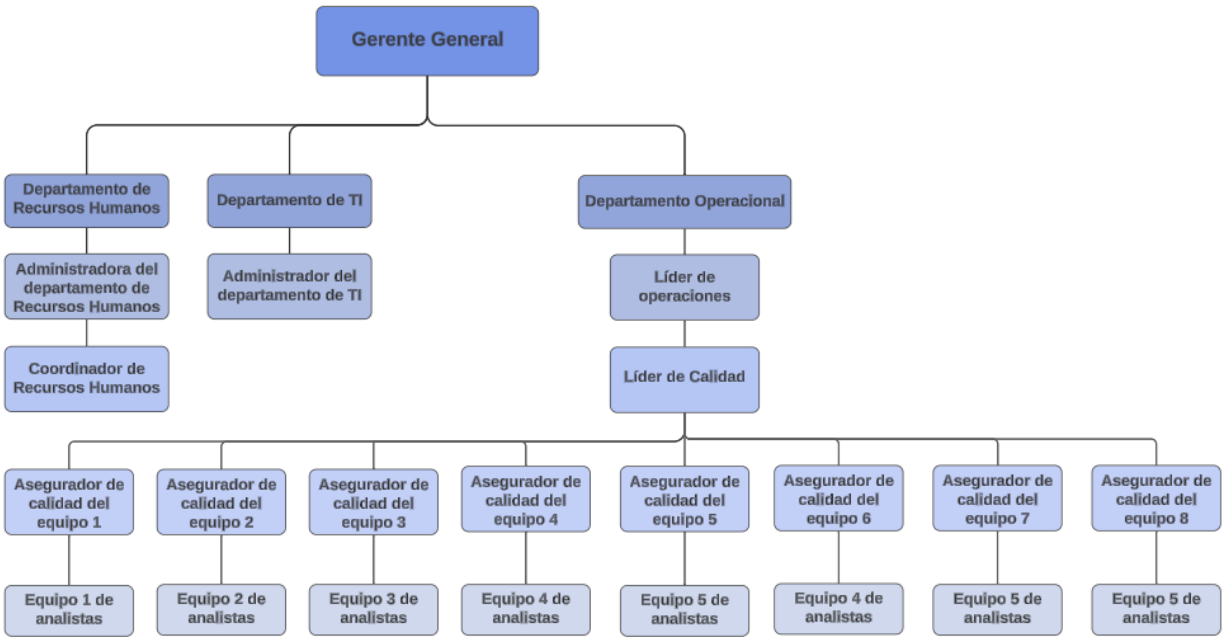
Entre sus clientes más importantes se encuentra una destacada empresa de bases de datos de bienes raíces, que ofrece sus servicios a miles de usuarios en todo el territorio estadounidense.

Esta empresa requiere que sus datos estén continuamente actualizados y mantengan un alto nivel de precisión, por ende, para cumplir con estas exigencias, Information Evolution Costa Rica ha dispuesto un equipo de aproximadamente 160 profesionales dedicados a asegurar la integridad y relevancia de la información manejada.

Estos equipos trabajan en diversos proyectos orientados para garantizar la integridad y la relevancia de la información que manejan, cumpliendo con las exigentes demandas del mercado inmobiliario estadounidense y adoptando una filosofía centrada en la prestación de servicios de primera calidad. Information Evolution Costa Rica destaca por su excepcional eficiencia operativa y su equipo altamente calificado, combinación que ha fortalecido su posición como una de las sedes más valoradas por los clientes estadounidenses.

Para lograr una comprensión conjunta de la empresa Information Evolution Costa Rica, a continuación, en la figura 1, se muestra el organigrama de la empresa, con el fin de entender su dinámica interna y delinear las diversas jerarquías y unidades funcionales que la integran.

Figura 1: Organigrama de la empresa Information Evolution Costa Rica



Nota: Elaboración propia

1.1.1.1. Misión

Brindar soluciones integrales en el manejo de información para el sector comercial estadounidense, mediante análisis de datos precisos, actualización constante de repositorios de información y optimización de cadenas de suministro de información, asegurando la satisfacción de nuestros clientes a través de un equipo altamente calificado y orientado a la excelencia. (Information Evolution, s.f)

1.1.1.2. Visión

Ser líderes en el ámbito del manejo de información para el sector comercial, siendo la referencia indiscutible en cuanto a precisión, integridad y relevancia de los datos; inspirando confianza en nuestros clientes y siendo un socio estratégico en la evolución de sus operaciones. (Information Evolution, s.f)

1.1.1.3. Valores

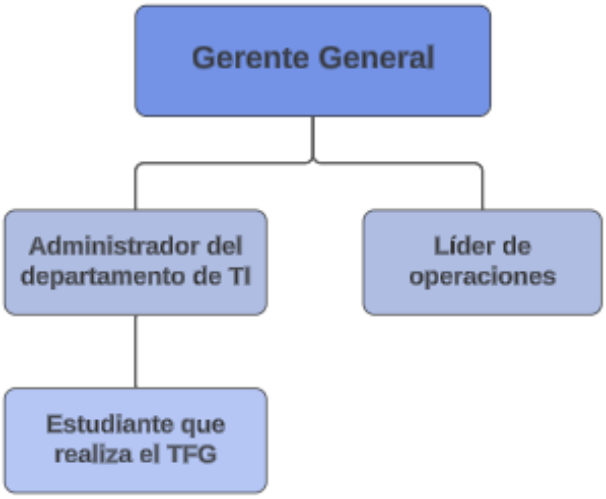
Information Evolution (s.f) define los siguientes valores como parte de su cultura:

- ***Éxito con el cliente:*** el récord de éxito con el cliente se debe al lanzamiento de nuevos servicios de información, dando muchas ventajas sobre la competencia, tales como: que las operaciones se mantengan dentro del presupuesto, se dé una aplicación inteligente de la innovación y se anticipen de futuras oportunidades de mejora.
- ***Innovación:*** el historial de éxito se debe a que se toma el riesgo con los start-ups, dándoles el éxito que necesitan con los nuevos servicios de información mediante el conocimiento profundo del diseño de cadenas de suministro de datos robustas y eficientes.
- ***Flexibilidad:*** los procesos y tecnologías son estructurados de forma tal que puedan ser adaptables a los picos de trabajo, ya sean bajos o altos, para que los clientes mantengan su enfoque en el éxito de su proyecto y así servir de una mejor manera.
- ***Transparencia:*** los clientes reciben acceso a la producción en tiempo real, permitiendo que los equipos sientan como si fueran manejados directamente por el cliente. También se ofrecen diferentes vías de comunicación (dependiendo del cliente), lo que permite una comunicación clara dentro de los equipos.
- ***Integridad:*** la empresa no tiene lazos comerciales con otros dueños, revendedores o comercializadores, lo que garantiza que nunca haya un conflicto de intereses; además de que la seguridad de datos se toma de manera muy seria y se sigue los lineamientos de los clientes para evitar que la información caiga en manos equivocadas.
- ***Decencia:*** la empresa tiene una fuerte reputación como un empleador justo y ético; ofrecen mejores salarios y beneficios que el promedio, y también tiene la larga tradición de favorecer a sus comunidades dando apoyo a diferentes organizaciones, iniciativas, universidades, entre otras, enfocadas en el cuido de salud, educación y esfuerzos de socorro en casos de desastre.
- ***Responsabilidad social:*** la empresa apoya a diferentes organizaciones (como universidades, organizaciones sin fines de lucro, entre otras) que se enfocan en el avance de los campos de ciencias de la información y en hacer nuestro futuro digital más robusto y accesible para todos.

1.1.1.4. Equipo de Trabajo

A continuación, en la figura 2 se presenta el organigrama correspondiente al equipo de trabajo que estará involucrado en el desarrollo del Trabajo Final de Graduación.

Figura 2: Organigrama del equipo de trabajo



Nota: Elaboración propia

Como se observa en la Figura 2, el equipo de trabajo consta del estudiante que realiza el Trabajo Final de Graduación, el Gerente General de la empresa, el Líder de Operaciones y el Administrador del Departamento de TI, ya que dicho departamento cuenta únicamente con una persona, el cuál sería el encargado directo del proyecto por parte de la empresa. Los roles del equipo de trabajo se detallan en la Tabla 1 presentada a continuación.

Tabla 1: Roles del equipo de trabajo

Rol	Funciones del rol en la empresa	Funciones del rol en el proyecto
Gerente General	- Dirección estratégica de la empresa - Toma de decisiones clave - Gestión de relaciones con los clientes - Supervisión operativa	- Apoyo de recursos para el desarrollo del proyecto - Gestión de aspectos administrativos - Juicio de experto sobre información clave de la empresa - Validación de cumplimiento de los intereses de la empresa

Rol	Funciones del rol en la empresa	Funciones del rol en el proyecto
Administrador del departamento de TI	- Gestión técnica de TI - Desarrollo e implementación de políticas de TI - Solución de problemas y mantenimiento de los equipos - Monitoreo continuo de los equipos y sistemas	- Aprobación de la propuesta - Asesoramiento técnico - Evaluación de las prácticas actuales - Apoyo con información de TI - Supervisión del avance de la propuesta a desarrollar por el estudiante
Líder de Operaciones	- Planificación estratégica de planes operativos - Gestión de proyectos - Gestión de recursos - Supervisión de las operaciones diarias - Optimización de procesos	- Asesoramiento técnico - Análisis de los procesos actuales - Apoyo con documentación interna - Apoyo en alineación con los estándares de la empresa
Estudiante que desarrolla el Trabajo Final de Graduación	- Colaboradora en la organización que desempeña funciones de mantenimiento de bases de datos y aseguramiento de la calidad de los datos para el cliente principal de la empresa	- Responsable de realizar el proyecto.

Nota: Elaboración propia

1.2.2. Proyectos Similares

En esta sección se detallan los proyectos similares a tomar en cuenta para el desarrollo del presente proyecto, tanto dentro como fuera de la organización. Estos proyectos servirán de guía conceptual para el desarrollo de la solución planteada.

1.2.2.1. Proyectos internos similares dentro de la organización.

Dado el corto tiempo que tiene de laborar Information Evolution Costa Rica desde su fundación hasta el presente año, y teniendo en cuenta que el departamento de TI cuenta con 4 meses de operaciones, actualmente no se cuentan con proyectos similares relacionados a riesgos de TI dentro de la organización.

1.2.2.2. Proyectos externos de la organización

Con respecto a los proyectos externos de la organización, para efectos de este proyecto se destacan tres, dos de estos proyectos fueron realizados como Trabajo Final de Graduación para la carrera de Administración de Tecnologías de información y un Proyecto de Grado para la maestría en Gobierno de Tecnología Informática.

1.2.2.2.1. Metodología para la gestión de riesgos de TI basada en COBIT 5

Este Trabajo Final de Graduación, elaborado por Jean Carlo Alfaro Campos en el año 2017, abordó una problemática específica que enfrentaba Deloitte: el incremento en los costos de recursos, tiempo y personal al ofrecer sus servicios de consultoría sin un marco estandarizado para la gestión de riesgos de TI. Esta situación se hacía particularmente crítica cuando se requería proveer dichos servicios de gestión de riesgos. En respuesta a este desafío, Alfaro Campos desarrolló una metodología para la gestión de riesgos de TI, fundamentada en COBIT 5 y alineada con las buenas prácticas de la norma INTE/ISO 31000, como proyecto final.

1.2.2.2.2. Propuesta de Estandarización y Automatización de Procesos Administrativos de la Empresa Suum Technologies

Este Trabajo Final de Graduación, elaborado por Dayana Vindas Sosa en el año 2021, abordó una problemática clave en la empresa Suum Technologies, la cual se caracterizaba por la creciente brecha entre los requerimientos empresariales y la capacidad de las herramientas tecnológicas disponibles, afectando así las operaciones diarias de la empresa. Frente a este problema, Vindas Sosa propuso una solución centrada en la estandarización y automatización de los procesos administrativos. Su enfoque incluyó la diagramación AS-IS, para representar los procesos actuales, y la diagramación TO-BE, para ilustrar los procesos mejorados, empleando la notación BPMN 2.0 para una definición clara y estructurada de los procesos, buscando optimizar las operaciones y alinear las herramientas tecnológicas con las necesidades reales de la empresa.

1.2.2.2.3. Diseño del Proceso De Gestión De Riesgos de TI de la multinacional “La Compañía” e implementación en el área de operaciones de TI Colombia

Este Proyecto de Grado, elaborado por Yamile Esther Dugarte Coll en el año 2017, abordó una problemática que consistía en la necesidad de un proceso unificado y estructurado para la gestión de riesgos de TI en una empresa, lo que llevó a inconformidades en las auditorías. Frente a este problema, Dugarte Coll, desarrolló un proceso integral para el diseño del proceso de gestión de riesgos de TI a través de las mejores prácticas de COBIT 5, la norma ISO 31000, la norma ISO 38500 y el PMI, con el fin de mejorar la identificación de riesgos y mitigar pérdidas.

1.3. Planteamiento del Problema

En esta sección se describe la situación actual que se presenta en la organización en cuanto a proyectos o servicios de gestión de riesgos de TI. El propósito es identificar claramente el problema que motiva la realización del trabajo final de graduación.

1.3.1. Situación problemática

Como se mencionó, Information Evolution Costa Rica se dedica al análisis de datos y al mantenimiento de bases de datos para el mercado inmobiliario de los Estados Unidos. Estas actividades cotidianas dependen críticamente del uso de sistemas informáticos, programas y equipos tecnológicos, por ende, es esencial mantener un control riguroso sobre estos recursos y desarrollar planes de contingencia en caso de fallos o problemas que afecten la operatividad para uno o más empleados.

Según Carlos Calderón Salazar (comunicación personal, 2024), quien es el Administrador del departamento de TI de la empresa Information Evolution Costa Rica y cuya minuta de la reunión se encuentra en el Apéndice J, a lo largo de su primer año, la empresa ha experimentado un crecimiento exponencial, impulsado por su alto rendimiento y resultados positivos. No obstante, las actividades cotidianas de Information Evolution Costa Rica dependen críticamente del uso de sistemas informáticos, programas y equipos tecnológicos, por ende, es esencial mantener un control riguroso sobre estos recursos y desarrollar planes de contingencia en caso de fallos o problemas debido a que el acelerado avance ha venido acompañado de un aumento en las incidencias técnicas, afectando principalmente a los sistemas informáticos y al hardware empleado por los trabajadores.

A pesar de estos avances y los incidentes de TI que han ocurrido en los últimos meses, la organización aún no ha implementado una metodología efectiva de gestión de riesgos de TI. Esta carencia afecta tanto al departamento de TI como a la dirección general, limitando su capacidad para prevenir problemas potenciales y responder de manera eficaz y eficiente cuando estos ocurren.

Este vacío en la gestión de riesgos de TI ha llevado a situaciones en las que la continuidad de las operaciones y la seguridad de la información y los sistemas se ve comprometida, lo cual es particularmente crítico dada la naturaleza de los servicios que ofrece la empresa. La necesidad de una estrategia preventiva en la gestión de riesgos no solo deja a la empresa vulnerable a posibles fallos antes de que ocurran, sino que también dificulta el establecimiento de procedimientos eficaces para la resolución rápida de estos problemas. La necesidad de una estrategia preventiva es crucial para evitar que pequeñas complicaciones escalen a problemas más significativos, afectando la productividad y poniendo en riesgo la continuidad operativa de la empresa.

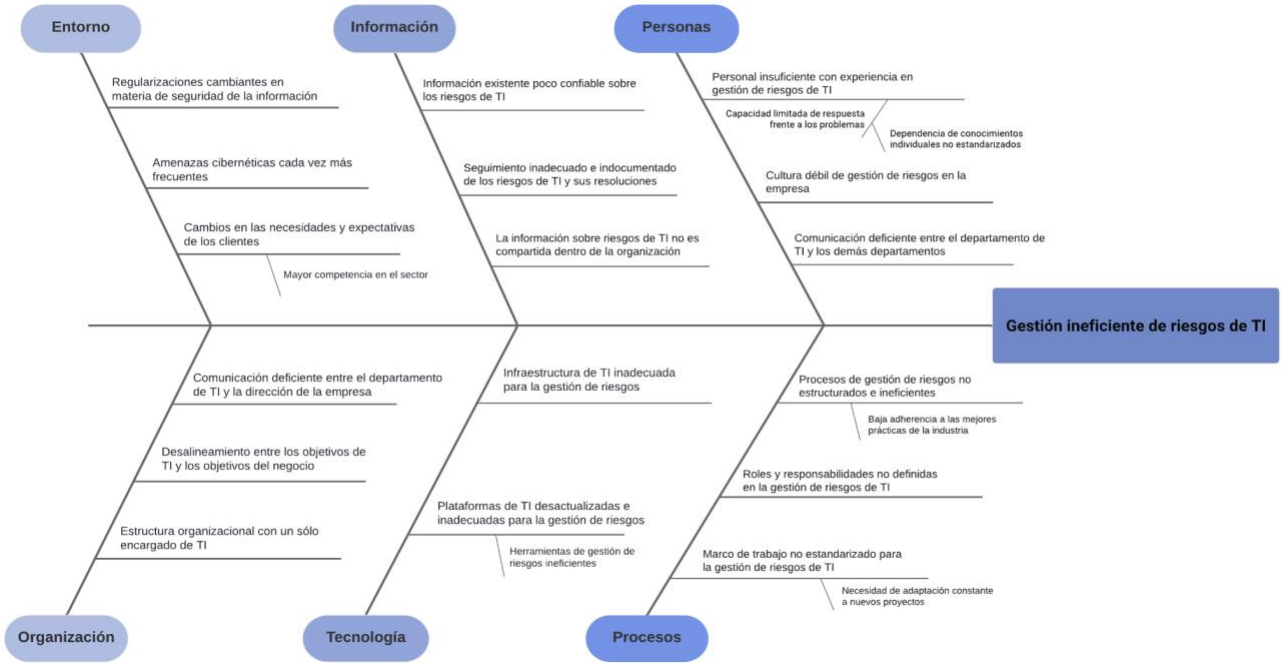
Según Carlos Calderón Salazar (comunicación personal, 2024), esta problemática descrita se debe a múltiples motivos como los que se exponen a continuación:

- **Necesidad de una estructura y roles definidos:** el bajo nivel de especificación de roles de TI, especialmente para la gestión de riesgos de TI, genera una sobrecarga de trabajo y un enfoque deficiente en la identificación, evaluación y tratamiento preventivo de los riesgos asociados. Es crucial definir claramente los roles para que la gestión de riesgos sea efectiva desde el inicio y se prevengan incidentes.
- **Infraestructura y herramientas inadecuadas:** el uso de plataformas de TI desactualizadas y la ineficiencia de herramientas específicas para la gestión de riesgos dificultan la recopilación, análisis y seguimiento preventivo de los riesgos de TI. Contar con una infraestructura actualizada y herramientas adecuadas permite identificar y mitigar riesgos antes de que se materialicen.
- **Procesos ineficientes y necesidad de adherencia a las mejores prácticas:** la necesidad de una estructura en los procesos de gestión de riesgos, seguimiento y documentación adecuada, y el no adoptar las mejores prácticas en materia de gestión de riesgos de TI, impiden una gestión preventiva y proactiva de los riesgos. Implementar procesos eficientes y alineados con las mejores prácticas ayuda a anticipar y prevenir problemas.
- **Información deficiente y baja comunicación:** la baja cantidad de datos confiables sobre los riesgos de TI y el deficiente seguimiento y comunicación dificultan la toma de decisiones informadas y la gestión preventiva de riesgos. Una mejor comunicación y datos confiables permiten anticipar y mitigar riesgos de manera oportuna.
- **Entorno dinámico y exigente:** las constantes regulaciones cambiantes, el aumento de las amenazas cibernéticas, los cambios en las necesidades de los clientes y competencia en el sector generan nuevos riesgos y desafíos que actualmente no se identifican y gestionan de manera oportuna. Estar al tanto de estos cambios y adaptarse rápidamente es esencial para prevenir y mitigar riesgos antes de que se conviertan en incidentes.

Como se mencionó, la empresa enfrenta varios desafíos significativos que afectan su operatividad y la necesidad de una metodología efectiva de gestión de riesgos de TI ha resultado en varios incidentes de TI en los últimos meses, provocando interrupciones en las operaciones y afectando la continuidad del negocio. Por ende, se vuelve imperativo implementar una metodología robusta de gestión de riesgos de TI que permita a la empresa anticipar, identificar y gestionar proactivamente los riesgos, asegurando así la estabilidad y continuidad de sus operaciones.

Es posible ver la situación planteada, anteriormente, de manera visual en la Figura 3, la cual representa el diagrama de Ishikawa del problema, el cual contiene las causas del problema en cuestión y la problemática a abordar.

Figura 3: Diagrama de Ishikawa del problema



Nota: Elaboración propia

1.3.2. Justificación del Proyecto

En un mundo actual y cambiante donde el uso de las tecnologías de información ha pasado de ser una ventaja competitiva a un requisito indispensable para competir en el mercado actual es de vital importancia comprender que estas tecnologías son vitales para las empresas, pero también conllevan riesgos asociados que, si no se gestionan adecuadamente, pueden tener consecuencias decisivas para las operaciones diarias y la posición de la empresa en la industria. La mala gestión de riesgos puede llevar a la pérdida de datos críticos, interrupciones en el servicio y un aumento significativo de los costos operativos.

Gracias a esto, la implementación de una metodología de gestión de riesgos de TI es de vital importancia en el contexto empresarial actual, especialmente para empresas como Information Evolution Costa Rica, que enfrentan desafíos relacionados con la seguridad y protección de datos, la continuidad operativa y la eficiencia en la respuesta ante incidentes. En un entorno donde las tecnologías de información no solo apoyan, sino que impulsan la estrategia de negocio, gestionar los riesgos asociados a estas tecnologías se vuelve un requisito indispensable. Los riesgos de TI son capaces de comprometer la operatividad, generar pérdidas financieras, afectar la reputación de la empresa e incluso poner en riesgo su sostenibilidad a largo plazo.

Ante esta situación problemática, Information Evolution Costa Rica enfrenta altos costos y vulnerabilidades en sus operaciones diarias, producto de una gestión de riesgos que no está formalmente estructurada ni alineada con las mejores prácticas de la industria. Aplicar una metodología como la propuesta en este proyecto permitirá a la empresa avanzar de un enfoque reactivo a uno proactivo en la gestión de sus riesgos de TI, permitiendo una detección y mitigación anticipada de posibles amenazas. Este cambio es crucial, pues le otorgará a la organización un marco sólido para identificar, evaluar y tratar los riesgos antes de que se materialicen y generen consecuencias significativas para sus operaciones.

La metodología propuesta, basada en estándares internacionales como ISO 31000 y COBIT 2019, proporciona una estructura sistemática y adaptable que no solo responde a los desafíos específicos de la empresa, sino que también promueve la alineación con los objetivos estratégicos y el cumplimiento de regulaciones. Esto es particularmente importante para Information Evolution Costa Rica, ya que una gestión de riesgos formalizada le permitirá optimizar el uso de sus recursos, minimizar interrupciones y establecer controles preventivos y correctivos efectivos, asegurando que los incidentes se reduzcan en frecuencia e impacto.

Además, la aplicación de esta metodología no solo atiende las vulnerabilidades actuales, sino que también contribuye al fortalecimiento de la cultura organizacional en torno a la seguridad y resiliencia de TI. A través de la capacitación, la definición de roles y responsabilidades claras, y la implementación de procesos estandarizados, la empresa podrá construir una cultura de gestión de riesgos que favorezca la colaboración y la responsabilidad compartida en toda la organización. Esto no solo incrementa la eficiencia operativa, sino que también refuerza la confianza de los clientes y de las partes interesadas, quienes verán a la empresa como una entidad confiable y comprometida con la protección de su información.

Por otra parte, esta metodología fomenta una cultura organizacional orientada a la gestión de riesgos, a través de capacitaciones, revisión de políticas y establecimiento de roles y responsabilidades. Esto fortalece la resiliencia organizacional y permite a la empresa estar mejor preparada frente a posibles amenazas, garantizando la confianza de clientes y partes interesadas. Este proyecto proporciona un marco estructurado en el ámbito de la auditoría de TI que asegura que los procesos y controles de TI cumplan con las necesidades empresariales y los requisitos regulatorios de la industria. El marco COBIT 2019 ofrece una perspectiva completa del gobierno de TI, esencial para realizar auditorías efectivas y evaluar la eficacia de las políticas y controles implementados para gestionar los riesgos.

Esto garantiza una gestión proactiva y coherente de la seguridad, la auditoría y los riesgos en un entorno TI cada vez más complejo y desafiante, haciendo que este proyecto sea crucial para cualquier Administrador de Tecnologías de Información que busque excelencia en su función y un aporte significativo en la gestión de riesgos de TI para la empresa en que labore.

1.3.3. Beneficios esperados del proyecto

En esta sección se explican cuáles son los beneficios tanto directos como indirectos que se generarán producto del Proyecto.

1.3.3.1. Beneficios Directos

- **Establecimiento de una metodología estandarizada de gestión de riesgos de TI:** tanto el marco de trabajo COBIT 2019 como la ISO 31000 proporcionan un marco estructurado que ayuda a definir roles y responsabilidades claras dentro de la gestión de riesgos, asegurando que cada miembro del equipo conozca sus tareas específicas en relación con la identificación, evaluación y mitigación de riesgos.
- **Definición de procesos de gestión de riesgos de TI:** estructura y estandariza las operaciones de TI, mejorando así la eficiencia y la efectividad en la gestión de riesgos, ya que, al contar con procesos claramente definidos, a través de las mejores prácticas, la empresa podrá identificar, evaluar y manejar los riesgos de TI de manera más sistemática y alineada con las mejores prácticas.
- **Documentación y seguimiento actualizado:** al utilizar una metodología de gestión de riesgos basada en la ISO 31000, se facilita la documentación sistemática y el seguimiento continuo de los riesgos de TI, lo que mejora la gestión y la visibilidad de estos dentro de la organización, aparte de proporcionar información veraz y actualizada de cómo tratar los riesgos identificados en el momento en que se materializan.

1.3.3.2. Beneficios Indirectos

- **Mejora en la continuidad operativa:** al reducir las incidencias técnicas con una respuesta proactiva a riesgos, la empresa podrá mejorar su continuidad operativa, lo que significa que podrá seguir funcionando sin interrupciones incluso en caso de que se produzca un incidente, lo que es especialmente importante para Information Evolution Costa Rica, ya que sus servicios son críticos para el mercado inmobiliario de los Estados Unidos.

- **Adopción de mejores prácticas:** el marco de COBIT 2019 y la ISO 31000 están alineados con las mejores prácticas internacionales y normativas de gestión de TI, lo que ayudará a Information Evolution a adherirse a estándares reconocidos y mejorar la eficacia de sus operaciones de TI.

- **Toma de decisiones informada:** la propuesta de una metodología de gestión de riesgos basada en COBIT 2019 y la ISO 31000 proporcionará a la empresa información fiable sobre sus riesgos de TI, lo que le permitirá tomar decisiones más informadas sobre cómo gestionar esos riesgos. Esto ayuda a la empresa a evitar riesgos costosos y a aprovechar oportunidades que de otro modo habría pasado por alto.

- **Mejora en la cultura organizacional:** la propuesta de un marco estructurado para la gestión de riesgos fortalece la cultura de riesgo dentro de la empresa, fomentando una mayor sensibilidad y comprensión de la importancia de la gestión de riesgos entre los empleados.

- **Fortalecimiento de la seguridad de la información:** una metodología estructurada y alineada con estándares internacionales como ISO 31000 y COBIT 2019 permite a la empresa identificar y evaluar de forma proactiva los riesgos relacionados con la confidencialidad, integridad y disponibilidad de los datos.

1.4. Objetivos

Esta sección establece los objetivos planteados para el desarrollo del trabajo. Primeramente, se establece el objetivo general y después los objetivos específicos que aplican a la resolución del problema.

1.4.1. Objetivo General

Proponer una metodología de gestión de riesgos de TI para Information Evolution Costa Rica, alineada con las mejores prácticas de la industria, para la definición de una estrategia y proceso operativo de la gestión de riesgos de TI durante el segundo semestre del 2024.

1.4.2. Objetivos Específicos

- Analizar la situación actual de las prácticas de gestión de riesgos de TI utilizadas por Information Evolution Costa Rica, identificando las fortalezas y debilidades, para la detección de las brechas presentes en la empresa.

- Comparar las mejores prácticas de la industria de gestión de riesgos de TI, para la selección de aquellas que mejor se adapten a las necesidades de gestión de riesgos de Information Evolution Costa Rica.

- Crear un conjunto de artefactos, para la instrumentalización y estandarización de la metodología estratégica de la gestión de riesgos de TI según el estado deseado del proceso.

1.5. Alcance

El presente Trabajo Final de Graduación tiene como objetivo proponer una metodología de gestión de riesgos de TI específicamente diseñada para Information Evolution Costa Rica, alineada con las mejores prácticas de la industria. Para la elaboración de este trabajo, el alcance está estructurado en tres fases.

En la Fase I, se evaluarán las prácticas actuales de gestión de riesgos de TI en la empresa mediante una revisión de la documentación existente y entrevistas con los colaboradores. Esta evaluación permitirá identificar fortalezas, debilidades y áreas de mejora de las prácticas existentes. A partir de esta evaluación, se generarán los diagramas AS-IS del proceso de gestión de riesgos de TI y se realizará un análisis de brechas entre las prácticas actuales y las mejores prácticas de la industria, de tal manera que se obtenga la información necesaria para la generación de los diagramas TO-BE del proceso de gestión de riesgos de TI.

En la Fase II, se investigarán las mejores prácticas de la industria en la gestión de riesgos de TI y se compararán tanto entre ellas mismas como con las prácticas actuales de la empresa, evaluando la aplicabilidad y efectividad de estas prácticas en el contexto de la empresa, para así seleccionar las prácticas que mejor se adapten a las necesidades específicas de gestión de riesgos de la empresa.

Por último, en la Fase III, se propondrá el diagrama TO-BE del proceso deseado de gestión de riesgos de TI y se revisarán las brechas identificadas en la Fase I de acuerdo con las mejores prácticas seleccionadas y el proceso propuesto, validando también la capacidad y mejoras logradas en el proceso propuesto. También, se crearán los artefactos y la estructura de la metodología de gestión de riesgos de TI adaptada a las necesidades de la empresa. Para ello, se tomará como base el proceso EDM03 de COBIT 2019, denominado "Asegurar la optimización del Riesgo", el cual garantiza que los aspectos relevantes sobre los riesgos de TI, como el apetito y la tolerancia al riesgo, se comprendan, articulen y comuniquen adecuadamente dentro de la organización. Posteriormente, se utilizará el proceso APO12 de COBIT 2019, denominado "Gestionar el Riesgo", que consiste en identificar, evaluar y reducir los riesgos relacionados con la tecnología de información de manera continua y alineada con las políticas establecidas. También, la ISO 31000 se empleará para alinear estas prácticas y definir el ciclo de gestión de riesgos de TI, exceptuando la práctica de "Alcance, contexto y criterios" que se abarca en la fase anterior. Finalmente, se diseñará una hoja de ruta que sirva como guía para la implementación de la propuesta.

Una vez finalizadas estas tres fases, este proyecto proporcionará un enfoque integral y estructurado para mejorar la gestión de riesgos de TI en Information Evolution Costa Rica, asegurando que las prácticas adoptadas no solo sean efectivas y eficientes, sino también alineadas con los estándares y mejores prácticas de la industria. Las tres fases definidas permiten una evaluación exhaustiva, una comparación detallada con las mejores prácticas y el desarrollo de una metodología robusta y adaptada a las necesidades específicas de la empresa.

1.6. Supuestos

En esta sección se indica el listado de los factores, elementos que se asumen como verdaderos, tanto de parte de la empresa Information Evolution Costa Rica como por parte del Tecnológico de Costa Rica, para cumplir con el éxito de los objetivos planteados en el proyecto:

- Acceso a información veraz y actualizada sobre lo relacionado con la gestión de riesgos de TI y sus procesos y políticas involucradas por parte de Information Evolution Costa Rica, así como a cualquier otra información necesaria para el desarrollo de la propuesta.
- Disposición de canales de comunicación adecuados y efectivos entre las partes involucradas en el desarrollo del proyecto.
- Dedicación del tiempo pertinente para el apoyo del desarrollo de la propuesta por parte de los involucrados, mediante la asistencia a reuniones, revisiones y consultas que surjan durante el desarrollo.
- Aceptación de la propuesta metodológica de la gestión de riesgos de TI por parte de la empresa Information Evolution Costa Rica.
- El proyecto utiliza un enfoque de desarrollo de una propuesta, en consecuencia, esta no se implementará y su implementación es responsabilidad de Information Evolution Costa Rica.
- Conocimiento en el área de gestión de riesgos de TI y Tecnologías de Información como tal por parte de las personas involucradas en el proyecto.

1.7. Entregables del Proyecto

En esta sección se describen los principales entregables generados como parte del proyecto y se contemplan tres tipos: los entregables académicos, los entregables del producto y los entregables de la gestión del proyecto.

1.7.1. Entregables Académicos

Los entregables académicos corresponden a los documentos que son entregados como parte del desarrollo del Trabajo Final de Graduación y están dirigidos a la Coordinación del Trabajo Final de Graduación y al profesor tutor asignado para la elaboración del proyecto. Para efectos de este proyecto se tienen los siguientes entregables académicos:

- Avances solicitados tanto por el profesor tutor como por la coordinación
- Informe final del Trabajo Final de Graduación
- Presentación y defensa del Trabajo Final de Graduación.

1.7.2. Entregables del Producto

Los entregables del producto son entregables que se generan al alcanzar cada uno de los objetivos específicos planteados para el proyecto, por tanto, estos están asociados de forma directa al cumplimiento de estos y están orientados a ser entregados a la organización en donde se desarrolla el Trabajo Final de Graduación. Para efectos de este proyecto se tienen los siguientes entregables del producto:

1.7.2.1. **Objetivo 1.** Analizar la situación actual de las prácticas de gestión de riesgos de TI utilizadas por Information Evolution Costa Rica, identificando las fortalezas y debilidades, para la detección de las brechas presentes en la empresa.

- Informe de diagnóstico de la situación actual de la gestión de riesgos TI.
- Diagramas AS-IS del proceso de gestión de riesgos de TI.
- Análisis FODA de la gestión de riesgos TI.
- Análisis de brechas del proceso de gestión de riesgos de TI.
- Diagramas TO-BE del proceso de gestión de riesgos de TI.

1.7.2.2. **Objetivo 2.** Comparar las mejores prácticas de la industria de gestión de riesgos de TI, para la selección de aquellas que mejor se adapten a las necesidades de gestión de riesgos de Information Evolution Costa Rica.

- Análisis comparativo de las mejores prácticas de la industria en la gestión de riesgos de TI.
- Selección de las mejores prácticas de la industria de acuerdo con las necesidades de la empresa.

1.7.2.3. **Objetivo 3.** Crear un conjunto de artefactos, para la instrumentalización y estandarización de la metodología estratégica de la gestión de riesgos de TI según el estado deseado del proceso.

- Artefactos específicos para la gestión de riesgos de TI Tanto del EDM03 como de APO12 y la ISO 31000.
- Estructura de la metodología de la gestión de riesgos de TI.
- Documentación de la estandarización realizada al proceso de gestión de riesgos de TI.
- Hoja de ruta para la implementación de la propuesta.

1.7.3. Gestión del proyecto

Los entregables de gestión tienen como objetivo asegurar la correcta ejecución del proyecto, tomando en consideración aspectos clave como el tiempo, costo, alcance y calidad; de modo que, a continuación, se detallan los entregables de gestión del proyecto.

1.7.3.1. Minutas

En esta sección se presenta la plantilla a utilizar como para las minutas de las reuniones que serán pertinentes durante el desarrollo del Trabajo Final de Graduación, con el fin de mantener un control estandarizado de los temas planteados. Se utilizará la plantilla adjunta en el Apéndice B. Aparte de esto, en el Apéndice C se presenta la plantilla para entrevistas a utilizar cuando sea pertinente el uso de la herramienta.

1.7.3.2. Gestión del Cambio

En esta sección se presenta la plantilla a utilizar en el proyecto para las solicitudes de gestión de cambio, con el fin de documentar de manera correcta los cambios solicitados durante el transcurso del Trabajo Final de Graduación. Se utilizará la plantilla adjunta en el Apéndice D.

1.7.3.3. Cronograma

En esta sección se presenta el diagrama de Gantt correspondiente al cronograma que hace referencia a la elaboración del proyecto, el cuál enmarca la realización y las entregas de cada una de las secciones pertinentes para la construcción del informe del Trabajo Final de Graduación. Cabe resaltar que las semanas 14 y 15 serán exclusivas para correcciones oportunas y revisiones del presente proyecto. Se utilizará el cronograma adjunto en el Apéndice A.

1.8. Exclusiones del Proyecto

En esta sección se indican los aspectos y entregables que no son tomados en cuenta para el desarrollo de la propuesta metodológica para la gestión de riesgos de TI, en consecuencia, dichos aspectos y entregables no forman parte de los resultados obtenidos por el desarrollo del proyecto.

- El desarrollo de un plan o procedimiento para el mantenimiento y mejora continua de la metodología propuesta para Information Evolution Costa Rica.
- La ejecución, propuesta o pruebas piloto de procesos o actividades de gestión de riesgos de TI en Information Evolution Costa Rica o en alguno de sus clientes.
- La realización de cualquier proceso de COBIT 2019 u otros estándares y marcos relacionados con la gestión y gobernanza de TI que no se estudie en el proyecto.
- La provisión de materiales o recursos humanos para la implementación, uso o actualización de la metodología propuesta.
- La definición y diagramación de procesos que no estén directamente relacionados con el proceso de gestión de riesgos y que no sean pertinentes para el desarrollo de este proyecto.
- La implementación o recomendación de herramientas tecnológicas para apoyar la gestión de riesgos de TI en la empresa.
- La generación de diagramas fuera del proceso de gestión de riesgos de TI y que no correspondan a la estandarización del proceso de gestión de riesgos de TI.

- El desarrollo de simulaciones de los procesos que responden a la propuesta planteada a través de las buenas prácticas de la industria.
- El desarrollo de capacitaciones sobre el uso de la metodología propuesta o de los procesos y marcos de referencia utilizados en su elaboración, así como la creación de manuales o guías para la utilización de la metodología.
- La implementación de solicitudes de organizaciones externas a Information Evolution o de profesionales internos que no formen parte del equipo de trabajo del proyecto.

Por último, es importante aclarar que ni el estudiante ni el Instituto Tecnológico de Costa Rica son responsables de cualquier consecuencia negativa que resulte a través de la implementación de la metodología desarrollada como parte de este proyecto. Esta metodología se lleva a cabo específicamente para Information Evolution Costa Rica y no para otras firmas miembro de la multinacional o alguno de sus clientes, de modo que, el uso de la metodología por parte de otras entidades externas a Information Evolution Costa Rica es responsabilidad exclusiva de la empresa.

1.9. Limitaciones del Proyecto

En esta sección se detallan los factores y elementos que fueron previstos y que en alguna medida restringen el desarrollo del proyecto para así evitar conflictos y gestionar de manera correcta cada una de las actividades planteadas para el desarrollo del plan trazado.

- Bajo nivel de experiencia por parte de los colaboradores de la organización en el uso de marcos de trabajo para la gestión de riesgos de TI como COBIT 2019.
- Disponibilidad limitada por parte de los involucrados en el proyecto para el apoyo en el desarrollo de la propuesta.
- Complicaciones en la integración de los distintos marcos de referencia utilizados para la elaboración de la propuesta metodológica de gestión de riesgos de TI.
- Cambios organizacionales en el personal involucrado para el desarrollo del proyecto.
- Documentación inexistente de los procesos relacionados con la gestión de riesgos de TI.
- Inexistencia de simulaciones de los procesos utilizando una metodología de definición de riesgos al no ser incluidos en el alcance.
- Utilización única de la documentación y prácticas existentes por parte de Information Evolution Costa Rica y no de otras sedes como Estados Unidos e India.

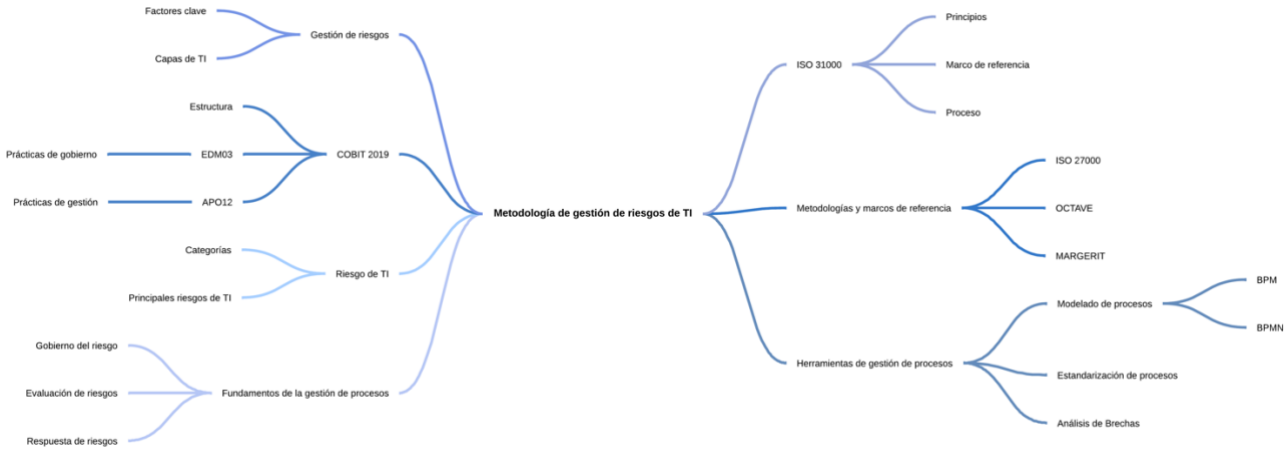
2. Marco Conceptual

En este capítulo se presenta el marco conceptual del proyecto, el cual tiene como objetivo proporcionar una base teórica y metodológica sólida para el desarrollo de una propuesta de gestión de riesgos de TI en Information Evolution Costa Rica. A través de este capítulo, se abordarán los conceptos clave y las mejores prácticas que sustentan el enfoque propuesto para la identificación, evaluación, y tratamiento de riesgos asociados con las tecnologías de información en la empresa.

Este apartado explora los conceptos clave relacionados con los riesgos de TI y su gestión, destacando la importancia de identificar y mitigar amenazas y vulnerabilidades. También, se presentará la aplicación de los marcos COBIT 2019 e ISO 31000, los cuales proporcionan una estructura sólida para el gobierno y la gestión de riesgos, se revisarán metodologías y herramientas como BPMN y el análisis de brechas, esenciales para documentar y mejorar los procesos. Finalmente, se abordarán las mejores prácticas y la estandarización de procesos, fundamentales para garantizar una gestión de riesgos efectiva y alineada con estándares internacionales.

Este marco conceptual servirá como guía teórica para la implementación de una metodología robusta y alineada con las mejores prácticas internacionales, asegurando que Information Evolution Costa Rica pueda gestionar sus riesgos de TI de manera proactiva y eficiente. A continuación, en la Figura 4, se presenta el mapa mental referente a los conceptos abordados en este capítulo.

Figura 4: Mapa mental de los conceptos abordados en el marco conceptual



Nota: Elaboración propia

2.1. Riesgos de TI

Esta sección tiene como objetivo contextualizar los marcos utilizados a lo largo del proyecto, comenzando desde la definición propia de lo que es un riesgo de TI, sin embargo, antes de comprender lo que este término trae consigo, es necesario comprender la definición de riesgo.

Según lo expuesto por Alvarado y Zumba (2015), "el riesgo es la probabilidad de que un evento ocurra y cause consecuencias (daños o pérdidas) que afecten la habilidad de alcanzar los objetivos" (p. 85), lo que liga el término "riesgo" con una probabilidad de que algo ocurra, dando paso a la incertidumbre, el no saber con exactitud si un evento ocurrirá o no.

Sin embargo, Cienfuegos Spikin (2013) expuso que, aunque no hay una definición general consensuada de riesgo en la literatura, podría haber algunas características comunes que podemos mencionar:

- El riesgo es igual a la pérdida esperada.
- El riesgo es igual a la desutilidad esperada.
- El riesgo es la probabilidad de un resultado adverso.
- El riesgo es una medida de la probabilidad y la gravedad de los efectos adversos.
- El riesgo es el hecho de que una decisión se tome en condiciones de probabilidades conocidas.
- El riesgo es la combinación de la probabilidad de un suceso y sus consecuencias.
- El riesgo se define como un conjunto de escenarios, cada uno de los cuales tiene una probabilidad y una consecuencia.

Ahora bien, si es posible comprender la definición de riesgo como la incertidumbre de que pase algo, es posible entrar a la definición de un riesgo de TI, o bien, un riesgo de Tecnologías de Información.

Dado lo anterior se llega a la investigación de Acronis (2021) quien comentó que "El riesgo de TI se define como la posibilidad de pérdida o daño cuando una amenaza se aprovecha de una vulnerabilidad en los recursos informáticos de una organización, incluida la infraestructura de TI, las aplicaciones y datos." Entonces, es posible definir el riesgo de TI como esa incertidumbre de que pase algo que afecte al área de TI de la organización, incluidos sus recursos, infraestructura e información.

2.1.1. Categorías de Riesgos de TI

Alvarado y Zumba (2015) mencionaron que al hablar de riesgos de TI se incluye pérdida de productividad o negocios, responsabilidad por brechas de seguridad, multas por violaciones de normas y la imposibilidad de defenderse de demandas debido a la conservación inadecuada de registros, haciendo posible categorizar los riesgos de TI en tres grupos:

- **Riesgo de generación de valor de T.I. (ESTRATÉGICO):** volver a centrarse en los riesgos para evaluar cómo la capacidad de las TI está alineada con las estrategias empresariales y cómo se puede aprovechar para mejorar la eficiencia y efectividad de los procesos de negocio. (p. 80)

- **Riesgo en la entrega de programas y proyectos de T.I (PROYECTO)**: la gestión de riesgos debe centrarse en la capacidad para comprender y manejar proyectos complejos, asegurando que las TI contribuyan adecuadamente a las soluciones o mejoras. (p. 80)
- **Riesgo en la entrega de servicios y operaciones de T.I. (OPERACIONAL):** aquellos riesgos que podrían afectar la efectividad de los servicios respaldados por TI y su infraestructura de soporte, recordando que el rendimiento y la disponibilidad de los servicios de TI pueden impactar directamente el valor de la empresa, reduciéndolo o incluso destruyéndolo. (p. 81)

Este enfoque de Alvarado y Zumba (2015) proporciona una manera estructurada de entender y abordar los riesgos de TI al dividirlos en tres categorías clave: estratégico, de proyectos y operacional, tomando como riesgos de proyectos los riesgos a nivel técnicos y los operacionales como riesgos a nivel operativo. Ahora bien, al identificar estos grupos, se facilita la priorización de las acciones necesarias para alinear las capacidades tecnológicas con los objetivos de negocio, gestionar proyectos complejos y asegurar la continuidad y eficiencia de los servicios. Resaltando la importancia de una gestión integral de riesgos que considere las múltiples dimensiones en las que las TI pueden afectar a una organización.

2.1.2. Principales riesgos de TI

Pérez Abersú (2014) explicó que en las empresas existen siete principales riesgos de TI de los que, al presentarse una intensificación de alguno, es posible crear una falla de escala similar a una gran crisis financiera. Estos siete principales riesgos que explica Pérez Abersú se exponen a continuación:

- **Manejo de TI interno:** el tener toda la estructura de TI internamente, sin subcontrataciones, puede dar una acumulación de problemas difíciles de manejar para una sola organización.
- **Asociaciones con contrapartes:** al trabajar en un proyecto conjunto con una organización externa, ya sea un competidor o socio, pueden existir riesgos de una interconexión directa entre ambas partes y que compartan información.
- **Subcontratación de servicios:** se tiene que tomar precauciones al tener proveedores externos de servicios, como Recursos Humanos, Legal o de TI; hay que revisar que no se compartan datos de más entre las dos partes.
- **Riesgos cibernéticos a cadenas de suministro:** las cadenas de suministro y logística tradicionales pueden sufrir severas interrupciones con ataques cibernéticos.
- **Tecnologías disruptivas:** las nuevas tecnologías, como las redes inteligentes, traen consigo nuevos efectos inadvertidos, que todavía no están en la mira de los profesionales de informática.

- **Infraestructura ascendente:** actualmente hay sociedades y economías que son sustentadas por infraestructuras informáticas, ya sean sus sistemas de electricidad o telecomunicaciones, que, de sufrir alteraciones, como una potencial regulación de Internet, crearían riesgos para cualquier organización.
- **Crisis externas:** los riesgos que están fuera del sistema, en los cuales la organización no tiene ningún control, tal como una pandemia de *malware,* pueden tener un efecto cascada.

Ahora bien, el análisis de Pérez Abersú ofrece una visión amplia de los principales riesgos de TI que enfrentan las empresas, destacando cómo cada uno de ellos puede escalar hasta convertirse en una crisis de gran magnitud, subrayando la complejidad y la interconectividad de los riesgos en el entorno empresarial actual que alienta a las organizaciones a adoptar una estrategia de gestión de riesgos más holística y proactiva, considerando tanto los factores internos como externos que pueden afectar su estabilidad y continuidad operativa.

2.2. Gestión de riesgos de TI

Una vez comprendido lo que el concepto "riesgo de TI" implica, es importante comprender a lo que se refiere la gestión de este, por lo que, según lo formulado por Valencia et al. (2016) "la gestión de TI se centra en administrar e implementar la estrategia tecnológica del día a día, y su enfoque está más orientado al suministro interno de TI" (p. 67). Aparte de esto, Valencia et al. también define la gestión de riesgos de TI como un "método sistemático que permite planear, identificar, analizar, evaluar, tratar y monitorear los riesgos asociados con una actividad, función o proceso, para que la organización pueda reducir pérdidas y aumentar sus oportunidades" (p. 67).

Así también, "entendido el gobierno de TI, tal como lo establece el estándar internacional ISO/IEC 38500:2008 como un sistema que dirige y controla la utilización actual y futura de las TIC" (Valencia et al., 2016, pág. 67). En la gestión de riesgos de TI, el gobierno de TI se ve como ese órgano de dirección en las organizaciones para lo relacionado con las tecnologías de información, mientras que, según el análisis de Valencia et al., la gestión de riesgos de TI se entiende como un proceso integral que se enfoca en minimizar las amenazas y maximizar las oportunidades dentro del entorno tecnológico de una organización. Sin embargo, aparte de estos dos componentes, Kumsuprom (2010) propuso que se debe tomar en cuenta el gobierno de seguridad de la información, el cual tiene como una de sus principales funciones el proveer a las organizaciones de una estrategia general para la seguridad de su información.

Analizando estos tres componentes propuestos por los diversos autores, un enfoque estructurado en estos dos gobiernos y la gestión de TI ofrece un enfoque sistemático que permite proteger los activos y operaciones, alineándose estratégicamente con los objetivos de negocio y asegurando que la tecnología actúe como un facilitador clave para el éxito organizacional, garantizando que las inversiones tecnológicas sean seguras, rentables y sostenibles a largo plazo.

También, Valencia et al (2016), en su investigación, explicaron algunos de los marcos de referencia y metodologías de gestión de riesgos de TI más utilizados actualmente, de los cuales se hablará más adelante, sin embargo, a partir de estas metodologías y marcos de referencia, estos autores concluyen que, independientemente del proceso de gestión de riesgos de TI que se utilice, este proceso, visto desde un punto de vista metodológico, cuenta con siete fases de común entre ellos:

- Establecimiento del contexto.
- Identificación de riesgos.
- Análisis de riesgos.
- Valoración de riesgos.
- Plan de tratamiento de riesgos.
- Comunicación y consulta.
- Monitoreo.

También, estos autores mencionaron la importancia de la medición del impacto de la gestión de riesgos de TI en las organizaciones, ya que según Valencia et al. (2016) “Si bien el impacto de cualquier riesgo en la organización afecta sus objetivos, el impacto directo de los riesgos de tecnologías de información, […], son medidos por lo general a través de la triada confidencialidad, integridad y disponibilidad” (p. 74). Estos tres criterios son explicados a continuación, según lo expuesto por Valencia et al. en su investigación.

- **Confidencialidad:** consiste en un término asociado con el acceso y uso de la información solo por parte de quienes se encuentran autorizados y tienen la necesidad de conocerla, convirtiéndola en accesible únicamente por los entes autorizados.
- **Integridad:** consiste en la capacidad de proteger la precisión e integridad de la información y de los activos tecnológicos frente a su modificación o destrucción no autorizada, evaluando aspectos como la precisión, completitud y validez de la información.
- **Disponibilidad:** consiste en el nivel de accesibilidad de la información y los activos tecnológicos en el momento en que sean requeridos.

Del mismo modo, Valencia et al. (2016) destacaron en su investigación la estructura fundamental que compone el proceso de gestión de riesgos de TI, identificando siete fases clave que son comunes en la mayoría de las metodologías utilizadas hoy en día, además de subrayar la relevancia de evaluar el impacto de estos riesgos en las organizaciones, considerando cómo los principios de confidencialidad, integridad y disponibilidad juegan un papel central en la medición de dicho impacto. Estos aspectos no solo proporcionan un marco para entender cómo se gestiona el riesgo de TI, sino que también abren la puerta a un análisis más detallado sobre los componentes esenciales que aseguran una gestión efectiva y alineada con los objetivos organizacionales.

2.2.1. Factores clave en la gestión de riesgos de TI

Así como lo expresó Kumsuprom (2010) “El mejor enfoque de la gestión de riesgos de las TIC en una organización consiste en abordar los problemas desde varias perspectivas, incluida la consideración de los entornos externos” (p. 19); es por ello que en su análisis, hizo referencia a cuatro factores clave que sirven como base al realizar el análisis del riesgo de TI, los cuales se exponen a continuación:

2.2.1.1. Gestión de Recursos Humanos

De acuerdo con Kumsuprom (2010), la gestión de riesgos de TI se basa en una integración sólida entre la gestión de recursos humanos y la estructura organizacional, donde los encargados deben enfrentar desafíos como la falta de conocimiento, sesgos en los datos y la influencia de la política interna, siendo fundamental desarrollar competencias internas y sensibilizar a los empleados sobre la exposición a riesgos de TIC, abarcando aspectos como la seguridad de la información, la disponibilidad y la recuperación.

2.2.1.2. Gestión de TI

Según lo mencionó Kumsuprom (2010), la importancia de la gestión de TI para una adecuada gestión de riesgos radica en que esta permite conocer los recursos y la capacidad de TI, incluyendo la integración de hardware, software, personal y telecomunicaciones, haciendo esencial comprender la configuración de la infraestructura y realizar análisis de riesgos para mitigar posibles amenazas.

2.2.1.3. Gestión de la seguridad de la información

Siguiendo la perspectiva que formuló Kumsuprom (2010), la gestión de la seguridad de la información se enfoca en proteger los datos y la información mediante controles de acceso, autenticación, confidencialidad, integridad y no repudio, buscando salvaguardar la información relacionada con los procesos comerciales frente a posibles riesgos y resaltando la importancia de evaluar amenazas, implementar contramedidas adecuadas y educar al personal en seguridad.

2.2.1.4. Controles para la gestión de riesgos de TI

Como lo explicó Kumsuprom (2010) los controles para la gestión de riesgos de TI se centran en la integración del control de TI con los procesos empresariales para asegurar que las políticas, procedimientos y estructuras organizativas estén alineados con los objetivos del negocio y puedan prevenir, detectar y corregir riesgos de manera efectiva, lo que convierte a un sistema de control interno crucial para limitar la incertidumbre y mitigar los riesgos a un nivel aceptable, asegurando la integridad de la información, incluyendo estrategias de prevención y mitigación utilizadas para reducir la probabilidad y el impacto de riesgos adversos.

2.2.2. Capas de TI para el análisis de riesgo

Con respecto a las capas de TI para el análisis de riesgos tenemos la perspectiva de Valencia et al. (2016) que refirieron lo siguiente:

> Los riesgos de TIC cubren por lo general dos tipos de recursos, la información y los activos tecnológicos, sin embargo, frente a la evolución de la función de Tecnologías de Información, ha surgido un tercero, denominado servicios de TIC, como concepto integrador de recursos y cuyo origen se da al pasar de una gestión de recursos tecnológicos a una gestión de servicios de Tecnologías de Información (p. 71).

Como lo explicaron estos autores, la evolución de la gestión de Tecnologías de la Información ha ampliado el enfoque tradicional de los riesgos de TI, que inicialmente se centraba en la información y los activos tecnológicos, surgiendo de ellos los servicios de TI como tercer componente, integrando estos recursos en una gestión más holística. A partir de este tercer componente y el análisis de distintos modelos de gestión de riesgos de TI para los activos, Valencia et al. crean un modelo de doce capaz tecnológicas, de tal manera que el fallo de una de ellas implique el fallo de una única capa, explicando la gestión de riesgos de TI como un enfoque integral e interdependiente. En la Figura 5, se muestran las doce capas planteadas por estos autores.

Figura 5: Capas de tecnologías de información planteadas por Valencia et al

1	PROCESOS DE NEGOCIO
2	SERVICIOS DE TI
3	DATOS/INFORMACIÓN/CONOCIMIENTO
4	SISTEMAS DE INFORMACIÓN TRANSACCIONALES
5	SISTEMAS DE INFORMACIÓN SOPORTE
6	MOTORES DE BASES DE DATOS
7	SISTEMAS OPERATIVOS
8	PC's DE ESCRITORIO E IMPRESORAS
9	SERVIDORES (Físicos, virtuales y en la nube)
10	CENTROS DE REDES Y CABLEADO
11	CENTROS DE COMPUTO
12	ENERGIA

Nota: Recuperado de (Valencia et al., 2016, p. 72)

El modelo propuesto por estos autores subraya que el fallo en cualquiera de estas capas puede desencadenar un efecto dominó que afecte a todo el sistema, reforzando la necesidad de un enfoque de gestión de riesgos que considere todos estos elementos de manera coordinada y holística, garantizando así la resiliencia y continuidad de las operaciones en un entorno tecnológico cada vez más complejo y dependiente de la integración de múltiples recursos.

2.3. Marco de referencia COBIT 2019

A continuación, se presenta COBIT 2019 como el pilar central en la estructura de gestión de riesgos de TI dentro de este proyecto, ya que este marco juega un papel crucial al ofrecer un enfoque integral para el gobierno y la gestión de las tecnologías de información, asegurando que las estrategias de TI estén alineadas con los objetivos empresariales de Information Evolution Costa Rica.

Según lo expuesto por ISACA (2018):

> COBIT es un marco para el gobierno y la gestión de las tecnologías de la información de la empresa, dirigido a toda la empresa. La I&T empresarial significa toda la tecnología y procesamiento de la información que la empresa utiliza para lograr sus objetivos, independientemente de dónde ocurra dentro de la empresa. (p. 13)

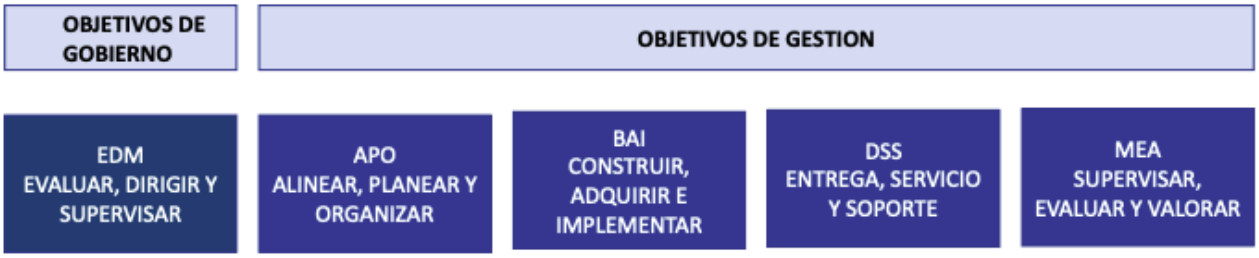
Este es el marco principal de desarrollo del proyecto, ya que COBIT 2019 proporciona una guía práctica y detallada para optimizar la gestión de riesgos de TI, abordando todos los aspectos críticos, desde la identificación hasta el tratamiento de riesgos, de manera coherente y eficiente. Además, al ser un estándar ampliamente reconocido a nivel internacional, garantiza que las prácticas implementadas no solo sigan las mejores prácticas globales, sino que también sean lo suficientemente flexibles para adaptarse a las particularidades y demandas específicas de la empresa, asegurando que la gestión de riesgos se realice de manera efectiva, contribuyendo al éxito y la sostenibilidad del negocio.

2.3.1. Estructura de COBIT 2019

Siguiendo los datos expuestos por ISACA (2018) encontramos que “el marco de referencia COBIT hace una distinción clara entre gobierno y gestión. Estas dos disciplinas abarcan distintos tipos de actividades, requieren distintas estructuras organizativas y sirven diferentes propósitos.” (p. 13).

A partir de esta división entre gobierno y gestión de TI, se destaca que la estructura de COBIT 2019, según lo planteado por ISACA (2018), se organiza en torno a objetivos de gobierno y objetivos de gestión en cinco dominios clave, los cuales son fundamentales para el alineamiento estratégico y la efectiva administración de las tecnologías de la información dentro de una organización. Los objetivos de gobierno están orientados a evaluar, dirigir y supervisar el uso de la tecnología en la empresa, asegurando que las TI apoyen los objetivos empresariales de manera coherente y eficiente, y, por otro lado, los objetivos de gestión se centran en la alineación, planificación, implementación, entrega, servicio, soporte, y la supervisión continua de los procesos de TI. En la Figura 6 se presentan los cinco dominios clave según COBIT 2019.

Figura 6: Dominios COBIT 2019



Nota: Recuperado de (ISACA, 2018)

Cada uno de estos dominios desempeña un papel esencial en el ciclo de vida del gobierno y la gestión de TI, asegurando que las iniciativas tecnológicas sean administradas de manera integral y efectiva.

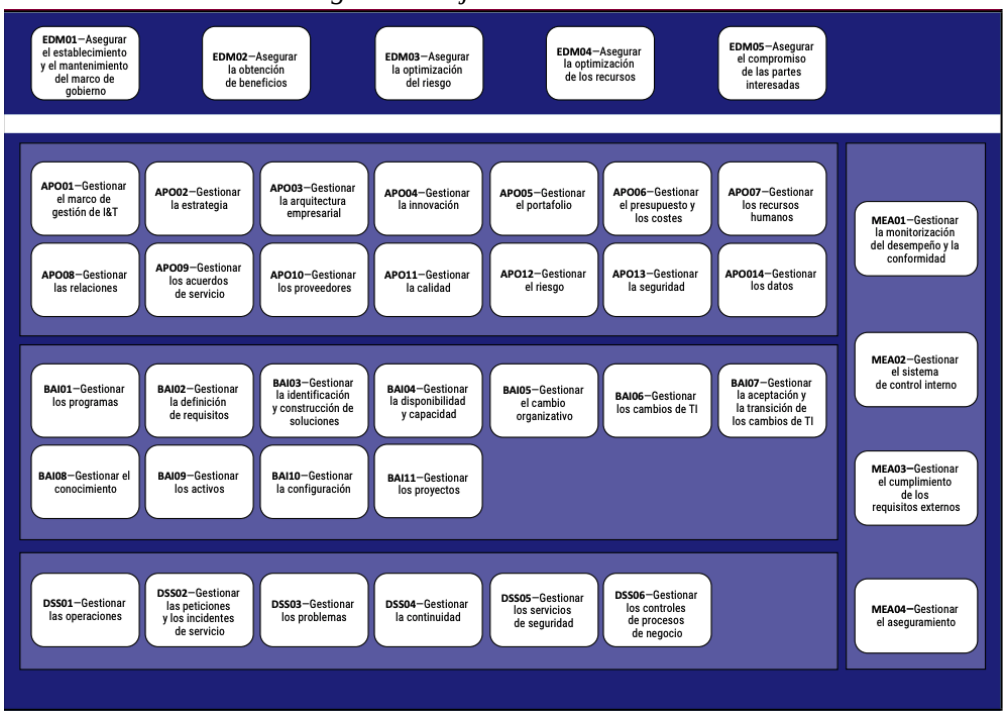
Ahora bien, cada uno de esos dominios se subdivide en distintos objetivos. Los objetivos de gobierno se agrupan en el dominio Evaluar, Dirigir y Monitorizar. En este dominio, el órgano de gobierno evalúa las opciones estratégicas, guía a la alta gerencia con respecto a las opciones estratégicas elegidas y monitoriza el logro de la estrategia. (ISACA, 2018, pág. 11).

Por otro lado, con respecto a los objetivos de gestión, ISACA (2018) afirmó que estos se agrupan en cuatro dominios:

- Alinear, Planificar y Organizar (APO): aborda la organización general, estrategia y actividades de apoyo para la información y la tecnología (I&T).
- Construir, Adquirir e Implementar (BAI): se encarga de la definición, adquisición e implementación de soluciones y su integración en los procesos de negocio.
- Entregar, Dar Servicio y Soporte (DSS): aborda la entrega operativa y el soporte de los servicios de información y tecnología (I&T), incluida la seguridad.
- Monitorizar, Evaluar y Valorar (MEA): aborda la monitorización del rendimiento y la conformidad de I&T con los objetivos de rendimiento internos, los objetivos de control interno y los requisitos externos.

Según esta estructura, ISACA (2018) explica que “Un objetivo de gobierno está relacionado con un proceso de gobierno, mientras que un objetivo de gestión está relacionado con un proceso de gestión” (p. 20). Formando de esta manera un marco de trabajo conformado por 35 objetivos de gestión y cinco objetivos de gobierno. Esta estructura se muestra en la Figura 7.

Figura 7: Objetivos COBIT 2019



Nota: Recuperado de (ISACA, 2018, p. 12)

Cada uno de estos dominios desempeña un papel esencial en el ciclo de vida del gobierno y la gestión de TI, asegurando que las iniciativas tecnológicas sean administradas de manera integral y efectiva. Como se observa en la Figura 8, estos dominios se subdividen en objetivos específicos que permiten una gestión detallada y estructurada de la información y la tecnología en la organización, agrupando los objetivos de gobierno bajo el dominio EDM donde el órgano de gobierno evalúa opciones estratégicas, guía a la alta gerencia y monitoriza el cumplimiento de la estrategia; y por otro lado, los objetivos de gestión se distribuyen en cuatro dominios clave: APO, BAI, DSS y MEA, cada uno con un enfoque específico en distintos aspectos de la gestión de TI.

Ahora bien, para asegurar que estos dominios y objetivos específicos funcionen de manera eficiente y coherente a lo largo de todos los procesos de gestión y gobierno de TI, COBIT 2019 introduce una serie de componentes de apoyo que se mantienen constantes a través de cada uno de estos dominios, los cuales son fundamentales para proporcionar la estructura necesaria que permite la implementación y sostenibilidad de las prácticas de gobierno y gestión en la organización. En la Figura 8 se muestran los componentes de apoyo de COBIT 2019 según ISACA (2018).

Figura 8: Componentes de apoyo COBIT 2019

Nota: Recuperado de (ISACA, 2018, p. 22)

En COBIT 2019, los componentes de apoyo son consistentes a lo largo de los diferentes objetivos de gestión, ya que este marco utiliza un enfoque estructurado para garantizar que cada objetivo, tanto de gestión como de gobierno esté respaldado por un conjunto integral de recursos y prácticas.

Dentro de este marco general, el proyecto se centrará particularmente en dos objetivos clave: EDM03, que aborda la optimización del riesgo, y APO12, que se enfoca en la gestión del riesgo. Estos dos objetivos son fundamentales para asegurar que los riesgos de TI sean identificados, evaluados y gestionados de manera eficaz, alineándose con la estrategia empresarial y optimizando el uso de los recursos disponibles.

2.3.2. EDM03: Asegurar la Optimización del Riesgo

ISACA (2018) formuló lo siguiente con respecto al EDM03:

> El objetivo EDM03 de COBIT 19 consiste en asegurar que el apetito y la tolerancia al riesgo de la empresa se entiendan, articulen y comuniquen, y que se identifique y gestione el riesgo para el valor de negocio relacionado con el uso de I&T. (p. 41).

Así mismo, ISACA (2018) expuso que el propósito de este objetivo consiste en lo siguiente:

> Asegurarse de que el riesgo de negocio relacionado con la I&T no exceda el apetito y tolerancia al riesgo de la empresa, que se identifique y gestione el impacto del riesgo de I&T para el valor de negocio y que se minimicen los posibles fallos de cumplimiento. (p. 41).

Según lo expuesto, el objetivo EDM03 de COBIT 19 se centra en asegurar que la empresa tenga una comprensión clara de hasta qué punto está dispuesta a asumir riesgos en su uso de

tecnología, y en garantizar que estos riesgos se identifiquen y gestionen adecuadamente para no afectar negativamente el negocio. Este objetivo no solo busca asegurar que los riesgos asociados con la tecnología no excedan la tolerancia establecida por la empresa, sino que también se enfoca en la identificación, gestión y mitigación de esos riesgos para proteger y maximizar el valor del negocio a través de tres prácticas de gobierno que plantea COBIT 2019.

2.3.2.1. Prácticas de Gobierno del EDM03

2.3.2.1.1. EDM03.01: Evaluar la gestión de riesgos.

Según ISACA (2018) la práctica EDM03.01 consiste en lo siguiente:

> Examinar y evaluar continuamente el efecto del riesgo sobre el uso actual y futuro de las I&T en la empresa. Considerar si el apetito al riesgo de la empresa es apropiado, y que se identifique y gestione el riesgo para el valor de la empresa relacionado con el uso de I&T. (p. 41)

2.3.2.1.2. EDM03.02: Dirigir la gestión de riesgos.

Según ISACA (2018) la práctica EDM03.02 consiste en lo siguiente:

> Dirigir el establecimiento de prácticas de gestión de riesgos para ofrecer una seguridad razonable de que las prácticas de gestión de riesgos de I&T son apropiadas y que el riesgo de I&T actual no sobrepasa al apetito al riesgo del consejo de administración. (p. 42)

2.3.2.1.3. EDM03.03: Monitorizar la gestión de riesgos.

Con respecto a este punto y siguiendo lo expresado por ISACA (2018) se llega a la idea de que “Monitorizar las metas y las métricas clave de los procesos de gestión de riesgos. Establecer cómo las desviaciones o los problemas se identificarán, se les dará seguimiento y se comunicarán para su solución.” (pág. 42)

Como se analizó, las tres prácticas de gobierno dentro del objetivo EDM03 proporcionan un enfoque integral para la gestión de riesgos en el contexto de TI, asegurando que se realice una evaluación continua de los riesgos, se dirija adecuadamente la gestión de estos, y se monitorice de manera efectiva. Estas prácticas permiten a la empresa mantener un control riguroso sobre los riesgos asociados con el uso de la tecnología, garantizando que dichos riesgos no superen los niveles aceptables y que se gestionen de manera que protejan y optimicen el valor del negocio; y, a través de la evaluación, dirección y monitoreo, se establezca un ciclo constante de mejora y adaptación en la gestión de riesgos, lo que es crucial para enfrentar los desafíos dinámicos que presenta el entorno tecnológico actual.

Aunque las prácticas de gobierno del EDM03 proporcionan una base sólida para la gestión de riesgos, es necesario complementar este enfoque con una gestión operativa y estratégica que permita una implementación efectiva y alineada con los objetivos de la empresa, tal y como lo plantea el objetivo APO12 de COBIT 19, el cual se centra en la identificación, evaluación y tratamiento de los riesgos de TI de manera más operativa y estratégica.

2.3.3. APO12: Gestionar el Riesgo

Según ISACA (2018) el objetivo de COBIT 2019 APO12 consiste en "Identificar, evaluar y reducir continuamente los riesgos relacionados con I&T dentro de los niveles de tolerancia establecidos por la gerencia ejecutiva de la empresa.", cuyo propósito consiste en "integrar la gestión del riesgo empresarial relacionado con la I&T con la gestión del riesgo empresarial global (ERM), y equilibrar los costes y beneficios de la gestión del riesgo empresarial relacionado con las I&T." (ISACA, 2018, pág. 131).

Como se definió en el párrafo anterior, el objetivo APO12 de COBIT 2019 trata de tener un proceso continuo que mantenga bajo control los riesgos tecnológicos, asegurándose de que estos no solo se gestionen de forma aislada, sino que se integren con la gestión global de riesgos de la empresa, de esta manera, se busca encontrar un equilibrio entre los costos de gestionar estos riesgos y los beneficios que se obtienen al mantenerlos bajo control, todo esto a través de las seis prácticas de gestión específicas que plantea COBIT 2019 para el APO12.

2.3.3.1. Prácticas de Gestión del APO12.

2.3.3.1.1. APO12.01: Recopilar datos.

"Identificar y recopilar datos relevantes para habilitar una efectiva identificación, análisis y reporte de los riesgos relacionados con I&T." (ISACA, 2018, p. 131)

2.3.3.1.2. APO12.02: Analizar el riesgo.

"Desarrollar una visión fundamentada del riesgo de I&T vigente, que soporte las decisiones de riesgo." (ISACA, 2018, p. 132)

2.3.3.1.3. APO12.03: Mantener un perfil de riesgo.

"Mantener un inventario de los riesgos conocidos y los atributos de riesgo, incluidos la frecuencia esperada, impacto potencial y respuestas. Documentar los recursos, capacidades y actividades de control actuales relacionados con elementos de riesgo." (ISACA, 2018, p. 132)

2.3.3.1.4. APO12.04: Articular el riesgo.

"Comunicar de manera oportuna información sobre el estado actual de las exposiciones y oportunidades relacionadas con I&T a todas las partes interesadas requeridas para obtener una respuesta apropiada." (ISACA, 2018, p. 133)

2.3.3.1.5. APO12.05: Definir un portafolio con acciones de gestión de riesgos.

"Gestionar las oportunidades para reducir el riesgo a un nivel aceptable como un portafolio." (ISACA, 2018, p. 133)

2.3.3.1.6. APO12.06: Responder al riesgo.

"Responder de manera oportuna a eventos de riesgo materializados con medidas eficaces para limitar la magnitud de las pérdidas." (ISACA, 2018, p. 134)

Una vez explicadas las seis prácticas de gestión en el objetivo APO12, es posible notar cómo estas abarcan el ciclo completo de la gestión de riesgos de TI, desde la recolección de datos hasta la respuesta ante eventos de riesgo materializados.

También, es importante resaltar que las prácticas APO12.01 (Recopilar datos), APO12.03 (Mantener un perfil de riesgo), y APO12.06 (Responder al riesgo) se apoyan y están directamente vinculadas con la información generada en el objetivo EDM03, lo que asegura una integración fluida entre la estrategia de gobierno de riesgos establecida en el EDM03 y su ejecución operativa bajo APO12, permitiendo que la empresa no solo identifique y gestione los riesgos de manera proactiva, sino que también mantenga una coherencia estratégica en toda su gestión de riesgos de TI, lo que refuerza la capacidad de la organización para manejar los riesgos de forma eficiente y alineada con sus objetivos empresariales.

2.4. ISO 31000:2018

En el contexto de la gestión de riesgos de TI en Information Evolution Costa Rica, la norma ISO 31000 se presenta como un complemento esencial al marco COBIT 2019, ya que mientras COBIT 2019 proporciona una estructura integral para el gobierno y la gestión de las tecnologías de información, la ISO 31000, en su última versión del 2018, aporta un enfoque específico y detallado para la gestión de riesgos, aplicable a cualquier tipo de organización, estableciendo principios, directrices y un marco de referencia que permiten identificar, evaluar y gestionar los riesgos de manera sistemática y consistente. Según Riveros (2020):

> La norma "ISO 31000:2018. Gestión del Riesgo. Directrices" es una norma fundamental en Risk Management. Se trata de un estándar internacional que establece las directrices para que cualquier tipo de organización, sea cual sea su sector y tamaño, pueda considerar el riesgo como elemento generador de valor. (párr.1)

Riveros (2020) destaca la importancia de la norma ISO 31000:2018 en la gestión de riesgos como un estándar internacional que proporciona directrices clave, valorada por su aplicabilidad universal, permitiendo a organizaciones de cualquier sector o tamaño integrar el riesgo en su estrategia como un factor que puede generar valor, enfoque que permite a las organizaciones no solo protegerse contra amenazas, sino también aprovechar las oportunidades que el riesgo bien gestionado puede ofrecer. Ahora bien, según Riveros (2020) "cualquier empresa que siga los principios de esta directiva en Gestión de Riesgos está comprometida con su mejora continua y se volverá más resiliente", esto a partir de la obtención de las siguientes ventajas:

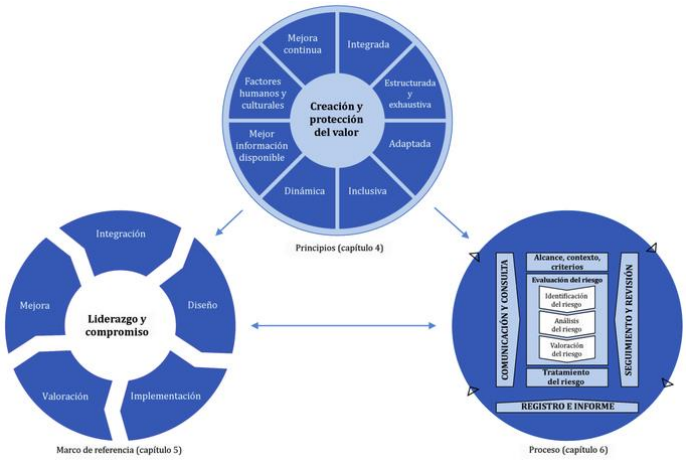
- Mejorar su eficiencia operativa.
- Tener una mejor gobernabilidad interna de la organización.
- Aumentar la confianza de partes externas.
- Mejorar su rendimiento y la sostenibilidad.
- Acentuar su calidad.
- Reducir los costes.
- La disminución o desaparición de incidentes inesperados.

Así mismo, Riveros (2020) planteó que:

> El estándar ISO 31000:2018 está estructurado en seis capítulos. Conocer su estructura y filosofía, es el primer paso para poder entender posteriormente toda la parte "ejecutiva" de la gestión del riesgo, la consideración de técnicas y herramientas y la forma de reportar para una mejor toma de decisiones. (párr.3)

Este autor también destacó la importancia de la comprensión de la estructura de esta norma, la cual se estructura en tres pilares fundamentales: principios, marco de referencia y procesos, tal y como se muestra en la Figura 9.

Figura 9: Estructura de la ISO 31000:2018



Nota: Recuperado de (ISO, 2018, p. vi)

A continuación, se exponen estos tres pilares que presenta la norma ISO 31000:2018 para la gestión de riesgos en las empresas.

2.4.1. Principios

La norma ISO 31000:2018 presenta ocho principios fundamentales que las organizaciones deben cumplir en todos sus niveles para lograr una gestión de riesgos eficaz. Estos principios, que son esenciales para estructurar un proceso de gestión de riesgos robusto, se muestran en la Figura 10 y se explican a continuación según lo establecido en la norma ISO 31000:2018.

Figura 10: Principios de la ISO 31000:2018

Nota: Recuperado de (ISO, 2018, p. 3)

2.4.1.1. Integrada

"La administración/gestión de riesgos es parte integral de todas las actividades de la organización." (ISO, 2018, p. 3)

2.4.1.2. Estructurada y exhaustiva

"Un enfoque estructurado y exhaustivo hacia la administración/gestión de riesgos contribuye a resultados coherentes y comparables". (ISO, 2018, p. 3)

2.4.1.3. Adaptada/Ajustada

"El marco de referencia y el proceso de la administración/gestión de riesgos se adaptan y son proporcionales a los contextos interno y externo de la organización relacionados con sus objetivos." (ISO, 2018, p. 3)

2.4.1.4. Inclusiva

"La participación apropiada y oportuna de las partes interesadas permite que se consideren sus conocimientos, puntos de vista y percepciones. Esto resulta en una mayor toma de concientización y una administración/gestión de riesgos informada." (ISO, 2018, p. 4)

2.4.1.5. Dinámica

"Los riesgos pueden aparecer, cambiar o desaparecer con los cambios de los contextos interno y externo de la organización. La administración/gestión de riesgos anticipa, detecta, reconoce y responde a esos cambios y eventos de una manera apropiada y oportuna." (ISO, 2018, p. 4)

2.4.1.6. Mejor información disponible

"Las entradas a la administración/gestión de riesgos se basan en información histórica y actualizada, así como en expectativas. La administración/gestión de riesgos tiene en cuenta explícitamente cualquier limitación e incertidumbre asociada con tal información y expectativas." (ISO, 2018, p. 4)

2.4.1.7. Factores Humanos y culturales

"El comportamiento humano y la cultura influyen considerablemente en todos los aspectos de la administración/gestión de riesgos en todos los niveles y etapas." (ISO, 2018, p. 4)

2.4.1.8. Mejora continua

"La administración/gestión de riesgos mejora continuamente mediante aprendizaje y experiencia." (ISO, 2018, p. 4)

Como es posible observar, los principios de la norma ISO 31000:2018 proporcionan una base sólida para la gestión de riesgos dentro de cualquier organización, asegurando que el riesgo se aborde de manera integral, estructurada y continua; y destacando la importancia de integrar la gestión de riesgos en todas las actividades de la organización, así como la necesidad de adaptar y ajustar los enfoques a los contextos específicos, considerando factores humanos y culturales, y asegurando que la información utilizada sea la mejor disponible.

Con estos principios definidos, es crucial entender cómo se estructuran y aplican en un marco organizacional coherente. A continuación, se explorará el marco de referencia propuesto por la norma ISO 31000:2018, el cual proporciona la estructura necesaria para implementar estos principios de manera efectiva en la gestión de riesgos de la organización.

2.4.2. Marco de Referencia

Sobre el marco de referencia se tienen diversos datos, pero siguiendo lo expuesto por la ISO (2018) se destaca qué:

> El propósito del marco de referencia de la administración/gestión de riesgos es apoyar a las organizaciones en integrar la administración/gestión de riesgos en todas sus actividades y funciones significativas. La efectividad de la administración/gestión de riesgos dependerá de su integración en la gobernanza de las organizaciones, incluyendo la toma de decisiones. (p. 4)

De igual forma, la ISO (2018) explica qué, el marco de referencia correspondiente a la ISO 31000:2018 está compuesto por seis componentes, tal y como se muestra en la Figura 11, de los cuales, el componente "Liderazgo y compromiso" funciona como un componente central aplicable a todo el ciclo de este marco, adaptando cada componente a las necesidades del negocio.

Figura 11: Componentes del marco de referencia de la ISO 31000:2018

Nota: Recuperado de (ISO, 2018, p. 5)

Dado lo anterior, a continuación se expone la definición de los seis componentes que forman el marco de referencia de la ISO 31000:2018:

2.4.2.1. Liderazgo y compromiso

Según ISO (2018), la alta dirección de las empresas debe velar por la integración de la gestión de riesgos a sus procesos diarios, demostrando su liderazgo y compromiso a partir de las siguientes actividades:

- Adaptando e implementando todos los componentes del marco de referencia.
- Publicando una declaración o una política que establezca un enfoque, un plan o una línea de acción para la administración/gestión de riesgos.
- Asegurando que los recursos necesarios se asignan para administrar/gestionar los riesgos.

- Asignando autoridad, responsabilidad y obligación de rendir cuentas en los niveles apropiados dentro de la empresa.

Estas actividades permiten definir los niveles de riesgo aceptables, guiando el desarrollo de criterios específicos que son comunicados a todas las partes interesadas, lo que a su vez destacada el valor de una gestión de riesgos efectiva. Además, fomenta un seguimiento continuo y sistemático de los riesgos, garantizando que el marco de gestión se mantenga relevante y adaptable al entorno dinámico de la organización, mejorando su capacidad para enfrentar desafíos futuros y tomar decisiones bien fundamentadas. de la organización.

2.4.2.2. Integración

Con respecto al punto de la integración, se toma como referencia lo establecido por la ISO (2018), la cual expresa qué::

> La integración de la administración/gestión de riesgos en las organizaciones es un proceso dinámico e iterativo, y se debiera adaptar a las necesidades y a la cultura de las organizaciones mismas. La administración/gestión de riesgos debiera ser una parte de, y no estar separada del propósito, la gobernanza, el liderazgo y compromiso, las estrategias, los objetivos y las operaciones de las organizaciones. (p. 6)

2.4.2.3. Diseño

Según la norma ISO 31000:2018, el componente de Diseño se divide en cinco actividades clave, las cuales, según lo que dicta la norma, se explican a continuación.

- **Comprensión de las organizaciones y su contexto:** las organizaciones deben analizar su contexto interno y externo al diseñar su marco de gestión de riesgos. El análisis externo incluye factores como los sociales, económicos y tecnológicos, así como las relaciones y expectativas de las partes interesadas, mientras que el análisis interno abarca la misión, gobernanza, cultura, capacidades y relaciones internas.

- **Articulación del compromiso con la administración/gestión de riesgos:** la alta dirección debe demostrar su compromiso con la gestión de riesgos mediante políticas o declaraciones que muestren cómo la gestión de riesgos se integra en la cultura, decisiones y operaciones de la organización, el cual debe ser comunicado a toda la organización y a las partes interesadas.

- **Asignación de roles, autoridades, responsabilidades y obligación de rendir cuentas en la organización:** la alta dirección debe asegurar que los roles, responsabilidades y rendición de cuentas en la gestión de riesgos se asignen claramente a todos los niveles de la organización, destacando que la gestión de riesgos es una responsabilidad clave.

- **Asignación de recursos:** la alta dirección debe garantizar que se asignen los recursos adecuados para la gestión de riesgos, incluyendo personas con habilidades y competencias, procesos y herramientas, sistemas de información, y necesidades de formación.

- **Establecimiento de la comunicación y la consulta:** las organizaciones deben establecer un enfoque formal para la comunicación y consulta sobre la gestión de riesgos a través de comunicación, la cual implica compartir información relevante, y consulta, que incluye la retroalimentación que influye en las decisiones y acciones. Ambos procesos deben ser oportunos y reflejar las expectativas de las partes interesadas.

2.4.2.4. Implementación

Las organizaciones deben implementar el marco de gestión de riesgos desarrollando un plan adecuado con plazos y recursos, identificando cómo se toman decisiones en toda la organización, modificando procesos de decisión según sea necesario y asegurando que las disposiciones para la gestión de riesgos sean claras y aplicadas. El éxito de la implementación depende del compromiso y la concientización de las partes interesadas, permitiendo abordar la incertidumbre en la toma de decisiones y adaptarse a cambios en el contexto, ya que un marco bien diseñado e implementado integrará la gestión de riesgos en todas las actividades y decisiones organizacionales.

2.4.2.5. Evaluación

Según ISO (2018), para evaluar la efectividad del marco de referencia de la administración/gestión de riesgos, las organizaciones deben:

- Medir periódicamente el desempeño del marco de referencia con relación a su propósito, sus planes para su implementación, sus indicadores y el comportamiento esperado.
- Determinar si se están logrando los resultados esperados y valorar el logro de los objetivos de las organizaciones mismas.

2.4.2.6. Mejora

Según la norma ISO 31000:2018, el componente de Mejora se divide en dos actividades clave, las cuales, según lo que dicta la norma, se explican a continuación.

- **Adaptación:** las organizaciones deben realizar el seguimiento continuo y adaptar el marco de referencia de la administración/gestión de riesgos en función de los cambios existentes. (p. 9)

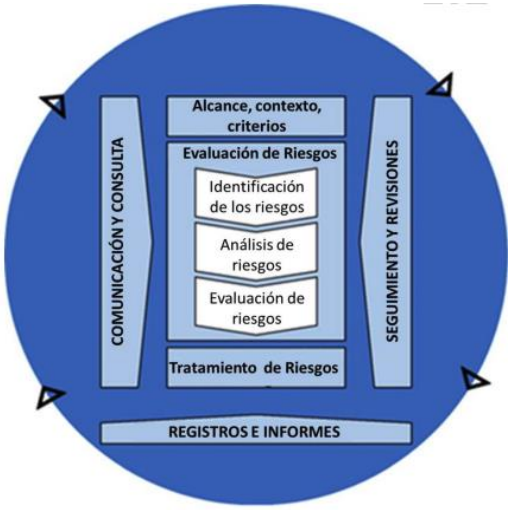
- **Mejora continua:** cuando se identifiquen brechas u oportunidades de mejora pertinentes, se deben desarrollar planes y tareas y asignarlas a quienes deben rendir cuentas de su implementación. Una vez implementadas, estas mejoras debieran contribuir al fortalecimiento de la administración/gestión de riesgos. (p. 9)

Ahora bien, el marco de referencia de la norma ISO 31000:2018 proporciona una estructura clara y coherente para la integración de la gestión de riesgos en todas las actividades y niveles de la organización, y, a través de sus seis componentes, se garantiza que la gestión de riesgos no sea un proceso aislado, sino una parte integral de la estrategia, la cultura y las operaciones diarias. Este enfoque permite a las organizaciones adaptarse a los cambios y desafíos de manera proactiva, asegurando que la gestión de riesgos sea efectiva y relevante en todo momento. Con esta base sólida establecida, es fundamental explorar el último pilar de la ISO 31000:2018: el proceso, el cual proporciona las directrices específicas para identificar, evaluar y mitigar los riesgos.

2.4.3. Proceso

Con respecto al Proceso, la ISO (2018) afirma que "El proceso de administración/gestión de riesgos implica la aplicación sistemática de políticas, procedimientos y prácticas a las actividades de comunicación y consulta, establecimiento del contexto y evaluación, tratamiento, seguimiento, revisión, registros y reportes de los riesgos." (p. 10). En la Figura 12 se muestra el proceso de gestión de riesgos según la ISO 31000:2018.

Figura 12: Proceso de gestión de riesgos según la ISO 31000:2018



Nota: Recuperado de (ISO, 2018, p. 10)

A continuación se detalla el proceso de gestión de riesgos según lo que dicta la norma ISO 31000:2018.

2.4.3.1. Comunicación y Consulta

Según ISO (2018), se afirma que:

> El propósito de la comunicación y consulta es apoyar a las partes interesadas pertinentes a comprender los riesgos, las bases con las que se toman decisiones y las razones por las que son necesarias acciones específicas. La comunicación busca

> promover la concientización y la comprensión de los riesgos, mientras que la consulta implica obtener retroalimentación e información para apoyar la toma de decisiones. (p. 11)

2.4.3.2. Alcance, contexto y criterios

Referente a este punto la ISO (2018) plantea que:

> El propósito del establecimiento del alcance, contexto y criterios es adaptar el proceso de la administración/gestión de riesgos, para permitir una evaluación de riesgos efectiva y un tratamiento apropiado de los riesgos mismos. El alcance, contexto y criterios implican definir el alcance del proceso, y comprender los contextos interno y externo. […]. Como el proceso de la administración/gestión de riesgos puede aplicarse a niveles distintos, […], es importante tener claro el alcance considerado, los objetivos pertinentes a considerar y su alineamiento con los objetivos de la organización. (p. 11)

Ahora bien, con respecto a los contextos internos y externos, según ISO (2018), "el contexto del proceso de la administración/gestión de riesgos debe establecerse a partir de la comprensión de los entornos interno y externo en los cuales opera las organizaciones y debe reflejar el entorno específico de la actividad." (p. 12)

Por último, con respecto a los criterios, la ISO 31000:2018 explica que es responsabilidad de las organizaciones definir la cantidad y el tipo de riesgos que están dispuestos a tomar de acuerdo con sus objetivos, junto a la definición de los criterios que utilizarán para evaluar la importancia de cada riesgo y apoyar el sistema de toma de decisiones, manteniendo siempre una alineación de estos criterios con el marco de referencia que se utilizará.

2.4.3.3. Evaluación de riesgos

Según ISO (2018):

> La evaluación de riesgos es el proceso global de identificación, análisis y evaluación de los riesgos mismos. La evaluación del riesgo se debiera llevar a cabo de manera sistemática, iterativa y colaborativa, basándose en el conocimiento y los puntos de vista de las partes interesadas. Se debiera utilizar la mejor información disponible, complementada por investigación adicional, si fuese necesario. (p. 13)

A continuación se definen las tres actividades pertinentes a la evaluación de riesgos según lo explicado en la ISO 31000:2018.

- **Identificación de riesgos:**

"El propósito de la identificación de riesgos es encontrar, reconocer y describir los riesgos que pueden ayudar o impedir a una organización lograr sus objetivos. Para la identificación de los riesgos es importante contar con información pertinente, apropiada y actualizada." (ISO, 2018, p. 13)

Se consideran factores como fuentes de riesgos, causas, oportunidades, vulnerabilidades, cambios en el contexto, indicadores de riesgos emergentes, activos, recursos, y limitaciones de conocimiento. Es crucial identificar riesgos, incluso aquellos fuera del control de la organización, y considerar múltiples resultados y consecuencias.

- **Análisis de riesgos:**

Referente al análisis de riesgos, ISO (2018) afirma que:

> El propósito del análisis de riesgos es comprender la naturaleza de los riesgos y sus características incluyendo, cuando sea apropiado, el nivel de los riesgos mismos. El análisis de los riesgos implica una consideración detallada de incertidumbres, fuentes de riesgo, consecuencias, probabilidades, eventos, escenarios, controles y su efectividad. (p. 13)

Es importante tener en cuenta que este análisis puede verse influenciado por sesgos, percepciones y la calidad de la información, y se recomienda utilizar una combinación de técnicas para eventos de alta incertidumbre.

- **Evaluación de riesgos:**

Según ISO (2018), es posible entender la evaluación de riesgos debido que:

> El propósito de la evaluación de los riesgos es apoyar a la toma de decisiones. La evaluación de los riesgos implica comparar los resultados del análisis del riesgo con los criterios para riesgos establecidos para determinar cuándo se requiere una acción adicional. (p. 14)

Las posibles decisiones incluyen no hacer nada, considerar opciones de tratamiento de riesgos, realizar análisis adicionales, mantener los controles actuales, o reconsiderar los objetivos. Es importante considerar el contexto amplio y las consecuencias, tanto reales como percibidas, por las partes interesadas internas y externas.

2.4.3.4. Tratamiento de los riesgos

Según lo expuesto por ISO (2018) "El propósito del tratamiento de los riesgos es seleccionar e implementar opciones para abordar los riesgos." (p.15). Bajo este contexto se tiene

que el proceso de tratamiento de los riesgos se divide en dos actividades clave, las cuales se explican a continuación de acuerdo con lo que dicta la ISO 31000:2018.

1. **Selección de las opciones para el tratamiento de riesgos:** "La selección de las opciones más apropiadas para el tratamiento de riesgos implica hacer un balance entre los beneficios potenciales, derivados del logro de los objetivos contra costos, esfuerzo o desventajas de la implementación." (ISO, 2018, p. 15)

2. **Preparación e implementación de los planes para el tratamiento de riesgos:** Según ISO (2018):

> El propósito de los planes para el tratamiento de los riesgos es especificar la manera en la que se implementarán las opciones elegidas para el tratamiento, de manera tal que los involucrados comprendan las disposiciones, y que pueda realizarse el seguimiento del avance respecto de lo planeado. El plan de tratamiento debiera identificar claramente el orden en el cual el tratamiento del riesgo se debiera implementar. (p. 16)

2.4.3.5. Seguimiento y revisiones

Según lo que aporta ISO (2018) con respecto al seguimiento y revisiones se destaca que:

> El propósito del seguimiento y las revisiones es asegurar y mejorar la calidad y efectividad del diseño, la implementación y los resultados del proceso. El seguimiento continuo y la revisión periódica del proceso de la administración/gestión de riesgos y sus resultados debiera ser una parte planeada del proceso de la administración/gestión de riesgos, con responsabilidades claramente definidas. (ISO, 2018, p. 16)

2.4.3.6. Registros e informes

El proceso de administración de riesgos y sus resultados deben ser documentados y reportados adecuadamente. De acuerdo con ISO (2018), estos registros y reportes tienen como propósito:

- Comunicar las actividades y resultados de la gestión de riesgos en toda la organización.
- Proveer información para la toma de decisiones.
- Mejorar las prácticas de gestión de riesgos.
- Facilitar la interacción con las partes interesadas, incluyendo aquellos con responsabilidades y obligaciones de rendición de cuentas.

El reporte es fundamental para la gobernanza organizacional, mejorando el diálogo con las partes interesadas y apoyando a la alta dirección en sus responsabilidades, aparte que factores como las necesidades de las partes interesadas, el costo, frecuencia, métodos de reporte y la relevancia de la información deben ser considerados.

2.5. Fundamentos clave de la gestión de riesgos

2.5.1. Gobierno del Riesgo

En la gestión de riesgos, uno de los fundamentos clave es el gobierno del riesgo, el cual establece el marco a través del cual las organizaciones gestionan y controlan los riesgos a los que se enfrentan, siendo esencial para garantizar que la gestión de riesgos se integre de manera coherente en todas las áreas de la organización, permitiendo una toma de decisiones informada y alineada con los objetivos estratégicos.

2.5.1.1. Apetito y tolerancia del riesgo

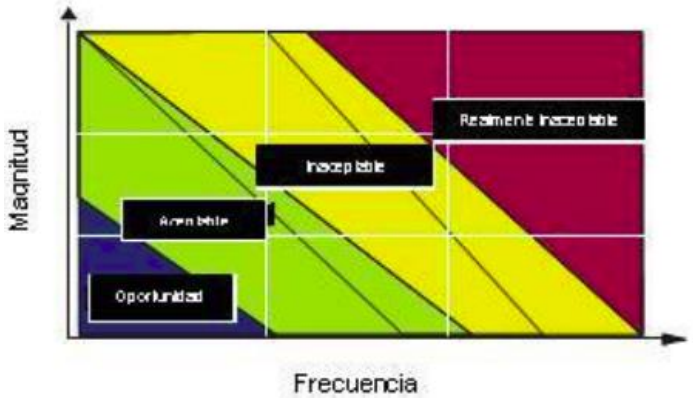
"El apetito de riesgo es la cantidad de riesgo que una entidad está dispuesta a aceptar cuando se trata de alcanzar sus objetivos." (ISACA, 2009, p. 17). A partir de este apetito, ISACA (2009) plantea dos factores clave para la definición de este en las empresas:

- La capacidad objetiva de la organización para absorber pérdida.
- La cultura o la predisposición a asumir riesgos-prudentes o agresivos.

De conformidad con lo definido por ISACA, el apetito de riesgo se entiende como la disposición de una organización a aceptar ciertos riesgos, definida en términos de la probabilidad de que ocurra un riesgo y la magnitud del impacto que tendría si se materializara, tomando en cuenta que este apetito varía entre organizaciones, ya que no existe un estándar universal que determine qué nivel de riesgo es aceptable o inaceptable para todas las empresas, si no que depende de su propio contexto.

Para la definición del apetito del riesgo, ISACA (2009) plantea que es posible definirlo a través de mapas de riesgo, en el que el nivel de importancia se diferencia de acuerdo con los colores que se utilicen. La Figura 13 muestra un ejemplo de mapa de riesgo para definir el apetito de riesgo.

Figura 13: Mapa de riesgo



Nota: Recuperado de (ISACA, 2009, p. 17)

ISACA (2009) explica la distinción de los colores expuestos en la Figura 12 de la siguiente manera:

- **Rojo:** indica que es un riesgo inaceptable. La organización estima que este nivel de riesgo es mucho más allá de su apetito de riesgo normal. Cualquier riesgo que se encuentre en esta banda podría desencadenar una respuesta inmediata de riesgos.
- **Amarillo:** indica riesgo elevado, es decir, también por encima de apetito de riesgo aceptable. La organización podría aceptarlo y requieren mitigación o respuesta adecuada a definir dentro de los límites de tiempo determinado.
- **Verde:** indica un nivel aceptable normal de riesgo, normalmente con ninguna acción especial requerida, excepto el mantenimiento de los controles actuales o de otras respuestas.
- **Azul:** indicio de un riesgo muy bajo, donde el ahorro del costo de oportunidades se puede encontrar al disminuir el grado de control o donde las oportunidades para asumir más riesgos pueden surgir.

El apetito de riesgo es una herramienta esencial para la gestión de riesgos dentro de una organización, ya que establece el nivel de riesgo que la entidad está dispuesta a asumir en su camino hacia el logro de sus objetivos, sin basarse únicamente en la capacidad de la organización para absorber pérdidas, sino también en su cultura y predisposición hacia los riesgos, ya sea de manera prudente o agresiva.

Ahora bien, según ISACA (2009):

> La tolerancia al riesgo es la desviación tolerable desde el nivel establecido por la definición del apetito de riesgo, por ejemplo, las normas o proyectos que deben realizarse dentro de los presupuestos y el tiempo, pero sobre costes del 10 por ciento del presupuesto o el 20 por ciento del tiempo son tolerados. (p. 17).

Según lo explicado, la tolerancia al riesgo se refiere a la flexibilidad que una organización tiene para manejar desviaciones de lo que considera un riesgo aceptable, a través de un margen dentro del cual se permiten ciertos imprevistos sin que se superen los límites que la empresa considera aceptables.

ISACA (2009) también establece lo siguiente sobre la tolerancia al riesgo:

- La tolerancia al riesgo se establece por las políticas organizacionales, permitiendo ciertas excepciones sin exceder el apetito de riesgo general. La flexibilidad en estas políticas es crucial para aprovechar oportunidades, aunque en algunos casos legales o regulatorios, la tolerancia al riesgo no es flexible.
- La tolerancia al riesgo debe ser claramente definida por el consejo de administración y comunicada a todas las partes interesadas, con un proceso establecido para manejar excepciones.

- Factores como nuevas tecnologías o cambios en el mercado pueden requerir revisiones periódicas del apetito y la tolerancia al riesgo, ajustando políticas según sea necesario.
- Si el costo de mitigar un riesgo es demasiado alto, la organización puede aceptar un mayor riesgo, optando por no cumplir con ciertas regulaciones si el costo de cumplimiento es prohibitivo.

La relación entre el apetito y la tolerancia al riesgo es esencial para la gestión de riesgo, ya que mientras que el apetito establece el nivel máximo de riesgo que una organización está dispuesta a asumir, la tolerancia define los márgenes dentro de los cuales se pueden aceptar ciertas variaciones sin exceder ese límite, por lo que estas dos dimensiones deben ajustarse continuamente en función de cambios en la tecnología, el mercado y otros factores, permitiendo a la organización equilibrar el riesgo y la oportunidad de manera estratégica.

2.5.1.2. Sensibilización y comunicación

Referente a este aspecto ISACA (2009) plantea lo siguiente:

> La concienciación de los riesgos es de reconocer que el riesgo es una parte integral de la organización. Esto no implica que todos los riesgos que deben ser evitadas o eliminadas, sino que se entienden y conocen los riesgos de TI, problemas de riesgo sean identificables, y la organización reconoce y utiliza los medios de manejar los riesgos de TI. (p.18).

Profundizando en lo anterior, ISACA (2009) también divide esta comunicación en tres tipos principales:

- **Expectativas de la gestión del riesgo:** es la comunicación esencial en la estrategia general de la organización hacia los riesgos de TI, y conduce todos los esfuerzos posteriores sobre la gestión del riesgo. En él se establecen las expectativas generales de la gestión de riesgos.
- **Capacidad actual de gestionar riesgos:** este control de la información permite saber el estado del motor de la gestión de riesgos en la organización, y es un indicador clave para la cultura de riesgo
- **Información con valor predictivo:** información sobre la situación real con respecto al riesgo de TI.

La sensibilización y comunicación de los riesgos implica reconocer que el riesgo es un elemento inevitable en cualquier organización, especialmente en el ámbito de TI y que no se trata de eliminar todos los riesgos, sino de comprenderlos y gestionarlos de manera efectiva, ya que al estar conscientes de los riesgos de TI, la organización puede identificar problemas potenciales y aplicar las estrategias adecuadas para manejarlos, asegurando así que los riesgos se controlen y se utilicen como parte de un enfoque proactivo en la gestión empresarial.

2.5.1.3. Cultura de Riesgo

"Una cultura de riesgos asumidos ofrece un entorno en el que los componentes de riesgo se discuten abiertamente, y los niveles de riesgo aceptables se entienden y se mantienen." (ISACA, 2009, p. 22). Una cultura de riesgos consiste en esa conciencia y aceptación de parte de la organización sobre la existencia de los riesgos y las maneras en que se abordan, disminuyendo el desorden y la resistencia por parte de esta misma.

ISACA (2009) explica que en una inadecuada cultura de riesgos existen sentimientos de culpa cuando estos son materializados, lo que ocasiona una búsqueda de culpables en lugar de seguir los planes para los riesgos. Aparte de esto, una forma sencilla de detectar problemas en la cultura de riesgo es la existencia de una desalineación entre el apetito de riesgo actual de la empresa y las políticas de la empresa, ya que resulta en comportamientos agresivos por parte de la dirección general al materializarse un riesgo.

La importancia de la cultura de riesgo radica en la reducción de la confusión y la resistencia dentro de la organización, facilitando una respuesta más coherente y alineada cuando los riesgos se materializan, evitando un ambiente de culpabilidad y resistencia al cambio en las organizaciones.

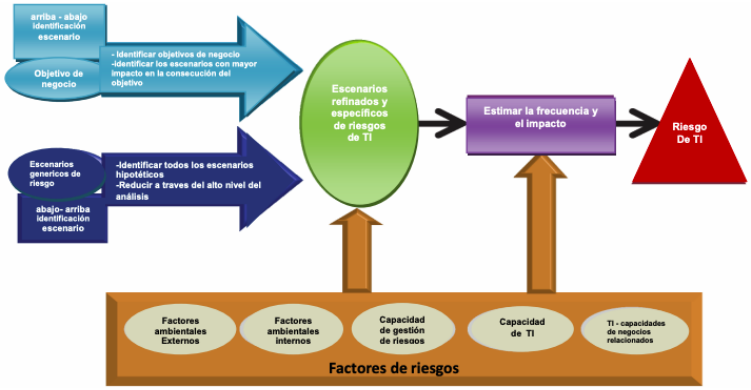
2.5.2. Evaluación de riesgos

La evaluación de riesgos es un proceso fundamental en la gestión de riesgos, ya que permite identificar, analizar y priorizar los riesgos que podrían afectar a una organización. A través de este proceso, se obtiene una comprensión detallada de los riesgos potenciales y su impacto, lo que facilita la toma de decisiones informadas sobre cómo manejarlos.

2.5.2.1. Escenarios de Riesgos de TI

Un escenario de riesgo es la descripción de un evento relacionado con TI que puede conducir a un impacto en el negocio (ISACA, 2009, p. 26). Estos escenarios se generan a través de dos distintos mecanismos. La Figura 14 muestra estos mecanismos.

Figura 14: Desarrollo de escenarios de riesgo de TI



Nota: Recuperado de (ISACA, 2009, p. 25)

ISACA (2009) explica estos mecanismos de generación de escenarios de la siguiente manera:

- Un enfoque de arriba abajo, en el que se parte de los objetivos generales y se realiza un análisis de los escenarios de riesgos de TI más relevantes y probables que impacten en los objetivos de negocio. Si los criterios de impacto están bien alineados con los controladores de valor real de la organización, los escenarios de riesgo relevantes se desarrollarán.
- Un enfoque de abajo arriba, en el que se utiliza una lista de escenarios genérico para definir un conjunto de escenarios más concretos y personalizados, aplicados a la situación de la organización individual

Referente a la Figura 13, ISACA (2009) explica que los dos enfoques expuestos se complementan y deben aplicarse de manera conjunta y los escenarios de riesgo deben ser relevantes y estar conectados con los riesgos reales del negocio. Al mismo tiempo, utilizar un conjunto de escenarios de riesgo genéricos ayuda a garantizar que no se omitan riesgos importantes, proporcionando así una perspectiva más amplia y completa sobre los riesgos de TI.

Ahora bien, cuando los escenarios genéricos del riesgo están definidos, se procede a utilizarlos para realizar el análisis del riesgo, en el que se debe evaluar la frecuencia y el impacto que tienen los escenarios en la organización a través de diversos componentes, tal y como se muestran en la Figura 15.

Figura 15: Componentes de los escenarios de riesgos

Nota: Recuperado de (ISACA, 2009, p. 25)

Los componentes de los escenarios de riesgo, como se observa en la Figura 15, incluyen factores clave como el tipo de amenaza, el actor que la origina, la acción específica que desencadena el riesgo, los activos o recursos afectados, y el tiempo en que ocurre, convirtiéndolos en elementos fundamentales para realizar un análisis de riesgo exhaustivo, permitiendo a la organización evaluar cómo la frecuencia y el impacto de estos escenarios pueden influir en su operación. ISACA (2009) define cada uno de los componentes de la siguiente manera:

- **Actor:** ente que genera la amenaza, pueden ser internos o externos y pueden ser humano o no humano.
- **Tipo de amenaza:** la naturaleza propia del evento.
- **Acción:** evento que tiene el escenario y que define la acción que genera el escenario.
- **Activo:** es el recurso sobre el cual el escenario actúa.
- **Tiempo:** planificación del tiempo que define aspectos como la duración y el momento específico en el que ocurre el evento.

2.5.2.2. Factores de Riesgo

"Los factores de riesgo son aquellos factores que influyen en la frecuencia y / o impacto en el negocio de los escenarios de riesgo, ya que pueden ser de diferente naturaleza." (ISACA, 2009, p. 24). Al provenir de distintas fuentes, estos factores tienen un alto grado de influencia en la manera en que un riesgo se materializa y afecta a la organización, por lo que, comprender estos factores resulta crucial para una gestión de riesgos efectiva.

Según ISACA (2009) los factores de riesgo se clasifican en dos categorías:

- **Factores ambientales:** estos se pueden dividir en factores internos y externos, diferenciándose en el grado de control que una organización tiene sobre ellos:
  - **Factores internos:** están bajo el control de la organización, aunque no siempre son sencillos de cambiar.
  - **Factores externos:** están fuera del control de la organización.
- **Capacidades:** el grado de capacidad de una organización en las actividades relacionadas con TI. Se distinguen según los tres marcos principales de ISACA:
  - **Capacidades de gestión de riesgos de TI:** ¿En qué medida es la organización madura en el desempeño de la gestión del riesgo de los procesos definidos en el marco de RISK IT?
  - **Capacidades de TI:** ¿Cuán buena es la organización realizando los procesos de TI definidos en COBIT?
  - **Capacidades de negocio relacionadas con TI:** ¿Cómo se alinean las actividades de gestión de valor de la organización con las expresadas en los procesos de Val IT?

Los factores de riesgo, al actuar como las causas que desencadenan la materialización de riesgos juegan un papel crucial en la gestión del riesgo dentro de una organización, entonces, al identificar y clasificar estos factores, es posible abordar de manera más precisa el origen de los riesgos, lo que es esencial para evitar que estos se materialicen y, en caso de hacerlo, minimizar sus consecuencias.

2.5.3. Respuesta de riesgos

Al finalizar la evaluación de riesgos, es fundamental definir cómo la organización responderá a cada uno de los riesgos identificados, lo que implica desarrollar estrategias y acciones específicas para abordar los riesgos que podrían afectar negativamente los objetivos de la organización. Este proceso no solo se centra en mitigar o eliminar los riesgos, sino también en identificar oportunidades que pueden ser aprovechadas para el beneficio de la organización.

2.5.3.1. Indicadores de Riesgo

Según ISACA (2009):

> Los indicadores de riesgos métricos son capaces de demostrar que la empresa está sujeta a, o tiene una alta probabilidad de, estar sometida a un riesgo que excede del apetito de riesgo definido. Son específicos para cada empresa y su selección depende de una serie de parámetros en el entorno interno y externo. (p. 27)

A partir de esto es posible inferir que los indicadores de riesgo son métricas clave que permiten a una organización medir y anticipar la posibilidad de que ciertos riesgos puedan materializarse y afectar sus operaciones, funcionando como señales de advertencia temprana que muestran cuándo un riesgo puede estar acercándose a niveles que exceden el apetito de riesgo establecido, y, al ser específicos para cada empresa, su definición y selección dependen de las necesidades de la organización. ISACA (2009) explica un proceso de tres pasos base para definir los indicadores de riesgo en las organizaciones:

1. Considerar las distintas partes interesadas en la empresa para asegurar un mayor aporte y alineación de estos a las necesidades empresariales.
2. Incluir en la selección a los indicadores de los resultados (indicando el riesgo después de que hayan ocurrido los hechos), indicadores principales (lo que indica que las capacidades están en el lugar apropiado para evitar que se produzcan acontecimientos) y las tendencias (análisis de indicadores en el tiempo o la correlación de los indicadores para obtener información).
3. Asegurar que los indicadores seleccionados detallen el origen de la causa de los eventos.

A través de esos tres pasos es posible asegurar una mejor selección de indicadores; sin embargo, entre los indicadores seleccionados, deben definirse los indicadores clave de riesgo (RSIK), los cuáles, según ISACA (2009) “se distinguen por ser de gran relevancia, por poseer una alta probabilidad de predecir o por que indican un riesgo importante.” (p.27). Para la selección de estos indicadores, ISACA (2009) define cuatro criterios:

1. **Impacto:** los indicadores de riesgo con alto impacto comercial son más propensos a ser RISK.

2. **Esfuerzo para aplicar, medir y reportar:** Los indicadores diferentes que son equivalentes en la sensibilidad, el criterio debe ser la facilidad.
3. **Fiabilidad:** el indicador debe poseer una alta correlación con el riesgo y ser un buen vaticinador o medida de resultado.
4. **Sensibilidad:** el indicador debe ser representativo para el riesgo y capaz de indicar con precisión las diferencias en el riesgo.

En este contexto es importante resaltar que la fiabilidad se refiere a la capacidad de un sistema o herramienta para funcionar de manera consistente y predecible, asegurando que siempre responda de la misma manera cuando ocurre una situación específica, mientras que la sensibilidad indica cuán capaz es ese sistema o herramienta de detectar un evento o condición en función de ciertos criterios o niveles establecidos.

Los indicadores clave de riesgo juegan un papel crucial en este proceso, ya que están vinculados directamente con el apetito y la tolerancia al riesgo, por lo que, definir niveles de activación adecuados para cada indicador permite que la organización actúe de manera proactiva, tomando decisiones informadas en el momento preciso para mitigar potenciales amenazas.

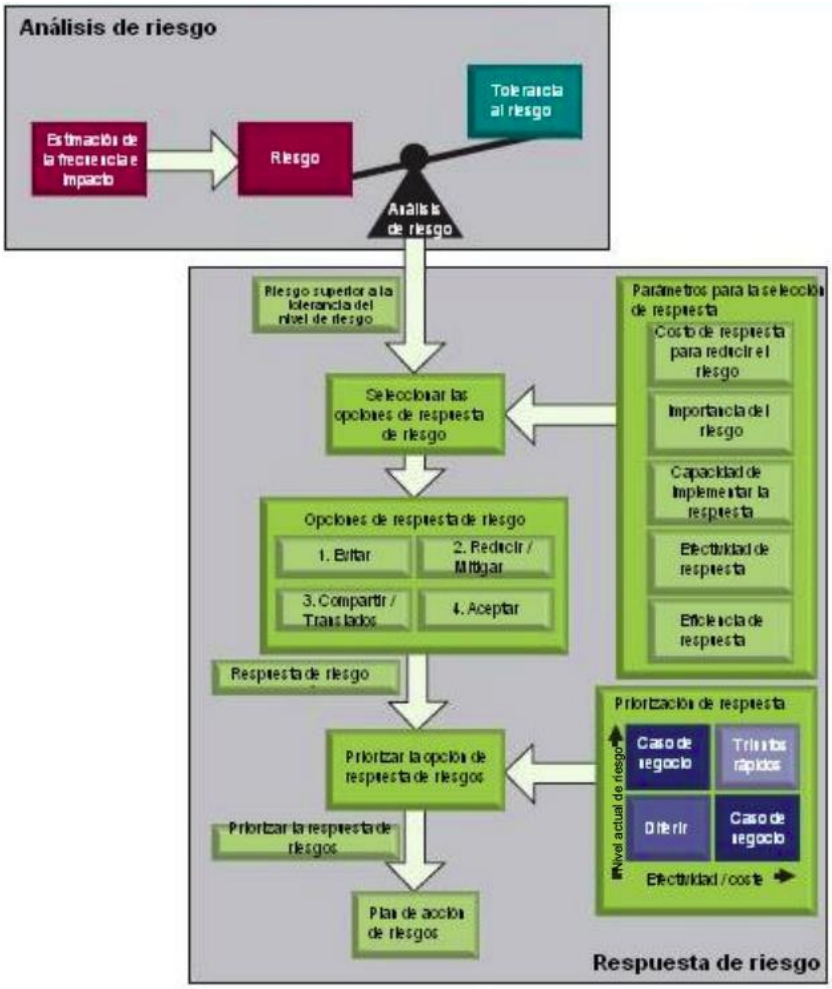
2.5.3.2. Definición, selección y priorización de la respuesta al riesgo

ISACA (2009) explica que:

> El objetivo de definir una respuesta al riesgo es llevar el riesgo al mismo nivel que el apetito de riesgo definido para la empresa después del análisis de riesgo. En otras palabras, una respuesta tiene que ser definida tal que el futuro riesgo residual (respuesta de riesgo definida y puesta en práctica) es, tanto como sea posible (por lo general dependerá de los recursos económicos disponible), dentro de los límites de tolerancia de riesgo. (p. 27).

El proceso de respuesta a riesgos no implica únicamente identificar las acciones necesarias para manejar los riesgos inherentes, sino que también implica asegurar que el riesgo residual, es decir, el riesgo que permanece después de haber aplicado las medidas de control y mitigación se mantenga dentro de los límites aceptables de tolerancia definidos por la organización. En otras palabras, la gestión del riesgo residual es un equilibrio entre los recursos económicos disponibles y la necesidad de mantener la exposición al riesgo en niveles controlables, reflejando así una gestión de riesgos efectiva y alineada con los objetivos estratégicos de la empresa. La Figura 16 ilustra el proceso de respuesta a riesgos.

Figura 16: proceso de respuesta a riesgos



Nota: Recuperado de (ISACA, 2009, p. 29)

La Figura 16 muestra cuatro distintas opciones de respuesta a los riesgos, las cuales son definidas de la siguiente manera:

2.5.3.2.1. Evitar riesgos

"Evitar significa salir de las actividades o de las condiciones que dan lugar a riesgo. Evitar riesgos se aplica cuando no hay otra respuesta adecuada." (ISACA, 2009, p. 28). Los riesgos son evitados, según ISACA (2009), en los siguientes escenarios:

- No hay otra medida rentable que logre reducir la probabilidad o el impacto del riesgo por debajo de los límites establecidos según el apetito de riesgo.
- El riesgo no puede ser compartido o transferido a otras partes.
- La administración considera que el riesgo es inaceptable.

2.5.3.2.2. Reducción de riesgos / Mitigación

"La reducción significa, que medidas están tomadas para detectar el riesgo, seguido por la acción para reducir la frecuencia y/o el impacto de un riesgo." (ISACA, 2009, p. 28). Para mitigar los riesgos, ISACA (2009) explica las dos estrategias más comunes:

- Fortalecer las prácticas de gestión de riesgos de TI, asegurando una madurez adecuada en la gestión de riesgos y la definición de procesos dentro del marco de TI.
- Introducir controles específicos que disminuyan la probabilidad de un evento adverso o el impacto empresarial si llegara a ocurrir. Este tema se explora más a fondo en el resto de la sección.

2.5.3.2.3. Riesgo compartido / Transferencia

"Compartir significa reducir la frecuencia de riesgo o impacto mediante la transferencia o distribución de una parte del riesgo." (ISACA, 2009, p. 28). Esta respuesta a riesgos se utiliza cuando existe otra parte implicada en el riesgo, por ejemplo, en la subcontratación o bien en la adquisición de seguros.

2.5.3.2.4. Aceptación del riesgo

Con respecto a este punto, ISACA (2009) refiere que la "Aceptación significa que no se tomen medidas relativas con un riesgo particular, y la pérdida es aceptada cuando y si se produce." (p. 28). A diferencia de ignorar el riesgo, aceptarlo significa que este ha sido identificado y que la administración ha decidido de manera deliberada asumirlo, lo cual requiere establecer claramente quién será responsable de afrontarlo.

Ahora bien, para seleccionar y priorizar la respuesta al riesgo, ISACA (2009) plantea cinco criterios clave para tener en cuenta en el proceso:

- **Costo de la respuesta:** evalúa el gasto necesario para implementar la respuesta al riesgo, como primas de seguro o costos de mitigación.
- **Importancia del riesgo gestionado:** considera la gravedad del riesgo en función de su probabilidad e impacto en el mapa de riesgos.
- **Capacidad organizacional:** mide si la organización tiene los recursos y habilidades necesarias para aplicar la respuesta.
- **Efectividad de la respuesta:** determina si la medida reduce eficazmente la probabilidad y el impacto de los riesgos.
- **Eficiencia de la respuesta:** compara los beneficios obtenidos con el costo, en relación con otras inversiones o respuestas posibles.

Una vez evaluados los criterios, según ISACA (2009) es necesario asignar una prioridad a estas respuestas a través de tres posibles opciones:

- **Triunfos rápidos:** respuestas que son muy eficientes y eficaces para manejar riesgos altos de forma rápida.
- **Caso de negocio efectuado:** respuestas más costosas y complejas para riesgos altos, pero eficaces y eficientes para riesgos menores.
- **Aplazamiento:** respuestas que resultan costosas y se aplican a riesgos menores, entonces se decide posponer la acción.

El proceso de respuesta a riesgos requiere una planificación meticulosa y la asignación de recursos adecuados, con un enfoque en equilibrar la exposición al riesgo con las capacidades financieras y operativas de la organización, lo que hace necesario adoptar un enfoque dinámico que se adapte a las circunstancias cambiantes y que esté alineado con la estrategia organizacional, asegurando que las decisiones tomadas sean conscientes y sostenibles a largo plazo.

2.6. Metodologías y Modelos de Gestión de Riesgos de TI

La gestión de riesgos no solo se apoya en marcos como COBIT 2019 y la ISO 31000, sino también en diversas metodologías y modelos que proporcionan una estructura coherente y estandarizada para abordar los riesgos de manera integral, los cuales llegan a ser esenciales para garantizar que la gestión de riesgos esté alineada con las mejores prácticas internacionales y con los objetivos estratégicos de la organización. A continuación, se explicarán algunos de los marcos y modelos más reconocidos en la gestión de riesgos en la industria.

2.6.1. OCTAVE

"OCTAVE establece un conjunto de herramientas, técnicas y métodos de información basado en los riesgos de seguridad de evaluación y planificación estratégica." (Vanegas, 2013, p. 60). Esta es una de las metodologías más reconocidas, la cual utiliza distintos métodos para el establecimiento de guías detalladas que ayuden a la evaluación y gestión de los riesgos en las empresas. Según Alemán (2015):

> "Octave evalúa los riesgos de seguridad de la información y propone un plan de mitigación de los mismos dentro de una organización" lo cual la convierte en una metodología robusta para evaluaciones específicas en la parte de seguridad informática de las organizaciones." (p. 75)

Dado lo anterior, Vanegas (2013) también mencionó que esta metodología consta de tres libros distintos en el que cada uno cuenta con un respectivo enfoque para así adaptarse a diversos tipos de organizaciones según las necesidades que presenten, desde pequeñas organizaciones hasta organizaciones multinacionales y con enfoques específicos en activos de información. La Figura 17 muestra la estructura utilizada por OCTAVE para la gestión de riesgos de TI.

Figura 17: Estructura de OCTAVE: principios, atributos y salidas

Nota: Recuperado de (Vanegas, 2013, p. 60)

El modelo OCTAVE, con su enfoque integral y estructurado, ofrece a las organizaciones una metodología robusta para la gestión de riesgos de seguridad de la información, adaptándose a diversas necesidades y contextos, aparte que la claridad y precisión con las que OCTAVE aborda la identificación y mitigación de riesgos lo convierten en una herramienta esencial en la protección de activos de información críticos.

2.6.2. MARGERIT 3.0

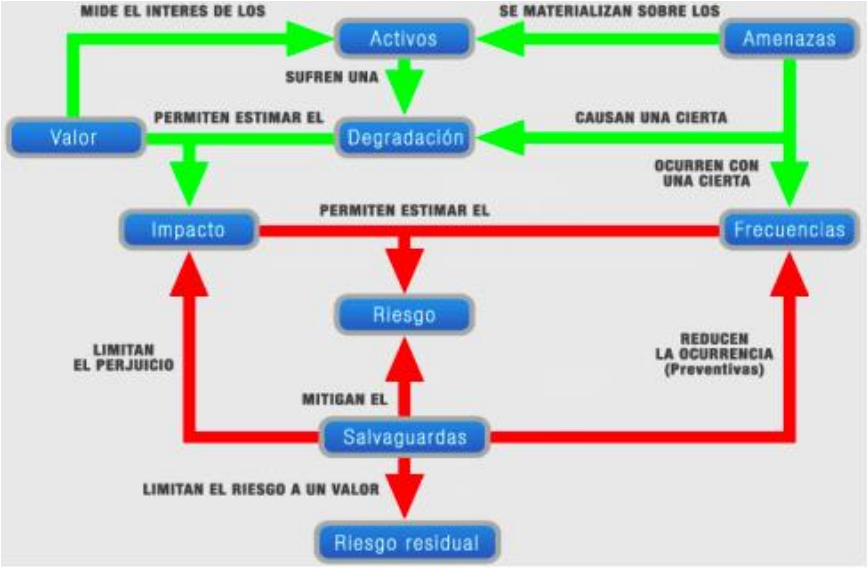
Según Vanegas (2013), en la metodología MARGERIT "El proceso de gestión de riesgos debe identificar y tratar de manera urgente los riesgos críticos, de modo que pueda tratar progresivamente los riesgos de menor prioridad." (p.57). Esta es una metodología que se alinea con la norma ISO 31000 en su proceso de gestión de riesgos, por lo que cuenta con actividades de planificación y seguimiento de los riesgos.

Del mismo modo, Alemán (2015) explicó lo siguiente sobre MARGERIT:

> Siguiendo la terminología de la norma ISO 31000, Estándar sobre principios y directrices para la gestión de riesgo, Magerit responde a lo que se denomina "Proceso de Gestión de los Riesgos", […], es decir, Magerit 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. (p. 76)

En la Figura 18 se presenta la estructura de esta metodología para una gestión efectiva de riesgos.

Figura 18: Estructura de MARGERIT



Nota: Recuperado de (Vanegas, 2013, p. 57)

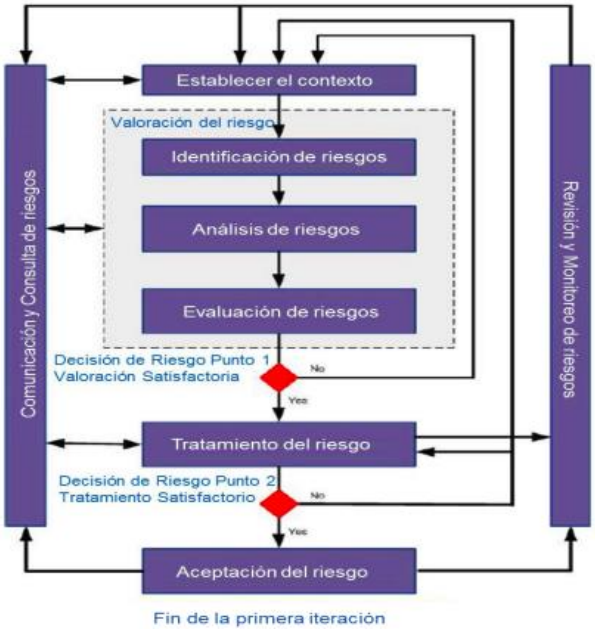
Esta metodología proporciona una estructura clara que permite a los órganos de gobierno tomar decisiones informadas, considerando los riesgos asociados al uso de tecnologías de la información, ya que la capacidad de MARGERIT para integrar la gestión de riesgos en la toma de decisiones estratégicas refuerza su relevancia en entornos donde la tecnología desempeña un papel crucial.

2.6.3. ISO/IEC 27005

Según lo planteado por ESGinnova Group (2017) "La norma ISO 27005 contiene diferentes recomendaciones y directrices generales para la gestión de riesgo en Sistemas de Gestión de Seguridad de la Información.". Vanegas (2013) explicó que "esta norma no establece ningún método específico para la gestión de riesgos de seguridad de la información, depende de la organización definir su enfoque en la gestión de riesgos." (p. 50). En este contexto, la norma ISO/IEC 27005, en su versión más actualizada del 2022, soporta la aplicación de Sistemas de Gestión de Seguridad de la Información con un enfoque estandarizado y adaptable para la gestión de riesgos de seguridad de la información de acuerdo con las necesidades de cada tipo de organización.

En su estructura, la norma ISO/IEC 27005 se divide en once cláusulas que van desde el establecimiento del contexto de la gestión de riesgo en la empresa hasta la revisión y monitoreo continuo del mismo. La Figura 19 presenta la estructura de esta norma.

Figura 19: Estructura de la norma ISO/IEC: 27005



Nota: Recuperado de (Vanegas, 2013, p. 51)

La norma ISO/IEC 27005 se presenta como una herramienta clave para la gestión de riesgos en sistemas de gestión de seguridad de la información, ofreciendo un enfoque adaptable que se ajusta a las necesidades específicas de cada organización. A diferencia de la ISO 31000, que proporciona un marco más amplio y general para la gestión de riesgos en cualquier contexto organizacional, la ISO/IEC 27005 se enfoca específicamente en la seguridad de la información, integrando de manera más profunda los aspectos técnicos y operativos relevantes para esta área, aparte de destacar por su capacidad de adaptarse a las particularidades de la seguridad de la información, permitiendo un enfoque más detallado y específico.

2.7. Herramientas de Gestión de Procesos

En la gestión de riesgos, contar con herramientas adecuadas es fundamental desde la etapa de análisis de la situación actual de la empresa hasta el mantenimiento de la metodología utilizada, ya que las herramientas permiten a las organizaciones no solo detectar posibles amenazas, sino también tomar decisiones informadas y estratégicas para minimizar su impacto. A continuación, se explicarán algunas de las principales herramientas utilizadas en la gestión de riesgos que serán de importancia en el desarrollo del proyecto.

2.7.1. Modelado de Procesos

Antes de abordar el modelado de procesos, resulta fundamental entender qué se entiende por un proceso y su relevancia dentro de una organización. Un proceso se define como un "conjunto de las fases sucesivas de un fenómeno natural o de una operación artificial" (RAE, 2024). En el ámbito empresarial, según SYDLE (2024) los procesos consisten en un "conjunto de actividades

que están relacionadas, en la rutina de la empresa, con el objetivo de entregar algún valor a los clientes". Es por esto qué, comprender cómo se definen, gestionan y optimizan los procesos es esencial para mejorar la eficacia operativa, la calidad de los productos o servicios, y la capacidad de la empresa para adaptarse a los cambios y desafíos del entorno.

Ahora bien, la RAE (2024) define el significado de modelo como "representación en pequeño de alguna cosa" y define modelar como "ajustarse a un modelo", por lo que, bajo estas definiciones es posible decir que el modelado implica la representación de un aspecto particular a través de un modelo específico. A partir de esto, según Vanner (2020) "el modelado de procesos es la representación gráfica de los procesos o flujos de trabajo de una empresa". Este modelado es posible lograrlo a través de la gestión de procesos de negocio cuyas siglas son BPM (*Business Process Management*), la cual, según Gartner (s.f) "es una disciplina que utiliza diversos métodos para descubrir, modelar, analizar, medir, mejorar y optimizar los procesos empresariales".

Dentro del BPM se tiene el BPMN, el cual, según Vanner (2020) consiste en una:

> Notación estándar de modelado de procesos de negocio, la cual permite a las organizaciones comunicar sus procedimientos de manera estándar mediante el uso de una representación visual universal y fácil de entender de los pasos dentro de un proceso empresarial. (párr. 5)

De este modo, se puede ver que esta etapa de BPM es crucial, ya que permite el entendimiento y mejora de los procesos al proporcionar un conocimiento preciso sobre la situación actual de los procesos de un negocio a través de una notación BPMN que representa de manera visual estos procesos de negocio.

2.7.1.1. Diagramas AS-IS

Una vez comprendida la importancia del modelado de procesos, es necesario introducir una herramienta fundamental para este análisis: los diagramas AS-IS. SYDLE (2023) explica que "el mapa de los procesos AS IS demuestra la situación actual y la realidad de los procesos organizacionales, con sus errores y aciertos.". Estos diagramas representan la situación actual de un proceso dentro de la organización, proporcionando una visión clara y detallada de cómo se están llevando a cabo las actividades en su estado actual.

Es importante saber que el proceso de modelado AS-IS comienza con la identificación de la situación actual del proceso, para así obtener una comprensión completa de lo que está pasando y, posteriormente, pasar a la fase de diagramación utilizando distintas herramientas para el modelado de los procesos, de tal manera que, una vez que el diagrama está completo, iniciar una etapa de validación para garantizar la calidad del modelado. Por este motivo y analizando este proceso se puede decir que diagramación AS-IS es una representación visual del estado de un

proceso en un momento determinado, la cual será herramienta clave para el desarrollo de este proyecto.

2.7.1.2. Diagramas TO-BE

Ahora bien, después de haber comprendido y diagramado el estado actual de los procesos a través de los diagramas AS-IS, el siguiente paso en el modelado de procesos es la creación de los diagramas TO-BE. Según SYDLE (2023) “hacer un mapa de procesos TO BE, por otro lado, está estipulando a dónde quieres llegar al final de la evolución del proceso. El mapa debe estar alineado con la planificación estratégica de la organización en su conjunto.”. Esto nos dice que los diagramas TO-BE se centran en la representación del estado futuro deseado de los procesos, es decir, cómo deberían funcionar idealmente una vez implementadas las mejoras y optimizaciones necesarias, aparte que permiten visualizar el proceso optimizado, facilitando la planificación de los cambios y asegurando que las mejoras propuestas estén alineadas con los objetivos estratégicos de la organización.

2.7.2. Estandarización de Procesos

Antes de profundizar en la estandarización de procesos, es esencial entender qué implica el concepto de "estandarizar". Según la RAE (s.f) estandarizar se refiere a “Ajustar (algo o a alguien) a un estándar o patrón”, entonces, si el término para estandarizar implica acoplarse a un patrón, y se une a la definición de proceso que se estudió en el punto anterior, la estandarización de un proceso se enlaza a la idea de un ajuste de ese proceso a un molde estándar. Según SYDLE (2021) “La estandarización de procesos es el ajuste de las etapas de los procesos dentro de una empresa para que éstos se asemejen a un modelo en común.”. Esto quiere decir que consiste en el establecimiento de normas o patrones que aseguren la uniformidad y coherencia en la realización de actividades o en la implementación de prácticas dentro de una organización.

Entonces, al estandarizar un proceso se busca que se garantice que las operaciones se lleven a cabo de manera consistente, minimizando variaciones y mejorando la eficiencia y la calidad, ya que se obtiene una guía estándar que determina la serie de pasos a seguir, de tal forma que, sin importar las variaciones en la organización, este camino sea el mismo. Según SYDLE (2021), con la estandarización de procesos se busca que se sea capaz de responder a las siguientes preguntas:

- ¿Cuál es el objetivo del proceso?
- ¿Dónde comienza y dónde termina?
- ¿Qué empleados son responsables de cada etapa de ejecución?
- ¿Existe un flujo de trabajo previamente definido?
- ¿Cuáles son las secuencias de ejecución?
- ¿Qué resultados deben entregarse al final y cuál es el plazo de finalización?

Al contar con la capacidad de responder preguntas clave sobre el propósito de un proceso en particular, la responsabilidad, el flujo de trabajo, la secuencia de ejecución y los resultados esperados, la estandarización de procesos proporciona una estructura sólida que contribuye a la mejora continua y a la optimización del rendimiento organizacional. Al comprender el valor de la estandarización, se puede apreciar mejor su aplicación en la gestión de procesos, lo que contribuye a alcanzar un desempeño óptimo y alineado con los objetivos organizacionales.

2.7.3. Análisis de Brechas

Para comprender el significado de lo que es un análisis de brechas, es importante comprender primero lo que es analizar y lo que son las brechas, así, al hablar de análisis se hace referencia, por un lado, a la "distinción y separación de las partes de algo para conocer su composición" (RAE, s.f). Por otro lado, a la "diferencia o distancia entre situaciones, cosas o grupos de personas, especialmente por la falta de unión o cohesión" lo que según la RAE (s.f) define lo que es una brecha

Ahora bien, según lo que mencionó Delta Protect (2023):

> El análisis GAP o análisis de brechas (del inglés gap analysis) consiste en una evaluación del desempeño real de una empresa, con la cual se busca contrastar el punto en que se encuentra y el punto al que quiere llegar en su desarrollo y crecimiento como organización.(párr.3)

Tomando en cuenta lo que explicó Delta Protect, el análisis de brechas es una herramienta clave que permite identificar las diferencias entre la situación actual de una organización y sus objetivos futuros, permitiendo una detección de las áreas donde existen discrepancias o carencias a través de la identificación de los puntos fuertes y débiles de la empresa, lo que facilita la toma de decisiones informadas para cerrar esas brechas y alcanzar los resultados deseados.

No obstante, para realizar un análisis de brechas, según Delta Protect (2023), es necesario comenzar con la definición de las áreas clave de enfoque, según el proceso a evaluar para las metas en estas áreas, de tal manera que se facilite el seguimiento del progreso. Una vez establecidos estos criterios se evalúa la situación actual del negocio para entender las diferencias entre el estado actual y las metas propuestas y se identifican las brechas para así entender su origen y elaborar un plan de acción que ayude al alcance de esas metas de manera efectiva.

Este análisis no solo ayuda a diagnosticar las áreas donde existen debilidades, sino que también proporciona una hoja de ruta clara para cerrar esas brechas y avanzar hacia las metas establecidas, aparte que, al entender y abordar las brechas, las empresas tienen la posibilidad de tomar decisiones más informadas y estratégicas, lo que les permite mejorar su desempeño y alcanzar un desarrollo más coherente y alineado con sus objetivos a largo plazo.

Una vez analizados y comprendidos los conceptos relevantes que sustentan la gestión de riesgos de TI y su aplicación dentro de las organizaciones, se procederá en el siguiente capítulo a detallar el marco metodológico del proyecto, el cual abordará los aspectos técnicos clave que se utilizaron para llevar a cabo el proyecto, asegurando su alineación con las mejores prácticas de la industria y las necesidades específicas de la empresa.

3. Marco Metodológico

Para iniciar la formulación del marco metodológico se debe recurrir a diversos expertos como Azuero (2019) quien mencionó que:

> La formulación del marco metodológico es permitir, descubrir los supuestos del estudio para reconstruir datos, a partir de conceptos teóricos habitualmente operacionalizados. Significa detallar cada aspecto seleccionado para desarrollar dentro del proyecto de investigación que debe ser justificado por el investigador. (p. 110)

De modo que, con lo expuesto, este capítulo muestra el marco metodológico a utilizar en el trabajo final de graduación, detallando elementos como el diseño y tipo de estudio, las metodologías aplicadas, las fuentes y los sujetos involucrados, así como los instrumentos y técnicas empleadas para la recolección de datos.

3.1. Tipo de Investigación

Con respecto al tipo de investigación Esteban Nieto (2018) afirmó que:

> Hay diferentes tipos de investigación, en la cual muchos investigadores tienen su punto de vista, Gay 1996, Rodríguez 1986, Piscoya 1982, Ñaupas y otros 2013, distinguen dos tipos: la investigación básica pura o fundamental (...) y concluimos sobre la investigación aplicada o tecnológica (Ñaupas et. al, 2013) que tiene una importancia trascendental en estos últimos tiempos. (p. 1)

Asimismo, y siguiendo las ideas de Esteban Nieto (2018), se define que la investigación aplicada:

> Está orientada a resolver los problemas que se presentan en los procesos de producción, distribución, circulación, y consumo de bienes y servicios de cualquier actividad humana. Se denomina aplicadas; porque con base en la investigación básica, pura o fundamental en las ciencias fácticas o formales se formulan problemas o hipótesis de trabajo para resolver los problemas de la vida productiva de la sociedad. (p. 3)

Dada la explicación anterior, el tipo de investigación aplicada fue el ideal para este proyecto debido a su enfoque directo en la aplicación práctica de conocimientos teóricos para resolver problemas específicos y mejorar procesos existentes en el campo de la gestión de TI y riesgos, y, por la naturaleza del proyecto, este no solo se apoya en una estructura teórica sólida, sino que apunta a ofrecer soluciones concretas y directamente implementables que tienen un impacto real y medible en las prácticas de TI.

3.2. Enfoque de investigación.

Siguiendo lo mencionado por Hernández-Sampieri, R., & Mendoza, C. (2020) sobre la investigación se llega a la afirmación que:

> La investigación científica se concibe como un conjunto de procesos sistemáticos y empíricos que se aplican al estudio de un fenómeno; es dinámica, cambiante y evolutiva. Se puede manifestar de tres formas o seguir tres rutas: cuantitativa, cualitativa y mixta. (p. xxxiii)

Dada esta perspectiva, existen diversos tipos de enfoque de investigación, y la elección de uno o de otro depende del investigador. El objetivo es explorar áreas desconocidas dentro de un tema específico.

De este modo, Hernández-Sampieri, R., & Mendoza, C. (2020) explicaron que “La ruta cuantitativa es apropiada cuando queremos estimar las magnitudes u ocurrencia de los fenómenos y probar hipótesis.” (p. 7). Con esta ruta el investigador busca una mayor objetividad sobre el proceso y sus resultados a través del seguimiento de patrones estructurados, obteniendo los resultados a través de métodos críticos y la búsqueda de relaciones entre los fenómenos que brinden resultados válidos y confiables a través de las estadísticas numéricas.

Así también, Hernández-Sampieri, R., & Mendoza, C. (2020) mencionaron el enfoque mixto el cual afirma que:

> Los métodos mixtos o híbridos representan un conjunto de procesos sistemáticos, empíricos y críticos de investigación e implican la recolección y el análisis de datos tanto cuantitativos como cualitativos, así como su integración y discusión conjunta, para realizar inferencias producto de toda la información recabada (denominadas metainferencias) y lograr un mayor entendimiento del fenómeno bajo estudio (p. 10).

Con respecto al enfoque mixto Hernández-Sampieri, R., & Mendoza, C explicaron que no es únicamente realizar una combinación entre un enfoque cualitativo y mixto, si no que este es la integración sistemática de datos de tipo cualitativos y de tipo cuantitativos de tal forma que se

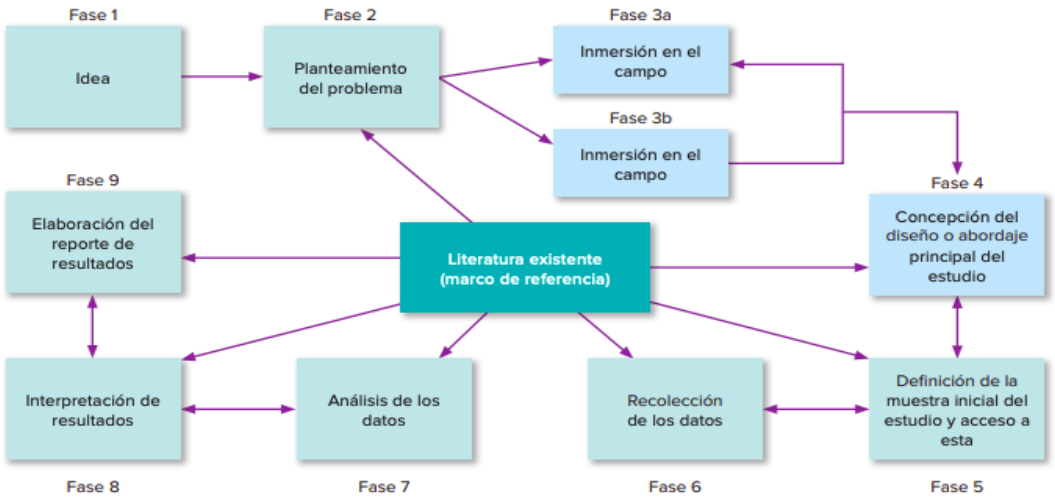
obtenga una perspectiva completa del fenómeno a analizar, conservando las estructuras de ambas rutas o bien adaptándolas a las necesidades de la investigación.

Ahora bien, Hernández-Sampieri, R., & Mendoza, C. (2020) afirmaron que:

> Con el enfoque cualitativo también se estudian fenómenos de manera sistemática. Sin embargo, en lugar de comenzar con una teoría y luego "voltear" al mundo empírico para confirmar si esta es apoyada por los datos y resultados, el investigador comienza el proceso examinando los hechos en sí y revisando los estudios previos, ambas acciones de manera simultánea, a fin de generar una teoría que sea consistente con lo que está observando qué ocurre. (pág. 7)

Dado lo anterior fue posible inferir que el enfoque cualitativo es eficaz para investigar fenómenos organizacionales, ya que comienza la investigación sin teorías preestablecidas, permitiendo a los investigadores observar y adaptar sus teorías a los datos reales. La Figura 20 representa una aproximación al proceso que utiliza una investigación con enfoque cualitativo.

Figura 20: Proceso de investigación cualitativa



Nota: Recuperado de Hernández-Sampieri, R., & Mendoza, C. (2020)

En la ruta cualitativa, aunque obviamente se efectúa una revisión inicial de la literatura, esta puede complementarse en cualquier etapa del estudio y apoyar desde el planteamiento del problema hasta la elaboración del reporte de resultados (la vinculación entre la teoría y las etapas del proceso se representa mediante flechas). (Hernández-Sampieri, R., & Mendoza, C., 2020).

Algunas de las características del enfoque cualitativo presentadas por Hernández-Sampieri, R., & Mendoza, C. (2020) son las siguientes:

- El investigador plantea un problema, pero no sigue un proceso preestablecido con claridad.
- El proceso de indagación resulta más flexible y se desplaza entre la experiencia, la acción y los resultados, por una parte; y el desarrollo de la teoría, por la otra. Su propósito es "reconstruir" la realidad, tal como la observan los actores de un sistema social definido previamente.
- En la mayoría de los estudios cualitativos no se prueban hipótesis, sino que se generan durante el proceso y van refinándose conforme se recaban más datos; son un resultado del estudio.
- La investigación cualitativa resulta interpretativa pues pretende encontrar sentido a los fenómenos y hechos en función de los significados que las personas les otorguen.
- El enfoque se basa en métodos de recolección de datos no estandarizados al inicio ni completamente predeterminados.

Para este estudio, se optó por un enfoque de investigación cualitativo, ya que permite evaluar los componentes de la organización, identificar problemas y desarrollar soluciones adecuadas a estas dificultades, aparte de que, para efectos de este trabajo, fue necesaria una evaluación de los aspectos existentes en el entorno organizacional, por ende, se construyó una solución de acuerdo con los objetivos y contexto actual de la empresa Information Evolution Costa Rica.

3.2.1. Diseño de Investigación

Sin importar cuál haya sido el método o enfoque elegido, se requiere un enfoque de diseño que se adapte a lo realizado en la investigación. Para efectos de este proyecto se hizo uso de un enfoque de investigación de tipo cualitativa, por ende, en la Tabla 2, se definieron los tipos de investigación cualitativa existentes.

Tabla 2: Tipos de diseños de investigación cualitativa

Diseño	Información proporcionada	Pregunta de investigación
Teoría fundamentada	Categorías del proceso o fenómeno y sus vínculos. Teoría que explica el proceso o fenómeno (problema de investigación).	Preguntas sobre procesos y relaciones entre conceptos que conforman un fenómeno.
Etnográfico	Descripción y explicación de los elementos y categorías que integran al sistema social: historia y evolución, estructura (social, política, económica, entre otros.), interacciones, lenguaje, reglas y normas, patrones de conducta, mitos y ritos.	Preguntas sobre las características, estructura y funcionamiento de un sistema social (grupo, organización, comunidad, subcultura, cultura), desde una familia, hermandad o hinchada hasta una megaciudad.

Diseño	Información proporcionada	Pregunta de investigación
Narrativo	Historias sobre procesos, hechos, eventos y experiencias, siguiendo una línea de tiempo, ensambladas en una narrativa general. Categorías relacionadas con tales historias y narrativa.	Preguntas orientadas a comprender una sucesión de eventos, a través de las historias o narrativas de quienes la vivieron (experiencias de vida bajo una secuencia cronológica). Eventos como una catástrofe, una elección, la biografía de un individuo, entre otros.
Fenomenológico	Experiencias comunes y distintas. Categorías que se presentan frecuentemente en las experiencias.	Preguntas sobre la esencia de las experiencias: lo que varias personas experimentan en común respecto a un fenómeno o proceso.
Investigación / acción	Preguntas sobre problemáticas o situaciones de un grupo o comunidad (incluyendo cambios).	Diagnóstico de problemáticas sociales, políticas, laborales, económicas, entre otros., de naturaleza colectiva. Categorías sobre las causas y consecuencias de las problemáticas y sus soluciones.

Nota: Adaptado de Preguntas de investigación cualitativas, diseños cualitativos e información que se obtiene al implementarlos. (pág. 525), por Hernández-Sampieri, R., & Mendoza, C. (2020)

Ahora bien, como se analizó en la Tabla 2, el diseño de Investigación/acción se centra en el diagnóstico de problemáticas de distintos tipos, entre estas laborales y las categorías sobre las causas y consecuencias de las problemáticas, así como sus soluciones, por lo tanto, para efectos de este proyecto, el diseño de investigación seleccionado fue el de Investigación/acción dado que la propuesta pretende resolver una problemática identificada en la empresa Information Evolution Costa Rica a partir de las buenas prácticas y marcos de referencia acordes a la solución, que sean de ayuda para la toma de decisiones y gestión de los riesgos que se puedan presentar.

Hernández-Sampieri, R., & Mendoza, C. (2020), en colaboración con distintos autores de literatura, plantearon que el diseño de Investigación/acción consta de cuatro fases para lograr un proceso completo.

1. Detectar el problema de investigación, clarificarlo y diagnosticarlo (ya sea una problemática social, la necesidad de un cambio, una mejora, entre otros).
2. Formulación de un plan o programa para resolver la problemática implicada o introducir el cambio.
3. Implementar el plan o programa y evaluar resultados.
4. Realimentación, la cual conduce a un nuevo diagnóstico y a una nueva espiral de reflexión y acción.

Sin embargo, dado el alcance del proyecto y la razón de ser de este, al tratarse de una propuesta metodológica para la gestión de riesgos de TI, únicamente se completaron las dos primeras fases del proceso explicado.

3.3. Fuentes de datos e Información

A continuación, se detallan las fuentes de información relevantes para la elaboración del proyecto, estas se clasificaron en fuentes de información primarias y fuentes de información secundarias.

3.3.1. Fuentes Primarias

Según lo expuesto por Guzmán Stein (1982) "Las fuentes primarias, como la palabra expresa, son aquellas en donde los datos o la información provienen de una fuente directa, sea una persona, institución y otro medio.", por lo tanto, entendemos como fuentes primarias aquellas que ofrecen datos originales, testimonios directos o documentos oficiales y no han sido modificados o interpretados por terceros. En la Tabla 3 se presentan las fuentes primarias a utilizar en la elaboración del proyecto.

Tabla 3: Fuentes primarias

Fuente	Importancia
COBIT 2019	Al ser un marco internacional que proporciona principios y prácticas para la gestión efectiva de la gobernanza y las TI, su aplicación en el proyecto ayudará a establecer un enfoque estructurado y bien definido para la gestión de riesgos de TI, asegurando que las TI soporten y extiendan los objetivos organizacionales de la empresa.
Norma INTE/ISO 31000	Al ser una norma internacional que proporciona directrices sobre los principios de gestión de riesgos y su implementación, es esencial para establecer una metodología de gestión de riesgos que sea sistemática, transparente y confiable.
Norma ISO/IEC 19510	Al ser una norma internacional que específica los estándares para modelar procesos de negocio utilizando BPMN, es crucial para la documentación y visualización de procesos en la organización.
Libros sobre metodología de la investigación	Son esenciales para diseñar el proyecto de manera efectiva, asegurando que la metodología propuesta esté bien fundamentada y organizada, siguiendo estándares académicos y profesionales rigurosos.
Personal de la empresa	Es crucial por su conocimiento experto de los procesos actuales, validando datos y asegurando la aplicabilidad de las soluciones propuestas, lo que facilita la identificación de brechas y la aceptación de nuevas prácticas.
Documentación	La documentación interna ofrece una base objetiva y detallada, permitiendo una

Fuente	Importancia
de la empresa	evaluación precisa y fundamentada de mejoras, al compararla con las mejores prácticas de la industria.

Nota: Elaboración Propia

3.3.2. Fuentes Secundarias

Según lo investigado por Guzmán Stein (1982) “Las fuentes secundarias por otra parte, permiten conocer hechos o fenómenos a partir de documentos o datos recopilados por otros.”, por ende, se entienden como fuentes secundarias aquellas que analizan, interpretan o critican fuentes primarias y son esenciales para proporcionar contexto, análisis previos y teorías existentes. En la Tabla 4 se presentan las fuentes secundarias a utilizar en la elaboración del proyecto.

Tabla 4: Fuentes secundarias

Fuente	Importancia
Publicaciones académicas sobre gestión del riesgo de TI y definición de procesos.	Las investigaciones y trabajos académicos proporcionan una guía y actualizaciones sobre las mejores prácticas y tendencias en la gestión de riesgos de TI y la definición de procesos.
Sistema de Bibliotecas del Instituto Tecnológico de Costa Rica.	SIBITEC ofrece acceso a una amplia colección de recursos académicos y profesionales que incluyen libros, revistas especializadas, tesis y artículos, que son vitales para el soporte teórico del proyecto.
Libros y revistas.	Aportan una base teórica sólida y ofrecen ejemplos de estudios de caso, análisis de tendencias y técnicas de gestión de riesgos y definición de procesos que brindan la posibilidad de adaptarse y aplicarse en el contexto específico del proyecto.
Páginas de internet y blogs.	Sirven de base para obtener información actualizada y opiniones sobre las prácticas contemporáneas en gestión de riesgos de TI y desarrollos en marcos como COBIT 2019.

Nota: Elaboración Propia

3.4. Sujetos de Investigación

Como parte del proceso investigativo del proyecto, fue necesaria la participación de diversos colaboradores de la empresa Information Evolution Costa Rica para el proceso de recolección y aceptación tanto de la información como de la propuesta metodológica final, así que, en la Tabla 5 se especificaron los sujetos de investigación relevantes para el desarrollo del proyecto.

Tabla 5: Sujetos de Investigación

Rol	Años de experiencia	Caracterización del sujeto	Justificación
Gerente general de la empresa	20 años	La dirección estratégica de la empresa guía la planificación a largo plazo y toma de decisiones clave, mientras se enfoca en gestionar eficazmente las relaciones con los clientes y supervisar las operaciones diarias para asegurar eficiencia y calidad.	Este sujeto brindó apoyo de recursos empresariales y de una gestión eficaz de los aspectos administrativos, aparte del juicio de expertos, que evaluó y aportó perspectivas críticas sobre información clave de la empresa. Además, funcionó como evaluador para asegurar que todas las actividades cumplieran con los intereses y objetivos de la empresa
Administrador del departamento de TI	6 meses	La administración de TI abarca el desarrollo e implementación de políticas específicas que guían el uso y la seguridad de la tecnología en la empresa para asegurar su funcionamiento óptimo y la prevención de fallos.	Como contacto directo en la empresa, el administrador de TI jugó un papel importante en la aprobación de la propuesta y en la evaluación de las prácticas actuales para identificar áreas de mejora. Además, brindó apoyo con información de TI esencial para el desarrollo del proyecto y supervisó continuamente el avance de la propuesta, asegurando su alineación con los objetivos establecidos.
Líder de operaciones	4 años	El líder de operaciones supervisa y coordina las actividades operativas diarias, asegurando que los procesos se ejecuten de manera eficiente y alineados con los objetivos estratégicos de la organización, mejorando continuamente los procesos y resolviendo problemas operativos.	El líder de operaciones garantizó que las mejoras se integraran adecuadamente en las operaciones diarias. Su conocimiento de los procesos operativos le permitió identificar y resolver obstáculos, asegurando que las actividades mantuvieran la eficiencia y contribuyeran al cumplimiento de los objetivos estratégicos de la empresa.

Nota: Elaboración Propia

3.5. Variables de la Investigación

Según lo expuesto por Hernández-Sampieri, R., & Mendoza, C. (2020) "Las variables de la investigación son las propiedades medidas y que forman parte de las hipótesis o simplemente que se pretenden explorar o describir" (p. 319)

Las variables de la investigación se obtuvieron a través de los objetivos específicos planteados en el proyecto, por ende, definieron qué medir para el cumplimiento de estos. En la Tabla 6 se definieron las variables que afectan a la investigación, su tipo, los indicadores y el detalle de cada una.

Tabla 6: Variables de investigación por objetivo específico

Objetivo específico: Analizar la situación actual de las prácticas de gestión de riesgos de TI utilizadas por Information Evolution Costa Rica, identificando las fortalezas y debilidades, para la detección de las brechas presentes en la empresa.			
Variable	**Definición Conceptual**	**Indicador**	**Definición Instrumental**
Situación actual de las prácticas de gestión de riesgos de TI.	Estado actual de los métodos y procedimientos utilizados por Information Evolution Costa Rica para gestionar los riesgos de TI.	Descripción de los métodos y procedimientos actuales.	Revisión documental, entrevistas semiestructuradas y notación BPMN
Fortalezas y debilidades en las prácticas actuales.	Aspectos positivos y negativos, o bien, aspectos eficientes e ineficientes de las prácticas actuales de gestión de riesgos de TI de la empresa.	Listado de fortalezas y debilidades encontradas.	Revisión de documental de los procesos, entrevista y Análisis FODA.
Brechas de los procesos de gestión de riesgos.	Diferencias entre los procesos actuales de gestión de riesgos de TI y el proceso estandarizado de gestión de riesgos de TI.	Listado de brechas entre la situación actual y la situación esperada	Revisión documental y grupo focal

Objetivo específico: Comparar las mejores prácticas de la industria de gestión de riesgos de TI, para la selección de aquellas que mejor se adapten a las necesidades de gestión de riesgos de Information Evolution Costa Rica.			
Variable	**Definición Conceptual**	**Indicador**	**Definición Instrumental**
Mejores prácticas en la gestión de riesgos de TI	Metodologías reconocidas que optimizan la identificación, evaluación y mitigación de riesgos en tecnología de información, alineadas con estándares internacionales.	Tabla comparativa de mejores prácticas de gestión de riesgos de TI	Revisión documental y Análisis comparativo
Mejores prácticas de la industria seleccionadas.	Metodologías reconocidas que cumplen en un mayor grado las necesidades de la empresa y fueron elegidas para el desarrollo de la metodología.	Nivel de alineación de las mejores prácticas con las necesidades de la empresa	Lista de verificación.
Objetivo específico: Crear un conjunto de artefactos, para la instrumentalización y estandarización de la metodología estratégica de la gestión de riesgos de TI según el estado deseado del proceso.			
Variable	**Definición Conceptual**	**Indicador**	**Definición Instrumental**
Artefactos para la metodología	Herramientas y documentos clave que apoyen la implementación y seguimiento de la metodología de gestión de riesgos de TI.	Lista de artefactos desarrollados	Revisión documental y plantillas de artefactos.
Metodología de Gestión de Riesgos de TI	Enfoque estructurado que guía la identificación, evaluación, y mitigación de riesgos en tecnología de información	Cantidad de descripciones de las prácticas a realizar en cada fase de la gestión de riesgos de TI	Revisión documental, notación BPMN y hoja de ruta de implementación.
Estandarización de la metodología	Proceso de unificar y formalizar el proceso de la gestión de riesgos de TI para garantizar que las actividades se realicen de manera consistente y eficiente.	Nivel de estandarización del proceso según las mejores prácticas de la industria. Nivel de capacidad del proceso.	Lista de verificación para garantizar que todas las actividades estén cubiertas. Lista de verificación para el nivel de capacidad del proceso

Nota: Elaboración Propia

3.6. Técnicas de Instrumentos de Recolección de Datos

Según lo expuesto por Hernández-Sampieri & Mendoza (2020) la técnica de instrumentos de recolección de datos en la ruta de investigación cualitativa consiste en el investigador como tal, haciendo uso de diversas herramientas como las entrevistas, la observación y las sesiones grupales.

Para efectos del desarrollo de este Trabajo Final de Graduación y el desarrollo de la propuesta de metodología para la gestión de riesgos de TI, se empleó una serie de métodos recomendados en la literatura para la recolección de datos cualitativos. En esta sección, se detallaron estos métodos, para proporcionar una visión general y comprensiva de cada uno.

Cabe mencionar que, para la creación de las herramientas de recolección de datos y la documentación del Trabajo Final de Graduación, se utilizaron las aplicaciones de Microsoft Office 365, y, en caso de utilizar cuestionarios con los participantes, se optó por un gestor de encuestas digitales como lo es Google Forms o algunas de las herramientas gratuitas existentes.

En la Tabla 7, se exponen las técnicas de recolección de datos utilizadas durante el desarrollo del Trabajo Final de Graduación, por lo cual se presenta el nombre de la técnica, su definición y la importancia que tienen en el desarrollo del presente proyecto.

Tabla 7: Técnicas de instrumentos de recolección de datos

Técnica	Definición Conceptual	Importancia en el Proyecto
Revisión documental	Consiste en un procedimiento para la recopilación de datos de la realidad utilizando los sentidos en un contexto real. (Hernández-Sampieri, R., & Mendoza, C., 2020)	La observación documental fue crucial para recopilar información detallada y precisa sobre los procesos y políticas actuales de gestión de riesgos de TI de la empresa, permitiendo revisar la documentación existente. Se utilizó para obtener una comprensión profunda de la documentación existente, lo que fue fundamental para identificar las brechas y áreas de mejora en la gestión de riesgos. En el Apéndice E se encuentra la plantilla utilizada para la Revisión Documental
Entrevista	Consiste en una reunión para conversar e intercambiar información entre una persona (el entrevistador) y otra (el entrevistado) u otras (entrevistados). (Hernández-Sampieri, R., & Mendoza, C., 2020)	Las entrevistas proporcionaron información valiosa y detallada directamente de los involucrados en la gestión de riesgos de TI. Estas entrevistas permitieron obtener perspectivas cualitativas sobre las prácticas actuales, desafíos y necesidades específicas, ayudando a construir una metodología que se adapte a las realidades operativas de la empresa. En el Apéndice C se encuentra la plantilla utilizada para las entrevistas realizadas.

Técnica	Definición Conceptual	Importancia en el Proyecto
Grupos Focales	Consisten en reuniones de grupos pequeños o medianos en las cuales los participantes conversan a profundidad en torno a uno o varios temas en un ambiente relajado e informal bajo la conducción de un especialista. (Hernández-Sampieri, R., & Mendoza, C., 2020)	Los grupos focales fueron esenciales para generar discusión y obtener diferentes puntos de vista sobre la gestión de riesgos de TI, reuniendo al equipo de TI, el gerente general, y otros posibles involucrados. Se utilizó para identificar colectivamente oportunidades de mejora y validar las propuestas de la nueva metodología, asegurando que las soluciones sean prácticas y aceptadas por todos los implicados. En el Apéndice F se encuentra la plantilla utilizada para la elaboración de grupos focales.
Análisis Comparativo	Es una técnica para examinar las diferencias y similitudes entre casos, procesos o fenómenos, que busca identificar patrones o excepciones. (Tilly, 1991)	El análisis comparativo fue crucial para el proyecto, ya que permitió evaluar y comparar las mejores prácticas de la industria entre ellas, identificando aquellas que se adaptaban mejor a las necesidades específicas de la empresa, lo que ayudó a seleccionar enfoques optimizados, garantizando que la metodología propuesta estuviera alineada con las tendencias y estándares más efectivos del sector. En el Apéndice G se encuentra la plantilla utilizada para la elaboración de cuestionarios.
Análisis FODA	Consiste en identificar las fortalezas y debilidades dentro de la organización, y por otro lado las oportunidades y amenazas en el contexto externo de la empresa. (Sarli et al., 2015)	El análisis FODA fue fundamental para identificar y analizar las fortalezas, debilidades, oportunidades y amenazas en la gestión de riesgos de la empresa, ya que proporcionó una visión clara de las áreas que ya funcionaban bien y aquellas que necesitaban mejoras, sirviendo como base para desarrollar estrategias que potencien los aspectos positivos y minimicen las debilidades de la gestión de riesgos actual. En el Apéndice I se encuentra la plantilla utilizada para la elaboración del análisis FODA.
Lista de verificación	Consisten en una serie de ítems o criterios que deben ser revisados y marcados para confirmar su cumplimiento o existencia. (Concha-Torre *et al.*, 2020)	La lista de verificación se utilizó para asegurar que se contara con todos los elementos necesarios en el proceso de gestión de riesgos y para medir el nivel de alineación con las mejores prácticas establecidas, garantizando precisión en la evaluación de la gestión de riesgos, asegurando que no se pasaran por alto aspectos críticos en el proceso. En el Apéndice H se encuentra la plantilla utilizada para la elaboración de listas de verificación.

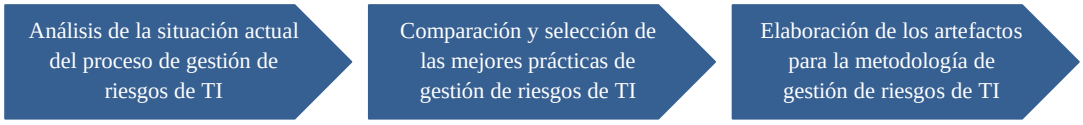
Técnica	Definición Conceptual	Importancia en el Proyecto
Notación BPMN	Es una notación gráfica estandarizada para representar la secuencia de actividades en los procesos de negocio de una organización. (SYDLE, 2022)	La notación BPMN fue utilizada para representar visualmente tanto el proceso actual de gestión de riesgos mediante diagramas AS-IS, como el proceso idealizado con diagramas TO-BE, facilitando la comprensión y comunicación de los procesos y permitiendo una comparación clara entre el estado actual y el estado deseado, y ayudando a identificar las áreas de cambio necesarias para mejorar la gestión de riesgos en la empresa.

Nota: Elaboración Propia

3.7. Procedimiento Metodológico de la Investigación

El presente proyecto consistió en la elaboración de una propuesta metodológica para la gestión de riesgos de TI para la empresa Information Evolution Costa Rica. El alcance se definió en tres fases, las cuales se presentan en la Figura 21 y se detallan más adelante.

Figura 21: Fases del proyecto



Nota: Elaboración propia

El contenido de esta metodología se estructuró en tres fases, en donde la primera fase se basó en la situación actual de la empresa, la segunda fase en las mejores prácticas de gestión de riesgos de TI de la industria y la tercera fase en los procesos complementarios propuestos por COBIT 2019 y la ISO 31000. El primer proceso, EDM03, abordó aspectos estratégicos relacionados con las políticas y lineamientos de la gestión de riesgos. El segundo proceso, APO12, se enfocó en la ejecución de las actividades correspondientes a la gestión de riesgos de TI, el cual, junto con la ISO 31000, logró un enfoque integral de gestión de riesgos de TI.

El desarrollo de las actividades definidas para cada fase permitió, de manera integral, la elaboración de la propuesta de una metodología para la gestión de riesgos de TI para su uso por parte del departamento de TI en la identificación, tratamiento y optimización de los riesgos presentados. Es importante recalcar que este proyecto no buscó implementar el ciclo de gestión de riesgos de TI o establecer la estrategia específica de gestión de riesgos de TI, sino que se trató de una propuesta que sirviera como guía para realizar dicho proceso de manera óptima, siguiendo las mejores prácticas de la industria referentes a la gestión de riesgos de TI.

3.7.1. Fase I: Análisis de la Situación Actual del Proceso de Gestión de Riesgos de TI

En la primera fase, se llevó a cabo un análisis del estado actual del proceso de gestión de riesgos de TI implementado por Information Evolution Costa Rica, el cual comenzó con la comprensión de los procedimientos y la arquitectura vigente. Se recopilaron y revisaron todos los documentos relevantes, incluidos manuales de procedimientos, políticas de seguridad y registros de incidentes. Además, se realizaron entrevistas estructuradas con los responsables y miembros clave del equipo de TI para comprender los procedimientos actuales y la arquitectura del proceso de gestión de riesgos de TI.

Posteriormente, se crearon diagramas AS-IS del proceso utilizando la notación BPMN. Se identificaron todos los subprocesos actuales relacionados con la gestión de riesgos de TI y se diseñaron diagramas que representaron visualmente estos subprocesos, proporcionando una vista clara y precisa de las operaciones.

Por último, se realizó el análisis de brechas y oportunidades de mejora, a través de la comparación de los procesos actuales con las mejores prácticas reconocidas en la industria para identificar diferencias y áreas de mejora. Se documentaron las brechas existentes entre los procesos actuales y las mejores prácticas, especificando las deficiencias y oportunidades de mejora. Además, se desarrollaron propuestas de acciones específicas para cerrar las brechas identificadas, enfocándose en la alineación con las mejores prácticas de la industria.

3.7.2. Fase II: Comparación y Selección de las Mejores Prácticas de Gestión de Riesgos de TI

En la segunda fase, se compararon algunas de las mejores prácticas de la industria de gestión de riesgos de TI para seleccionar aquellas que mejor se adaptaran a las necesidades de gestión de riesgos de Information Evolution Costa Rica. Para ello, se llevó a cabo la investigación de la literatura sobre las mejores prácticas en gestión de riesgos de TI, identificando las prácticas recomendadas por COBIT 19, ISO 31000 y otras normativas relevantes. Estas prácticas se compararon entre sí, examinando sus fortalezas y debilidades, lo que permitió una comprensión completa de las prácticas más efectivas y cómo podían beneficiar a la empresa.

Una vez comparadas las mejores prácticas entre ellas, se realizó un benchmarking, en el que se compararon las prácticas actuales de Information Evolution Costa Rica con las mejores prácticas seleccionadas de la industria. Este análisis incluyó una evaluación basada en criterios de efectividad, eficiencia y alineación con los objetivos estratégicos de la empresa. Se tomó en cuenta no solo los resultados actuales, sino también la capacidad de estas prácticas para adaptarse a las necesidades futuras de la empresa en un entorno de TI en constante cambio.

Por último, a partir de esta comparación entre las mejores prácticas y las necesidades actuales de gestión de riesgos de TI de la empresa, se seleccionaron las prácticas que mejor se adaptaron a las necesidades específicas de la empresa, garantizando una gestión de riesgos de TI más robusta y alineada con las mejores prácticas de la industria. Esto aseguró que la empresa adoptara un enfoque basado en evidencia, utilizando prácticas que no solo cumplieran con los estándares internacionales, sino que también se integraran de manera efectiva en su entorno operativo específico.

3.7.3. Fase III: Elaboración de los Artefactos para la Metodología de Gestión de Riesgos de TI

En la tercera fase, se llevó a cabo la elaboración de los artefactos que integraron la metodología de gestión de riesgos de TI, con el objetivo de desarrollar un enfoque integral y estructurado. Como primer punto, una vez finalizado el análisis de brechas de la situación actual y la selección de las mejores prácticas a utilizar, se procedió a realizar los diagramas TO-BE del proceso mejorado de Gestión de Riesgos de TI. De esta manera, se estableció una base sólida para la optimización de la gestión de riesgos de TI en la organización, asegurando que los procesos actuales fueran comprendidos y mejorados de manera continua y efectiva.

Ahora bien, para el desarrollo de la metodología se integraron tres pilares fundamentales: el proceso EDM03 de COBIT 2019, el proceso APO12 de COBIT 2019 y las directrices de la ISO 31000, para garantizar que todos los aspectos críticos de la gestión de riesgos fueran abordados de manera coherente y alineada con las mejores prácticas de la industria, tal como se muestra en la Figura 22.

Figura 22: Pilares para la metodología de gestión de riesgos de TI

Nota: Elaboración propia

Como primer punto de la tercera fase, se tomó como base el proceso EDM03 de COBIT 2019, denominado "Asegurar la optimización del Riesgo", que pertenece al dominio "Evaluar, Orientar y Supervisar" de los procesos de Gobierno de TI. El proceso EDM03 garantizó que los aspectos relevantes sobre los riesgos de TI, como el apetito y la tolerancia al riesgo, se comprendieran, articularan y comunicaran adecuadamente dentro de la organización. Además, aseguró que el

riesgo asociado al uso de tecnologías de información fuera identificado y gestionado correctamente.

Para esta fase, se abordaron las tres prácticas clave de Gobierno que COBIT 2019 sugiere para proponer este proceso, las cuales permitieron evaluar, orientar y monitorear constantemente la gestión de riesgos de TI. Estas prácticas se presentan en la Figura 23.

Figura 23: Prácticas clave de Gobierno del EDM03

Nota: Adaptado de COBIT 2019

El objetivo de aplicar estas prácticas clave de Gobierno contempladas en el EDM03 fue establecer una propuesta integral que delimitara las responsabilidades gerenciales en cuanto a la optimización de los riesgos críticos de TI.

Como segundo punto de la tercera fase, se tomó como base el proceso APO12 de COBIT 2019 junto con la ISO 31000. Con respecto al APO12, denominado "Gestionar el Riesgo", que pertenece al dominio "Alinear, Planificar y Organizar" dentro del área de procesos de Gestión de TI. Según COBIT 2019, el proceso APO12 consistió en identificar, evaluar y reducir los riesgos relacionados con la tecnología de información de manera continua y en consonancia con los niveles de tolerancia y las políticas establecidas por la dirección ejecutiva.

Para gestionar este proceso, COBIT 2019 sugiere seis prácticas clave de gestión que recopilar y analizar datos sobre riesgos, mantener un perfil actualizado de riesgos y definir acciones para responder adecuadamente a ellos. Estas prácticas se presentan en la Figura 24.

Figura 24: Prácticas de Gestión del APO12

Fuente: Adaptado de COBIT 2019

Ahora bien, con respecto a la ISO 31000, denominada “Gestión del riesgo”, se buscó crear una alineación con las prácticas del APO12 y de esta manera definir el ciclo de la gestión de riesgos de TI, utilizando la comunicación y consulta a través de todo el proceso.

Figura 25: Etapas del ciclo de gestión del riesgo

Nota: Adaptado de ISO 31000:2018

El objetivo de aplicar estas prácticas de Gestión, como las contempladas en el APO12, alineadas con las fases del ciclo de gestión del riesgo de la ISO 31000, fue desarrollar una propuesta completa que abordara los controles, plantillas y la matriz de gestión de riesgos de Tecnologías de la Información específicamente dirigidos al departamento de TI en su totalidad.

Ahora bien, para garantizar que la metodología de gestión de riesgos de TI pudiera ser implementada de manera efectiva en Information Evolution Costa Rica, se desarrolló una hoja de ruta como último artefacto. Esta hoja de ruta detalló los pasos específicos, los recursos necesarios y los plazos establecidos para poner en marcha la metodología, asegurando así una transición ordenada y controlada hacia un entorno de gestión de riesgos más robusto y alineado con las mejores prácticas de la industria.

Por último, se evalúa la estandarización y alineación del proceso propuesto con respecto a las mejores prácticas de la industria mediante la verificación de las directrices establecidas por dichas prácticas y el contenido desarrollado en la metodología, asegurando su cumplimiento y adaptabilidad al contexto empresarial. Además, se incluye la evaluación de la capacidad del proceso propuesto utilizando el Modelo de Madurez de la Capacidad (CMMI), lo cual permite medir el nivel de implementación alcanzado y las áreas de mejora necesarias para consolidar la gestión de riesgos de TI de manera efectiva y estandarizada.

3.8. Operacionalización de las Variables

De acuerdo con los objetivos específicos planteados en este trabajo, que se detallan a continuación:

- **OE 1:** Evaluar la situación actual de las prácticas de gestión de riesgos de TI utilizadas por Information Evolution Costa Rica, identificando las fortalezas y debilidades, para la detección de las brechas presentes en la empresa.

- **OE 2:** Comparar las mejores prácticas de la industria de gestión de riesgos de TI, para la selección de aquellas que mejor se adapten a las necesidades de gestión de riesgos de Information Evolution Costa Rica.

- **OE 3:** Crear un conjunto de artefactos, para la instrumentalización y estandarización de la metodología estratégica de la gestión de riesgos de TI según el estado deseado del proceso.

Y las fases para la elaboración del proyecto definidas anteriormente:

- **I:** Fase I: Análisis de la situación actual del proceso de gestión de riesgos de TI
- **II:** Fase II: Comparación y selección de las mejores prácticas de gestión de riesgos de TI
- **III:** Fase III: Elaboración de los artefactos para la metodología de gestión de riesgos de TI

En la Tabla 8, se describe la operacionalización de las variables de investigación correspondientes al presente Trabajo Final de Graduación.

Tabla 8: Tabla de operacionalización de las variables

Objetivo	Fase	Variable	Instrumentos	Sujetos de Investigación
OE 1	I	Situación actual de las prácticas de gestión de riesgos de TI.	- Revisión documental del proceso de gestión de riesgos (Apéndice E) - Entrevista semiestructurada (Apéndice C) - Notación BPMN	- Administrador de TI - Gerente general - Líder de operaciones
		Fortalezas y debilidades en las prácticas actuales.	- Revisión documental del proceso. (Apéndice E) - Entrevista semiestructurada (Apéndice C) - Análisis FODA (Apéndice I)	- Administrador de TI - Líder de operaciones
		Brechas de los procesos de gestión de riesgos.	- Revisión documental del proceso (Apéndice E) - Grupo focal (Apéndice F)	- Administrador de TI - Líder de operaciones
OE 2	II	Mejores prácticas en la gestión de riesgos de TI	- Revisión documental de las mejores prácticas de la industria - Análisis comparativo entre las mejores prácticas (Apéndice G)	Los instrumentos no se aplican a sujetos de información.
		Mejores prácticas de la industria seleccionadas	- Lista de verificación de las mejores prácticas y las necesidades de la empresa. (Apéndice H)	- Administrador de TI - Líder de operaciones
OE 3	III	Artefactos para la metodología	- Notación BPMN - Plantillas de los artefactos desarrollados - Revisión documental de las mejores prácticas	Los instrumentos no se aplican a sujetos de información.

Objetivo	Fase	Variable	Instrumentos	Sujetos de Investigación
		Metodología de Gestión de Riesgos de TI	- Revisión documental de las mejores prácticas - Hoja de ruta de implementación	Los instrumentos no se aplican a sujetos de información.
		Estandarización de la ejecución del proceso	- Lista de verificación para garantizar que todas las actividades estén cubiertas (Apéndice H) - Lista de verificación para el nivel de capacidad del proceso (Apéndice O)	- Administrador de TI - Líder de operaciones

Nota: Elaboración propia

3.9. Tabla Resumen del Procedimiento Metodológico

A continuación, en la Tabla 9, se presentan las fases del proyecto con el objetivo u objetivos que se atendieron en la fase y sus entregables correspondientes.

Tabla 9: Tabla resumen de las fases del proyecto

Fase	Objetivo	Actividades	Entregables
I	OE 1	- Comprensión detallada de los procedimientos y la arquitectura vigente - Diagramación AS-IS del proceso de gestión de riesgos de TI - Análisis FODA del proceso de gestión de riesgos de TI - Análisis de brechas existentes	- Informe de diagnóstico de la situación actual de la gestión de riesgos TI - Diagramas AS-IS del proceso de gestión de riesgos de TI - Análisis FODA de la gestión de riesgos TI - Análisis de Brechas del proceso de gestión de riesgos de TI

Fase	Objetivo	Actividades	Entregables
II	OE 2	- Identificación y comprensión de las mejores prácticas de gestión de riesgos - Análisis comparativo entre las mejores prácticas de la industria - Análisis comparativo entre las mejores prácticas y las prácticas de la empresa - Identificación de las mejores prácticas de acuerdo con las necesidades de la empresa	- Análisis comparativo de las mejores prácticas de la industria en la gestión de riesgos de TI - Selección de las mejores prácticas de la industria de acuerdo con las necesidades de la empresa
III	OE 3	- Comprensión del objetivo EDM03 de COBIT 2019 - Evaluación del apetito y tolerancia al riesgo - Propuesta de la metodología para las tres prácticas clave de Gobierno del EDM03 - Comprensión del objetivo APO12 de COBIT 2019 y la ISO 31000 - Identificación y evaluación de los riesgos de TI - Tratamiento de riesgos y mantenimiento de un perfil actualizado - Propuesta de sistema de seguimiento y revisión de los riesgos - Propuesta del ciclo de gestión de riesgos - Diagramación TO-BE del proceso de gestión de riesgos de TI mejorado - Propuesta de hoja de ruta para la implementación de la metodología - Aplicación de instrumento para determinar la estandarización y alineación del proceso con respecto a las mejores prácticas. - Definición del nivel de capacidad del proceso	Artefactos pertinentes al EDM03 - Evaluación del apetito del riesgo - Políticas de gestión de riesgos - Establecimiento de los mecanismos de monito Artefactos pertinentes al APO12 y a la ISO 31000 - Identificación de los riesgos. - Análisis de los riesgos. - Evaluación de los riesgos. - Tratamiento de los riesgos. - Estructura de la metodología de la gestión de riesgos de TI. - Diagramas TO-BE del proceso de gestión de riesgos de TI. - Hoja de ruta de implementación. - Documentación de la estandarización realizada del proceso de gestión de riesgos de TI. - Documentación del nivel de capacidad del proceso

Nota: Elaboración Propia

4. Análisis de Resultados

En la siguiente sección se presentan los resultados obtenidos de la ejecución de lo descrito en la sección 3.7, los cuales corresponden a la investigación previa de la propuesta metodológica de gestión de riesgos de TI propuesta para la empresa. Los resultados comprenden:

- Fase 1: Evaluación de la situación actual de las prácticas de gestión de riesgos de TI.
- Fase 2: Comparación y selección de las mejores prácticas de la industria en la gestión de riesgos de TI.
- Fase 3: Elaboración de los artefactos para la metodología de gestión de riesgos de TI.

Estos resultados, junto con los datos e información recopilados, constituyen un componente esencial para el logro de los objetivos establecidos en este trabajo final de graduación, sirviendo como base fundamental para la toma de decisiones y el desarrollo de mejoras en la gestión de riesgos dentro de la organización.

4.1. Fase I: Análisis de la Situación Actual del Proceso de Gestión de Riesgos de TI

En la Fase I del proyecto, se realiza la evaluación de la situación actual de las prácticas de gestión de riesgos de TI en Information Evolution Costa Rica. Esta fase incluye la revisión de la documentación existente y entrevistas con los principales actores involucrados en el proceso de gestión de riesgos, para así identificar las fortalezas, debilidades y brechas en las prácticas actuales, proporcionando una base sólida para la posterior comparación con las mejores prácticas de la industria. A continuación, se presentan los resultados de esta evaluación, destacando los puntos clave que impactan en la gestión de riesgos dentro de la organización.

4.1.1. Procedimiento Actual del Proceso de Gestión de Riesgos de TI de la Empresa.

Para el análisis de la situación actual se realizó una entrevista al encargado del departamento de TI, la cual se visualiza en el apéndice K. Las respuestas obtenidas en la entrevista sobre la situación actual del proceso de gestión de riesgos de TI en Information Evolution Costa Rica revela varias áreas críticas que requieren atención. En primer lugar, la empresa no cuenta con un enfoque proactivo para la identificación de riesgos; los riesgos se manejan sobre la marcha y solo se reconocen cuando ya se han convertido en incidentes, de tal forma que no existen estrategias de mitigación ni protocolos definidos para evaluar, monitorear o responder a los riesgos, lo cual evidencia una carencia significativa en la gestión estructurada de riesgos.

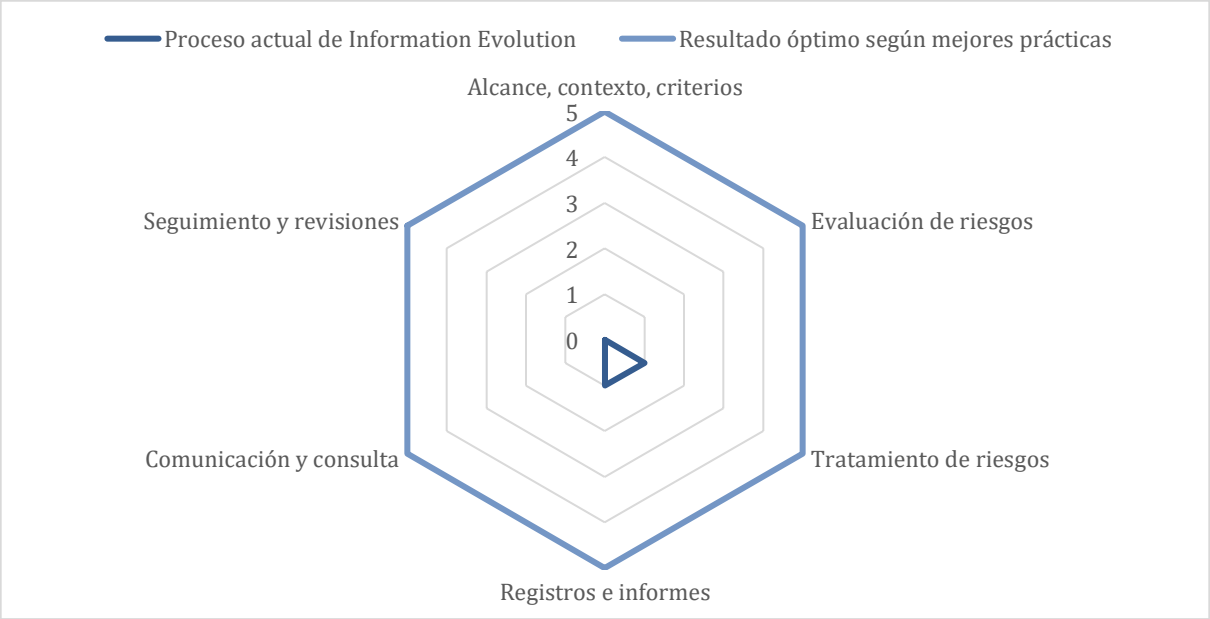
Las fortalezas actuales se limitan al manejo de inventario de activos, con un margen de seguridad del 3%, lo que ha permitido a la empresa mantener la producción sin retrasos significativos, incluso ante imprevistos. Sin embargo, la falta de procedimientos específicos y la documentación adecuada de los riesgos y las acciones tomadas han resultado en una gestión

reactiva y no preventiva, lo cual genera incertidumbre sobre cómo actuar ante diversas eventualidades.

En cuanto a las debilidades, destaca la ausencia de un protocolo formal para la gestión de riesgos y la inexistencia de un proceso claro y definido, lo que dificulta la creación de una cultura organizacional sólida en este aspecto. Las respuestas indican que la empresa carece de personal capacitado y de recursos específicos que faciliten la gestión de riesgos, lo cual es fundamental para mejorar en esta área.

Finalmente, se identificó una deficiencia cultura organizacional respecto a la gestión de riesgos de TI y resistencia al cambio por parte del personal según la entrevista realizada, lo que resalta la necesidad de capacitaciones y sensibilización sobre la importancia de gestionar los riesgos de manera estructurada y alineada con las mejores prácticas internacionales. En la Figura 26 se muestra las diferencias entre la situación actual de la empresa y un resultado óptimo de la empresa alineado a las mejores prácticas, especialmente las fases del ciclo de gestión de riesgos según la ISO 31000.

Figura 26: Diferencias entre las actividades sugeridas por las mejores prácticas de la industria y las actividades del proceso de Information Evolution



Nota: Elaboración Propia

El gráfico radial utiliza una escala del 0 al 5 en donde 5 es un resultado alineado de manera completa a un ciclo de gestión de riesgos según el uso de mejores prácticas de la industria y 0 un proceso inexistente por parte de la empresa en el rubro evaluado. A continuación, se explica a detalle la escala:

- **Nivel 0 - Inexistente:** no hay evidencia de que la actividad evaluada esté presente o implementada en la organización.
- **Nivel 1 - Inicial:** la actividad se encuentra en un estado muy básico, informal o reactivo.
- **Nivel 2 - Parcialmente implementado:** la actividad tiene elementos iniciales implementados, pero no se ejecuta de manera consistente o alineada con las mejores prácticas.
- **Nivel 3 - Moderadamente implementado:** existen procesos o actividades alineadas parcialmente con las mejores prácticas, pero aún presentan deficiencias en su alcance, formalización o integración dentro del ciclo de gestión de riesgos.
- **Nivel 4 - Implementado con limitaciones:** la actividad está alineada de manera significativa con las mejores prácticas, pero presenta áreas de mejora en aspectos específicos que limitan su efectividad o alcance.
- **Nivel 5 - Óptimo:** la actividad está completamente alineada con las mejores prácticas de la industria, implementada de forma sistemática y documentada.

Este gráfico evidencia claras discrepancias entre el proceso actual de gestión de riesgos de Information Evolution y las fases de un proceso de gestión de riesgos alineado con las mejores prácticas de la industria. La puntuación baja en las áreas de alcance, contexto, criterios, evaluación, seguimiento y revisiones, y comunicación y consulta sugiere que la empresa no está alineada con los estándares óptimos de la gestión de riesgos de TI y que, de hecho, no existe del todo un proceso definido para estas fases criterio. En el caso de la fase de registros e informes, la empresa presenta un 1 de puntuación, ya que se documenta un solo tipo de riesgos, sin embargo, este se documenta una vez materializado, por lo que únicamente cuentan con una base de conocimiento de la importancia de la documentación de riesgos. También, en la parte de tratamiento de riesgos, la empresa tiene una previsión extra de equipo en caso de riesgos por activos de TI, sin embargo, no cuentan con nada más.

Particularmente, el proceso de gestión de riesgos de TI actual presencia deficiencias significativas, indicando que los métodos y herramientas utilizadas actualmente no permiten una detección proactiva y un análisis exhaustivo de los riesgos, por lo que tampoco existen respuestas estandarizadas a riesgos. La inexistencia de un proceso formal y sistemático en la evaluación de riesgos también pone de manifiesto que Information Evolution opera de manera reactiva, lo que podría poner en peligro la estabilidad y seguridad de sus operaciones.

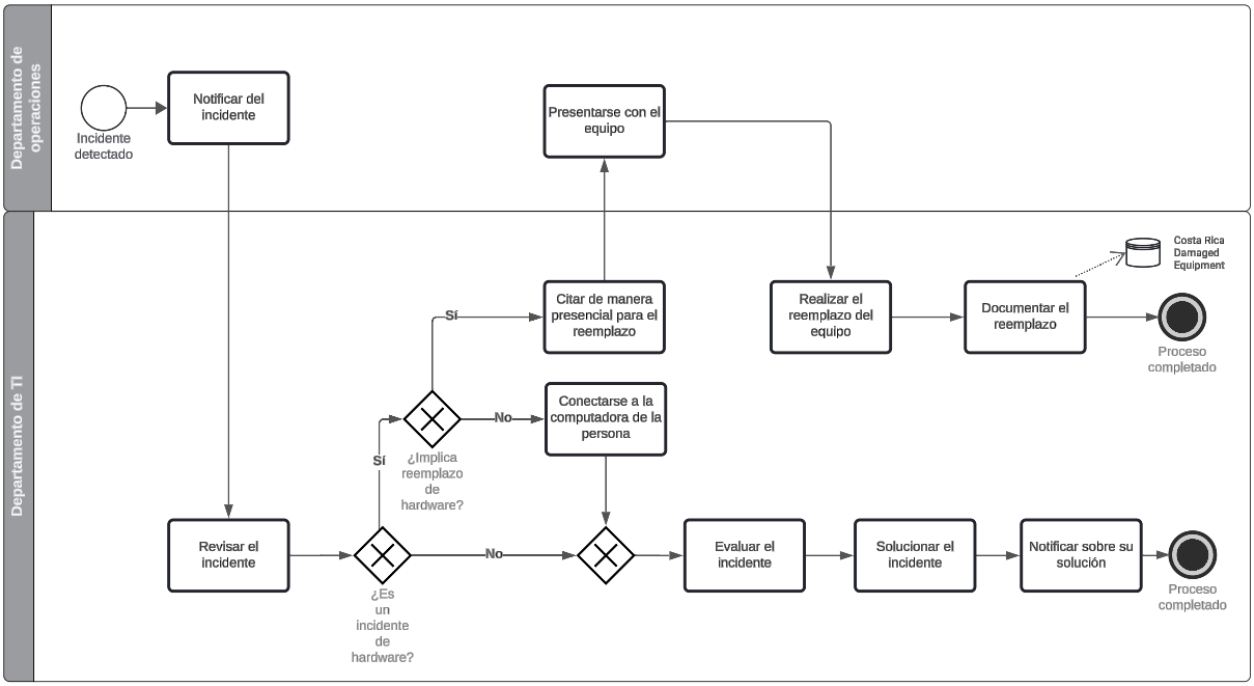
Por último, para analizar la situación actual se planteó la revisión documental del proceso de gestión de riesgos de la empresa, sin embargo, actualmente solo se cuenta con un documento que tiene como objetivo registrar los riesgos materializados. A partir del análisis realizado en el Apéndice N, se identifican varias limitaciones significativas: los registros se centran exclusivamente en activos de TI y no abarcan todos los riesgos posibles, además, el documento no se actualiza de manera constante, lo que limita la capacidad para realizar un seguimiento preciso y exhaustivo de los incidentes y sus soluciones. Por otro lado, no se proporciona una línea base clara

o justificación para las soluciones aplicadas, lo que dificulta la trazabilidad y la replicación de respuestas eficaces a incidentes similares en el futuro. Todo esto evidencia una falta de formalización y sistematización en la documentación y gestión de riesgos, subrayando la necesidad de implementar un proceso formal y estandarizado para mejorar la efectividad y cobertura de la gestión de riesgos de TI en la empresa.

4.1.2. Diagrama AS-IS de la Situación Actual de Gestión de Riesgos de TI.

A continuación, se presenta el diagrama AS-IS que representa la situación actual de gestión de riesgos de TI de la empresa. Es importante destacar que la empresa no cuenta con un proceso formal de gestión de riesgos de TI como tal, de hecho, no cumplen con ninguna de las etapas de este tipo de procesos. Sin embargo, existe un proceso específico para tratar eventos de riesgo de tipo incidentes, los cuales constituyen eventos que generan un impacto significativo, ya sea patrimonial, reputacional o en el cumplimiento de objetivos, y tienen un carácter relevante para la empresa. Este proceso es el único referente a la gestión de riesgos que la empresa maneja actualmente, y por ello se ha diagramado para visualizar cómo se gestionan los incidentes una vez que se presentan y contrastar con la nueva propuesta metodológica, la cual ayudaría a que la empresa reaccione de manera proactiva y así disminuyan este tipo de eventos. La Figura 27 presenta este diagrama.

Figura 27: Diagrama AS-IS del proceso de gestión de eventos de riesgo de tipo incidentes de la empresa Information Evolution Costa Rica



Nota: Elaboración Propia

El diagrama AS-IS del proceso actual de gestión de eventos de riesgo de tipo incidentes en la empresa revela que no existe un proceso formal y definido para gestionar los riesgos de TI y el enfoque se limita únicamente a la reacción reactiva ante riesgos ya materializados. A continuación, se explica cada actividad representada en el diagrama:

- **Incidente detectado:** el departamento de operaciones detecta un incidente relacionado con TI.
- **Notificar del incidente:** el incidente es notificado al Departamento de TI mediante un mensaje, iniciando la gestión reactiva.
- **Revisar el incidente:** el departamento de TI revisa el incidente para evaluar su naturaleza y determinar los pasos a seguir.
- **¿Es un incidente de hardware?:** en este punto de decisión, se evalúa si el incidente está relacionado con problemas de hardware.
- **¿Implica reemplazo de hardware?:** si se trata de un incidente de hardware, se verifica si es necesario reemplazar el equipo.
- **Presentarse con el equipo:** en caso de que se requiera una intervención física, el equipo se presenta en el lugar del incidente.
- **Citar de manera presencial para el reemplazo:** si se requiere reemplazo, se coordina una cita para realizarlo de manera presencial.
- **Conectarse a la computadora de la persona:** para incidentes que no requieren reemplazo de hardware, se procede a una conexión remota para intentar resolver el problema.
- **Realizar el reemplazo del equipo:** en los casos donde el hardware necesita ser reemplazado, el equipo de TI lleva a cabo esta tarea.
- **Evaluar el incidente:** si el incidente no está relacionado con hardware o no requiere reemplazo, se realiza una evaluación para decidir la solución adecuada.
- **Solucionar el incidente:** el equipo de TI aplica la solución determinada para resolver el incidente.
- **Notificar sobre su solución:** después de resolver el incidente, se comunica al usuario afectado sobre la acción tomada.
- **Documentar reemplazo:** los incidentes y las soluciones aplicadas son documentados en el archivo "*Costa Rica Damaged Equipment*".
- **Proceso completado:** el proceso concluye con la documentación o notificación de la solución.

Por último, como se planteó, el diagrama afirma que la empresa carece de un proceso preventivo y proactivo para la gestión de riesgos de TI, limitándose a una respuesta reactiva solo cuando los riesgos ya se han materializado como incidentes, lo que evidencia la necesidad de establecer un proceso integral de gestión de riesgos que no solo gestione incidentes, sino que también incluya la identificación, evaluación, y mitigación de riesgos antes de que estos se

conviertan en problemas, ya que sin una estrategia clara y preventiva, la empresa sigue expuesta a pérdidas y problemas operativos que podrían haberse evitado.

4.1.3. Identificación de las Fortalezas y Debilidades del Proceso.

Para comprender mejor la situación actual de la gestión de riesgos de TI en Information Evolution y a partir del análisis del proceso actual de gestión de riesgos de la empresa, se ha desarrollado un análisis FODA para determinar las áreas clave de este proceso, tanto sus fortalezas, debilidades, amenazas y oportunidades de mejora que tiene el proceso para así diseñar la metodología que mejor se adapte a sus necesidades. La Tabla 10 presenta este análisis.

Tabla 10: Análisis FODA de la situación actual del proceso de gestión de riesgos de TI de la empresa

FORTALEZAS	DEBILIDADES
- Manejo eficiente de un inventario extra del 3% para mitigar los impactos operativos en caso de incidentes con los equipos. - Capacidad operativa del equipo para adaptarse rápidamente y ofrecer soluciones temporales efectivas ante incidentes. - Alto nivel de conocimiento técnico y experiencia del equipo en la resolución de incidentes, permitiendo una rápida recuperación y manejo eficiente de situaciones imprevistas.	- Ausencia de procedimientos formales y estandarizados para la gestión de riesgos, aumentando la vulnerabilidad de la organización ante eventos no planificados y dificultando la respuesta efectiva. - Resistencia organizacional al cambio debido a la falta de una cultura consolidada de gestión de riesgos. - Falta de documentación sistemática sobre los riesgos de TI y sus estrategias de gestión. - Dependencia de conocimientos informales y no documentados sobre riesgos de TI. - Escasez de recursos humanos y técnicos dedicados a la gestión de riesgos. - Dependencia excesiva en reacciones inmediatas ante la materialización de riesgos. - Cultura organizacional débil en cuanto a la gestión de riesgos, caracterizada por la falta de comunicación efectiva y de políticas de gestión de riesgos. - Riesgo significativo de pérdida de datos críticos debido a la falta de estrategias de respaldo y recuperación.

OPORTUNIDADES	AMENAZAS
- Implementación de un proceso formalizado para la gestión de riesgos de TI. - Desarrollo de programas de capacitación enfocados en la importancia de la gestión de riesgos. - Integración de herramientas automatizadas y plantillas predefinidas para mejorar la eficiencia en la gestión de riesgos de TI. - Potencial significativo para fortalecer la resiliencia organizacional mediante la implementación de estrategias de gestión de riesgos de TI. Incorporación de normativas y estándares internacionales en el proceso de gestión de riesgos.	- Exposición continua a riesgos no identificados previamente que pueden materializarse. - Cambios regulatorios y legales en los procesos de TI y seguridad de la información. - Incremento en la frecuencia y sofisticación de ciberataques. - Pérdida de competitividad en el mercado. - Exposición a fluctuaciones en regulaciones de TI y privacidad de datos. - Impacto de eventos naturales o desastres en infraestructura de TI

Nota: Elaboración Propia

El análisis FODA revela un panorama integral de la situación actual de la gestión de riesgos de TI en la organización, destacando fortalezas como la capacidad operativa y el conocimiento técnico del equipo, que permiten una respuesta rápida y efectiva ante incidentes, sin embargo, también resalta debilidades críticas, como la ausencia de procedimientos formales y una cultura consolidada de gestión de riesgos, lo cual incrementa la vulnerabilidad ante eventos no planificados y dificulta la implementación de estrategias preventivas.

En términos de oportunidades, la empresa puede beneficiarse significativamente de la formalización de procesos, la capacitación del personal, y la adopción de herramientas automatizadas y estándares internacionales, lo cual podría fortalecer la resiliencia organizacional. Por otro lado, las amenazas identificadas, como la exposición a riesgos no gestionados, la dependencia de respuestas reactivas, y los crecientes desafíos de ciberseguridad, subrayan la necesidad urgente de avanzar hacia un enfoque proactivo y sistemático en la gestión de riesgos.

Por último, este análisis enfatiza la importancia de aprovechar las fortalezas y oportunidades detectadas para desarrollar un marco robusto y formalizado de gestión de riesgos que aborde de manera efectiva las debilidades y amenazas actuales, asegurando así una mayor protección y continuidad operativa para la organización.

4.1.4. Estado Deseado y Desafíos del Proceso de Gestión de Riesgos de TI

Una vez identificado el proceso actual de gestión de riesgos de TI de la empresa y elaborado el análisis FODA de este proceso, se realizó un grupo focal con el encargo del departamento de TI y el líder de operaciones, el cual se visualiza en el Apéndice L, para así detectar el estado deseado del proceso y comprender los principales desafíos que enfrenta la empresa.

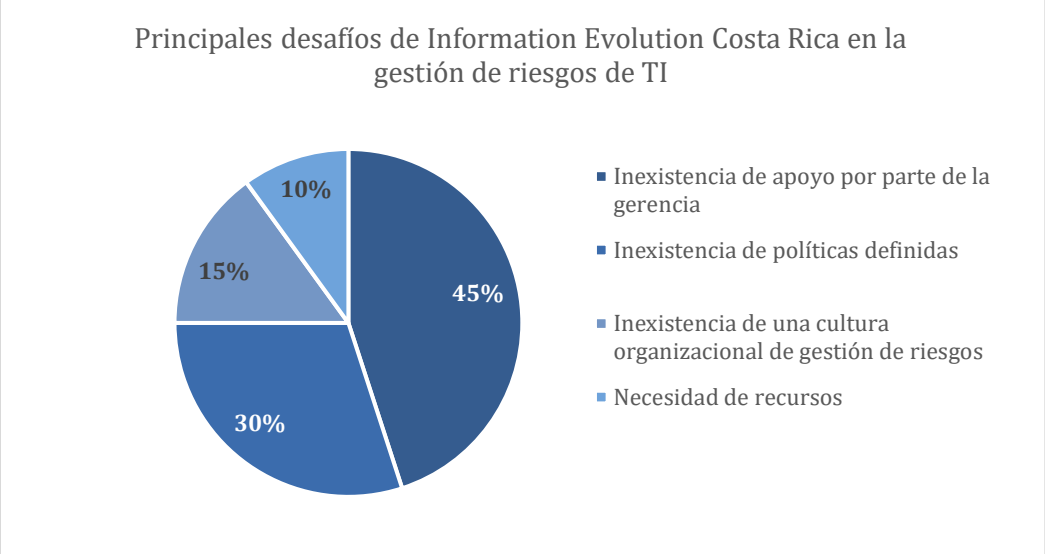
El análisis de las respuestas obtenidas en el grupo focal revela una serie de brechas críticas en el proceso actual de gestión de riesgos de TI de la empresa. Como primer punto, se destaca la ausencia de un proceso formal de gestión de riesgos, lo que lleva a la dependencia de respuestas reactivas ante incidentes y una falta de documentación sistemática, desatando desafíos principales como la falta de apoyo de la alta dirección, la necesidad de recursos y conocimientos técnicos específicos, y una baja cultura organizacional en torno a la gestión de riesgos.

También, se observó que, aunque el equipo puede identificar riesgos, carecen de la capacitación necesaria para gestionarlos adecuadamente, lo que resalta la importancia de desarrollar capacidades internas y establecer procesos claros y estandarizados, obteniendo sugerencias de mejora como la creación de políticas definidas, la estandarización de procesos mediante plantillas, y la necesidad de una comunicación más efectiva y planes de capacitación para alinear a todo el equipo en torno a la gestión de riesgos.

Por último, en cuanto a la visión ideal del proceso de gestión de riesgos, se busca una cultura organizacional fuerte con procesos estandarizados, globalización de la comunicación de riesgos, y una sólida base de políticas, siendo evaluados con indicadores de éxito como la reducción en la cantidad y el impacto de los riesgos materializados.

La Figura 28 representa un gráfico pastel en el que se exponen los principales desafíos del estado actual que presenta la organización referente a la gestión de riesgos y su importancia para los departamentos involucrados. Cabe destacar que, para estos resultados, durante el grupo focal el equipo definió los principales desafíos que enfrenta la empresa y los priorizó utilizando una puntuación total a repartir de 100pts, logrando un consenso en el impacto que ha tenido el desafío para la gestión de riesgos de TI en la empresa.

Figura 28: Principales desafíos que enfrenta la empresa en temas de gestión de riesgos de TI



Nota: Elaboración Propia

El gráfico pastel refleja un porcentaje considerable en la inexistencia de apoyo de la gerencia, el cual representa el 45% del total, lo que indica que el liderazgo y el compromiso de la alta dirección son áreas críticas que requieren atención inmediata para mejorar la gestión de riesgos, en especial por el desconocimiento de esta acerca de la importancia de este proceso. La inexistencia de políticas definidas también constituye un desafío significativo (30%), lo que resalta la necesidad de formalizar y estandarizar los procesos de gestión de riesgos para asegurar una respuesta consistente y efectiva ante incidentes y la prevención de estos a través de las distintas estrategias.

También, la inexistencia de una cultura organizacional en torno a la gestión de riesgos (15%) evidencia que la empresa necesita fortalecer la conciencia y la educación sobre la importancia de los riesgos de TI entre los empleados. Por último, la necesidad de recursos, que ocupa el 10%, sugiere que, aunque no es el mayor desafío, la provisión de recursos adecuados, especialmente en el área de personal capacitado en gestión de riesgos de TI, es esencial para apoyar la implementación de prácticas efectivas de gestión de riesgos.

4.1.4.1. Análisis de Brechas del Proceso de Gestión de Riesgos de TI

El análisis de brechas tiene como objetivo identificar las diferencias entre el estado actual del proceso de gestión de riesgos de TI en Information Evolution Costa Rica y el estado futuro deseado. A través de este análisis, se busca comprender las brechas existentes y proponer acciones que permitan alcanzar los objetivos estratégicos establecidos. En la Tabla 11 se presenta el análisis detallado, en el cual se destaca el estado actual del proceso, el estado deseado a lograr, las brechas que impiden este estado deseado y las acciones para mitigarlas.

Tabla 11: Cuadro resumen del análisis de brechas para el proceso de gestión de riesgos de TI

Estado Actual	Estado deseado	Brechas	Acciones para cerrar la brecha
Apoyo inexistente por parte de la gerencia.	Gerencia comprometida y apoyando la gestión de riesgos de TI.	- Desconocimiento de la gerencia sobre la importancia de la gestión de riesgos de TI.	- Realizar charlas de concientización sobre la gestión de riesgos de TI para la alta gerencia. - Reportar sobre los riesgos identificados y su impacto.
Inexistencia de políticas de gestión de riesgos de TI.	Políticas claras y formalizadas para la gestión de riesgos de TI.	- Desconocimiento sobre cómo implementar políticas de gestión de riesgos de TI. - Falta de liderazgo para la implementación del proceso.	- Establecer un marco para la definición de políticas basado en las mejor prácticas.
Inexistencia de una cultura organizacional de gestión de riesgos de TI.	Cultura organizacional fuerte con conciencia y práctica activa de gestión de riesgos de TI.	- Desconocimiento sobre la gestión de riesgos por parte de la organización. - Resistencia al cambio por parte del personal.	- Capacitar al equipo sobre la gestión de riesgos de TI y cómo implementar el proceso. - Fomentar la cultura de gestión de riesgos a través de charlas.
Escasez de recursos y conocimientos técnicos.	Recursos técnicos adecuados y personal capacitado en gestión de riesgos.	- Falta de herramientas de gestión de riesgos de TI. - Formación específica en gestión de riesgos de TI.	- Diseñar plantillas específicas para la gestión de riesgos de TI. - Proponer capacitaciones sobre gestión de riesgos de TI para fortalecer los conocimientos técnicos del equipo.
Inexistencia de procesos de identificación y evaluación de riesgos de TI.	Proceso estandarizado establecido de identificación y evaluación continua de riesgos.	- Falta de un proceso formal. - Necesidad de herramientas para la gestión de riesgos.	- Diseñar un proceso de gestión de riesgos basado en las mejores prácticas. - Seleccionar herramientas para la identificación y evaluación de riesgos.
No existen estrategias de mitigación o respuesta a riesgos.	Estrategias definidas y documentadas para la mitigación y respuesta a riesgos.	- Falta de conocimiento sobre estrategias de mitigación y respuesta a riesgos. - Inexistencia de herramientas para definir estrategias efectivas.	- Diseñar plantillas y estrategias de respuestas a riesgos basados en las mejores prácticas. - Capacitar al equipo en la elaboración de planes de mitigación y respuesta a riesgos.

Estado Actual	Estado deseado	Brechas	Acciones para cerrar la brecha
Desconocimiento de la necesidad de monitoreo y revisión de riesgos.	Proceso continuo de monitoreo y revisión de riesgos.	- Inexistencia de protocolos de monitoreo y seguimiento. - Desconocimiento de la importancia del monitoreo continuo.	- Diseñar protocolos de monitoreo y revisión continua de riesgos. - Establecer indicadores para evaluar la efectividad del monitoreo y revisión de riesgos.
Documentación informal y no actualizada.	Documentación formal y actualizada regularmente sobre la gestión de riesgos.	- Ausencia de estándares y lineamientos claros para la documentación.	- Estandarizar la documentación de gestión de riesgos conforme a los lineamientos de las mejores prácticas. - Establecer plantillas y herramientas para mantener la documentación actualizada.
Ausencia de canales de comunicación efectivos para la gestión de riesgos.	Comunicación fluida y estructurada sobre la gestión de riesgos en todos los niveles de la organización.	- Desconocimiento sobre la importancia de la comunicación. - Falta de protocolos de comunicación de la información.	- Diseñar un plan de comunicación de la información - Capacitar sobre la importancia de la comunicación en la gestión de riesgos.
Falta de criterios claros para la definición y priorización de riesgos.	Definición y priorización de riesgos basados en criterios claros y consistentes.	- Inexistencia criterios y procedimientos para la clasificación y evaluación de riesgos.	- Establecer una metodología para la evaluación y priorización de riesgos.
Falta de integración de la gestión de riesgos en la planificación estratégica de la empresa.	Gestión de riesgos integrada con la estrategia y objetivos de la empresa.	- Gestión de riesgos de TI vista como un proceso separado, sin conexión con los objetivos estratégicos.	- Incorporar la gestión de riesgos de TI en la planificación estratégica mediante la alineación con mejores prácticas en gobernanza de TI.
Ausencia de métricas para evaluar la eficacia de las respuestas a los riesgos.	Sistema de métricas y KPIs para evaluar la efectividad de las respuestas a los riesgos.	Desconocimiento de sistemas de monitoreo y revisión continua de las respuestas a los riesgos implementados.	- Establecer indicadores y utilizar herramientas de monitoreo continuo para la revisión y mejora de las respuestas a los riesgos.

Nota: Elaboración Propia

El análisis de brechas realizado muestra una serie de desafíos clave en la gestión de riesgos de TI en la empresa, destacando áreas críticas que necesitan mejoras significativas para alcanzar un nivel óptimo de gestión requerido. Entre las brechas identificadas se incluyen la falta de apoyo y compromiso de la gerencia, la inexistencia de políticas, procesos claros y cultura organizacional en torno a la gestión de riesgos, acompañadas por la ausencia de recursos técnicos y conocimientos especializados, la falta de procedimientos de identificación, evaluación y respuesta a los riesgos, y la carencia de un sistema de monitoreo y revisión continua.

Para cerrar estas brechas, se proponen acciones específicas alineadas con las mejores prácticas en gestión de riesgos de TI de la industria, incluyendo la implementación de programas de capacitación, la creación de políticas y procedimientos claros, el desarrollo de herramientas y plantillas para la gestión de riesgos, y el establecimiento de sistemas de métricas y KPIs para evaluar la efectividad de las respuestas, de tal forma que no solo se busque cerrar las brechas actuales, sino que también se fortalezca la resiliencia y capacidad de respuesta de la organización frente a los riesgos de TI, alineando estos esfuerzos con los objetivos estratégicos de la empresa y promoviendo una cultura organizacional proactiva y consciente de la importancia de la gestión de riesgos.

4.2. Fase II: Comparación y Selección de las Mejores Prácticas de Gestión de Riesgos de TI

La Fase II del proyecto se centra en la comparación y selección de las mejores prácticas de la industria en la gestión de riesgos de TI. Para ello, se lleva a cabo un análisis comparativo y, posteriormente un análisis de alineación, utilizando criterios específicos que permiten evaluar la aplicabilidad y efectividad de mejores prácticas de gestión de riesgos de TI en el contexto de la empresa. Esta fase busca identificar las prácticas más adecuadas para ser implementadas en la organización, asegurando una alineación óptima con sus necesidades estratégicas.

4.2.1. Comparación entre las Mejores Prácticas de Gestión de Riesgos de TI

A partir del instrumento creado en el apéndice G, se lleva a cabo una comparación entre las prácticas de COBIT 2019, ISO 31000, ISO 27005, OCTAVE y Margerit, a partir de criterios clave de gestión de riesgos de TI, permitiendo identificar similitudes, diferencias y puntos de alineación entre los enfoques seleccionados. El análisis busca ofrecer una visión integral de cómo cada marco aborda la gestión de riesgos en el ámbito de las tecnologías de la información, facilitando la selección y adaptación de las mejores prácticas según las necesidades de la empresa. A continuación, en la Tabla 12, se presentan los resultados de este análisis.

Tabla 12: Análisis comparativo entre las mejores prácticas de la industria

	COBIT 2019	ISO 31000	ISO 27005	MARGERIT	OCTAVE
Enfoque de gestión de riesgos	Gobernanza y gestión de riesgos alineada a los objetivos estratégicos.	Gestión continua de riesgos en toda la organización.	Gestión de riesgos de la seguridad de la información sin métodos específicos.	Gestión de riesgos centrada en TI y la toma de decisiones en administración pública, con un enfoque centrado en la gestión de riesgos de los activos de TI.	Evaluación y mitigación de riesgos de seguridad de la información y planificación estratégica.
Estructura	Incluye dominios de gobierno (EDM), de gestión (APO, BAI, DSS, MEA) y componentes clave**.** Cada dominio contiene objetivos de gobierno y gestión específicos.	Compuesta por tres partes principales: Principios de gestión de riesgos, Marco de referencia, Proceso de gestión de riesgos**.**	Estructura alineada con los Sistemas de Gestión de Seguridad de la Información basados en ISO 27001. Incluye principios y directrices, pero no define un método específico	Estructura definida por un marco de referencia que incluye una metodología específica para la gestión de riesgos de TI en el sector público alineada con la ISO 31000.	Se divide en principios, atributos, y fases**.** Incluye directrices detalladas para la evaluación y mitigación de riesgos y permite adaptar los principios
Proceso	Se enfoca en los procesos EDM03 (Asegurar la optimización del riesgo) **y** APO12 (Gestionar el riesgo)**.** El EDM03 asegura que los riesgos de TI se optimicen, se comprendan y se comuniquen, mientras que el APO12 gestiona el riesgo identificándolo, evaluándolo y manteniendo un perfil actualizado.	Crea un ciclo de gestión de riesgos: establecer el contexto, identificación, análisis, evaluación, tratamiento, monitoreo y revisión, comunicación y consulta. Todo esto conforma un proceso iterativo y adaptable a la organización.	Compone un ciclo continuo de establecer el contexto, identificación de riesgos, análisis, evaluación, Tratamiento, monitoreo y revisión, similar a ISO 31000, pero con un enfoque específico en la seguridad de la información.	El proceso está compuesto por establecer el contexto, identificación y valoración de activos y riesgos, análisis y evaluación, tratamiento del riesgo, monitoreo y revisión**.**	Divide el proceso en tres fases: identificación de activos, amenazas y vulnerabilidades, evaluación del impacto y riesgo, planificación de la mitigación de riesgos**.**

	COBIT 2019	ISO 31000	ISO 27005	MARGERIT	OCTAVE
Alcance	Organizaciones, de cualquier tamaño y distintos sectores, que buscan alinear sus operaciones de TI con los objetivos empresariales, facilitando un marco estructurado para la gobernanza y la gestión de TI.	Aplicable a cualquier tipo de organización, independientemente de su tamaño o sector, proporcionando principios y directrices genéricas para la gestión de riesgos.	Orientada a entidades que manejan grandes volúmenes de datos sensibles y buscan cumplir con estándares internacionales de seguridad que busquen gestionar los riesgos de su SGSI.	Orientado principalmente hacia organizaciones que manejan TI, con un enfoque especial en las administraciones públicas.	Diseñado para organizaciones con un fuerte enfoque en TI y seguridad, incluyendo empresas que operan en sectores críticos como banca, salud y tecnología.
Nivel de detalle	Directrices detalladas que incluyen prácticas específicas de gobierno y gestión, abarcando desde la evaluación de riesgos hasta la implementación de controles y auditorías.	Principios generales que guían la gestión de riesgos sin prescribir métodos o procesos específicos, permitiéndole ser flexible y adaptarse a las necesidades de diversas organizaciones.	Directrices específicas para la gestión de riesgos dentro de un SGSI, a través de un conjunto estructurado de procesos y controles, aunque no prescribe un método único, lo que permite cierto grado de personalización.	Proporciona un procedimiento detallado con herramientas específicas para la evaluación y gestión de riesgo con un detalle mayor en los activos de TI.	Procedimientos específicos para evaluación de riesgos.
Integración con otros marcos	Compatible con normas internacionales y otros marcos de gestión, como ISO 31000 y ITIL, lo que facilita su integración en entornos empresariales.	Compatible con otros estándares y marcos de gestión, lo que permite su uso en conjunto con normativas como las ISO y otros marcos de referencia.	ISO 27005 está específicamente alineado con ISO 27001 y otros estándares de SGSI, lo que asegura una integración fluida en organizaciones	Basado en la ISO 31000 y es alineable con otros marcos de gestión de riesgos, lo que le permite integrarse fácilmente en organizaciones que utilizan múltiples enfoques de gestión de riesgos.	Alineado con otros marcos de gestión de TI, incluyendo ITIL y NIST, lo que facilita su integración en organizaciones que buscan un enfoque multidimensional.

	COBIT 2019	ISO 31000	ISO 27005	MARGERIT	OCTAVE
Participación de las partes interesadas	Involucra a la alta dirección y a las partes interesadas clave en la gobernanza y gestión de TI, promoviendo una cultura de colaboración y responsabilidad compartida.	Enfatiza la participación de todas las partes interesadas en la gestión de riesgos, desde los altos directivos hasta los empleados en todos los niveles, fomentando una cultura de gestión de riesgos integrada en toda la organización.	Requiere la participación de las partes interesadas en la seguridad de la información, asegurando que los riesgos sean gestionados con la colaboración de todos los niveles organizacionales.	Se enfoca en la comunicación y participación activa de las partes interesadas, incluyendo la alta dirección, los gestores de TI y otros responsables de la toma de decisiones	Involucra a todos los niveles de la organización, incluyendo a los usuarios finales y a los equipos de gestión de TI
Mejora continua	Promueve la mejora continua a través de revisiones y auditorías periódicas, asegurando que la gestión de riesgos y la gobernanza de TI se mantengan alineadas con los cambios en el entorno empresarial y tecnológico.	Incorpora un enfoque claro en la mejora continua, permitiendo que las organizaciones revisen y mejoren constantemente sus procesos de gestión de riesgos para adaptarse a nuevos desafíos y oportunidades.	Enfatiza la mejora continua en la gestión de seguridad de la información, mediante la revisión periódica de los riesgos y la implementación de controles adicionales según sea necesario.	Incluye un enfoque en la revisión y mejora continua, asegurando que los procesos de gestión de riesgos se actualicen y adapten según los cambios en el entorno de TI y los requisitos del sector público.	Enfatiza la mejora continua mediante la revisión de las fases de gestión de riesgos, permitiendo a las organizaciones ajustar sus estrategias y controles en respuesta a nuevos riesgos o cambios en el entorno de TI.

Nota: Elaboración Propia

La comparación entre las mejores prácticas de gestión de riesgos de TI reveló enfoques y estructuras diversas que reflejan la adaptabilidad y los distintos niveles de detalle según el marco de referencia. COBIT 2019 se distingue por su integración de la gobernanza y gestión de riesgos alineada a los objetivos estratégicos de la organización, con un enfoque robusto en la mejora continua a través de auditorías y revisiones periódicas. La ISO 31000, por otro lado, ofrece un marco flexible y adaptable, orientado a gestionar riesgos de manera continua en toda la organización sin prescribir métodos específicos, lo cual le otorga una aplicabilidad amplia y versátil.

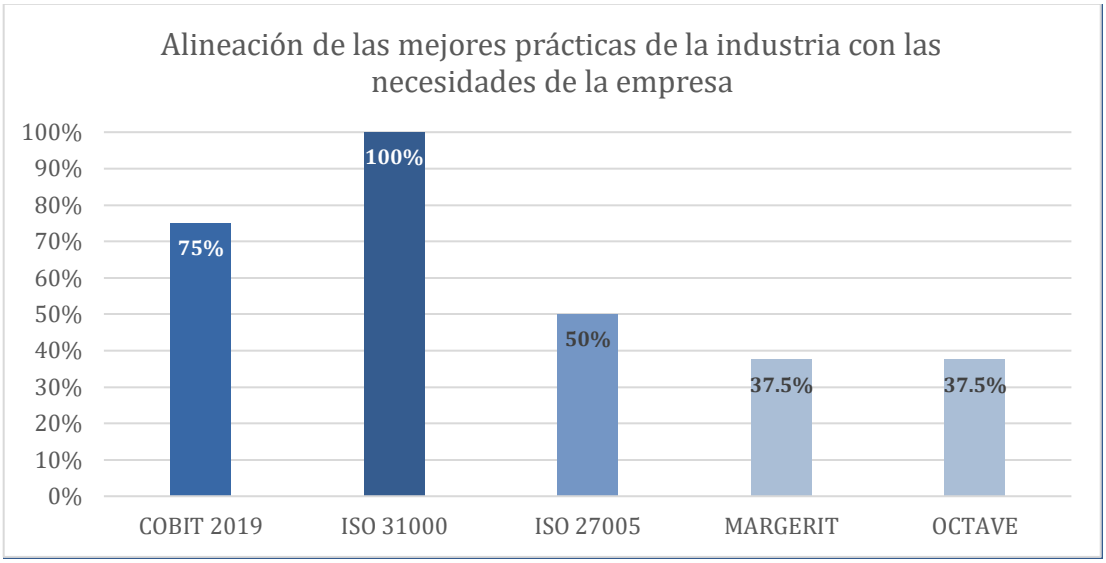
Por otro lado, la ISO 27005 proporciona directrices específicas para la gestión de riesgos en sistemas de gestión de seguridad de la información, alineándose estrechamente con otros estándares SGSI, mientras que Magerit ofrece un enfoque detallado para la gestión de riesgos de TI en el sector público, integrando directrices de la ISO 31000 y enfocándose en la evaluación y gestión de activos críticos de TI. Por su parte, OCTAVE se centra en la evaluación y mitigación de riesgos de seguridad de la información con un enfoque práctico en la planificación estratégica y la adopción de principios de gestión de riesgos.

Por último, este análisis comparativo subraya la importancia de seleccionar y adaptar el marco adecuado para satisfacer las necesidades particulares de cada organización, teniendo en cuenta factores como las necesidades específicas de la empresa de forma que facilite una integración más efectiva de la gestión de riesgos en las operaciones diarias y la estrategia global de la organización.

4.2.2. Selección de las Mejores Prácticas de Gestión de Riesgos de TI

Una vez comparadas las mejores prácticas de gestión de riesgos de TI, se realiza un análisis de alineación para seleccionar las más adecuadas para la empresa. Este análisis, detallado en el Apéndice M, considera criterios fundamentales como la aplicabilidad al tipo de empresa, la facilidad de implementación inicial sin necesidad de conocimiento previo, el coste de implementación, y la integración con normativas y recursos humanos y técnicos existentes, entre otros, los cuales fueron definidos de acuerdo a los hallazgos de las necesidades de la empresa presentados en el grupo focal, el cual se encuentra en el Apéndice L, y son fundamentales para identificar cuáles de estas prácticas son más adecuadas para implementar en la organización, dado su contexto y características específicas. A continuación, en la Figura 29, se presenta un gráfico que visualiza los resultados de este análisis, facilitando la comparación entre las distintas prácticas evaluadas y su grado de alineación con los requisitos de la empresa.

Figura 29: Gráfico de alineación de las mejores prácticas de la industria a las necesidades de la empresa



Nota: Elaboración Propia

El análisis muestra que tanto COBIT 2019 como la ISO 31000 cumplen con la mayoría de los criterios establecidos, con porcentajes de alineación del 75% y 100% respectivamente, destacándose como las opciones más completas y adecuadas. La ISO 31000, con una alineación del 100%, se distingue por su flexibilidad y aplicabilidad a diferentes tipos de organizaciones, además de su facilidad de implementación y enfoque integral en la mejora continua, lo cual es crucial para empresas sin experiencia previa en la gestión de riesgos.

Por otro lado, COBIT 2019, aunque también muestra una alta alineación, presenta algunos desafíos en términos de coste y facilidad de implementación, debido a la complejidad de sus directrices y la posible necesidad de capacitación adicional, sin embargo, su enfoque robusto y detallado en la integración de la gestión de riesgos con los objetivos estratégicos lo hace una opción valiosa para el desarrollo de este proyecto.

Las otras prácticas evaluadas, como ISO 27005, Magerit, y OCTAVE, muestran menores niveles de alineación, principalmente debido a su enfoque especializado o restricciones en su implementación dentro del contexto específico de la empresa. Estas prácticas no cumplen adecuadamente con varios de los criterios clave, como la aplicabilidad general a la gestión de riesgos de TI más allá de la seguridad de la información, y la compatibilidad con los recursos y capacidades actuales de la organización.

Por lo tanto, después de comparar y analizar los resultados obtenidos, se determina que las mejores prácticas seleccionadas para la gestión de riesgos de TI en la empresa son COBIT 2019 y la ISO 31000, ya que ofrecen un equilibrio entre detalle, flexibilidad, y enfoque estratégico, permitiendo que la organización aborde sus necesidades específicas y establezca un marco sólido y eficiente para la gestión de riesgos de TI.

4.3. Fase III: Elaboración de los Artefactos para la Metodología de Gestión de Riesgos de TI

En la Fase III, dentro de la sección de análisis de resultados, se presentan los hallazgos derivados de la propuesta del diagrama TO-BE para la metodología de gestión de riesgos de TI, diseñado con base en las mejores prácticas y adaptado a las necesidades específicas de la empresa. Además, se realiza un análisis detallado sobre el grado de cumplimiento del proceso propuesto en relación con las brechas identificadas durante la Fase I, las cuales revelaron áreas clave que requerían mejoras y ajustes en el contexto actual de la organización. Esta sección permite evaluar cómo el diseño del proceso propuesto aborda dichas brechas, asegurando un avance hacia un sistema robusto y alineado con los objetivos estratégicos de la gestión de riesgos.

4.3.1. Diagramación TO-BE del Proceso Propuesto

En esta sección se presenta el diagrama TO-BE del proceso de Gobierno de TI y del proceso de Gestión de Riesgos de TI, el cual define el estado deseado que se propone para la empresa, basado en las mejores prácticas de COBIT 2019 y la ISO 31000.

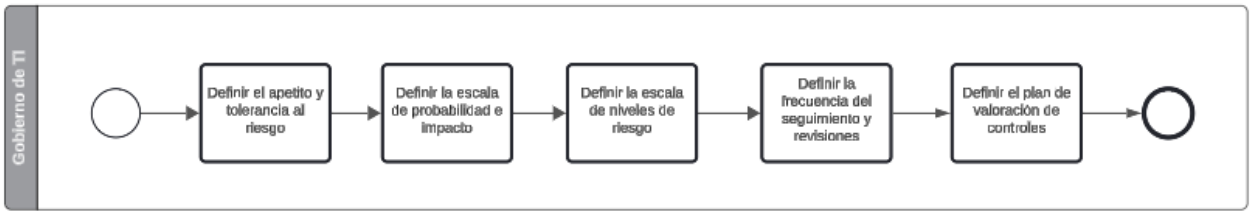
4.3.1.1. Diagrama TO-BE del proceso de Gobierno de TI

El diagrama TO-BE del proceso de Gobierno de TI se desarrolla conforme a las prácticas establecidas por COBIT 2019, asegurando un enfoque estructurado y alineado con los objetivos estratégicos de la organización. Para facilitar su comprensión y ejecución, este proceso se divide en tres partes fundamentales: Evaluar, Dirigir y Monitorear, las cuales permiten abordar de manera integral los aspectos clave del Gobierno de TI.

4.3.1.1.1. Evaluar la Gestión de Riesgos

El proceso de Evaluar la Gestión de Riesgos busca asegurar que el apetito al riesgo de la empresa sea apropiado, y que los riesgos relacionados con la información y tecnología sean identificados y gestionados de manera efectiva, promoviendo la protección y generación de valor para la organización. Este proceso es esencial para alinear la gestión de riesgos con los objetivos estratégicos de la empresa. La Figura 30 muestra el diagrama propuesto.

Figura 30: Diagrama TO-BE del proceso de Gobierno de TI "Evaluar la Gestión de Riesgos"



Nota: Elaboración Propia

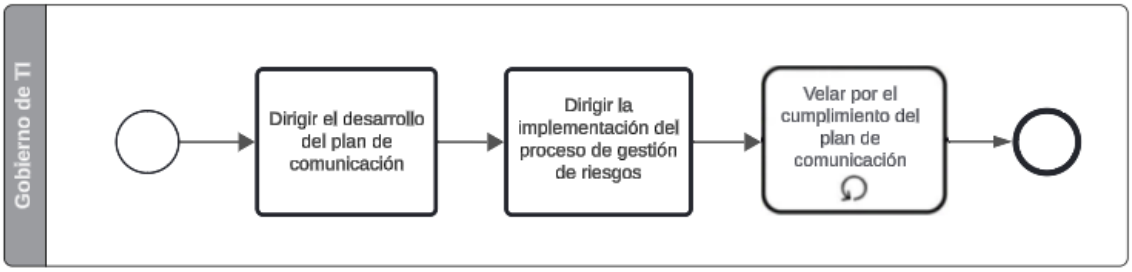
En el diagrama presentado en la Figura 30, se pueden observar las actividades necesarias para llevar a cabo esta evaluación, explicadas a continuación:

- **Definir el apetito y tolerancia al riesgo:** se establece el nivel de riesgo aceptable para la organización, considerando sus objetivos estratégicos y operativos.
- **Definir la escala de probabilidad e impacto:** se determina la escala de probabilidad y la escala de impacto de los riesgos de acuerdo con las necesidades empresariales.
- **Definir la escala de niveles de riesgo:** se categoriza el nivel de riesgo en base a la combinación de probabilidad e impacto, facilitando la priorización y tratamiento de los riesgos.
- **Definir la frecuencia del seguimiento y revisiones:** se determina la periodicidad con la que se revisarán los riesgos y controles, garantizando su actualización y relevancia.
- **Definir el plan de valoración de controles:** se diseña un plan que establece cómo se evaluará la efectividad de los controles existentes, identificando áreas de mejora.

4.3.1.1.2. Dirigir la Gestión del Riesgo

El proceso de Dirigir la Gestión de Riesgos se enfoca en establecer prácticas efectivas de gestión de riesgos que garanticen que los riesgos de información y tecnología no superen el apetito al riesgo definido por el consejo de administración. La Figura 31 muestra el diagrama propuesto.

Figura 31: Diagrama TO-BE del proceso de Gobierno de TI "Dirigir la Gestión de Riesgos"



Nota: Elaboración Propia

En el diagrama presentado en la Figura 31, se pueden observar las actividades necesarias para llevar a cabo este proceso de tal forma que se establezca un enfoque integral y estratégico en la gestión de riesgos, dichas actividades se explican a continuación:

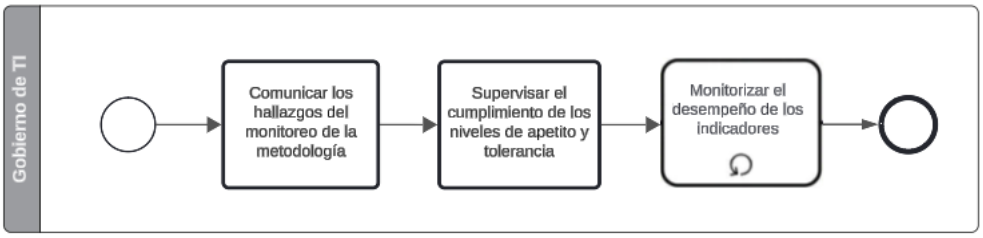
- **Dirigir el desarrollo del plan de comunicación:** asegurar que exista un plan claro para comunicar los riesgos, las respuestas a estos, y las responsabilidades asociadas, promoviendo una gestión colaborativa y bien informada.
- **Dirigir la implementación del proceso de gestión de riesgos:** supervisar la puesta en marcha de la metodología de gestión de riesgos, garantizando que las actividades se realicen de acuerdo con las directrices y objetivos establecidos.

- **Velar por el cumplimiento del plan de comunicación:** monitorear continuamente que el plan de comunicación sea aplicado de manera efectiva, facilitando una gestión transparente y alineada con los intereses de todas las partes interesadas.

4.3.1.1.3. Monitorear la Gestión de Riesgos

El proceso de Monitorear la Gestión de Riesgos tiene como objetivo supervisar las metas y métricas clave relacionadas con los procesos de gestión de riesgos, asegurando su alineación con las prácticas definidas y el cumplimiento de los objetivos organizacionales. La Figura 32 muestra el diagrama del proceso propuesto.

Figura 32: Diagrama TO-BE del proceso de Gobierno de TI "Monitorear la Gestión de Riesgos"



Nota: Elaboración Propia

En el diagrama presentado en la Figura 32, se pueden observar las actividades necesarias para llevar a cabo esta evaluación, explicadas a continuación:

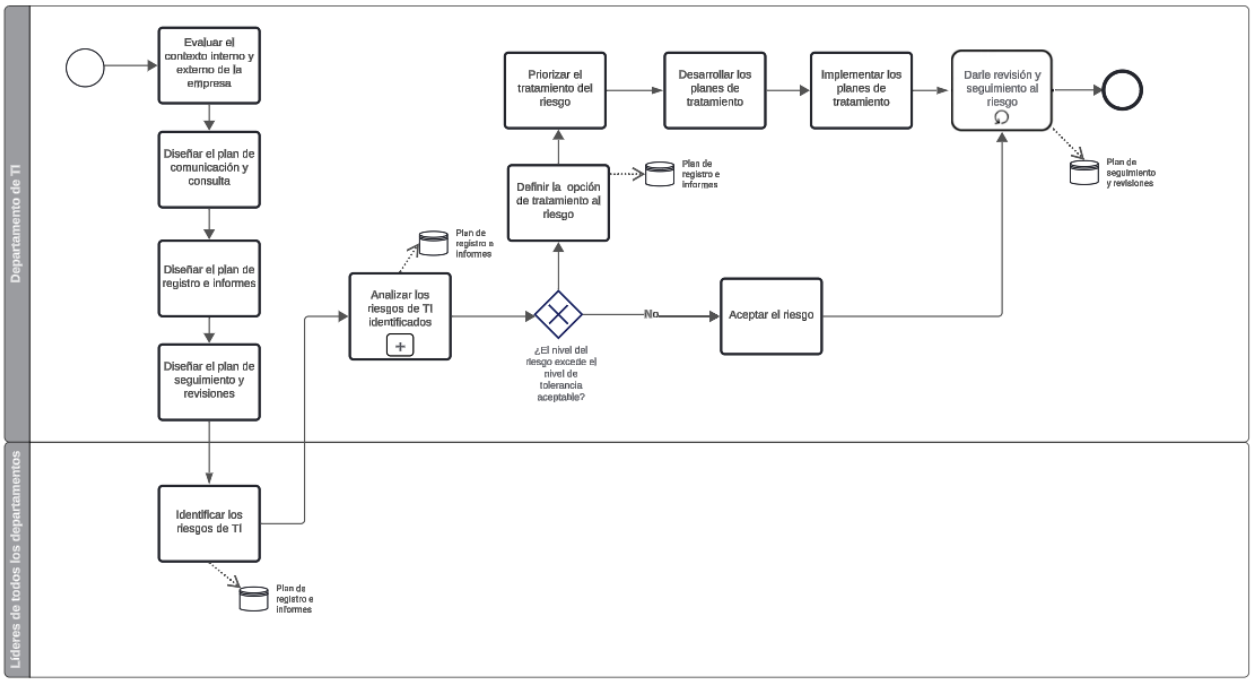
- **Comunicar los hallazgos del monitoreo de la metodología:** garantizar que los resultados y observaciones derivados del seguimiento del proceso de gestión de riesgos sean compartidos con las partes interesadas relevantes, fomentando la transparencia y la mejora continua.
- **Supervisar el cumplimiento de los niveles de apetito y tolerancia**: asegurar que las prácticas de gestión de riesgos se mantengan dentro de los límites definidos por el apetito y la tolerancia al riesgo, alineándose con la estrategia y los valores organizacionales.
- **Monitorizar el desempeño de los indicadores:** evaluar regularmente el desempeño de los indicadores clave de riesgo (KRIs) y los indicadores clave de desempeño (KPIs) para garantizar la eficacia y eficiencia del proceso de gestión de riesgos.

4.3.1.2. Diagrama TO-BE del proceso de Gestión de Riesgos de TI

A diferencia del proceso actual, que carece de una estructura formal para la gestión de riesgos de TI, el diagrama TO-BE propuesto proporciona un marco integral y sistematizado para identificar, evaluar, mitigar, y monitorear los riesgos de TI a través de las directrices de la ISO 31000, el cual no busca solo establecer un proceso formal y continuo de gestión de riesgos, sino también alinear este proceso con los objetivos estratégicos de la empresa, asegurando que los

riesgos sean gestionados de manera proactiva y efectiva. La Figura 31 muestra el diagrama TO-BE del proceso de Gestión de Riesgos de TI propuesto.

Figura 33: Diagrama TO-BE del proceso de Gestión de Riesgos de TI



Nota: Elaboración Propia

Este diagrama propuesto integra las directrices de la ISO 31000, alineando las actividades clave con las necesidades y características específicas de la empresa, incluyendo actividades que permiten la identificación, análisis, tratamiento y seguimiento continuo de los riesgos, evitando que la empresa deba reaccionar siempre de manera reactiva, tal y como se viene haciendo. A continuación, se explican las actividades del diagrama:

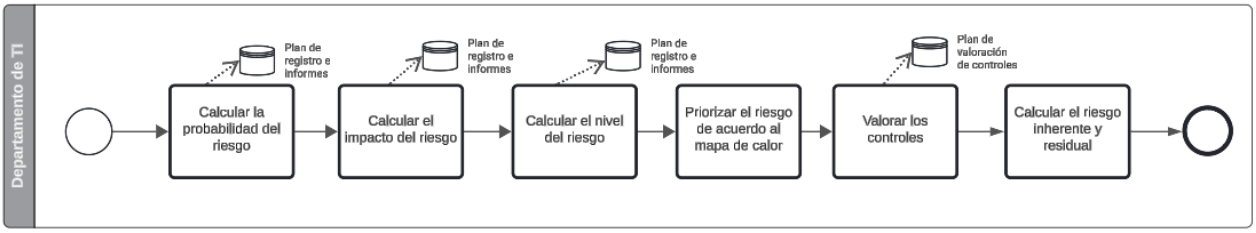
- **Evaluar el contexto interno y externo de la empresa:** analizar las condiciones internas y externas que afectan la identificación y tratamiento de los riesgos de TI. Esta actividad se realiza solo la primera vez y se le da seguimiento con cada iteración.
- **Diseñar el plan de comunicación y consulta:** creación de un plan que defina cómo y cuándo se comunicarán los riesgos a los interesados y cómo se realizará la consulta con las partes clave, tanto internas como externas. Esta actividad se realiza solo la primera vez y se le da seguimiento con cada iteración.
- **Diseñar el plan de registro e informes:** establecer cómo se documentarán los riesgos identificados, sus tratamientos y el seguimiento. Esta actividad se realiza solo la primera vez y se le da seguimiento con cada iteración.

- **Diseñar el plan de seguimiento y revisiones:** definir la frecuencia y los métodos de seguimiento que se utilizarán para revisar los riesgos y los controles establecidos, tomando en cuenta la importancia de los indicadores clave de riesgo y de desempeño. Esta actividad se realiza solo la primera vez y se le da seguimiento con cada iteración.
- **Identificar los riesgos de TI:** consiste en la identificación de los riesgos que podrían afectar a la organización en términos de TI, como riesgos operacionales, de seguridad, regulatorios, entre otros.
- **Analizar los riesgos de TI identificados:** se evalúa tanto la probabilidad como el impacto de los riesgos para obtener el nivel del riesgo y calcular el riesgo residual e inherente. Este subproceso se detalla en la Figura 32.
- **Definir la opción de tratamiento al riesgo:** aquí se elige una respuesta adecuada para tratar el riesgo, ya sea evitarlo, mitigarlo, transferirlo o aceptarlo, de acuerdo con el nivel de riesgo aceptado.
- **Priorizar el tratamiento del riesgo:** consiste en priorizar los riesgos de acuerdo con su nivel del riesgo y tratamiento definido.
- **Desarrollar los planes de tratamiento:** se crean los planes específicos para implementar las medidas necesarias para el tratamiento del riesgo.
- **Implementar los planes de tratamiento:** se ejecutan las acciones necesarias para mitigar, transferir, evitar o aceptar el riesgo.
- **Dar seguimiento y revisión al riesgo:** es una actividad iterativa que se repite según la frecuencia definida para el seguimiento de los riesgos, evaluando continuamente su estado y los controles aplicados.

4.3.1.2.1. Subproceso: Analizar los Riesgos de TI Identificados.

A continuación, en la Figura 32, se presenta el diagrama TO-BE del subproceso “Analizar los riesgos de TI identificados” explicado anteriormente.

Figura 34: Diagrama TO-BE del subproceso Analizar los riesgos de TI identificados



Nota: Elaboración Propia

El subproceso Analizar los riesgos de TI identificados incluye la documentación detallada de cada una de las actividades realizadas, desde la evaluación de la probabilidad e impacto, hasta la priorización y el establecimiento de las opciones de tratamiento para cada riesgo identificado, facilitando no sólo el registro de las decisiones tomadas, sino que también sirve como referencia para futuras revisiones y auditorías del proceso.

Adicionalmente, este flujo se repite en las etapas de seguimiento y revisiones definidas en la metodología, garantizando así que los riesgos sean evaluados de manera continua y se mantengan alineados con los objetivos estratégicos de la organización y los cambios en el entorno interno y externo.

4.3.1.3. Cumplimiento del proceso propuesto con respecto a las brechas identificadas

A continuación, se presenta el análisis de cumplimiento del proceso propuesto con respecto a las brechas identificadas durante la Fase I del proyecto. Para ello, se incluye una tabla que detalla el estado deseado, las acciones necesarias para cerrar las brechas y las evidencias de cumplimiento alcanzado según la propuesta desarrollada y las mejores prácticas utilizadas.

Es importante destacar que aquellas acciones que no se cumplen están relacionadas con aspectos excluidos del alcance del proyecto, como se definió en la sección de exclusiones. Estas acciones, aunque no forman parte directa de la metodología propuesta, se abordan en la sección de recomendaciones, brindando lineamientos para su implementación futura y complementando la gestión integral de riesgos de TI en la organización. La Tabla 13 muestra la tabla de cumplimiento del cierre de brechas.

Tabla 13: Cumplimiento del proceso propuesto y las mejores prácticas con el cierre de brechas

Estado deseado	Acciones para cerrar la brecha	Cumplimiento según el proceso propuesto y las mejores prácticas
Gerencia comprometida y apoyando la gestión de riesgos de TI.	- Realizar charlas de concientización sobre la gestión de riesgos de TI para la alta gerencia. - Reportar sobre los riesgos identificados y su impacto.	Se propone un proceso para la comunicación de la metodología y una sección de registros e informes según la ISO 31000 y las prácticas de monitoreo del EDM03.
Políticas claras y formalizadas para la gestión de riesgos de TI.	- Establecer un marco para la definición de políticas basado en las mejor prácticas.	Se establece un proceso para la definición de una estructura de Gobierno de TI y la definición de criterios específicos.
Cultura organizacional fuerte con conciencia y práctica activa de gestión de riesgos de TI.	- Capacitar al equipo sobre la gestión de riesgos de TI y cómo implementar el proceso. - Fomentar la cultura de gestión de riesgos a través de charlas.	No se cumple en el proceso propuesto, sin embargo, se agrega en la sección de Recomendaciones.
Recursos técnicos adecuados y personal capacitado en gestión de riesgos.	- Diseñar plantillas específicas para la gestión de riesgos de TI. - Proponer capacitaciones sobre gestión de riesgos de TI para fortalecer los conocimientos técnicos del equipo.	Como parte de la propuesta de solución, se diseñan plantillas específicas para cada actividad según las necesidades de la empresa

Estado deseado	Acciones para cerrar la brecha	Cumplimiento según el proceso propuesto y las mejores prácticas
Proceso estandarizado establecido de identificación y evaluación continua de riesgos.	- Diseñar un proceso de gestión de riesgos basado en las mejores prácticas. - Seleccionar herramientas para la identificación y evaluación de riesgos.	Se proponen el proceso completo de gestión de riesgos de TI según la ISO 31000, y como parte de la evaluación de riesgos, se proponen distintas herramientas para su correcta implementación.
Estrategias definidas y documentadas para la mitigación y respuesta a riesgos.	- Diseñar plantillas y estrategias de respuestas a riesgos basados en las mejores prácticas. - Capacitar al equipo en la elaboración de planes de mitigación y respuesta a riesgos.	El proceso de gestión de riesgos propone actividades de respuesta a riesgos y, como parte de la propuesta de solución, se proponen estrategias de tratamiento y respuesta a riesgos, aparte de su correcta priorización según su grado de impacto.
Proceso continuo de monitoreo y revisión de riesgos.	- Diseñar protocolos de monitoreo y revisión continua de riesgos. - Establecer indicadores para evaluar la efectividad del monitoreo y revisión de riesgos.	Se proponen actividades de revisión y seguimiento de los riesgos que incluyen indicadores y objetivos a cumplir.
Documentación formal y actualizada regularmente sobre la gestión de riesgos.	- Estandarizar la documentación de gestión de riesgos conforme a los lineamientos de las mejores prácticas. - Establecer plantillas y herramientas para mantener la documentación actualizada.	Se proponen documentos para la correcta documentación de los riesgos de TI y seguimiento y revisiones de estos, aparte de actividades específicas donde esto se debe realizar.
Comunicación fluida y estructurada sobre la gestión de riesgos en todos los niveles de la organización.	- Diseñar un plan de comunicación de la información - Capacitar sobre la importancia de la comunicación en la gestión de riesgos.	Se proponen actividades para el desarrollo de un plan de comunicación y monitoreo del cumplimiento de este, aparte de la propuesta de una matriz de comunicación como parte de la propuesta de solución.
Definición y priorización de riesgos basados en criterios claros y consistentes.	- Establecer un proceso para la evaluación y priorización de riesgos.	Se proponen actividades específicas para la definición y priorización de los riesgos de TI, aparte de priorización de opciones de respuesta a estos riesgos.
Gestión de riesgos integrada con la estrategia y objetivos de la empresa.	- Incorporar la gestión de riesgos de TI en la planificación estratégica mediante la alineación con mejores prácticas en gobernanza de TI.	Se propone el proceso de Gobierno de TI con el fin de lograr la alineación entre los objetivos estratégicos de la empresa y los objetivos de TI.
Sistema de métricas y KPIs para evaluar la efectividad de las respuestas a los riesgos.	Establecer indicadores y utilizar herramientas de monitoreo continuo para la revisión y mejora de las respuestas a los riesgos.	Se proponen actividades dedicadas al monitoreo de los riesgos de TI y, como parte de la propuesta de solución, se proponen indicadores para su correcta evaluación.

Nota: Elaboración Propia

Según la Tabla 13, el proceso propuesto demuestra una alineación sólida con las mejores prácticas de la industria seleccionadas en la Fase 2 y aborda de manera integral las brechas identificadas en el diagnóstico inicial de la empresa. La implementación de este proceso no solo garantiza la definición clara de elementos clave, como el apetito y la tolerancia al riesgo, sino que también establece las bases para un sistema robusto de gestión de riesgos de TI que incluye actividades específicas de seguimiento, revisión y documentación.

Es importante destacar que, aunque algunas acciones identificadas para cerrar las brechas no se cumplen dentro del alcance del proyecto, estas se justifican como actividades recomendadas para ser abordadas en fases futuras, reflejando el compromiso de la propuesta con la mejora continua y su adaptabilidad a las necesidades organizacionales a largo plazo y logrando así que el proceso propuesto no solo asegure la mitigación de riesgos de TI, sino que también contribuye a la sostenibilidad y resiliencia operativa de la empresa.

Por último, la tabla de cumplimiento evidencia un cambio en el enfoque del proceso actual de la empresa, que ha pasado de ser un proceso completamente reactivo, limitado a la gestión de eventos de riesgos de tipo incidentes, a un proceso integral de gestión de riesgos de TI como tal. Este nuevo enfoque permite no solo reaccionar ante los riesgos que se materializan, sino también gestionar de manera proactiva los riesgos de TI, anticipándose a posibles escenarios y estableciendo estrategias claras para su identificación, evaluación, tratamiento y monitoreo continuo.

5. Propuesta de Solución

En este capítulo se presenta la propuesta de metodología para la gestión de riesgos de TI en la empresa, con el objetivo de establecer un marco estructurado y efectivo que permita identificar, evaluar y mitigar los riesgos relacionados con las tecnologías de información. Esta metodología se desarrolla a partir de una combinación de las mejores prácticas de COBIT 2019 e ISO 31000, integrando los principios y procesos más relevantes de ambos marcos para adaptar la gestión de riesgos a las necesidades específicas de la empresa, por lo que esta propuesta no solo busca alinear la gestión de riesgos con los objetivos estratégicos de la organización, sino también diseñar una cultura de riesgo que facilite una toma de decisiones informada y proactiva en todos los niveles.

5.1. Fase III: Elaboración de los Artefactos para la Metodología de Gestión de Riesgos de TI

La Fase 3 en la propuesta de solución se centra en la elaboración de los artefactos para el diseño de la propuesta de metodología para la gestión de riesgos de TI de la empresa, alineada con sus necesidades específicas. Durante esta fase se crean artefactos específicos para el gobierno de riesgos de TI, siguiendo los lineamientos del dominio EDM03 de COBIT 2019 y se define el proceso de gestión de riesgos de TI, alineado con los estándares de la ISO 31000 y los objetivos de APO12, asegurando un enfoque integral y estandarizado.

Además, se diseña una hoja de ruta detallada para la implementación de la metodología propuesta, estableciendo los pasos necesarios para su ejecución efectiva y proporcionando así una estructura clara y coherente para la gestión de riesgos de TI, lo que facilita su integración con los objetivos estratégicos de la empresa para promover una cultura de gestión de riesgos robusta y proactiva.

Complementariamente, se realiza un análisis de alineación en el que se evaluará tanto el contenido de las mejores prácticas a utilizar como el contenido de la metodología propuesta, para así determinar el nivel de estandarización logrado de la metodología con respecto a las mejores prácticas.

5.1.1. Gobierno de Riesgos de TI

Para implementar una gestión efectiva de riesgos en la empresa, es importante contar con un Gobierno de riesgos de TI que incluya una política definida para orientar la gestión de los riesgos de TI, la cual debe establecer claramente las responsabilidades de todos los roles implicados en el proceso, así como proporcionar los lineamientos y directrices necesarias para garantizar que las actividades de gestión de riesgos se lleven a cabo de manera correcta y conforme a las mejores prácticas y necesidades de la empresa.

Además, la política debe incluir mecanismos para la revisión y actualización continua, asegurando que las prácticas de gestión de riesgos se adapten a los cambios en el entorno de la

organización y los objetivos estratégicos, de tal manera que se cree una estructura de gobierno de TI que promueva la consistencia y efectividad en la gestión de riesgos a lo largo de toda la organización, alineada con los marcos internacionales y los requerimientos específicos de la empresa.

La propuesta de Gobierno de Riesgos de TI se fundamenta en el proceso descrito en la sección 4.3.1.1. Diagrama TO-BE del proceso de Gobierno de TI, el cual establece una estructura clara y detallada para la definición, dirección y monitoreo de la gestión de riesgos en la empresa. Este proceso permite alinear la gestión de riesgos de TI con los objetivos estratégicos de la organización y garantizar un enfoque integral y continuo. A continuación, se proponen los criterios específicos de Gobierno de Riesgos de TI, diseñados según el contexto actual de la empresa y las necesidades identificadas durante el análisis.

5.1.1.1. Apetito y Tolerancia del Riesgo.

La definición del apetito y la tolerancia al riesgo es un paso crucial en la implementación de un proceso efectivo de gestión de riesgos de TI, ya que al establecer claramente estos parámetros, sirven como referencia en la evaluación y tratamiento de los riesgos a lo largo del proceso, siendo el apetito al riesgo el que refleja la cantidad y tipo de riesgo que la organización está dispuesta a aceptar, mientras que la tolerancia al riesgo es el que define los límites específicos dentro de los cuales se considera aceptable la exposición a ciertos riesgos.

Los niveles de tolerancia al riesgo son definidos por el negocio en función de sus necesidades y capacidades, clasificándose en riesgos aceptables y no aceptables según el apetito de riesgo que la empresa haya determinado, lo que permite a la organización priorizar sus esfuerzos y recursos en la gestión de los riesgos más críticos y asegurar que los riesgos que no son aceptables se gestionen de manera proactiva y efectiva. La correcta definición de estos niveles no solo proporciona un marco para la toma de decisiones, sino que también facilita una alineación clara con los objetivos estratégicos del negocio, asegurando que la gestión de riesgos contribuya al éxito organizacional.

Dado que la empresa actualmente no tiene un proceso formal de gestión de riesgos y actúa de manera reactiva solo cuando los riesgos se materializan como incidentes, el nivel de tolerancia al riesgo debería ser conservador y debe enfocarse en minimizar riesgos y establecer una baja tolerancia para cualquier tipo de riesgo que pueda impactar sus operaciones, activos o metas estratégicas. La Tabla 14 presenta la matriz propuesta para el apetito y tolerancia del riesgo, elaborada según las necesidades de la empresa.

Tabla 14: Matriz del apetito y tolerancia del riesgo

Apetito	Tolerancia	Descripción
Bajo	Aceptable	Riesgos con un impacto mínimo que son fácilmente gestionables con las capacidades actuales de la empresa. Se aceptan y se priorizan acciones preventivas para evitar que los riesgos se materialicen.
Moderadamente bajo	Aceptable	Riesgos que tienen un impacto limitado y manejable. Se aceptan, aunque requieren una atención y controles básicos para asegurar que no se agraven.
Moderadamente	No Aceptable	Riesgos que pueden comprometer significativamente las operaciones o los activos de la empresa. No son aceptables dado el nivel actual de gestión y respuesta a los riesgos.
Moderadamente alto	No Aceptable	Riesgos que pueden comprometer significativamente las operaciones o los activos de la empresa. No son aceptables dado el nivel actual de gestión y respuesta a los riesgos.
Muy Alto	No Aceptable	Riesgos con potencial de causar daños graves a la empresa. Requieren una urgente mitigación o evitación debido a la incapacidad de la empresa para gestionar estos riesgos proactivamente.

Nota: Elaboración Propia

La matriz propuesta clasifica el apetito y la tolerancia al riesgo de la empresa en cinco niveles, utilizando un enfoque cualitativo adecuado para el nivel de madurez actual de la gestión de riesgos de TI. Esta clasificación permite identificar rápidamente qué riesgos son aceptables y cuáles requieren acciones inmediatas, haciendo que los niveles más bajos, como "Moderadamente Bajo" y "Bajo," se consideran aceptables, mientras que los niveles superiores no lo son, indicando la necesidad de mitigación o evitación.

Además, es importante tener en cuenta que el dueño del riesgo tiene la flexibilidad de ajustar el nivel de aceptación según las capacidades operativas y necesidades específicas de la empresa, facilitando una gestión de riesgos más adaptativa y contextualizada a las necesidades cambiantes de la empresa.

5.1.1.2. Probabilidad del Riesgo

La probabilidad se refiere a la posibilidad de que un riesgo identificado ocurra y puede ser medida en función de dos aspectos clave: la frecuencia y la factibilidad.

- **Frecuencia:** cantidad de veces que un evento de riesgo podría suceder durante un período específico.

- **Factibilidad:** posibilidad con la que un riesgo podría materializarse dadas las condiciones actuales.

Del mismo modo, hay otras consideraciones que pueden influir en la calificación de la probabilidad del riesgo, tales como:

- **Ambiente externo:** factores como cambios en el mercado, regulaciones nuevas o la modernización de los ciberataques.
- **Capacidades actuales:** preparación de la organización para enfrentar riesgos, incluyendo la existencia de controles adecuados, personal capacitado y tecnología.
- **Historial de incidentes:** la revisión de incidentes pasados puede proporcionar un indicador sobre la frecuencia con que los riesgos similares han ocurrido y qué tan probable es que se repitan.
- **Condiciones operativas:** cambios en la operación, como la implementación de nuevas tecnologías o procesos.

Para establecer la probabilidad de un riesgo, es fundamental definir una escala que refleje los niveles de probabilidad basados en estos factores, la cual se utiliza para evaluar los riesgos y priorizarlos adecuadamente, permitiendo a la empresa focalizar sus esfuerzos en aquellos riesgos que son más probables que ocurran. En la Tabla 15 se presenta la propuesta de escala para calcular la probabilidad del riesgo, ajustada a las capacidades y contexto actual de la empresa, facilitando así un análisis semicuantitativo que se alinea con sus capacidades actuales y necesidades operativas.

Tabla 15: Escala de probabilidad propuesta

Nivel	Valor	Descripción
Improbable	1	Ocurre o podría ocurrir en circunstancias extraordinarias.
Poco probable	2	Ocurre o podría ocurrir alguna vez.
Probable	3	Ocurre o podría ocurrir regularmente.
Muy probable	4	Ocurre o podría ocurrir constantemente.
Altamente probable	5	Ocurre o podría ocurrir casi siempre.

Nota: Elaboración Propia

La tabla presentada proporciona una escala semicuantitativa para evaluar la probabilidad de ocurrencia de los riesgos en la empresa a través de la frecuencia de estos por medio de una escala de cinco niveles que van desde "Improbable" hasta "Altamente probable". Cada nivel está asociado con un valor numérico del 1 al 5 y una descripción que facilita la clasificación de la probabilidad, ayudando a la empresa a estandarizar la evaluación de la probabilidad de que los riesgos ocurran.

5.1.1.3. Impacto del Riesgo

El impacto se refiere a la medida de las consecuencias que un riesgo podría tener sobre los objetivos de la organización si llegara a materializarse y es posible evaluarlo considerando los efectos potenciales en diversas áreas, como las finanzas, la reputación, la operatividad y el cumplimiento regulatorio, sin embargo, la definición y evaluación del impacto pueden variar según las capacidades y el contexto de cada empresa.

En este caso, de acuerdo con las necesidades y la madurez actual de la empresa en la gestión de riesgos, se ha optado por utilizar una escala semicuantitativa para evaluar el impacto de manera práctica y accesible a través de su nivel de impacto en las operaciones, facilitando así la comprensión y aplicación de la evaluación de impacto por parte de los equipos involucrados en la gestión de riesgos de TI. La Tabla 16 presenta la escala propuesta para la evaluación del impacto de los riesgos de TI identificados.

Tabla 16: Escala de impacto propuesta

Nivel	Valor	Descripción
Bajo	1	El impacto generado es casi imperceptible en los procesos de negocio, usuarios y clientes.
Moderado	2	El impacto generado limita la operación en algún área de negocio por un período corto.
Medio	3	El impacto generado afecta a varias áreas del negocio por un período que va de corto a moderado o a procesos vitales por un período corto.
Alto	4	El impacto generado afecta a varias áreas del negocio por un período que va de medio a alto o a procesos vitales por un período prolongado.
Muy alto	5	El impacto generado afecta la continuidad de la operación por horas y hasta días de todos los procesos.

Nota: Elaboración Propia

La tabla de impacto proporciona una escala cualitativa para evaluar el grado de afectación que un riesgo podría tener sobre la empresa, a través de niveles que van desde “Bajo” hasta “Muy alto”, asignando valores del 1 al 5 respectivamente, con descripciones detalladas a través de una escala cualitativa en la afectación operativa de la empresa, que ayudan a entender las posibles consecuencias de cada nivel

5.1.1.4. Nivel del Riesgo

El nivel del riesgo permite determinar la gravedad de un riesgo al combinar dos aspectos clave: la probabilidad de que el riesgo ocurra y el impacto que este tendría en la empresa, multiplicando los valores asignados a la probabilidad y al impacto; y obteniendo como resultado

una cifra que facilita la priorización y el tratamiento de los riesgos, de tal forma que sea posible identificar qué riesgos requieren atención inmediata y cuáles pueden ser gestionados con menor urgencia.

La escala utilizada para definir el nivel del riesgo se basa en las escalas de probabilidad e impacto previamente definidas, y puede ser ajustada para reflejar mejor las necesidades específicas de la empresa y sus políticas internas, permitiéndole adaptar su enfoque de gestión de riesgos de TI en función de su capacidad operativa, la tolerancia al riesgo y otros factores contextuales.

Para este caso, se propone una escala semicuantitativa de 5 niveles que clasifica los niveles del riesgo desde “Bajo” hasta “Muy alto”, facilitando una comprensión clara y directa de la exposición al riesgo de la empresa. La Tabla 17 muestra la escala propuesta para la evaluación de los riesgos según su nivel de probabilidad e impacto.

Tabla 17: Escala de los niveles de riesgo propuestos

Nivel	Calificación
Bajo	Menor que 3.
Moderadamente bajo	Mayor o igual que 3, pero menor que 5.
Moderado	Mayor o igual que 5, pero menor que 10.
Moderadamente alto	Mayor o igual que 10, pero menor que 20.
Muy Alto	Mayor o igual que 20.

Nota: Elaboración Propia

Una vez identificado el nivel del riesgo mediante la combinación de la probabilidad y el impacto, es posible visualizar estos riesgos de manera gráfica utilizando un mapa de calor, el cual consiste en una herramienta visual clave que facilita la comprensión y priorización de los riesgos, al representar gráficamente dónde se concentran los riesgos más críticos en una matriz que cruza la probabilidad y el impacto, permitiendo así tomar decisiones informadas sobre las acciones de mitigación y priorización de recursos. La Tabla 18 presenta el mapa de calor propuesto para ubicar los riesgos según el nivel determinado.

Tabla 18: Mapa de calor propuesto

		Impacto				
		Bajo	Moderado	Medio	Alto	Muy alto
Probabilidad	**Valor**	**1**	**2**	**3**	**4**	**5**
Improbable	**1**					
Poco probable	**2**					
Probable	**3**					
Muy probable	**4**					
Altamente probable	**5**					

Nota: Elaboración Propia

5.1.1.5. Frecuencia del Seguimiento de Riesgos

Definir la frecuencia de seguimiento de los riesgos es un paso crucial en la gestión efectiva de riesgos de TI, ya que permite a la organización priorizar y adaptar los controles, medidas y planes de contingencia según la criticidad y evolución de cada riesgo, por lo que, establecer una periodicidad adecuada para la revisión y monitoreo de los riesgos asegura que la empresa no solo responda a los riesgos de manera proactiva, sino que también anticipe y mitigue posibles amenazas antes de que se materialicen.

Este proceso permite ajustar los recursos y esfuerzos de gestión de acuerdo con la magnitud y complejidad de los riesgos enfrentados, alineando la estrategia de respuesta con los objetivos organizacionales y las capacidades operativas de la empresa. Entonces, la correcta definición de estas frecuencias, basada en el apetito y tolerancia al riesgo previamente establecidos, es esencial para mantener la resiliencia y continuidad de las operaciones, priorizando los riesgos más críticos y asegurando una gestión proactiva y efectiva. La Tabla 19 presenta la frecuencia de seguimiento a riesgos propuesta según el nivel del riesgo definido en el apetito.

Tabla 19: Matriz de frecuencia del seguimiento del riesgo propuesta

Nivel del riesgo	Frecuencia de seguimiento	Revisiones necesarias	Indicadores
Bajo	Semestral	Revisión de estado general y validación de medidas.	- Frecuencia de incidentes. - Cumplimiento de procesos.
Moderadamente bajo	Trimestral	Asegurar que las medidas preventivas siguen en efecto.	- Tasa de errores menores. - Uso de recursos para mitigación.

Nivel del riesgo	Frecuencia de seguimiento	Revisiones necesarias	Indicadores
Moderado	Mensual	Verificar efectividad de los controles establecidos.	- Cantidad de desviaciones en los procesos de gestión.
Moderadamente alto	Mensual	Revisar controles y ajustar según cambios operativos.	- Frecuencia de eventos de alto impacto. - Frecuencia de revisiones de controles.
Muy Alto	Mensual	Evaluar mitigación y planes de contingencia urgentes.	- Número de incidentes críticos. - Tiempo de respuesta.

Nota: Elaboración Propia

Además de la frecuencia de seguimiento del riesgo, la matriz propuesta incluye dos columnas adicionales: "Revisiones necesarias" e "Indicadores". Estas columnas se han añadido con el objetivo de proporcionar una guía más detallada sobre las revisiones específicas a realizar y los indicadores clave a monitorear, según el nivel de riesgo, ya que las revisiones y los indicadores propuestos están diseñados para alinearse con las necesidades actuales de la empresa en términos de gestión del riesgo, y buscan mejorar el seguimiento y la gestión de estos.

Del mismo modo, es importante resaltar que, aunque la frecuencia de seguimiento está predeterminada según el nivel de riesgo, este enfoque permite la flexibilidad para que el dueño del riesgo ajuste la frecuencia si lo considera necesario, adaptándola a la criticidad o particularidades del riesgo en cuestión. Esta flexibilidad asegura una gestión más dinámica y efectiva de los riesgos dentro de la empresa.

5.1.1.6. Controles

Los controles son medidas o acciones implementadas para modificar, mitigar, o manejar los riesgos identificados y pueden incluir políticas, procedimientos, prácticas, o estructuras organizativas diseñadas para reducir la probabilidad y/o el impacto de riesgos identificados, por lo que una implementación y evaluación efectiva de los controles es esencial para asegurar que los riesgos se mantengan dentro de los límites de tolerancia establecidos por la organización y para apoyar el logro de sus objetivos estratégicos, aparte de que estos ayudan a determinar con precisión el riesgo residual, que es el nivel de riesgo que persiste después de aplicar los controles.

Ahora bien, la identificación y evaluación de los controles es una actividad clave para asegurar que los riesgos sean gestionados de manera efectiva y se mantengan dentro de los niveles aceptables definidos por la organización por lo que, para la correcta identificación y evaluación de estos, se proponen las siguientes actividades clave:

- **Identificación de controles existentes:** evaluar los controles ya implementados en la organización que puedan influir en la gestión de riesgos.
- **Evaluación de la eficacia de los controles:** analizar la efectividad de los controles existentes en términos de su capacidad para reducir la probabilidad o el impacto de los riesgos.
- **Identificación de brechas en los controles:** identificar áreas donde los controles son insuficientes o inexistentes.
- **Clasificación y priorización de controles:** clasificar los controles según su importancia y efectividad para gestionar los riesgos, priorizando los controles críticos que requieren una supervisión más estricta o una mejora inmediata.
- **Documentación de controles:** registrar todos los controles identificados y evaluados, incluyendo su descripción, objetivo, propietario, y la evaluación de su efectividad.

Aparte de esto, para evaluar los controles identificados, se propone una serie de aspectos que la empresa debe tener en consideración:

- **Alineación con objetivos de negocio:** asegurarse de que los controles apoyen directamente los objetivos estratégicos y operativos de la empresa.
- **Cultura organizacional:** considerar cómo la cultura y la estructura organizacional pueden afectar la efectividad de los controles.
- **Cambios en el entorno:** evaluar cómo los cambios en el entorno de riesgos de TI (internos o externos) pueden impactar la efectividad de los controles existentes.
- **Coste contra beneficio:** analizar el coste de implementar o mantener un control frente al beneficio que proporciona en términos de reducción de riesgos de TI.
- **Adaptabilidad y flexibilidad:** asegurarse de que los controles sean lo suficientemente flexibles para adaptarse a los cambios del entorno de riesgos de TI.

Para la documentación de los controles definidos por la empresa, se presenta una propuesta de plantilla para la identificación y evaluación de controles, la cual incluye una propuesta de datos predefinidos según las capacidades actuales que presenta la empresa, sin embargo, estos datos y columnas pueden cambiar y adecuarse a sus futuras necesidades. La Figura 36 presenta una imagen de la plantilla propuesta junto a la visualización de cada menú desplegable que incluye.

Figura 35: Plantilla propuesta para la identificación y evaluación de controles

Nota: Elaboración Propia

A continuación, se explican las columnas de esta plantilla:

- **ID del control:** identificador único para cada control.
- **Nombre del control:** nombre breve y descriptivo del control.
- **Descripción:** resumen claro y conciso de la función del control.
- **Objetivo**: resultado esperado del control, por ejemplo, mitigar un riesgo específico.
- **Tipo de control:** clasificación del control como preventivo, correctivo o detectivo.
- **Responsable:** área o persona encargada del control.
- **Efectividad:** evaluación del control.
- **Frecuencia de revisión:** periodicidad con la cual se revisa el control.
- **Acciones correctivas:** medidas para mejorar el control según la evaluación.

Ahora bien, para la evaluación de los controles es esencial contar con una escala de evaluación clara y adecuada a las capacidades y necesidades de la empresa, de esta manera, la escala propuesta en la Tabla 20, proporciona cinco niveles de evaluación que van desde "Inefectivo" hasta "Totalmente efectivo" a través de una valoración cualitativa y comprensible del desempeño de los controles, asegurando no solo que los controles implementados estén alineados

con los objetivos de gestión de riesgos de TI de la empresa, sino que también funcionan de manera eficaz para mantener los riesgos dentro de los límites de tolerancia definidos.

Tabla 20: Escala de evaluación de controles

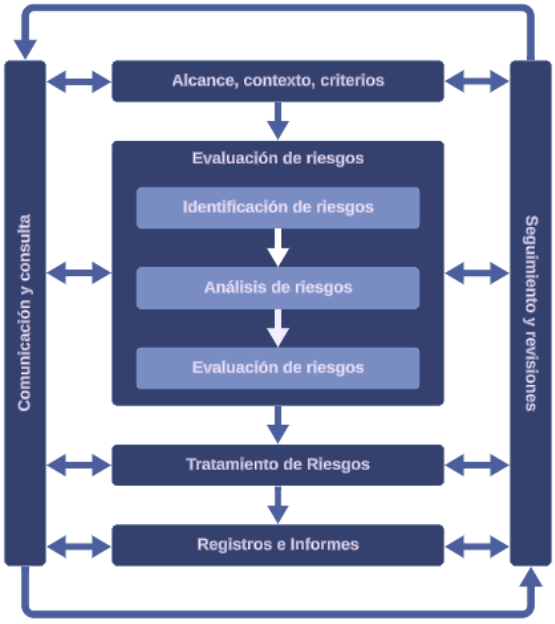
Nivel	Valor	Descripción
Inefectivo	1	El control no cumple con su propósito y no logra mitigar el riesgo asociado. Se requiere una revisión completa y rediseño del control.
Necesita mejora significativa	2	El control tiene deficiencias importantes que limitan su efectividad. Se requiere mejoras sustanciales para que el control funcione adecuadamente.
Parcialmente efectivo	3	El control cumple parcialmente con su propósito. Mitiga el riesgo de manera limitada y necesita ajustes menores para ser completamente efectivo.
Mayormente efectivo	4	El control funciona bien y mitiga la mayoría del riesgo asociado, pero aún puede optimizarse para mejorar su efectividad.
Totalmente efectivo	5	El control cumple completamente con su propósito, mitiga el riesgo de manera efectiva y no se requieren mejoras adicionales.

Nota: Elaboración Propia

5.1.2. Proceso de Gestión de Riesgos de TI

El proceso de gestión de riesgos de TI constituye el núcleo principal de la metodología propuesta, ya que detalla el ciclo de gestión de riesgos que la empresa debe seguir para una gestión efectiva de los riesgos de TI. Este ciclo de gestión de riesgos de TI está constituido según los lineamientos de COBIT 2019 y se estructura de acuerdo con las fases de gestión del riesgo establecidas por la ISO 31000: alcance, contexto y criterios; evaluación de riesgos, que abarca la identificación, análisis y evaluación de los riesgos; tratamiento de riesgos, comunicación y consulta, además de seguimiento y revisiones. La Figura 37 presenta el proceso propuesto para la metodología.

Figura 36: Proceso de gestión de riesgos de TI propuesto para Information Evolution Costa Rica



Nota: Adaptado de (ISO, 2018, p. 5)

Estas fases trabajan en conjunto para garantizar una gestión de riesgos integral y alineada con los objetivos estratégicos de la empresa, de tal manera que cumpla con una estructura completa para la correcta gestión de riesgos de TI según lo que dictan las mejores prácticas. Este proceso propuesto está alineado con el proceso descrito en la sección 4.3.1.2. Diagrama TO-BE del proceso de Gestión de Riesgos de TI según las directrices propuestas por la ISO 31000.

A continuación, se detallan cada una de estas con sus respectivos artefactos desarrollados para la metodología.

5.1.2.1. Alcance, contexto y criterios

Esta fase proporciona un marco claro y definido dentro del cual se llevará a cabo todo el proceso de gestión de riesgos de TI, asegurando que los riesgos sean gestionados en función de los objetivos organizacionales y las capacidades actuales de la empresa. A continuación, se detalla cada una de las tres secciones clave: Alcance del proceso, Contexto y Criterios de evaluación.

5.1.2.1.1. Alcance

El Alcance del proceso de gestión de riesgos de TI define los límites y áreas que serán abarcadas por la metodología propuesta, asegurando que todos los elementos críticos de la gestión de riesgos TI sean cubiertos de acuerdo con las necesidades de la empresa. En este caso, el alcance abarca lo propuesto en las fases de identificación, análisis, tratamiento, seguimiento y registro de los riesgos de TI, las cuales se explican a lo largo de esta propuesta de solución, así como el

establecimiento de un marco de gobernanza alineado con las mejores prácticas establecido en la sección anterior de Gobierno de riesgos de TI y la definición de la estructura del equipo de trabajo para la implementación de la metodología.

Es importante resaltar que este alcance proporciona una estructura integral para la gestión de riesgos de TI, considerando las debilidades actuales de la empresa analizadas en la Fase I: Análisis de la situación actual del proceso de gestión de riesgos de TI, de tal manera que se desarrolle un proceso que sea práctico, ajustado a las necesidades y que fomente una gestión proactiva y madura a largo plazo, es por esto que sus artefactos también son adaptados a este contexto y habilidades de la empresa.

5.1.2.1.2. Contexto

El Contexto define tanto al entorno interno como externo en el cual la empresa opera y que influye en la manera en que los riesgos de TI son percibidos y gestionados, ayudando a garantizar que la gestión de riesgos esté alineada con los objetivos estratégicos de la organización.

A continuación, se presentan una serie de propuestas a tomar en cuenta por la empresa tanto para el contexto externo como el interno, las cuales fueron consideradas para el desarrollo de la propuesta:

5.1.2.1.2.1. Contexto externo

El contexto externo abarca las regulaciones, el entorno competitivo y otros factores externos que afectan la gestión de riesgos. Actualmente la empresa se encuentra en un entorno influenciado por varios factores externos, que pueden impactar sus operaciones de TI y aumentar la probabilidad de ocurrencia de ciertos riesgos. Algunos de los contextos externos que deben ser considerados son:

- **Cambios regulatorios y legales:** dado que la empresa opera en un entorno que está sujeto a regulaciones sobre la protección de datos y la seguridad cibernética, cualquier modificación o nueva ley podría afectar directamente el proceso de gestión de riesgos de TI.
- **Factores económicos:** un cambio en la estabilidad económica del país puede impactar el presupuesto disponible para la gestión de TI, afectando la capacidad de la empresa para implementar controles efectivos.
- **Amenazas cibernéticas:** el aumento de ciberataques puede elevar el nivel de exposición de la empresa a riesgos de seguridad.
- **Avances tecnológicos:** la empresa debe tener en cuenta que los avances tecnológicos rápidos, como la introducción de nuevas tecnologías emergentes, pueden representar tanto una oportunidad como un riesgo si no se gestionan adecuadamente.

- **Condiciones ambientales:** los desastres naturales o condiciones ambientales extremas pueden afectar la infraestructura de TI y provocar interrupciones en los servicios.

5.1.2.1.2.2. Contexto interno

El contexto interno involucra las capacidades actuales, los recursos disponibles y la estructura organizacional, y, en este caso la empresa no cuenta actualmente con un proceso maduro de gestión de riesgos de TI, por lo que algunos de los contextos internos que deben ser considerados son:

- **Infraestructura de TI limitada:** la empresa maneja su infraestructura de TI de manera reactiva y sin un proceso claro para identificar o mitigar riesgos.
- **Recursos humanos:** existe una falta de personal capacitado para la gestión de riesgos de TI, lo que podría limitar la capacidad de implementar controles adecuados o llevar a cabo un monitoreo efectivo de los riesgos.
- **Cultura organizacional:** la resistencia al cambio y una baja madurez en la cultura de gestión de riesgos de TI dificultan la adopción de prácticas más proactivas.
- **Políticas y procedimientos no formales:** aunque la empresa reconoce la importancia de la gestión de riesgos de TI, actualmente no cuenta con políticas formalizadas, lo que crea brechas en la identificación y respuesta a los riesgos.

Ahora bien, para la definición de los contextos que afectan a la organización, se propone la plantilla definida en la Tabla 21.

Tabla 21: Definición del contexto interno y externo

Elemento del Contexto	Descripción	Situación Actual	Observaciones

Nota: Elaboración Propia

La tabla presenta una estructura que facilita la identificación y evaluación del contexto interno y externo de la empresa en relación con la gestión de riesgos de TI, permitiendo tener una visión más clara y organizada de los factores que influyen en la gestión de riesgos y las posibles acciones a tomar. A continuación, se explica lo que debe incluirse en cada columna:

- **Elemento del Contexto:** se debe identificar el factor clave que influye en la gestión de riesgos, como recursos internos, regulaciones externas, o factores tecnológicos.
- **Descripción:** breve explicación de lo que implica el contexto, especificando qué incluye o qué aspecto cubre.
- **Situación Actual:** estado actual de la empresa respecto al contexto. Por ejemplo, si la empresa está preparada o enfrenta desafíos específicos en ese ámbito.
- **Observaciones:** comentarios adicionales o recomendaciones, como sugerencias para mejorar, acciones futuras, o notas importantes relacionadas con el contexto.

5.1.2.1.3. Criterios

Los criterios de evaluación de riesgos de TI establecen los parámetros mediante los cuales los riesgos serán analizados y valorados, definiendo las pautas para determinar qué riesgos son aceptables y cuáles no, en función del apetito y tolerancia de riesgo, aparte de sus niveles de riesgo previamente definidos en la sección de Gobierno de Riesgos de TI.

5.1.2.2. Evaluación del riesgo

La sección de evaluación del riesgo se centra en comprender y manejar los riesgos que podrían afectar los objetivos de la empresa y se divide en tres fases clave: la identificación de los riesgos, el análisis de los riesgos y la evaluación de los riesgos. Estas fases permiten identificar los riesgos potenciales, analizar su impacto y probabilidad, y determinar cuáles requieren acciones adicionales para ser gestionados de manera efectiva, asegurando una gestión de riesgos estructurada y alineada con los objetivos organizacionales.

Esta etapa del proceso se integra de manera transversal con la fase de Registro e Informes, cuya explicación detallada se encuentra más adelante en este documento. Durante esta etapa, los resultados, hallazgos y cualquier información relevante obtenida en cada una de las actividades que se proponen deben ser documentados de manera sistemática y estructurada utilizando la plantilla específicamente propuesta para esta fase.

Adicionalmente, la plantilla propuesta en la sección de Registro e Informes detalla los elementos clave que deben ser incluidos para cumplir con los estándares de mejores prácticas y las necesidades específicas de la empresa. En dicha sección se explica el contenido de esta plantilla, así como las instrucciones para su correcto uso, asegurando que el registro de información sea consistente, completo y útil.

5.1.2.2.1. Identificación de los riesgos

La identificación de los riesgos consiste en reconocer y registrar todos los riesgos potenciales que podrían afectar los objetivos de la organización en caso de que lleguen a ocurrir, lo que permite anticiparse a posibles eventos adversos y oportunidades, proporcionando la base para la evaluación y tratamiento de los riesgos. Identificar correctamente los riesgos asegura que

la empresa pueda gestionar de manera proactiva sus amenazas, reduciendo la probabilidad de impactos negativos y fortaleciendo su resiliencia operativa.

5.1.2.2.1.1. Herramientas para la identificación de riesgos

Las herramientas para la identificación de riesgos permiten estructurar y sistematizar la manera en que se identifican los posibles riesgos, por lo que facilita la recolección de datos, fomenta la participación del equipo y asegura que se consideren diferentes perspectivas, mejorando no solo la precisión en la identificación de riesgos, sino que también incrementa la efectividad del proceso al proporcionar un enfoque claro para detectar posibles riesgos.

A continuación, se proponen una serie de herramientas para facilitar el proceso de identificación de riesgos según el contexto de la empresa analizado en la situaciónón actual del análisis de resultados:

- **Listas de verificación:** ayudan a sistematizar la identificación de riesgos al proporcionar un conjunto predefinido de riesgos comunes que se pueden revisar regularmente.
- **Entrevistas y encuestas:** recolectan información directamente de los empleados e interesados clave sobre posibles riesgos en sus áreas de trabajo o experiencia.
- **Análisis FODA (Fortalezas, Oportunidades, Debilidades y Amenazas**): facilita la identificación de riesgos al analizar tanto los factores internos como externos que pueden influir en la empresa.
- **Grupos focales:** reúnen a grupos de trabajo para identificar riesgos de manera colaborativa, aprovechando la experiencia colectiva y diversa de los participantes.
- **Lluvia de ideas:** promueve la generación rápida de ideas y posibles riesgos en sesiones abiertas, permitiendo una identificación creativa y participativa de riesgos.

5.1.2.2.1.2. Fuentes de información para la identificación de riesgos

Las fuentes de información proporcionan los datos y el contexto necesarios para reconocer de manera efectiva los riesgos potenciales, es por esto que la diversidad y calidad de las fuentes utilizadas influyen directamente en el nivel de detalle y precisión del proceso de identificación, ofreciendo una base sólida para comprender tanto los riesgos internos como los externos, y permitiendo a la empresa anticiparse a las amenazas y adaptar sus estrategias de gestión de riesgos de manera proactiva y bien informada.

A continuación, se proponen una serie de fuentes de información para facilitar el proceso de identificación de riesgos según el contexto de la empresa:

- **Reportes y datos históricos de incidentes:** revisar incidentes pasados ayuda a identificar patrones de riesgo y áreas recurrentes de vulnerabilidad en la organización.

- **Auditorías y evaluaciones internas:** proporcionan una visión detallada de los procesos y controles existentes, revelando posibles áreas de riesgo.
- **Normativas y estándares de la industria:** consultar guías y estándares internacionales ayuda a identificar riesgos comunes y alinearse con las mejores prácticas.
- **Revisión de cambios en el entorno externo:** analizar factores externos como cambios regulatorios, económicos o tecnológicos que podrían introducir nuevos riesgos para la empresa.
- **Revisión de los objetivos estratégicos de la empresa:** alinear la identificación de riesgos con los objetivos organizacionales asegura que se consideren los riesgos de TI más críticos para el éxito del negocio.
- **Informes externos:** analizar informes de la industria y análisis de riesgos que afectan a otras empresas del sector, proporcionando una perspectiva más amplia.
- **Resultados de benchmarking:** comparar las prácticas de gestión de riesgos de la empresa con las de sus competidores o líderes del sector, identificando áreas de mejora y riesgos potenciales.

5.1.2.2.1.3. Escenarios de riesgos

Los escenarios de riesgos proporcionan una representación detallada y estructurada de posibles eventos adversos que podrían afectar a la organización, lo que permite a las empresas anticiparse a situaciones potenciales, evaluando tanto la probabilidad como el impacto de estos eventos sobre los objetivos estratégicos, operacionales y de TI.

Estos escenarios se utilizan para identificar riesgos específicos relacionados con la tecnología de la información y su alineación con los objetivos del negocio, facilitando la comunicación sobre los riesgos, ya que describen situaciones comprensibles que ayudan a todas las partes interesadas a entender los posibles desafíos y a participar activamente en la planificación de respuestas adecuadas.

Ahora bien, para la creación de escenarios de riesgos la guía de ISACA propone incluir los siguientes componentes que se presentan en la Tabla 22.

Tabla 22: Componentes de los escenarios de riesgos

Componente	Descripción	Posibles opciones
Tipo de amenaza	Identifica la naturaleza del riesgo.	- Malicioso - Accidental - Fallo del sistema - Errores humanos - Fallo de procesos - Naturales

Componente	Descripción	Posibles opciones
Actor	Determina quién o qué podría causar el riesgo.	- Interno - Externo - Automatización fallida
Acción	Describe la acción que lleva al riesgo.	- Divulgación de información - Interrupción de servicios - Modificación no autorizada - Robo de datos - Destrucción de activos - Uso indebido
Activos/Recursos	Especifica los activos afectados por el riesgo.	- Personas - Procesos - Tecnología (hardware, software) - Información confidencial - Infraestructura (red, servidores)
Tiempo	Define el contexto temporal del riesgo.	- Corto plazo (0-3 meses) - Mediano plazo (3-12 meses) - Largo plazo (>12 meses) - Momento específico (calendario de incidencias críticas)

Nota: Elaboración Propia

Ahora bien, la creación de escenarios de riesgo se puede abordar desde dos enfoques diferentes: de arriba hacia abajo (descendente) y de abajo hacia arriba (ascendente), brindando a la empresa una guía estructurada para identificar y priorizar los riesgos de TI que pueden impactar en los objetivos de negocio y adaptándose a las necesidades y características específicas de la empresa. A continuación, en la Tabla 23, se explica cada enfoque:

Tabla 23: Enfoques para la creación de escenarios

Enfoque	Descripción	Importancia
Descendente	Se parte de los objetivos generales de la organización y busca identificar los escenarios de riesgo de TI más relevantes y probables que podrían afectar dichos objetivos.	Al alinear los criterios de impacto con los verdaderos controladores de valor de la organización, se asegura de que los escenarios de riesgo sean relevantes y estén bien enfocados en los aspectos críticos del negocio, permitiendo a la empresa concentrarse en los riesgos que realmente pueden influir en el logro de sus metas estratégicas, facilitando una gestión de riesgos más efectiva y alineada con sus prioridades corporativas.

Ascendente	Se parte de una lista de escenarios genéricos y se trabaja para definir un conjunto de escenarios más específicos y personalizados que se adapten a la situación particular de la organización.	Implica tomar escenarios de riesgo comunes en el ámbito de TI y ajustarlos para reflejar las condiciones y necesidades específicas de la empresa, lo que ayuda a identificar riesgos que podrían no ser inmediatamente obvios desde una perspectiva estratégica, pero que tienen un impacto significativo en la operación diaria.

Nota: Elaboración Propia

Para el contexto de la empresa, ambos enfoques pueden ser valiosos en la generación de escenarios de riesgo, ya que, al utilizar un enfoque descendente, la empresa puede comenzar con sus objetivos de negocio clave y evaluar cómo los riesgos de TI podrían afectarlos directamente, asegurando que los esfuerzos de gestión de riesgos estén alineados con sus metas estratégicas. Por otro lado, el enfoque descendente le permite a la empresa tomar escenarios genéricos de la industria de TI y adaptarlos a su contexto particular, ayudando a identificar riesgos específicos que podrían ser pasados por alto si solo se centraran en los objetivos de negocio. Sin embargo, es posible combinar ambos enfoques, asegurando que la empresa desarrolle una visión completa y bien equilibrada de los riesgos de TI.

Por último, para la descripción de los riesgos se recomienda utilizar la estructura de ***Causa*** **+** ***Evento*** **+** ***Impacto***, en donde la causa hace referencia a qué provoca el riesgo, el evento lo que puede ocurrir y el impacto la manera en que este afecta en los objetivos. Esta descripción del riesgo se debe documentar en la plantilla propuesta en la sección de Registro e Informes, la cual se explicará en la sección 5.1.2.4 del documento.

5.1.2.2.2. Análisis de los riesgos

El análisis de riesgos consiste en evaluar la probabilidad de ocurrencia y el impacto potencial de los riesgos identificados, permitiendo priorizar los riesgos y tomar decisiones informadas sobre cómo gestionarlos, asegurando que los recursos se asignen de manera eficiente para mitigar o controlar aquellos riesgos que podrían afectar significativamente a la empresa y su importancia radica en su capacidad para proporcionar una comprensión clara y cuantificable del perfil de riesgo de la empresa, lo cual es fundamental para la toma de decisiones estratégicas.

Ahora bien, es esencial no solo evaluar la probabilidad e impacto de los riesgos, sino también identificar y evaluar los controles existentes correspondientes a las medidas, políticas o procedimientos implementados para reducir o mitigar los riesgos, disminuyendo así su probabilidad de ocurrencia o su impacto en caso de materializarse y permitiendo identificar su efectividad y determinar si son suficientes o si se necesitan ajustes adicionales para manejar los riesgos de manera adecuada.

Dado el nivel de madurez y las capacidades actuales de la empresa en la gestión de riesgos de TI, la propuesta de análisis debe estar adaptada a sus necesidades y recursos disponibles, es por

esto que la propuesta de análisis de riesgos presentada se enfoca en métodos cualitativos y en la utilización de herramientas y procesos que son manejables y prácticos para la empresa, alineándose con su contexto operativo y capacidad de implementación.

5.1.2.2.2.1. Probabilidad

Determinar la probabilidad de ocurrencia de un riesgo identificado es de suma importancia para realizar un análisis y evaluación precisos de su nivel mediante una puntuación que permite establecer qué tan probable es que el riesgo se materialice, lo cual es crucial para la priorización de su tratamiento. Para esta evaluación, se propone utilizar la escala de probabilidad previamente definida en la sección 5.1.2.2. del Gobierno de riesgos de TI. Una vez calculado el nivel de probabilidad del riesgo, se procede con el análisis del siguiente factor clave para la determinación del nivel del riesgo de TI.

5.1.2.2.2.2. Impacto

El impacto de un riesgo de TI identificado es el segundo factor fundamental para realizar un análisis y evaluación precisos del nivel del riesgo. Este proceso, mediante una puntuación, permite establecer qué tan grave serían las consecuencias si el riesgo se materializa, lo cual es crucial para la priorización de su tratamiento. Para esta evaluación, se propone utilizar la escala de impacto previamente definida en la sección 5.1.2.3. del Gobierno de riesgos de TI. Una vez calculado el nivel de impacto del riesgo, se procede a determinar el nivel del riesgo.

5.1.2.2.2.3. Nivel del riesgo

Una vez determinado el valor de la probabilidad y del impacto del riesgo se calcula el nivel de este riesgo a través de la multiplicación del valor asignado a la probabilidad de ocurrencia por el valor asignado al impacto del riesgo de ser el caso que se siga el mecanismo propuesto, si este cambiara se realizaría el cálculo definido. El resultado de esta operación determina el nivel de riesgo, el cual se clasifica según la escala propuesta en la sección 5.1.2.4 del Gobierno de riegos de TI. Este nivel indica cómo está el riesgo según los niveles de apetito y tolerancia de la empresa y dan paso a la definición de su tratamiento.

Entonces, una vez identificado el nivel del riesgo, el uso del mapa de calor permite identificar rápidamente qué riesgos requieren atención inmediata y cuáles pueden ser gestionados con un enfoque menos intensivo brindando una priorización previa de los riesgos, y, a partir de esto, se obtiene tanto el riesgo inherente como el riesgo residual.

Ahora bien, cabe destacar que el riesgo inherente consiste en el nivel de riesgo que se obtiene al multiplicar los valores de probabilidad e impacto, y representa la exposición al riesgo sin tener en cuenta ninguna medida de control que la organización haya implementado, reflejando qué tan vulnerables son los procesos o activos de la empresa en ausencia de controles preventivos o correctivos. Por otro lado, el riesgo residual es el nivel de riesgo que permanece después de

aplicar los controles y medidas de mitigación que la organización ha definido previamente, ya que considera la eficacia de los controles existentes y se ajusta para reflejar la reducción del riesgo gracias a estas medidas.

5.1.2.2.2.4. Valoración de controles

La asignación de un valor de efectividad a los controles ayuda a reducir el nivel de riesgo inherente previamente determinado, permitiendo así el cálculo del riesgo residual, sin embargo, la forma en que se combina el nivel de riesgo inherente con la evaluación de los controles para definir el riesgo residual depende del enfoque de gestión de riesgos de TI definido por la organización. Para esta identificación y evaluación de controles, se proponen las plantillas definidas en la sección 5.1.2.6. del Gobierno de riesgos de TI.

Generalmente, el riesgo residual se calcula restando el valor de efectividad de los controles al valor obtenido del riesgo inherente, obteniendo un resultado que refleja el nivel de riesgo que persiste tras considerar los controles, o sea, el riesgo residual, el cual es el enfoque para el cálculo que se recomienda para la empresa. Sin embargo, en algunos casos, los valores de los controles pueden promediarse o normalizarse para alinearse con la escala del nivel de riesgo, o bien, se puede utilizar una fórmula específica para este propósito según se alinee con las políticas de gestión de riesgos de TI establecidas por la organización, así como con las regulaciones y normativas a las que la empresa debe adherirse de existir el caso.

5.1.2.2.3. Evaluación de los riesgos

En la evaluación de los riesgos, se comparan los niveles de riesgo obtenidos con los criterios de tolerancia y apetito del riesgo definidos por la organización, permitiendo determinar la prioridad de los riesgos y establecer la respuesta más adecuada para cada uno. Este proceso asegura que las decisiones sobre los riesgos se tomen de manera consistente, basadas en un marco claro y alineado con la tolerancia al riesgo y los objetivos del negocio, además de facilitar la priorización de los recursos y esfuerzos hacia los riesgos que representan mayores amenazas para la organización.

Para efectos del contexto actual de la empresa, se propone una división de este punto en tres actividades, las cuáles se explican a continuación:

5.1.2.2.3.1. Comparación con criterios de riesgo

Los riesgos son evaluados en función de los criterios establecidos durante el análisis de los riesgos de la gestión de riesgos y el apetito y tolerancia al riesgo definidos, previo al proceso, reflejando así el apetito y la tolerancia al riesgo de la organización, así como sus objetivos estratégicos, lo que ayuda a identificar cuáles riesgos están por encima o por debajo del umbral aceptable y cuáles requieren una acción inmediata.

5.1.2.2.3.2. Priorización de los riesgos

Una vez determinado el nivel del riesgo en función con el apetito y tolerancia de la empresa, se realiza una priorización basada en la severidad del impacto y la probabilidad del riesgo, clasificando los riesgos desde los más críticos hasta los menos significativos, lo que ilustra el orden en que se abordarán los riesgos, optimizando la asignación de recursos. En este caso, los riesgos con valor 5 en la escala de probabilidad e impacto se priorizan sobre aquellos con menor valor de impacto y probabilidad, para esto, se recomienda el uso del mapa de calor para ver esta priorización de manera gráfica y clara.

5.1.2.2.3.3. Decisiones de tratamiento de riesgos

Basado en la evaluación realizada, se decide el curso de acción para cada riesgo: evitar, mitigar, transferir o aceptar el riesgo, dependiendo de los niveles de tolerancia de la empresa, entonces, los riesgos que excedan el nivel de apetito del riesgo definido necesitan planes de tratamiento de riesgos, los cuales se analizarán en la siguiente sección.

5.1.2.3. Tratamiento de riesgos

El tratamiento de riesgos permite a las organizaciones abordar y gestionar los riesgos identificados de manera proactiva, brindando la capacidad de evitar, mitigar, transferir o aceptar riesgos de TI, con el fin de alinearlos con los niveles de tolerancia establecidos y minimizar los posibles impactos negativos en la organización, de tal forma que se puedan implementar medidas específicas para reducir los riesgos a niveles aceptables, asegurando así la continuidad de las operaciones y el cumplimiento de sus objetivos estratégicos.

Para guiar el proceso de tratamiento de riesgos en este proyecto, es esencial definir claramente las diferentes respuestas para gestionar los riesgos de TI. En la Tabla 24, se presentan las distintas opciones de respuesta a riesgos que se propone utilizar y su descripción.

Tabla 24: Respuesta a riesgos

Estrategia	Descripción
Evitar	Implica dejar de realizar actividades o evitar condiciones que generan el riesgo, especialmente cuando no hay otras medidas efectivas disponibles.
Mitigar	Consiste en tomar acciones que reduzcan la probabilidad o el impacto de un riesgo, como fortalecer prácticas de gestión o implementar controles específicos.
Transferir	Se trata de disminuir el riesgo al transferir o compartir parte de este con otras partes, como mediante seguros o subcontrataciones.
Aceptar	Es la decisión consciente de no tomar medidas para mitigar un riesgo específico, aceptando las posibles pérdidas si llegaran a ocurrir.

Nota: Elaboración Propia

Ahora bien, para la selección de la respuesta al riesgo, se proponen una serie de factores a considerar de tal forma que se asegure que la selección de la respuesta no solo sea adecuada en el momento de su implementación, sino también sostenible y adaptable a medida que cambian las condiciones del entorno de riesgo y los objetivos de la empresa. Estos factores se explican a continuación:

- **Eficiencia de la respuesta:** evaluar qué tan efectiva es la respuesta para mitigar o eliminar el riesgo a través de la comparación de distintas respuestas, permitiendo identificar cuál ofrece la mayor reducción del riesgo con el menor costo y esfuerzo posible.
- **Posición del riesgo en el mapa:** se refiere a la ubicación del riesgo en el mapa de calor de riesgos, lo cual indica su gravedad y prioridad, es por esto que su comprensión ayuda a asegurar que la respuesta seleccionada esté alineada con la criticidad del riesgo y su potencial impacto en la organización.
- **Capacidad de la organización:** no todas las respuestas a riesgos son factibles para todas las organizaciones, es por esto que se debe evaluar si la organización cuenta con los recursos, capacidades técnicas y personal adecuado para implementar la respuesta de manera efectiva.
- **Efectividad de la respuesta:** la respuesta debe ser capaz de reducir el riesgo a un nivel aceptable según los criterios establecidos por la organización, en este caso se debe determinar cómo impactará la respuesta el nivel de riesgo y asegurarse de que se alinea con los objetivos de gestión de riesgos de TI, manteniéndolo dentro de los límites de tolerancia definidos.
- **Flexibilidad y adaptabilidad de la respuesta:** considerar si la respuesta puede ajustarse a cambios futuros en el entorno de riesgo de TI o en las operaciones de la organización.

Dado que los recursos organizacionales son limitados, no siempre es posible implementar todas las medidas de tratamiento de riesgos identificadas, en especial en el contexto de la empresa, es por esto que es recomendable priorizar las respuestas según las necesidades y criterios definidos por la organización, considerando el contexto organizacional y el apetito al riesgo. La Tabla 25 proporciona una propuesta de tres niveles para la priorización de las respuestas a los riesgos.

Tabla 25: Priorización de respuesta a riesgos

Prioridad	Criterio
Baja	Medidas inmediatas para tratar riesgos que amenazan la continuidad del negocio o la reputación de la organización
Media	Medidas a implementar en un plazo determinado para reducir la exposición a riesgos significativos.
Alta	Medidas para riesgos que pueden ser tolerados en el corto plazo, pero que requieren monitoreo continuo.

Nota: Elaboración Propia

El tratamiento de riesgos se aplica a los riesgos inherentes, sin embargo, es importante monitorear continuamente los riesgos residuales, ya que pueden cambiar con el tiempo debido a factores internos o externos, y, si el riesgo residual excede el apetito de riesgo de la organización, se deben desarrollar nuevas respuestas de tratamiento o ajustar las existentes, de manera que se garantice que los riesgos estén bajo control y no afecten significativamente el logro de los objetivos de la empresa.

5.1.2.4. Registros e informes

El registro e informes de riesgos es un componente clave en la gestión de riesgos de TI, ya que permite la sistematización y el seguimiento continuo de todos los aspectos relacionados con los riesgos que enfrenta la organización, lo que no solo facilita la creación de un registro histórico que puede servir de referencia para futuros análisis, sino que también proporciona una base sólida para la toma de decisiones informadas, asegurando que los riesgos se gestionen de manera efectiva y eficiente.

La importancia de los registros e informes de riesgos radica en su capacidad para ofrecer una visión clara y completa de la situación actual de los riesgos dentro de la empresa, incluyendo desde la identificación inicial del riesgo hasta las acciones correctivas y preventivas que se implementan, permitiendo un control exhaustivo del ciclo de vida de cada riesgo, por lo que estos registros deben mantenerse de forma continua y actualizada, reflejando fielmente el contexto, la identificación, el análisis, la evaluación, el tratamiento y el seguimiento de los riesgos.

Dentro del proceso de gestión de riesgos de TI, es esencial que la organización cuente con un sistema de registro detallado y accesible que permita a todos los interesados obtener la información necesaria de manera rápida y eficiente, lo que incluye no solo la documentación de los riesgos identificados, sino también de los incidentes ocurridos, las evaluaciones realizadas, las decisiones tomadas y las acciones ejecutadas para mitigar o gestionar los riesgos, aparte de que el registro de riesgos también debe incluir informes periódicos de seguimiento, que permitan evaluar la efectividad de las medidas implementadas y ajustar las estrategias según sea necesario.

Para el contexto de la empresa, que actualmente carece de un proceso formal de gestión de riesgos y actúa de manera reactiva ante la materialización de incidentes, se propone una plantilla para el registro e informes de riesgos con el fin de establecer un sistema de registros. La información necesaria para esta plantilla corresponde específicamente a las fases de Evaluación del Riesgo y Tratamiento de Riesgos, las cuales han sido explicadas previamente en este documento. Estas fases forman parte integral del proceso diseñado en la sección 4.3.1.2. Diagrama TO-BE del proceso de Gestión de Riesgos de TI. Además, esta recopilación es particularmente relevante en el contexto del subproceso descrito en la sección 4.3.1.3. Subproceso: Analizar los Riesgos de TI Identificados.

Adicionalmente, como parte de la plantilla propuesta, se han desarrollado instrucciones específicas sobre su uso, las cuales se incluyen en el mismo archivo de la plantilla. Estas instrucciones proporcionan lineamientos claros para asegurar que la información se registre correctamente y de manera consistente, optimizando su utilidad en el contexto del proceso propuesto. La Figura 38 presenta una imagen de la plantilla propuesta junto a la visualización de cada menú desplegable que incluye.

Figura 37: Plantilla propuesta para el registro e informes de los riesgos de TI

Nota: Elaboración Propia

Las columnas incluidas en la plantilla propuesta se explican a continuación:

- **ID del riesgo:** identificador único para cada riesgo, facilitando su seguimiento y referencia.
- **Descripción del riesgo:** detalle claro y conciso del riesgo, incluyendo su origen y posibles consecuencias.
- **Categoría del riesgo:** clasificación del riesgo según su naturaleza, como TI/Infraestructura, seguridad, operacional, entre otros.
- **Probabilidad:** estimación de la frecuencia con la que podría ocurrir el riesgo.
- **Impacto:** evaluación del posible impacto del riesgo en la organización.
- **Nivel de riesgo:** combinación de impacto y probabilidad que define la criticidad del riesgo.

- **Respuesta:** respuesta elegida para tratar el riesgo (evitar, aceptar, mitigar o transferir)
- **Prioridad:** prioridad definida para la respuesta al riesgo (alta, media, baja).
- **Acciones tomadas:** descripción de las medidas implementadas para mitigar, evitar, transferir o aceptar el riesgo.
- **Responsable:** persona o equipo encargado de gestionar el riesgo y asegurar que se tomen las acciones necesarias.
- **Fecha de registro:** momento en el cual se identificó y registró el riesgo en el sistema.
- **Estado actual:** situación actual del riesgo, como "Mitigado", "En proceso", "No mitigado".
- **Revisión programada:** fecha para la próxima revisión del riesgo, asegurando su monitoreo continuo.
- **Comentarios adicionales:** observaciones adicionales que puedan ser relevantes para el seguimiento o la gestión del riesgo.

Esta acción no solo permitirá organizar mejor la información relacionada con los riesgos, sino que también ayudará a crear una cultura de gestión de riesgos dentro de la organización, donde todos los actores involucrados estén informados y puedan colaborar de manera efectiva en la identificación y mitigación de riesgos

5.1.2.5. Seguimiento y revisiones

El seguimiento y las revisiones son componentes críticos en el proceso de gestión de riesgos, fundamentales para garantizar que los riesgos sean gestionados de manera efectiva y que las respuestas implementadas continúen siendo adecuadas con el tiempo, el cual no solo se realiza de manera puntual, sino que debe ser continuo y sistemático, abarcando todas las etapas del ciclo de gestión de riesgos, desde la identificación hasta la evaluación y el tratamiento de los riesgos.

La importancia del seguimiento y las revisiones radica en su capacidad para proporcionar una visión actualizada y precisa del entorno de riesgos al cual se enfrenta la organización, ya que permiten detectar cambios en los riesgos existentes, la aparición de nuevos riesgos, y la efectividad de los controles y medidas mitigadoras que se han implementado. Además, facilitan la identificación de áreas que requieren ajustes o mejoras, lo cual es esencial para la mejora continua del proceso de gestión de riesgos.

En el contexto de la empresa, donde actualmente no existe un proceso formal de gestión de riesgos y se opera de manera reactiva ante incidentes materializados, la implementación de un sistema robusto de seguimiento y revisiones es esencial, ya que permitirá a la empresa evolucionar hacia una gestión proactiva de riesgos, proporcionando los datos y las métricas necesarias para la toma de decisiones informadas, y, a través de este enfoque, la empresa podrá priorizar sus controles, medidas y planes de contingencia.

Ahora bien, para un correcto seguimiento y revisiones de la gestión de riesgos de TI, es importante definir una serie de indicadores de desempeño que ayuden a medir el desempeño del

proceso, por lo que, para el contexto de la empresa se proponen una serie de indicadores que se detallan a continuación.

5.1.2.5.1. Indicadores Clave de Riesgo

En la gestión de riesgos de TI, los Indicadores Clave de Riesgo (KRIs) son métricas utilizadas para monitorear la exposición al riesgo y la efectividad de los controles implementados, ya que permiten a la organización identificar y responder proactivamente a los riesgos antes de que se materialicen en eventos adversos. Los KRIs propuestos en la Tabla 26 están diseñados para reflejar los principales riesgos operativos y estratégicos de la empresa según sus necesidades, proporcionando una visión clara sobre el estado de los riesgos y ayudando a priorizar las acciones correctivas necesarias para mitigar estos riesgos.

Tabla 26: Indicadores Clave de Riesgo propuestos para la empresa

KRI	Descripción	Fórmula	Objetivo
Número de incidentes críticos	Mide la cantidad de incidentes con nivel alto ocurridos en un periodo mensual.	$\sum Incidentes\ críticos\ mensuales$	Reducir a cero incidentes críticos.
Frecuencia de eventos de alto impacto	Monitorea la frecuencia de ocurrencia de eventos que tienen un alto impacto en la operación.	$\sum Eventos\ alto\ impacto\ mensuales$	1 o menos eventos por mes.
Cumplimiento de controles	Evalúa el porcentaje de controles de riesgo implementados correctamente.	$\frac{\sum Controles\ implementados}{\sum controles\ planificados} x100$	100% cumplimiento.
Cantidad de desviaciones en procesos de gestión	Monitorea las desviaciones de los procesos de gestión establecidos en el marco de riesgo.	$\sum Desviaciones\ detectadas\ en\ revisiones$	Menos de 3 desviaciones por mes.
Uso de recursos para mitigación	Mide la eficiencia en el uso de recursos para mitigar riesgos identificados.	$\frac{\sum recursos\ usados}{\sum recursos\ asignados} x100$	Máximo 85% del presupuesto asignado.

Nota: Elaboración Propia

5.1.2.5.2. Indicadores Clave de Desempeño

Los Indicadores Clave de Desempeño (KPIs) son métricas esenciales para medir la eficiencia y efectividad de los procesos de gestión de riesgos de TI en la empresa, ya que proporcionan una evaluación del desempeño de los procesos y controles implementados, permitiendo a la organización asegurar que las actividades de gestión de riesgos se alinean con los objetivos estratégicos y operativos. La Tabla 27 presenta la definición de un conjunto de KPIs propuestos según el contexto de la empresa, los cuales incluyen indicadores que miden tanto la capacidad de respuesta a incidentes como la efectividad de las revisiones y controles, con el objetivo de mejorar continuamente la gestión de riesgos.

Tabla 27:Indicadores Clave de Desempeño propuestos para la empresa

KPI	Descripción	Fórmula	Objetivo
Tiempo de respuesta	Mide el tiempo promedio que tarda en responderse a los incidentes identificados.	$\frac{\sum(tiempo\ respuesta - tiempo\ identificación)}{\sum Incidentes}$	Menos de 2 horas.
Frecuencia de revisiones de control	Mide la cantidad de revisiones de controles realizadas con relación a lo planificado.	$\frac{\sum revisiones\ efectivas}{\sum revisiones\ planificadas} x100$	100% de revisiones planificadas
Tasa de errores menores	Mide la frecuencia de errores pequeños que no tienen impacto crítico, pero pueden indicar fallos.	$\sum Errores\ menores\ reportados$	Máximo 2 errores por mes
Frecuencia de incidentes	Mide la cantidad de incidentes reportados en un periodo, con un objetivo de mantenerlos bajos.	$\sum incidentes\ registrados\ mensualmente$	Menos de 4 incidentes menores al mes.

Nota: Elaboración Propia

Ahora bien, después de proponer los indicadores para el seguimiento y revisión, se propone una plantilla para la revisión y seguimiento de riesgos de TI diseñada para facilitar la sistematización y revisión de los riesgos a lo largo de todo el proceso de gestión, asegurando que cada riesgo sea gestionado de manera efectiva. La Figura 39 presenta una imagen de la plantilla propuesta junto a la visualización de cada menú desplegable que incluye.

Figura 38: Plantilla propuesta para el seguimiento y revisiones de los riesgos de TI

Nota: Elaboración Propia

Las columnas incluidas en la plantilla propuesta se explican a continuación:

- **ID del riesgo:** identificador único para cada riesgo.
- **Descripción del riesgo:** breve descripción del riesgo identificado.
- **Nivel de riesgo:** clasificación del riesgo (muy alto, moderadamente alto, moderado, moderadamente bajo, bajo).
- **Frecuencia de seguimiento:** periodicidad con la que se realiza el seguimiento (mensual, trimestral, semestral).
- **Acciones de mitigación:** acciones tomadas o planeadas para mitigar el riesgo.
- **Responsable del seguimiento:** persona o equipo encargado de monitorear el riesgo.
- **Fecha de la última revisión:** fecha en la que se realizó la última revisión del riesgo.
- **Resultados de la revisión:** resumen de los hallazgos durante la última revisión.
- **Revisiones necesarias:** revisión específica necesaria para el próximo período (evaluación de controles, ajuste de planes de contingencia, entre otros).
- **Indicador Clave de Riesgo (KRI):** indicadores usados para medir el riesgo y su impacto.
- **Indicador Clave de Desempeño (KPI):** indicadores usados para medir la efectividad de las acciones de mitigación.

- **Estado actual:** estado del riesgo (activo, controlado, cerrado).
- **Acciones correctivas:** medidas adicionales a tomar si los riesgos no están siendo gestionados adecuadamente.
- **Comentarios adicionales:** observaciones adicionales que sean relevantes para el riesgo.

En la plantilla propuesta, también se incluyen algunos datos predefinidos para facilitar el llenado de la plantilla, los cuales sirven como guía inicial y pueden ser modificados a medida que cambien las necesidades de la empresa o se ajusten las prioridades en la gestión de riesgos de TI, lo que permite una mayor flexibilidad y adaptación del proceso a las realidades cambiantes del entorno empresarial, garantizando que la plantilla siga siendo relevante y efectiva en el seguimiento y revisión de los riesgos de TI.

5.1.2.6. Comunicación y consulta

La comunicación y consulta son esenciales en todo el proceso de gestión de riesgos de TI, involucrando a los interesados internos y externos en cada fase de forma transversal, asegurando que la información necesaria llegue a los interesados de manera oportuna, facilitando decisiones alineadas con los objetivos organizacionales. Una estrategia efectiva de comunicación y consulta garantiza que la información se gestione correctamente, adaptándose a los roles y necesidades de la empresa.

Es importante resaltar que, esta matriz debe ser utilizada durante todo el ciclo de Gestión de Riesgos de TI y Gobierno de TI y por todas las partes involucradas en el proceso de gestión de riesgos, asegurando una interacción efectiva entre las partes interesadas en cada fase del proceso. La matriz de comunicación y consulta para la gestión de riesgos de TI, que se presenta en la Tabla 28, define aspectos como los canales de comunicación, la frecuencia y el objetivo de la comunicación, promoviendo la interacción y el flujo de información de manera transparente durante todo el ciclo de gestión de riesgos de TI.

Tabla 28: Matriz de comunicación para la gestión de riesgos de TI

Objetivo de la comunicación	Información por comunicar	Emisor	Receptor	Canal de Comunicación	Frecuencia

Nota: Elaboración Propia

A continuación, se explican los puntos clave de la matriz para su correcta implementación en el contexto de la empresa, asegurando que la información relevante fluya de manera efectiva y oportuna para respaldar la toma de decisiones y la implementación de la gestión de riesgos de TI:

- **Objetivo de la comunicación:** breve descripción del porqué es importante la comunicación que se da a conocer.
- **Información por comunicar:** breve descripción del tipo de información que se compartirá.
- **Emisor:** persona responsable de gestionar la comunicación y darla a conocer.
- **Receptor:** persona o equipo a quien va dirigida la comunicación.
- **Canal de comunicación:** medio por el que se comunicará la información (por ejemplo, correos electrónicos, reuniones, reportes).
- **Frecuencia:** frecuencia con la que se llevará a cabo la comunicación (por ejemplo, semestral, trimestral, mensual).

Ahora bien, no solo es importante comunicar los riesgos identificados y las estrategias de mitigación, sino también los roles y responsabilidades de los involucrados, las métricas de desempeño relacionadas con la gestión de riesgos, y cualquier cambio significativo en el perfil de riesgos de la organización. A continuación, se presentan una serie de ejemplos extra de información a comunicar para asegurar una transparencia y colaboración de las partes interesadas:

- Actualizaciones sobre los controles de riesgos implementados
- Revisiones periódicas de los riesgos
- Metodología de gestión de riesgos
- Planes de acción
- Reporte del resultado de los indicadores de riesgo

5.1.3. Matriz RACI

La matriz RACI, o bien, matriz de asignación de roles y responsabilidades, es una herramienta de gestión utilizada para definir roles y responsabilidades dentro de un proyecto o proceso, asignando niveles específicos de participación a cada actividad. Para efectos de la metodología propuesta de gestión de riesgos de TI, se adapta la matriz RACI al contexto de los roles existentes en la organización, proponiéndola como una recomendación de asignación que asegure una implementación clara, estructurada y alineada con los objetivos organizacionales.

Dado el contexto empresarial y la limitada disponibilidad de puestos en la organización, se propone que las responsabilidades relacionadas con el Gobierno de TI recaigan principalmente en la alta gerencia y en el administrador del departamento de TI. Esta asignación permite aprovechar los roles existentes dentro de la empresa para garantizar que las decisiones estratégicas y operativas relacionadas con la gestión de riesgos de TI sean tomadas de manera oportuna y alineadas con los objetivos organizacionales. La Tabla 29 muestra la matriz RACI propuesta para el desarrollo de la metodología de gestión de riesgos de TI propuesta.

Tabla 29: Matriz de roles y responsabilidades para el desarrollo de la metodología

Actividad	Departamento de TI de TI	Alta Gerencia	Departamento de Operaciones	Líderes departamentales	Todos los involucrados
Definir el Marco de Gobierno de TI	**R**	**R**	**C**	**I**	**I**
Evaluar el contexto externo e interno	**R**	**C**	**I**	**I**	**I**
Diseñar el plan de comunicación	**R**	**R**	**I**	**C**	**I**
Identificar los riesgos	**R**	**A**	**C**	**C**	**I**
Analizar los riesgos	**R**	**C**	**C**	**I**	**I**
Priorizar los riesgos	**R**	**I**	**C**	**I**	**I**
Desarrollar los planes de tratamiento	**R**	**A**	**I**	**I**	**I**
Implementar los planes de tratamiento	**R**	**A**	**C**	**I**	**I**
Monitorear y revisar el desempeño del proceso	**R**	**A**	**I**	**I**	**I**
Actualizar indicadores y controles	**R**	**R**	**C**	**I**	**I**

Nota: Elaboración Propia

A continuación, se explican los roles de la matriz RACI:

- **Responsable (R):** es quien realiza la actividad o ejecuta la tarea. Este rol tiene la obligación directa de completar la actividad o tarea asignada.
- **Aprobador (A):** es quien tiene la autoridad final para tomar decisiones y aprobar los resultados de la actividad. Este rol asegura que el trabajo realizado cumple con los estándares establecidos.
- **Consultado (C):** son las personas o grupos que son consultados para aportar su conocimiento, experiencia o retroalimentación. Aunque no son responsables directos, su participación es clave para el éxito de la tarea.
- **Informado (I):** son las personas o grupos que deben ser notificados sobre el progreso o los resultados de la actividad. No participan activamente en su ejecución, pero necesitan estar al tanto del estado para la toma de decisiones o acciones relacionadas.

Esta matriz propuesta no solo fomenta la colaboración entre las áreas involucradas, sino que también asegura que todos los participantes comprendan claramente su rol dentro de la implementación de la metodología propuesta para la gestión de riesgos de TI

5.1.4. Hoja de Ruta para la Implementación de la Metodología

Después de diseñar la propuesta de metodología de gestión de riesgos de TI para la empresa Information Evolution Costa Rica, se presenta una hoja de ruta que detalla la propuesta con los pasos a seguir para su futura implementación. Esta hoja de ruta es fundamental para garantizar que la metodología se adapte de manera efectiva y alineada con las necesidades específicas de la organización. Para efectos de la fase Registro e informes, esta es cíclica a través de todo el proceso de gestión de riesgos de TI, es por esto que se recomienda completar la plantilla después de cada actividad, de igual forma con el Seguimiento y revisiones durante su implementación y una vez que se monitoree el proceso, para esto se proponen las plantillas definidas con anterioridad. La Tabla 30 presenta la hoja de ruta propuesta para la implementación futura de la metodología de gestión de riesgos de TI.

Tabla 30: Hoja de ruta propuesta para la implementación de la propuesta metodológica

Actividad	Responsables	Cronograma											
		Mes 1				Mes 2				Mes 3			
		S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4
Fase 1: Preparación Inicial													
Revisión del alcance del proceso (recursos, activos, áreas cubiertas)	Administrador de TI												
Definición de la estructura del equipo y Gobierno de TI	Administrador de TI Gerente General												
Capacitación inicial del equipo en gestión de riesgos de TI	Empresa externa												
Fase 2: Definición del Marco de Gobierno de TI													
Definición de las políticas de gestión de riesgos de TI alineadas con los objetivos empresariales	Gobierno de TI Consultor externo												
Aprobación del apetito y tolerancia del riesgo	Gobierno de TI												
Aprobación de los criterios de probabilidad, impacto y nivel del riesgo	Gobierno de TI												
Definición de controles y criterios de evaluación	Gobierno de TI												
Aprobación de la frecuencia del seguimiento de riesgos según el apetito y tolerancia definidos	Gobierno de TI												
Aprobación de los indicadores clave de riesgo (KRIs) y desempeño (KPIs) propuestos	Gobierno de TI Consultor externo												
Fase 3: Implementación del proceso de Gestión de Riesgos de TI													
Identificación de riesgos y escenarios de riesgos	Administrador de TI Gerente General Líderes los departamentos												

Actividad	Responsables	Cronograma											
		Mes 1				Mes 2				Mes 3			
		S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4
Evaluación de la probabilidad e impacto de los riesgos identificados	Administrador de TI Consultor externo												
Evaluación del nivel del riesgo	Administrador de TI Consultor externo												
Cálculo del riesgo residual	Administrador de TI												
Priorización de los riesgos	Administrador de TI												
Definición del tratamiento de riesgos y planificación de respuestas	Administrador de TI Líder de operaciones												
Desarrollo de planes de acción para los riesgos	Administrador de TI Consultor externo												
Implementación de las acciones correctivas para riesgos identificados	Administrador de TI												
Fase 4: Evaluación inicial del proceso													
Monitoreo y evaluación inicial de la efectividad de la gestión de riesgos	Administrador de TI Líder de operaciones												
Revisión y ajuste del proceso en función de los resultados iniciales	Administrador de TI												
Mejora continua del proceso de gestión de riesgos de TI	Administrador de TI Gerente General												

Nota: Elaboración Propia

A continuación, se presenta una vista ejecutiva del proceso de implementación de la metodología de Gestión de Riesgos de TI, estructurada en cuatro fases principales. Estas fases representan los pasos clave a seguir propuestos para garantizar una correcta implementación y adopción de la metodología, de manera que responda a las necesidades específicas de la empresa. En la Figura 40 se muestra una línea de tiempo, que resume de manera gráfica la duración y el orden de cada una de las fases, proporcionando una visión clara y organizada del cronograma general para la implementación.

Figura 39: Línea de tiempo propuesta del proceso de implementación para la metodología de gestión de riesgos de TI

Nota: Elaboración Propia

5.1.5. Estandarización y Alineación del Proceso

Una vez desarrollada la propuesta de metodología para la gestión de riesgos de TI, es fundamental evaluar el nivel de estandarización del proceso y la alineación con las mejores prácticas de la industria, para asegurar que la metodología propuesta cumple con los lineamientos establecidos por los marcos de referencia internacionales que fueron seleccionados en la Fase 2: Comparación y Selección de las Mejores Prácticas de Gestión de Riesgos de TI. Enfatizando que para esta evaluación se utilizaron tres listas de verificación basadas en las prácticas de COBIT 2019 (EDM03 y APO12) y la ISO 31000. A continuación, en las Tablas 31, 32 y 33, se presentan las listas de verificación para la alineación de la propuesta.

Tabla 31: Lista de verificación para la práctica EDM03 de COBIT 2019

PRÁCTICA EVALUADA: EDM03 de COBIT 2019		
Criterio	**¿Se cumple?**	**Evidencia**
EDM03.01 Evaluar la gestión de riesgos	SÍ	En las secciones 5.1.2 se definen los distintos criterios a tomar en cuenta para la gestión de riesgos, los cuáles son definidos por el Gobierno de TI y se plantea una plantilla para la definición del contexto (5.1.3.1.2). Estas evidencias corresponden a las actividades número 1, 2 y 3 de la práctica.

PRÁCTICA EVALUADA: EDM03 de COBIT 2019		
Criterio	**¿Se cumple?**	**Evidencia**
EDM03.02 Dirigir la gestión de riesgos.	SÍ	La propuesta incluye definiciones de indicadores en la sección 5.1.3.5.1 y 5.1.3.5.2 y también un plan de comunicación en la sección 5.1.3.6. Estas evidencias corresponden a las actividades número 1, 2, 3, 4 y las bases para la actividad 5 de la práctica.
EDM03.03 Monitorizar la gestión de riesgos	SÍ	La propuesta incluye todo un plan con su respectiva plantilla para monitorizar el proceso de gestión de riesgos, el cual se incluye en la sección 5.1.3.5. También se incorpora el Gobierno de TI al plan de comunicación de la sección 5.1.2.6. Estas evidencias corresponden a las actividades número 1, 2 y 3 de la práctica.
Cantidad total de criterios: 3	**Criterios cumplidos: 3**	**Porcentaje de alineación: 100%**

Nota: Elaboración Propia

Tabla 32: Lista de verificación para la práctica APO12 de COBIT 2019

PRÁCTICA EVALUADA: APO12 de COBIT 2019		
Criterio	**¿Se cumple?**	**Evidencia**
APO12.01 Recopilar datos	SÍ	El objetivo comprende actividades como la evaluación de entornos, (5.1.3.1.2), definir escenarios de riesgos (5.1.3.2.1.3), y procesos generales de lo propuesto en la identificación de riesgos (5.1.3.2.1) y en los criterios de impacto de los riesgos (5.1.2.3). Estas evidencias corresponden a las actividades número 1, 2, 3 y 4 de la práctica.
APO12.02 Analizar el riesgo	SÍ	Este objetivo abarca lo propuesto en las fases de evaluación del riesgo (5.1.3.2) y las propuestas de respuestas a los riesgos que abarca la fase de tratamiento de riesgos (5.1.3.3.). Estas evidencias corresponden a las actividades número 1, 2, 3, 4 y 5 de la práctica.
APO12.03 Mantener un perfil del riesgo	SÍ	Trata actividades propuestas como el planteamiento de escenarios de riesgos (5.1.3.1.2), la documentación de la información sobre los riesgos propuesta en la fase de registro e informes (5.1.3.4). Estas evidencias corresponden a la actividad 3 de la práctica.
APO12.04 Articular el riesgo	SÍ	Trata actividades propuestas en la fase de comunicación y consulta (5.1.3.6). Estas evidencias corresponden a las actividades número 1, 2 y 3 de la práctica.
APO12.05 Definir un portafolio con acciones de gestión de riesgos	SÍ	Este objetivo abarca actividades propuestas en la identificación y evaluación de controles (5.1.2.6), registros e informes (5.1.3.4) y seguimiento y revisiones (5.1.3.5). Estas evidencias corresponden a la actividad número 1 de la práctica.

PRÁCTICA EVALUADA: APO12 de COBIT 2019		
Criterio	**¿Se cumple?**	**Evidencia**
APO12.06 Responder al riesgo	SÍ	El objetivo trata las actividades que se proponen en la fase de Tratamiento de riesgos (5.1.3.3) y el uso del plan de comunicación propuesto en la fase de comunicación y consulta (5.1.3.6). Estas evidencias corresponden a las actividades número 1 y 2 de la práctica.
Cantidad total de criterios: 6	**Criterios cumplidos: 6**	**Porcentaje de alineación: 100%**

Nota: Elaboración Propia

Tabla 33: Lista de verificación para la práctica EDM03 de COBIT 2019

PRÁCTICA EVALUADA: ISO 31000		
Criterio	**¿Se cumple?**	**Evidencia**
Alcance, contexto, criterios	SÍ	La sección 5.1.3.1 de la propuesta de solución corresponde a la fase de Alcance, contexto, criterios según lo establecido por la ISO, sin embargo, la parte de criterios se define en la sección 5.1.2.
Identificación de riesgos	SÍ	La sección 5.1.3.2.1 de la propuesta de solución corresponde a la fase de Identificación de riesgos, en la que se proponen una serie de herramientas, fuentes y escenarios para la identificación de los riesgos.
Análisis de riesgos	SÍ	La sección 5.1.3.2.2 de la propuesta de solución corresponde a la fase de análisis de riesgos en donde se explica el uso de los criterios de probabilidad, impacto y nivel del riesgo para su cálculo, aparte del uso de controles y priorización.
Evaluación de riesgos	SÍ	La sección 5.1.3.2.3 de la propuesta de solución corresponde a la fase de Evaluación de riesgos en donde se explica la evaluación de acuerdo con los niveles de tolerancia definidos.
Tratamiento de riesgos	SÍ	La sección 5.1.3.3 de la propuesta de solución corresponde a la fase de tratamiento de riesgos en donde se proponen las posibles respuestas a riesgos y cómo tratarlos.

PRÁCTICA EVALUADA: ISO 31000		
Criterio	**¿Se cumple?**	**Evidencia**
Registros e informes	SÍ	La sección 5.1.3.4 de la propuesta de solución corresponde a la fase de registros e informes en donde se propone una plantilla para la correcta documentación de los riesgos.
Seguimiento y revisiones	SÍ	La sección 5.1.3.5 de la propuesta de solución corresponde a la fase de seguimiento y revisiones en donde se definen indicadores clave y se propone una plantilla para su desarrollo continuo,
Comunicación y consulta	SÍ	La sección 5.1.3.6 de la propuesta de solución corresponde a la fase de comunicación y consulta en donde se propone la matriz de comunicaciones y se proponen una serie de temas de información a comunicar.
Cantidad total de criterios: 8	**Criterios cumplidos: 8**	**Porcentaje de alineación: 100%**

Nota: Elaboración Propia

La evaluación realizada evidencia que la propuesta cumple con las mejores prácticas de la industria. En cuanto al EDM03 de COBIT 2019, las tres prácticas de gobierno fueron satisfechas, demostrando que la propuesta aborda de manera integral la evaluación, dirección y monitoreo de los riesgos, adaptándolos al contexto empresarial. Por otro lado, en el APO12 de COBIT 2019, se cumplieron los seis criterios de gestión del riesgo, garantizando un enfoque completo que incluye actividades de documentación, seguimiento y priorización de controles, alineado con los lineamientos de COBIT 2019. Finalmente, en la ISO 31000, se evaluaron las seis fases del ciclo de gestión de riesgos, desde el alcance y contexto hasta el tratamiento, registro, revisiones y comunicación, cumpliendo con todos los criterios establecidos y asegurando que cada fase del ciclo esté cubierta en la propuesta.

Es importante destacar que, aunque el proceso propuesto utiliza prácticas específicas de COBIT 2019 como apoyo, su fundamento principal radica en la ISO 31000, lo que asegura un enfoque robusto y adaptado a las necesidades de la organización.

En la Figura 41, se presenta una visualización que muestra cómo las prácticas EDM03, APO12 de COBIT 2019 y la ISO 31000 se interrelacionan y apoyan mutuamente para asegurar la alineación de la metodología propuesta con las mejores prácticas internacionales en la gestión de riesgos de TI.

Figura 40: Interrelación de las mejores prácticas utilizadas para el desarrollo de la metodología propuesta

Nota: Elaboración Propia

Este resultado demuestra un proceso estandarizado y asegura que la gestión de riesgos de TI en la empresa está alineada con las mejores prácticas y estándares internacionales. Por lo tanto, la implementación de la metodología propuesta no solo garantizará una gestión efectiva de los riesgos, sino que también se traducirá en un sistema sólido y confiable, que promueve una gobernanza adecuada y un monitoreo continuo del riesgo dentro de la empresa.

5.1.5.1. Evaluación de la capacidad del proceso según el CMMI

La evaluación de la capacidad de un proceso según el modelo CMMI (*Capability Maturity Model Integration*) permite determinar el nivel de madurez en el que se encuentra un proceso organizacional, clasificándolo en una escala que va desde el nivel 0 (Incompleto), donde el proceso es informal o inexistente, hasta niveles más altos que representan optimización y madurez avanzada.

De acuerdo con la evaluación realizada en el Apéndice O, el proceso de gestión de riesgos de TI actualmente se encuentra en un nivel 0 (Incompleto), ya que aún no ha sido formalizado ni implementado dentro de la organización. Sin embargo, la propuesta del proyecto apunta claramente hacia un nivel 1 (Realizado), donde el proceso se establecería de manera inicial, con actividades específicas definidas, documentadas y repetibles, representando el primer paso hacia una gestión de riesgos más estructurada y efectiva. La Tabla 34 muestra una comparación de la evaluación del proceso en el Nivel 0 y el Nivel 1 del diagrama AS-IS y el diagrama TO-BE propuesto del proceso.

Tabla 34: Comparación de la evaluación de capacidad del proceso de gestión de riesgos de TI

Nivel de Capacidad	Criterios	*AS-IS*	*TO-BE*
0 - Incompleto	Existen políticas y procedimientos.	No Alcanzado	Alcanzado
	Se ejecutan los procedimientos según lo descrito en las políticas y procedimientos.	No Alcanzado	No Alcanzado
1 - Realizado	Las políticas y procedimientos se encuentran publicados y formalizados	No Alcanzado	No Alcanzado
	El proceso se ejecuta y se generan las salidas esperadas.	No Alcanzado	Alcanzado
	Existen roles y responsabilidades asignadas para el proceso.	No Alcanzado	Alcanzado
	Se cuentan con herramientas de apoyo para la ejecución del proceso (formularios, plantillas, etc.).	No Alcanzado	Alcanzado

Nota: Elaboración Propia

Los resultados obtenidos en la evaluación de la Tabla 34 muestran que el diagrama AS-IS de la situación actual no alcanza ninguno de los criterios evaluados, lo que refleja la ausencia de un proceso formal y estructurado para la gestión de riesgos de TI, manteniéndose en un nivel 0. Por otro lado, el diagrama TO-BE del proceso propuesto evidencia avances significativos, logrando cumplir con varios de los criterios establecidos para el nivel 1, tales como la existencia de roles asignados y herramientas de apoyo para la ejecución del proceso.

Aunque el diagrama TO-BE del proceso propuesto aún no alcanza el nivel 1 de capacidad debido a que este no ha sido implementado, refleja mejoras significativas en comparación con el diagrama AS-IS de la situación actual de la empresa. Para alcanzar el nivel 1 (Realizado), es crucial que el cliente formalice la propuesta de solución desarrollada en este proyecto y garantice que los procedimientos se ejecuten según lo establecido en la metodología propuesta.

5.2. Análisis de Viabilidad de la Propuesta

Una vez completada la Fase 3 del proyecto, que consistió en el desarrollo de los artefactos y la estructura de la metodología de gestión de riesgos de TI, es fundamental llevar a cabo un análisis de viabilidad para justificar su implementación en la empresa. Este análisis es crucial para garantizar que la propuesta no solo sea efectiva desde el punto de vista técnico, sino también sostenible desde el punto de vista financiero y operativo. Para ello, se realizará un análisis costo-beneficio, que permitirá evaluar el valor económico de la propuesta, el cual se centrará en tres actividades clave: cálculo del costo, cálculo del beneficio y cálculo del retorno de la inversión.

5.2.1. Cálculo del costo

A continuación, se presenta el cálculo de los costos totales para el análisis costo-beneficio del proyecto, que incluye tanto los costos de implementación como los correspondientes al primer año de producción. Los costos han sido estimados en función de los siguientes supuestos:

- Se utiliza el salario mínimo correspondiente al título de licenciado de la lista de salarios para el 2024 del Ministerio de Trabajo, equivalente a ₡765,985.67 mensuales.
- La distribución de tiempos para la implementación se basa en la hoja de ruta planteada, con un promedio de media jornada laboral por día.
- El proceso de seguimiento y revisiones se realizará conforme a la frecuencia definida una vez implementada la metodología. Esta será la única actividad considerada para el primer año de producción.
- La actividad “Monitoreo y evaluación inicial de la efectividad de la gestión de riesgos” está diseñada para realizar el monitoreo de una hora por día durante las 2 semanas definidas.
- La metodología propuesta utilizará los sistemas que ya tiene la empresa, sin necesidad de adquirir nueva tecnología o licencias adicionales; por tanto, estos costos no se consideran.
- El costo del consultor externo se calcula utilizando el precio promedio de las horas de un consultor junior en la empresa de consultoría Winit, que es de $25 dólares por hora, equivalente a ₡12,800 por hora según el tipo de cambio vigente.

Una vez definidos los supuestos se explican los cálculos de cada uno de los rubros de costos a tomar en cuenta:

- **Desarrollo del Trabajo Final de Graduación (TFG)**: La empresa cubrirá 1 hora por día del estudiante, acumulando un total de 80 horas para las 16 semanas del período. El costo se calcula incluyendo el aporte patronal del 26.67% y el aguinaldo, resultando en un total de ₡447,280.
- **Salario del Administrador de TI**: Para el Administrador de TI se consideran 210 horas distribuidas en las 12 semanas de la implementación de la metodología, obteniendo un costo total de ₡928,022.

- **Salario del Líder de Operaciones**: Se estima un total de 110 horas distribuidas en 7 semanas de participación, lo cual tiene un costo de ₡486,107.
- **Salario de los Líderes en la identificación de riesgos**: Para la identificación de riesgos se estiman 50 horas de participación divididas entre 5 líderes durante la semana correspondiente, obteniendo un costo total de ₡220,958.
- **Salario del Gerente General**: Se calculan 45 horas distribuidas en 3 semanas de participación, con un costo total de ₡198,862.
- **Salario del consultor externo**: Se toman en cuenta 30 horas distribuidas en 5 semanas, lo cual resulta en un costo de ₡384,000.
- **Formación y Capacitación**: El costo de formación incluye la capacitación "ISO 31000 Fundamentos de Gestión de Riesgos", ofrecida por Winit, cuyo costo aproximado es de $800, equivalente a ₡411,200.
- **Seguimiento y Revisiones**: Se estima un total de 160 horas anuales para el seguimiento y revisiones de riesgos. Estas horas están distribuidas según categorías de revisión (mensual, trimestral y semestral) y tiempos definidos (2 horas, 1.5 horas y 1 hora respectivamente), resultando en un costo total de ₡707,064 basado en el salario base definido para la persona responsable de esta actividad.

A continuación, la Tabla 35 desglosa los costos de la implementación y el primer año de producción de la metodología y su total.

Tabla 35: Costos de implementación y producción de la metodología

Detalle del costo	Implementación	Primer año de operaciones	Total
Desarrollo del TFG	₡353,532	₡0	₡353,532
Aportes patronales	₡94,287	₡0	₡94,287
Aguinaldo	₡29,461	₡0	₡29,461
Salario del Administrador de TI	₡928,022	₡0	₡928,022
Salario del Líder de Operaciones	₡486,107	₡0	₡486,107
Salario de los líderes de equipos	₡220,958	₡0	₡220,958
Salario del Gerente General	₡198,862	₡0	₡198,862
Consultor externo	₡384,000	₡0	₡384,000
Formación y Capacitación	₡411,200	₡0	₡411,200
Seguimiento y Revisiones	₡0	₡707,064	₡707,064
Total	**₡3,106,427**	**₡707,064**	**₡3,813,491**

Nota: Elaboración Propia

De acuerdo con la información de la Tabla 29, el costo total de implementación asciende a ₡3,106,427, mientras que el costo correspondiente al primer año de operación de la metodología es de ₡707,064, sumando así un costo total de ₡3,813,491.

5.2.2. Cálculo del Beneficio

Para calcular los beneficios derivados de la implementación de la metodología, se considerará el tiempo que actualmente invierte el administrador de TI, quien es el responsable del proceso de gestión de riesgos. No se incluirán las horas de otros colaboradores, ya que su participación en la resolución de incidentes y la gestión de riesgos de TI no tiene una línea definida.

A continuación, se detallan los cálculos de los beneficios estimados:

- **Respuesta proactiva a riesgos:** De acuerdo con la entrevista adjunta en el Apéndice K, el administrador de TI dedica entre 4 y 5 horas diarias a la solución de incidentes, lo que representa un total aproximado de 1,040 horas anuales, considerando 260 días laborales al año (5 días laborales por 52 semanas). Con base en los indicadores definidos en la metodología, se espera que, en el peor de los casos, se presenten de 4 a 6 incidentes menores al mes, lo que equivale a 72 incidentes anuales. Con un tiempo de respuesta de 1 hora por incidente, esto supone un total de 48 horas anuales. Asimismo, se espera 1 o menos eventos críticos al mes, que serían 12 eventos anuales, y se estima un tiempo de solución de 2 horas por evento, sumando 24 horas anuales. En total, se invertirían 96 horas anuales en la solución de incidentes, lo que representa un ahorro de 944 horas en comparación con el escenario actual, equivalente a un ahorro financiero de ₡4,171,678.
- **Estandarización del proceso:** Según Rosendahl & Paik (2024), la estandarización de un proceso puede generar un ahorro de entre el 5% y el 15% del tiempo de trabajo de los colaboradores. En el contexto de la empresa, actualmente no existe un proceso estandarizado, lo que implica un potencial ahorro, en el escenario más bajo, del 5% en las operaciones diarias del administrador de TI, quien está directamente involucrado en el proceso actual. Este ahorro equivale a 104 horas anuales, lo que representa un beneficio económico de ₡459,592.
- **Definición de roles y responsabilidades:** Según Rosendahl & Paik (2024), la consolidación de responsabilidades y la definición de una estructura clara de equipo pueden generar un ahorro de entre el 5% y el 10% del tiempo de trabajo de los colaboradores. Según lo planteado en la hoja de ruta y en la fase de alcance de la propuesta de solución, uno de los primeros pasos es establecer la estructura del equipo, y, al utilizar el escenario más bajo, esto se traduce en un ahorro de 104 horas anuales en las operaciones del administrador de TI, generando un beneficio financiero de ₡459,592.

A continuación, la Tabla 36 desglosa los beneficios económicos obtenidos en el primer año de operación de la metodología.

Tabla 36: Beneficios de implementar la metodología al primer año de operaciones

Detalle del beneficio	Monto
Respuesta proactiva a riesgos	₡4,171,678
Estandarización de proceso	₡459,592
Definición de roles y responsabilidades	₡459,592
Total	**₡5,090,861**

Nota: Elaboración Propia

De acuerdo con la información obtenida en la Tabla 30, al implementar la metodología de gestión de riesgos de TI, la empresa percibe un ahorro de ₡5,090,861 en el primer año de operaciones.

5.2.3. Cálculo del Retorno de Inversión (ROI)

Una vez determinado el costo total y los beneficios esperados, se puede calcular la rentabilidad del proyecto mediante el indicador de retorno sobre la inversión (ROI). Este indicador compara el costo total con los beneficios esperados para obtener el porcentaje de rendimiento de la inversión asociado al proyecto. La fórmula utilizada para calcular este indicador se presenta en la Figura 42.

Figura 41: Fórmula del ROI

ROI = (Valor actual – Costo de inversión / Costo de inversión) x 100

Nota: Recuperado de (Guy Birken, 2022)

Ahora bien, al aplicar la fórmula del ROI al contexto del proyecto, se tiene el siguiente resultado:

$$ROI = \frac{5{,}090{,}861 - 3{,}813{,}491}{3{,}813{,}491} \times 100$$

$$ROI = 33.49\%$$

El resultado del ROI del 33.49% en el primer año de operación de la metodología indica que la inversión realizada generó un retorno significativo en comparación con el costo incurrido. Este porcentaje refleja una rentabilidad positiva y sugiere que la metodología implementada tiene un impacto favorable, recuperando una parte considerable de la inversión y superando los costos.

6. Conclusiones

En este capítulo se presentan las conclusiones obtenidas como resultado final del Trabajo Final de Graduación. Dichas conclusiones están directamente relacionadas con cada uno de los objetivos planteados en la sección 1.4, y reflejan el cumplimiento exitoso de cada uno de ellos.

6.1. Objetivo Específico #1

Analizar la situación actual de las prácticas de gestión de riesgos de TI utilizadas por Information Evolution Costa Rica, identificando las fortalezas y debilidades, para la detección de las brechas presentes en la empresa.

- No existe una metodología de gestión de riesgos de TI definida y documentada en la empresa, por consiguiente, no existen actividades, métodos o instrumentos desarrollados para la gestión de los riesgos de TI, según los hallazgos de la sección 4.1.1 y la sección 4.1.3,
- La empresa únicamente cumple con el primer grado de la escala planteada en el área de registro y tratamiento de riesgos gracias a la documentación de cierto tipo de incidentes y previsión de inventario extra en caso de daños de equipo (Apéndice K), sin embargo, no realizan ninguna de las demás actividades sugeridas por las mejores prácticas, esto según las actividades realizadas por la empresa analizadas en la Figura 26.
- La empresa reacciona de manera reactiva ante los incidentes de TI que se presentan, tratando los riesgos hasta que ya estos se materializan y se convierten en eventos de riesgo de tipo incidente según el diagrama realizado en la sección 4.1.2.
- La sección 4.1.2 demuestra que, aparte de que no existe un proceso definido para la gestión de riesgos de TI, el proceso para la gestión de eventos de riesgos de tipo incidentes no está estandarizado y su desarrollo depende del tipo de incidente detectado.
- La empresa no documenta los posibles riesgos de TI ni los incidentes que se presentan, por lo que cada vez que se presenta uno nuevo, este se debe tratar desde cero, impidiendo la creación de una base de conocimiento sobre cómo resolverlos, según la entrevista realizada (Apéndice K) y el grupo focal realizado (Apéndice L).
- La entrevista realizada en el Apéndice K evidencia que el encargado del departamento de TI utiliza cinco horas diarias de su jornada para la resolución de incidentes de TI, ocupando el 62.5% de su tiempo e impidiéndole desarrollar mejoras para el crecimiento del departamento.
- Una de las mayores limitantes que tiene la empresa actualmente es el bajo nivel de apoyo por parte de la gerencia, representando el 45% de los desafíos identificados según la entrevista y el grupo focal realizados (Apéndice K y Apéndice L), aparte una baja cultura organizacional de gestión de riesgos de TI, lo que refleja el desconocimiento de los distintos

involucrados sobre la importancia de la gestión de riesgos de TI en las organizaciones, según lo planteado en la sección 4.1.4.

6.2. Objetivo Específico #2

Comparar las mejores prácticas de la industria de gestión de riesgos de TI, para la selección de aquellas que mejor se adapten a las necesidades de gestión de riesgos de Information Evolution Costa Rica.

- Las mejores prácticas evaluadas destacan la importancia de integrar la gestión de riesgos en los objetivos estratégicos y operativos de la organización, asegurando una alineación con la planificación estratégica y la toma de decisiones, lo cual es lo que se busca con la metodología propuesta, según la Tabla 12.
- La Figura 29 demuestra que tanto la ISO 31000 como COBIT 2019 son las opciones más adecuadas para el desarrollo de la metodología según el análisis de la situación actual de la empresa. En este caso, la ISO 31000 tienen una alineación del 100% con respecto a las necesidades claves de la empresa, mientras que COBIT 2019 presenta un 75% de alineación (Apéndice M).
- Prácticas como la ISO 27005, Margerit y Octave, muestran niveles de alineación significativamente bajos, con un 50%, 37.5%, y 37.5% respectivamente, ya que presentan limitaciones en su aplicabilidad y compatibilidad con los recursos y capacidades actuales de la organización, debido a su enfoque especializado y a la falta de flexibilidad que no se adaptan a los criterios requeridos por la organización según sus necesidades, esto según el análisis de alineación del Apéndice M y el gráfico de la Figura 29.

6.3. Objetivo Específico #3

Crear un conjunto de artefactos, para la instrumentalización y estandarización de la metodología estratégica de la gestión de riesgos de TI según el estado deseado del proceso.

- La metodología de gestión de riesgos de TI propuesta se compone de dos fases principales: Gobierno de Riesgos de TI y Proceso de Gestión de Riesgos de TI, en donde para cada fase se desarrollan los artefactos de cada una de las actividades, sumando un total de 13 artefactos, tablas explicativas y propuestas de indicadores.
- Según el diagrama de la situación actual planteado en la sección 4.1.2. y el diagrama del estado deseado del proceso propuesto en la sección 5.1.1. se demuestra un proceso estandarizado y propio de la gestión de riesgos de TI de acuerdo con lo propuesto por las mejores prácticas de la industria seleccionadas en la sección 4.2.2.

- Las brechas identificadas en la sección 4.1.4.1., que no se incluyen en las exclusiones del proyecto planteadas en la sección 1.8., se satisfacen con los artefactos propuestos para la metodología.
- Se propone una hoja de ruta que establece las actividades, distribución temporal, duración y responsables para la implementación de la metodología propuesta, de tal manera que esta se realice de manera estructurada y de acuerdo con lo que dictan las mejores prácticas a partir del estado deseado del proceso descrito en la sección 5.1.1.
- El proceso de gestión de riesgos de TI propuesto cuenta con un 100% de alineación según lo que dictan las mejores prácticas de la industria seleccionadas en la sección 4.2.2. Esto según el análisis de alineación realizado en la sección 5.1.5, en donde se comparó cada una de las prácticas definidas y el contenido de la metodología.

6.4. Objetivo General

Proponer una metodología de gestión de riesgos de TI para Information Evolution Costa Rica, alineada con las mejores prácticas de la industria, para la definición de una estrategia y proceso operativo de la gestión de riesgos de TI durante el segundo semestre del 2024.

- La implementación de la propuesta representa un ahorro anual de ₡5,090,861 por cada año de operación de la metodología propuesta, según el análisis de los beneficios realizado en la sección 5.2.2.
- La propuesta presenta un retorno de inversión (ROI) del 33.49% en su primer año de implementación, demostrando su viabilidad y rentabilidad para la empresa, según los resultados del análisis de viabilidad realizados en la sección 5.2.3.
- Según la metodología propuesta, se requiere al menos una capacitación formal sobre la gestión de riesgos de TI para las partes involucradas.
- La metodología propuesta se adapta al contexto específico de Information Evolution Costa Rica, asignando roles y responsabilidades clave para su implementación, según la sección 5.1.3.
- La propuesta incluye procesos de monitoreo y evaluación periódica, de tal manera que la gestión de riesgos de TI se mantenga alineada con los objetivos estratégicos de la organización, según las secciones 5.1.1.5, 5.1.1.6 y 5.1.2.5.

7. Recomendaciones

En este capítulo se presentan las recomendaciones derivadas del trabajo de investigación y de la propuesta de solución realizada, con el propósito de proporcionar lineamientos adicionales que la organización puede considerar para mejorar y fortalecer la implementación de la metodología de gestión de riesgos de TI.

- Destinar el tiempo necesario de los colaboradores implicados en el proceso de implementación de la metodología de gestión de riesgos de TI para así estandarizar el proceso y reducir las pérdidas por incidentes materializados.
- Capacitar a los colaboradores sobre la gestión de riesgos de TI según la ISO 31000 para que tengan conocimiento del proceso y su funcionamiento.
- Capacitar a los altos mandos sobre el gobierno de TI y la importancia de la gestión de riesgos de TI en las organizaciones.
- Darle seguimiento de manera periódica y actualizar la metodología de gestión de riesgos de TI propuesta y la documentación existente según la versión más actualizada de COBIT 2019 y la ISO 31000.
- Definir un plan de comunicación, a través de la plantilla propuesta, que permita la adopción de la metodología de gestión de riesgos de TI, de tal forma que se garantice la transparencia y su correcta implementación.
- Definir políticas formales sobre la gestión de riesgos de TI y los procesos del departamento de TI en general de tal forma que se trabaje sobre una base sólida y documentada.
- Realizar charlas de concientización para los distintos empleados de la organización sobre la importancia de trabajar bajo procesos estandarizados y de gestionar los riesgos de TI, de tal forma que se aumente el conocimiento y por consiguiente se reduzca la resistencia al cambio al poner en marcha la metodología propuesta.
- Definir los roles y responsabilidades del Gobierno de TI y los encargados de la gestión de riesgos de TI de tal manera que se establezca una base sólida y se mejore la comunicación y adopción de la metodología.
- Incluir la gestión de riesgos de TI en la planificación estratégica de la organización y darle seguimiento continuo de modo que esta se encuentre alineada a los objetivos empresariales.
- Monitorear y controlar el cumplimiento del proceso propuesto para la gestión de riesgos de TI y su impacto en la organización.
- Revisar y definir los indicadores clave de desempeño e indicadores clave de riesgos de tal manera que estos ayuden a monitorear los resultados deseados y estén alineados con las políticas definidas.
- Realizar reportes continuos a la alta gerencia sobre el seguimiento y revisión de los riesgos y el cumplimiento del proceso propuesto.

- Realizar monitoreos de la asistencia y participación activa de los participantes en las capacitaciones y charlas de concientización de tal forma que se mida el desempeño de estos y se reduzca la resistencia al cambio.
- Implementar un proceso de mejora continua utilizando el ciclo de Deming (Planificar, Hacer, Verificar, Actuar) para garantizar la actualización constante y efectividad de la metodología de gestión de riesgos de TI.
- Adoptar, al mediano o largo plazo, herramientas tecnológicas específicas para la gestión de riesgos de TI, como RSA Archer Suite, MetricStream o ServiceNow GRC, para automatizar el seguimiento, evaluación y tratamiento de riesgos, optimizando la eficiencia del proceso de gestión de riesgos de TI.

8. Referencias

Acronis. (2021, 24 de junio). *Gestión de riesgos de TI: Estrategias y mejores prácticas*. Acronis. https://www.acronis.com/es-mx/blog/posts/it-risk-management/

Alemán Novoa, H., & Rodríguez Barrera, C. (2015). Metodologías para el análisis de riesgos en los sgsi. Publicaciones E Investigación, 9, 73-86. https://doi.org/10.22490/25394088.1435

Alfaro Campos, J. (2017). *Metodología para la gestión de riesgos de TI basada en COBIT 5*. [Trabajo Final de Graduación, Instituto Tecnológico de Costa Rica]. https://repositoriotec.tec.ac.cr/bitstream/handle/2238/11060/metodologia_gestion_riesgos_ti_basada_cobit5.pdf?sequence=1&isAllowed=y

Alvarado, D. F., & Zumba, L. A. (2015). *Elaborar un Plan de Gestión de Riesgos de las Tecnologías de Información y Comunicación basada en el Marco COBIT 5 para Riesgos aplicado a la Universidad de Cuenca*. Tesis de Licenciatura, Universidad de Cuenca, Facultad de Ciencias Económicas y Administrativas, Cuenca. https://dspace.ucuenca.edu.ec/handle/123456789/22342

Azuero, Á. E. A. (2019). *Significatividad del marco metodológico en el desarrollo de proyectos de investigación*. Revista arbitrada interdisciplinaria Koinonía, 4(8), 110-127.

Concha-Torre, A., Alonso, Y. D., Blanco, S. Á., Allende, A. V., Mayordomo-Colunga, J., & Barrio, B. F. (2020, August). Las listas de verificación: ¿una ayuda o una molestia? In Anales de Pediatría (Vol. 93, No. 2, pp. 135-e1). Elsevier Doyma.

Delta Protect. (2023, 6 de enero). Análisis GAP: ¿Qué es, ¿cómo se hace y por qué es importante para las empresas?. LinkedIn. https://www.linkedin.com/pulse/an%C3%A1lisis-gap-qu%C3%A9-es-c%C3%B3mo-se-hace-y-por-importante-para-las-/

Dugarte Coll, Y. (2017). *Diseño del Proceso De Gestión De Riesgos de TI de la multinacional "La Compañía" e implementación en el área de operaciones de TI Colombia*. [Proyecto de Grado, Universidad del Norte]. https://manglar.uninorte.edu.co/bitstream/handle/10584/8546/129821.pdf?sequence=1&isAllowed=y

ESGinnova Group. (2017, 5 de enero). ISO 27005: Cómo identificar los riesgos. PMG. https://www.pmg-ssi.com/2017/01/iso-27005-como-identificar-los-riesgos/

Esteban Nieto, N. T. (2018). *Tipos de investigación*. Universidad Santo Domingo de Guzmán, 2, 1-2.

Gartner. (s. f.). Definition of Business Process Management (BPM) - Gartner Information

Guzmán Stein, L. (1982). *Las fuentes secundarias*. Escuela de Trabajo Social, Universidad de Costa Rica., Escuela de Trabajo Social, Universidad de Costa Rica. Recuperado de https://www.ts.ucr.ac.cr/binarios/docente/pd-000169.pdf

Guy Birken, E. (2023,10 de julio). ROI: What is return on investment? Forbes Advisor. https://www.forbes.com/advisor/investing/roi-return-on-investment/#:~:text=Commissions%20do%20not%20affect%20our,earned%20to%20evaluate%20its%20efficiency

Hernández-Sampieri, R., & Mendoza, C. (2020). *Metodología de la investigación: las rutas cuantitativa, cualitativa y mixta*.

Information Evolution. (s.f). *Company*. https://informationevolution.com/company/

International Organization for Standardization. (2018). *ISO 31000:2018: Gestión del riesgo - Directrices*. https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:es

ISACA. (2018). *COBIT 2019 Framework: Introduction and Methodology*. ISACA.

ISACA. (2018). *COBIT 2019 Framework: Introduction and Methodology*. ISACA.

ISACA. (2009). *Marco de Riesgos de TI*. ISACA.

ISACA. (2020). *RISK IT Framework*. ISACA.

Kumsuprom, S. (2010). *Structured approach to organisational ICT risk management: An empirical study in Thai businesses*., September, 353.

Ministerio de Trabajo y Seguridad Social de Costa Rica. (2024). Lista de salarios mínimos 2024. https://www.mtss.go.cr/temas-laborales/salarios/Documentos-Salarios/lista_salarios_2024.pdf

OpenAI. (2024). *ChatGPT (versión GPT-4).* https://www.openai.com/chatgpt

Pérez Arbesú, L. B. (2014, marzo 27). *Los 7 principales riesgos de TI para las organizaciones, de acuerdo con Zurich. ComputerWeekly*. https://www.computerweekly.com/es/cronica/Los-7-principales-riesgos-de-TI-para-las-organizaciones-de-acuerdo-con-Zurich

RAE. (s.f). *Análisis.* https://dle.rae.es/an%C3%A1lisis?m=form

RAE. (s.f). *Brecha*. https://dle.rae.es/brecha

RAE. (s.f). *Diagrama*. https://dle.rae.es/diagrama?m=form

RAE. (s.f). *Estandarizar*. https://www.rae.es/diccionario-estudiante/estandarizar

RAE. (s.f). *ISO*. https://dle.rae.es/iso?m=form

RAE. (s.f). *Modelo*. https://dle.rae.es/modelo?m=form

RAE. (s.f). *Procedimiento*. https://dle.rae.es/procedimiento?m=form

RAE. (s.f). *Proceso*. https://dle.rae.es/proceso?m=form

Riveros, A. (2020, 25 de junio). ¿Qué es la norma ISO 31000 y para qué sirve? EALDE Business School. https://www.ealde.es/iso-31000-para-que-sirve/

Rosendahl, M., & Paik, J. (2023,12 de julio). Have you fully cracked the efficiency code? McKinsey & Company. https://www.mckinsey.com/capabilities/operations/our-insights/operations-blog/have-you-fully-cracked-the-efficiency-code

Sarli, R., González, S. I., & Ayres, N. A. T. A. L. I. A. (2015). Análisis FODA. Una herramienta necesaria. Revista de la Facultad de Odontología, 9(1), 17-20.

Spikin, I. C. (2013). *Risk Management theory: the integrated perspective and its application in the public sector*. Estado, gobierno, gestión pública: Revista Chilena de Administración Pública, (21), 89-126.

SYDLE. (2022). *BPM, BPMN y BPMS: Entienda la diferencia entre estos términos*. https://www.sydle.com/es/blog/bpm-bpmn-bpms-60ba98c3a5c829237349b32f

SYDLE. (2021). Estandarización de procesos: Qué es, ventajas y cómo hacerla. SYDLE. Recuperado de https://www.sydle.com/es/blog/estandarizacion-de-procesos-60f723cfb2503757979bb13b

SYDLE. (2024). Procesos empresariales: ¿Qué son y cuáles son los más utilizados? SYDLE. Recuperado de https://www.sydle.com/es/blog/procesos-empresariales-62686abc355bcb08dcbe06ec

SYDLE. (2023). *Cómo mapear procesos AS-IS, TO-BE y TO-DO*. https://www.sydle.com/es/blog/mapear-procesos-as-is-to-be-to-do-60a81ebd22559e108ed7f51e

Technology Glossary. https://www.gartner.com/en/information-technology/glossary/business-process-managementbpm

Tilly, C. (1991). Grandes estructuras, procesos amplios, comparaciones enormes. Madrid: Alianza.

Valencia, F. J., Marulanda, C. E., & López, M. (2016). *Gobierno y gestión de riesgos de tecnologías de información y aspectos diferenciadores con el riesgo organizacional*. (R. Llamosa Villalba, Ed.) Gerencia Tecnológica Informática, 15(41), 65-77. http://revistas.uis.edu.co/index.php/revistagti/article/view/5911

Vanner, C. (2020, 15 de diciembre) What is Process Modeling? 6 Essential Questions Answered. Bizagi Site. https://www.bizagi.com/en/blog/what-is-process-modeling#:~:text=Process%20modeling%20is%20the%20graphical,context%20of%20the%20business%20environment.

Vanegas Devia, G. (2013). Armonización de múltiples modelos para el análisis de riesgos de las tecnologías de la información y desarrollo de software.

https://bibliotecadigital.usb.edu.co/entities/publication/07f6513b-30e0-4f64-b2c4-79b32ac5dfe3

Vindas Sosa, D. (2021). *Propuesta de Estandarización y Automatización de Procesos Administrativos de la Empresa Suum Technologies*. [Trabajo Final de Graduación, Instituto Tecnológico de Costa Rica]. https://repositoriotec.tec.ac.cr/bitstream/handle/2238/15054/TF%209749_BIB303772_Dayana%20Vindas%20Sosa.pdf?sequence=1&isAllowed=y

9. Apéndices

A. Apéndice A: Cronograma para la elaboración del proyecto

Actividad	Semana														
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Ajustes del anteproyecto															
Marco Metodológico del proyecto															
E Marco Conceptual del proyecto															
Elaboración de la Fase I															
Elaboración de la Fase II															
Elaboración de la Fase III															
Análisis financiero de la metodología propuesta															
Conclusiones y Recomendaciones															

B. Apéndice B: Plantilla de minuta de reunión

MINUTA DE REUNIÓN			
Reunión #	**Fecha:** *dd/mm/aaaa*	**Inicio:** *hh:mm*	**Fin:** *hh:mm*
Lugar:	*Indicar el lugar en donde se llevó a cabo la reunión*		
Objetivo:	*Indicar el objetivo de la realización de la reunión*		
Participantes:	*Indicar los participantes de la reunión*		
Temas Tratados			
#	**Asunto**	**Comentarios**	**Acuerdos**
#	*Indicar el asunto del tema*	*Indicar comentarios sobre el tema*	*Indicar los acuerdos*
Observaciones			
Indicar las observaciones sobre la reunión que son relevantes para el desarrollo del proyecto, entre ellas también se añaden firmas de ser necesario			

C. Apéndice C: Plantilla de entrevista.

La siguiente plantilla de entrevista se ha diseñado con el objetivo de recopilar información clave sobre el proceso de gestión de riesgos de TI actualmente implementado en Information Evolution Costa Rica, es por esto que, a través de una entrevista semiestructurada, se busca obtener una visión detallada de los métodos y procedimientos que la empresa utiliza para identificar, evaluar y gestionar los riesgos tecnológicos y las principales fortalezas y debilidades del proceso actual.

La información recopilada mediante estas entrevistas será fundamental para realizar un análisis exhaustivo de la situación actual y desarrollar una propuesta metodológica que se alinee con las mejores prácticas de la industria.

Preguntas base para la entrevista semiestructurada

- Métodos y procedimientos actuales
  - ¿Qué métodos y herramientas se utilizan actualmente para la identificación de riesgos de TI?
  - ¿Podría explicar el procedimiento que sigue la empresa para evaluar los riesgos una vez identificados?
  - ¿Qué estrategias se utilizan para mitigar o responder a los riesgos una vez evaluados?
  - ¿Existe un protocolo definido para monitorear y revisar los riesgos a lo largo del tiempo?
  - ¿Cómo se documentan los riesgos y las acciones tomadas para gestionarlos?
- Fortalezas y debilidades del proceso de gestión de riesgos
  - ¿Cuáles considera que son las principales fortalezas del proceso actual de gestión de riesgos?
  - ¿Qué aspectos del proceso actual cree que han contribuido más a la seguridad y estabilidad operativa de la empresa?
  - ¿Cuáles son las principales debilidades o desafíos que enfrenta el proceso actual de gestión de riesgos?
  - ¿Existen áreas específicas donde considere que el proceso de gestión de riesgos podría mejorar?
- Mejora del proceso de gestión de riesgos
  - En su opinión, ¿cómo podría mejorarse el proceso de gestión de riesgos actual?
  - ¿Qué recursos adicionales (herramientas, formación, personal) considera que serían necesarios para optimizar el proceso de gestión de riesgos?
  - ¿Cómo percibe la cultura organizacional en relación con la gestión de riesgos de TI? ¿Hay áreas que podrían fortalecerse?

Plantilla para la documentación de la entrevista

ENTREVISTA			
Entrevista #	**Fecha:** *dd/mm/aaaa*	**Inicio:** *hh:mm*	**Fin:** *hh:mm*
Objetivo:	*Indicar el objetivo que tiene la entrevista*		
Entrevistador:	*Indicar el nombre de la persona que entrevista*		
Entrevistado:	*Indicar el nombre de la persona que es entrevistada*		

Preguntas		
#	**Pregunta**	**Respuesta**
#	*Indicar la pregunta planteada por el entrevistador*	*Indicar la respuesta dada por el entrevistado*

Observaciones
Indicar las observaciones sobre la entrevista que son relevantes para el desarrollo del proyecto, entre ellas también se añaden firmas de ser necesario

D. Apéndice D: Plantilla para la gestión del cambio

SOLICITUD DE CAMBIO		
Datos Generales del Cambio		
Cambio #		
Solicitante:	*Indicar el nombre de la persona que solicita el cambio*	
Responsable de implementación	*Indicar el nombre de la persona responsable por la implementación del cambio*	
Fecha de Solicitud:		**Fecha de Implementación:**
Estado:	**( ) Aprobado** **( ) En Revisión** **( ) Rechazado**	
Detalles del Cambio		
Categoría:	*Indicar la categoría del cambio*	
Descripción:	*Indicar una descripción detallada del cambio a realizar*	
Justificación:	*Indicar la justificación de la importancia de realizar el cambio en el proyecto*	
Implicaciones:	*Indicar las implicaciones que el cambio trae consigo*	
Prioridad:	**( ) Alta** **( ) Media** **( ) Baja**	
Impacto:	**( ) Alto** **( ) Medio** **( ) Bajo**	
Observaciones:	*Indicar las observaciones pertinentes al cambio*	
Aprobación		
Elaborado por: *Nombre del estudiante* *Firma* (Estudiante)		**Aprobado por:** *Coordinadora del TFG* *Firma* (Coordinación TFG)
Revisado por: *Nombre del tutor* *Firma* (Profesor tutor)		**Revisado por:** *Representante de la empresa* *Firma* (Empresa)

E. Apéndice E: Plantilla del formulario para la revisión documental

La siguiente plantilla de revisión documental ha sido diseñada para registrar y analizar los puntos clave de cada documento relevante revisado en el contexto del proyecto de gestión de riesgos de TI en Information Evolution Costa Rica. Para cada documento revisado, se deberá completar una tabla que refleje los aspectos más importantes y pertinentes que el investigador considere esenciales para el análisis.

Esta estructura permite una revisión exhaustiva y organizada, facilitando la identificación de temas recurrentes y asegurando que toda la información relevante sea considerada en la propuesta metodológica.

Nombre del documento: ***Escribir el nombre del documento***
Objetivo del documento
Describir brevemente en lo que consiste el documento a analizar
Hallazgos encontrados
- *Resumir los aspectos de relevancia que encontramos en el documento y que son necesarios para el desarrollo del proyecto*

F. Apéndice F: Plantilla guía para la elaboración de grupos focales.

La siguiente plantilla para el grupo focal ha sido diseñada con el objetivo de analizar la situación actual del proceso de gestión de riesgos de TI en Information Evolution Costa Rica, por lo que este grupo focal se llevará a cabo para obtener perspectivas variadas y detalladas de los participantes, quienes compartirán sus experiencias, percepciones y sugerencias sobre el proceso actual de gestión de riesgos.

A través de la discusión guiada, se busca identificar fortalezas, debilidades, y áreas de mejora que contribuirán a un análisis exhaustivo de la situación actual. Los resultados obtenidos de este grupo focal serán fundamentales para desarrollar una propuesta metodológica que optimice la gestión de riesgos en la organización, alineándose con las mejores prácticas de la industria.

Guía base de preguntas para la ejecución del grupo focal

- Discusión sobre el proceso actual de gestión de riesgos de TI
    - ¿Cómo describirían el estado actual del proceso de gestión de riesgos de TI en su departamento?
    - ¿Cuáles consideran que son los principales desafíos o problemas que enfrentan actualmente en la gestión de riesgos de TI?

- Según su experiencia, ¿qué aspectos del proceso actual funcionan bien y cuáles no?
- ¿Cómo perciben la cultura organizacional en torno a la gestión de riesgos de TI? ¿Creen que el equipo está preparado para identificar y gestionar riesgos?

- Identificación de brechas
  - Basándonos en el análisis FODA previamente realizado, ¿qué brechas consideran más críticas entre el estado actual y el estado deseado del proceso de gestión de riesgos?
  - ¿Existen recursos, herramientas o capacidades específicas que creen que están faltando para cerrar estas brechas?
  - ¿Hay políticas o procedimientos actuales que necesiten ser ajustados o creados para mejorar la gestión de riesgos de TI?
  - ¿Cómo se podría mejorar la comunicación y colaboración entre los equipos de TI y otras áreas para gestionar los riesgos de manera más efectiva?

- Sugerencias para la mejora del proceso
  - ¿Cuál sería su visión ideal para el proceso de gestión de riesgos de TI? ¿Qué elementos clave deberían incluirse?
  - ¿Qué cambios específicos consideran necesarios para alcanzar ese estado futuro deseado?
  - ¿Qué indicadores de éxito utilizarían para medir que el proceso de gestión de riesgos ha mejorado?
  - ¿Cómo imaginan que se pueden integrar mejores prácticas de la industria en el proceso de gestión de riesgos de la empresa?

Plantilla para la documentación del grupo focal

GRUPO FOCAL			
Grupo Focal #	**Fecha:** *dd/mm/aaaa*	**Inicio:** *hh:mm*	**Fin:** *hh:mm*
Objetivo:	*Indicar el objetivo que tiene el grupo focal*		
Organizador:	*Indicar el nombre de la persona que organiza el grupo focal*		
Participantes:	*Indicar el nombre de las personas que participan en el grupo focal*		
Preguntas			
Pregunta		**Resultados**	
Indicar la pregunta planteada por el entrevistador		*Indicar los resultados obtenidos*	

Observaciones
Indicar las observaciones del grupo focal que son relevantes para el desarrollo del proyecto, entre ellas también se añaden firmas de ser necesario

G. Apéndice G: Plantilla guía para el análisis comparativo

La siguiente plantilla de análisis comparativo ha sido elaborada para facilitar la evaluación y comparación de las mejores prácticas de la industria en la gestión de riesgos de TI, por lo que permitirá identificar cuáles de estas prácticas se adaptan mejor a las necesidades específicas de Information Evolution Costa Rica.

La plantilla está diseñada para registrar las características clave de cada práctica, así como los criterios de comparación que el investigador considere relevantes.

	Metodología 1	**…**	**Metodología *n***
Criterio 1			
….			
Criterio n			

H. Apéndice H: Plantilla para la lista de verificación

La siguiente plantilla de lista de verificación ha sido diseñada para asegurar que todos los elementos necesarios en el proceso de gestión de riesgos de TI estén presentes y correctamente implementados, por lo que permitirá al investigador verificar y medir el nivel de alineación con las mejores prácticas establecidas.

LISTA DE VERIFICACIÓN: *NOMBRE DE LA PRÁCTICA*		
Criterio	**¿Se cumple?**	**Evidencia**
Criterio 1	*Sí/No*	*¿En qué parte del entregable se cumple?*
…	…	…
Criterio n	*Sí/No*	*¿En qué parte del entregable se cumple?*
Total de criterios: *X*	**Total de criterios cumplidos: *Y***	**Porcentaje de alineación: *(Y * 100) / X* %**

I. Apéndice I: Plantilla para el análisis FODA

La siguiente plantilla de análisis FODA se ha desarrollado para identificar y analizar las fortalezas, debilidades, oportunidades y amenazas en el proceso de gestión de riesgos de TI en Information Evolution Costa Rica., el cual proporcionará una visión clara y estructurada de los aspectos internos y externos que influyen en la gestión de riesgos, permitiendo al investigador formular estrategias que potencien las fortalezas, minimicen las debilidades, aprovechen las oportunidades y mitiguen las amenazas.

FORTALEZAS	OPORTUNIDADES
- Hallazgo 1 *- ...* *- Hallazgo n*	*- Hallazgo 1* *- ...* *- Hallazgo n*
DEBILIDADES	**AMENENAZAS**
- Hallazgo 1 *- ...* *- Hallazgo n*	*- Hallazgo 1* *- ...* *- Hallazgo n*

J. Apéndice J: Minuta de reunión para la definición del problema

MINUTA DE REUNIÓN			
Reunión #1	**Fecha: 15/04/2024**	**Inicio: 13:00**	**Fin: 14:00**
Lugar:	Reunión por medio de Google Meets		
Objetivo:	Situación problemática de la empresa Information Evolution Costa Rica		
Participantes:	Fabiana Herrera Madriz, Ingeniero Carlos Daniel Calderón Salazar (Administrador de TI)		
Temas Tratados			
#	**Asunto**	**Comentarios**	**Acuerdos**
1	Identificación de problemas en la empresa	Carlos Calderón explica las distintas situaciones problemáticas por las que enfrenta la empresa	Se definen las causas que dan paso al problema principal

2	Identificación del problema principal	Se realiza un análisis y se ordenan las distintas situaciones problemáticas	Se define el problema principal por el que se desencadenan las situaciones problemáticas

Observaciones

- Se realiza una reunión por medio de google meets, por ende, se adjunta la firma del Administrador del departamento de TI, Carlos Calderón Salazar, como constancia de la reunión.
- Carlos Calderón, junto con sus conocimientos en el campo de la investigación, ayuda a definir el problema que aborda la empresa

Firma por parte del Ingeniero Carlos Calderón Salazar.

K. Apéndice K: Entrevista para el análisis de la situación actual

ENTREVISTA			
Entrevista #2	**Fecha:** 04/09/2024	**Inicio:** 13:00	**Fin:** 14:00
Objetivo:	Análisis de la situación actual del proceso de gestión de riesgos de TI		
Entrevistador:	Fabiana Herrera Madriz		
Entrevistado:	Carlos Calderón Salazar		

Preguntas

#	Pregunta	Respuesta
1	¿Qué métodos y herramientas se utilizan actualmente para la identificación de riesgos de TI?	Se actúa sobre la marcha, no se identifican riesgos, lo que se hace es tener equipo en stock Cuando el riesgo ya se presenta y se convierte en incidente se comunica por chat de Gmail para conectarse a la computadora o bien pedir fotos y presentarse presencial a ver lo que pasó
2	¿Podría explicar el procedimiento que sigue la empresa para evaluar los riesgos una vez identificados	Lo único que se hace es saber que los riesgos pueden ocurrir y se tiene inventario por si son de activos, si no lo es se actúa sobre la marcha.
3	¿Qué estrategias se utilizan para mitigar o responder a los riesgos una vez evaluados?	No hay estrategias de mitigación o respuesta de riesgos.
4	¿Existe un protocolo definido para monitorear y revisar los riesgos a lo largo del tiempo?	No existe protocolo, actualmente se trabaja en la definición del proceso, sin embargo, solo existe un borrador.

5	¿Cómo se documentan los riesgos y las acciones tomadas para gestionarlos?	Cuando ocurre algún incidente se mantiene registro en caso de ser de activos, si no es de activos se registra en un documento de tareas diarias.
6	¿Cuáles considera que son las principales fortalezas del proceso actual de gestión de riesgos	La única fortaleza identificada es el manejo de inventario extra de un 3% en caso de un riesgo a nivel de activos.
7	¿Qué aspectos del proceso actual cree que han contribuido más a la seguridad y estabilidad operativa de la empresa?	Al mantener inventario la producción nunca se ve afectada, por lo que no existen atrasos de más de 24 horas.
8	¿Cuáles son las principales debilidades o desafíos que enfrenta el proceso actual de gestión de riesgos?	No existe un procedimiento específico para tratar los riesgos, por lo que si algo se presenta se debe actuar sobre la marcha con distintas soluciones, ya que al no tener todo registrado, muchas veces no se sabe cómo actuar ante eventualidades.
9	¿Existen áreas específicas donde considere que el proceso de gestión de riesgos podría mejorar?	En todo, se considera necesario definir un proceso de gestión de riesgos, ya que no hay un área fuerte como tal.
10	En su opinión, ¿cómo podría mejorarse el proceso de gestión de riesgos actual?	- Identificación de riesgos. - Catálogo de respuestas. - Manual de procedimiento de riesgos Se necesita un proceso estructurado que ayude a actuar de manera proactiva, ya que este proceso reactivo actual está tomando alrededor de 4-5 horas diarias de la jornada laboral del administrador de TI.
11	¿Qué recursos adicionales (herramientas, formación, personal) considera que serían necesarios para optimizar el proceso de gestión de riesgos?	Personal con experiencia sobre el tema y formación sobre gestión de riesgos y cómo se utiliza en una empresa.
12	¿Cómo percibe la cultura organizacional en relación con la gestión de riesgos de TI? ¿Hay áreas que podrían fortalecerse?	La cultura es baja, hay mucha resistencia al cambio, por lo que es necesario capacitación al personal sobre la importancia de la gestión de riesgos de TI en las organizaciones.
Observaciones		
La empresa no cuenta con documentación sobre riesgos ni una línea base a seguir para el proceso. **Firma de Carlos Calderón Salazar:** 		

L. Apéndice L: Grupo focal para el análisis del estado deseado del proceso de gestión de riesgos de TI

GRUPO FOCAL			
Grupo Focal #1	**Fecha:** 10/09/2024	**Inicio:** 9:00am	**Fin:** 10:00am
Objetivo:	Discutir sobre el estado futuro deseado del proceso de gestión de riesgos de TI		
Organizador:	Fabiana Herrera Madriz		
Participantes:	Carlos Calderón Salazar, Andrés Cabezas Marín		

Preguntas	
Pregunta	**Resultados**
¿Cómo describirían el estado actual del proceso de gestión de riesgos de TI en su departamento?	No existe nada sobre gestión de riesgos, solo se actúa sobre la marcha y se revisa el documento donde se apuntan los incidentes a ver si se puede resolver algo de la misma manera, o bien, dar equipo nuevo si fue incidente de activos.
¿Cuáles consideran que son los principales desafíos o problemas que enfrentan actualmente en la gestión de riesgos de TI?	Falta de apoyo por falta de los altos mandos. Necesidad de recursos y conocimiento técnico para gestionar riesgos. Necesidad de un proceso propio de gestión de riesgos. Baja gestión de conocimiento en temas de gestión de los incidentes ocurridos, ya que se depende solo de una persona que nos arregle con un proceso que no está escrito.
Según su experiencia, ¿qué aspectos del proceso actual funcionan bien y cuáles no?	Funciona bien tener stock extra en caso de incidentes relacionados con activos No funciona bien el no tener riesgos identificados, analizados y sus respectivos tratamientos o medidas en caso de presentarse
¿Cómo perciben la cultura organizacional en torno a la gestión de riesgos de TI? ¿Creen que el equipo está preparado para identificar y gestionar riesgos?	La cultura es baja, el equipo puede identificar los riesgos, sin embargo, no tienen el conocimiento necesario para gestionarlos, el líder de operaciones tiene conocimientos en gestión de riesgos, sin embargo, se necesitan capacitaciones.
Basándonos en el análisis FODA previamente realizado, ¿qué brechas consideran más críticas entre el estado actual y el estado deseado del proceso de gestión de riesgos?	La cultura organizacional baja = 30/100 Necesidad de apoyo por parte de la gerencia al desconocer la importancia de gestión de riesgos = 45/100 Necesidad de recursos = 10/100 Necesidad de políticas definidas = 15/100

¿Existen recursos, herramientas o capacidades específicas que creen que están faltando para cerrar estas brechas?	Conocimiento sobre la gestión de riesgos Plantillas estandarizadas para el proceso Políticas definidas
¿Hay políticas o procedimientos actuales que necesiten ser ajustados o creados para mejorar la gestión de riesgos de TI?	Se necesita crear todos los procesos y políticas, ya que la empresa no tiene nada sobre gestión de riesgos dado que la alta gerencia no conoce su importancia
¿Cómo se podría mejorar la comunicación y colaboración entre los equipos de TI y otras áreas para gestionar los riesgos de manera más efectiva?	Charlas sobre la importancia de gestión de riesgos Planes de comunicación para los procesos del equipo Capacitaciones sobre gestión de riesgos para que todo el equipo esté en la misma línea
¿Cuál sería su visión ideal para el proceso de gestión de riesgos de TI? ¿Qué elementos clave deberían incluirse?	Un proceso específico estandarizado para gestionar los riesgos de TI la organización Globalización con respecto a la comunicación de riesgos Cultura organizacional con conocimientos de la importancia de los procesos Políticas bases definidas.
¿Qué cambios específicos consideran necesarios para alcanzar ese estado futuro deseado?	Una cultura organizacional fuerte Capacitaciones al equipo sobre gestión de riesgos Definición de directrices y estandarización de operaciones
¿Qué indicadores de éxito utilizarían para medir que el proceso de gestión de riesgos ha mejorado?	Cantidad de riesgos materializados que se presentan Nivel de impacto de los riesgos materializados en la organización
¿Cómo imaginan que se pueden integrar mejores prácticas de la industria en el proceso de gestión de riesgos de la empresa?	Educación de las partes sobre la importancia de estandarizar las prácticas de acuerdo con lo que dictan las prácticas organizacionales.
Observaciones	
El equipo llegó al consenso de que es de suma importancia la documentación y correcta comunicación para el proceso, aparte de que el proceso actual es prácticamente inexistente y el nivel de madurez del proceso es sumamente bajo, prácticamente más cerca del 0 que del 1. Aparte que no deben regirse por normas impuestas por el cliente o internas de la empresa. En la pregunta número 5, el equipo priorizó los principales desafíos que enfrenta la empresa utilizando una puntuación total de 100pts, su resultado se encuentra en la respuesta de la pregunta. Firma de Carlos Calderón Firma de Andrés Cabezas	

M. Apéndice M: Listas de verificación para determinar el nivel de alineación de las mejores prácticas de la industria con las necesidades de la empresa

A continuación, se presenta la evaluación del nivel de alineación de cada una de las mejores prácticas de la industria en gestión de riesgos de TI que fueron evaluadas para el desarrollo del trabajo.

PRÁCTICA EVALUADA: COBIT 2019		
Criterio	**¿Se cumple?**	**Evidencia**
Aplicabilidad al tipo de empresa	SÍ	COBIT 2019 está diseñado para organizaciones de cualquier tamaño y sector con TI, independientemente si son públicas o privadas.
Implementación de un ciclo de gestión de riesgos adaptable a cualquier riesgo de TI	SÍ	Incluye procesos específicos como EDM03 y APO12 para gestionar riesgos de TI de manera integral, desde riesgos por activos de TI hasta riesgos de seguridad de la información.
Facilidad de implementación inicial sin conocimiento previo	NO	Puede ser complejo para empresas sin experiencia previa en gestión de riesgos, sin embargo, trae directrices detalladas para el proceso que sirven como guía clara para su implementación.
Coste de implementación accesible a presupuestos bajos	NO	Puede requerir una inversión considerable en capacitación y herramientas si la organización no cuenta con lo necesario,
Enfoque en mejora continua	SÍ	Promueve revisiones y auditorías periódicas para mejora continua.
Integración con normativas y otros marcos	SÍ	Compatible con otros estándares internacionales como las normas ISO.
Involucramiento de todas las partes interesadas de la organización	SÍ	Requiere la participación de la alta dirección y las partes interesadas clave.
Compatibilidad con los recursos humanos y técnicos existentes	SÍ	A pesar de que puede necesitar más personal capacitado del existente, su implementación es posible con los recursos de la empresa.
Cantidad total de criterios: 8	**Criterios cumplidos: 6**	**Porcentaje de alineación: 75%**

PRÁCTICA EVALUADA: ISO 31000		
Criterio	**¿Se cumple?**	**Evidencia**
Aplicabilidad al tipo de empresa	SÍ	La ISO 31000 está diseñada para organizaciones de cualquier tamaño y sector, independientemente de si son públicas o privadas.
Implementación de un ciclo de gestión de riesgos adaptable a cualquier riesgo de TI	SÍ	Define un ciclo de gestión de riesgos general que incluye todos los pasos clave para su implementación en la empresa.
Facilidad de implementación inicial sin conocimiento previo	SÍ	Es menos complejo y puede ser adoptado progresivamente, lo que lo hace ideal para empresas sin una gestión o conocimiento previo.
Coste de implementación accesible a presupuestos bajos	SÍ	No requiere inversiones significativas, adaptándose a presupuestos limitados.
Enfoque en mejora continua	SÍ	Incorpora un enfoque claro en la mejora continua de la gestión de riesgos, haciéndola adaptable a nuevos desafíos.
Integración con normativas y otros marcos	SÍ	Compatible con otros estándares internacionales de gestión, permitiendo flexibilidad y adaptación.
Involucramiento de todas las partes interesadas de la organización	SÍ	Enfatiza la importancia del compromiso de todas las partes interesadas, incluyendo la alta dirección.
Compatibilidad con los recursos humanos y técnicos existentes	SÍ	Puede ser gestionado con el personal y recursos actuales, facilitando su implementación.
Cantidad total de criterios: 8	**Criterios cumplidos: 8**	**Porcentaje de alineación: 100%**

PRÁCTICA EVALUADA: ISO 27005		
Criterio	**¿Se cumple?**	**Evidencia**
Aplicabilidad al tipo de empresa	SÍ	Diseñada para organizaciones de cualquier tamaño y sector que se interesen por la seguridad de la información.
Implementación de un ciclo de gestión de riesgos adaptable a cualquier riesgo de TI	NO	Su ciclo de gestión de riesgos está directamente alineado con la seguridad de la información, es por esto que incluye un enfoque integral para otros tipos de riesgos de TI.
Facilidad de implementación inicial sin conocimiento previo	NO	Requiere experiencia en gestión de SGSI, con la cual no cuenta la empresa.
Coste de implementación accesible a presupuestos bajos	NO	Su implementación puede ser costosa debido a la necesidad de implementar controles de SGSI.
Enfoque en mejora continua	SÍ	Promueve revisiones periódicas para la mejora continua de la seguridad de la información.
Integración con normativas y otros marcos	SÍ	Compatible con la ISO 27001 y otros estándares de SGSI.
Involucramiento de todas las partes interesadas de la organización	SÍ	Involucra la participación de todas las partes interesadas en TI y seguridad de la información.
Compatibilidad con los recursos humanos y técnicos existentes	NO	Se necesitan especialistas en seguridad de la información y recursos adicionales para la implementación del SGSI.
Cantidad total de criterios: 8	**Criterios cumplidos: 4**	**Porcentaje de alineación: 50%**

PRÁCTICA EVALUADA: MARGERIT		
Criterio	**¿Se cumple?**	**Evidencia**
Aplicabilidad al tipo de empresa	NO	Orientada especialmente a empresas con administraciones públicas.
Implementación de un ciclo de gestión de riesgos adaptable a cualquier riesgo de TI	NO	A pesar de que cuenta con todos los pasos para la gestión de riesgos, el enfoque de este ciclo es en los activos de TI y no presenta una evaluación integral de los otros tipos de riesgos.
Facilidad de implementación inicial sin conocimiento previo	NO	Al ser orientada a administraciones públicas con altas regulaciones, su implementación es específica y detallada a las normas públicas a las que se debe de alinear la empresa.
Coste de implementación accesible a presupuestos bajos	NO	Requiere inversiones significativas en herramientas y formación específica para el sector público.
Enfoque en mejora continua	SÍ	Incluye revisiones periódicas y un enfoque en mejora continua.
Integración con normativas y otros marcos	SÍ	Está basado en la ISO 31000 y es alineable con otros marcos de referencia.
Involucramiento de todas las partes interesadas de la organización	SÍ	Involucra a los altos mandos de TI de la organización y a los responsables de la toma de decisiones y departamento de TI.
Compatibilidad con los recursos humanos y técnicos existentes	NO	Requiere recursos y personal especializado no disponible en la empresa.
Cantidad total de criterios: 8	**Criterios cumplidos: 3**	**Porcentaje de alineación: 37.5%**

PRÁCTICA EVALUADA: OCTAVE		
Criterio	**¿Se cumple?**	**Evidencia**
Aplicabilidad al tipo de empresa	SÍ	Diseñado para organizaciones de cualquier tamaño y sector con un enfoque en TI y seguridad de la información.
Implementación de un ciclo de gestión de riesgos adaptable a cualquier riesgo de TI	NO	Enfocado más en la evaluación y mitigación de riesgos que en un ciclo integral de gestión de riesgos.
Facilidad de implementación inicial sin conocimiento previo	NO	Su implementación es técnica y específica en áreas de seguridad y TI.
Coste de implementación accesible a presupuestos bajos	NO	Involucra altos costos en herramientas y recursos capacitados en seguridad de la información.
Enfoque en mejora continua	SÍ	Enfatiza la mejora continua mediante la revisión de las fases de gestión de riesgos.
Integración con normativas y otros marcos	SÍ	Alineado con otros marcos de gestión de TI, facilitando su integración.
Involucramiento de todas las partes interesadas de la organización	NO	No enfatiza en la participación de la alta dirección en su metodología.
Compatibilidad con los recursos humanos y técnicos existentes	NO	Requiere personal especializado en seguridad y tecnología, aparte de recursos técnicos adicionales.
Cantidad total de criterios: 8	**Criterios cumplidos: 3**	**Porcentaje de alineación: 37.5%**

N. Apéndice N: Revisión documental existente de los riesgos de TI.

Nombre del documento: Costa Rica Damaged Equipment Template 2024
Objetivo del documento
Documentar los riesgos de TI que se han materializado (Incidentes) con la solución que se les ha dado.
Hallazgos encontrados
- Los incidentes registrados son únicamente referentes a Activos de TI - El documento no se actualiza constantemente y con cada incidente presentado, únicamente con los referentes a daños grandes de los equipos de TI entregados a los colaboradores - No se explica ni hay una línea base del porqué se aplicó esa solución, por lo que es difícil hacer una trazabilidad de los daños y las soluciones obtenidas en caso de que ocurra lo mismo. - El documento es informal del administrador del departamento de TI, por lo que únicamente él cuenta con este documento y es lo único existente acerca de los incidentes presentados o todo lo relacionado a riesgos.

O. Apéndice O: Evaluación de la capacidad del proceso *TO-BE*

- **Proceso Evaluado**: Gestión de Riesgos de TI.
- **Nivel Alcanzado**: 1 - Incompleto

Nivel de Capacidad del Proceso	Criterios	¿Criterios logrados? Sí / No	Resultado	Evidencia
0 - Incompleto	Existen políticas y procedimientos.	Sí	Alcanzado	Criterios y directrices para la gestión del riesgo
	Se ejecutan los procedimientos según lo descrito en las políticas y procedimientos.	No	No Alcanzado	No aplica.
1 - Realizado	Las políticas y procedimientos se encuentran publicados y formalizados	No	No Alcanzado	No aplica.
	El proceso se ejecuta y se generan las salidas esperadas.	Sí	Alcanzado	No aplica, se desarrollan las plantillas a llenar.
	Existen roles y responsabilidades asignadas para el proceso.	Sí	Alcanzado	Matriz RACI.
	Se cuentan con herramientas de apoyo para la ejecución del proceso (formularios, plantillas, etc.).	Sí	Alcanzado	Documentos y plantillas desarrolladas
	Se cuenta con métricas del proceso.	Sí	Alcanzado	KPIs y KRIs
2 - Gestionado	Las políticas y procedimientos se encuentran publicadas, formalizadas y actualizadas.	No	No Alcanzado	No aplica.
	El proceso se ejecuta y se generan las salidas esperadas.	No	No Alcanzado	No aplica.
	Existen roles y responsabilidades asignadas para el proceso y el personal acepta y ejecuta roles.	No	No Alcanzado	No aplica.
	Se cuentan con herramientas de apoyo para la ejecución del proceso y hay evidencia de su utilización.	No	No Alcanzado	No aplica.
	Se cuenta con métricas del proceso y se realiza la medición según lo definido.	No	No Alcanzado	No aplica.

Nivel de Capacidad del Proceso	Criterios	¿Criterios logrados? Sí / No	Resultado	Evidencia
	Se realiza la revisión y mejora del proceso.	No	No Alcanzado	No aplica.
3 - Definido	Las políticas y procedimientos se encuentran publicadas, formalizadas y actualizadas.	No	No Alcanzado	No aplica.
	El proceso se ejecuta y se generan las salidas esperadas.	No	No Alcanzado	No aplica.
	Existen roles y responsabilidades asignadas para el proceso, además el personal acepta y ejecuta roles.	No	No Alcanzado	No aplica.
	El personal se encuentra capacitado y tiene las competencias necesarias para ejecutar el proceso.	No	No Alcanzado	No aplica.
	Se cuentan con herramientas de apoyo para la ejecución del proceso de forma automatizada y hay evidencia de su utilización.	No	No Alcanzado	No aplica.
	Se cuenta con métricas del proceso, se realiza la medición según la periodicidad definida y sirven para la toma de decisiones.	No	No Alcanzado	No aplica.
	Se realiza la planificación de recursos para la atención del proceso, revisión y mejora del proceso.	No	No Alcanzado	No aplica.
4 - Gestionado Cuantitativamente	El proceso se mide y se gestiona utilizando datos cuantitativos y métricas establecidas.	No	No Alcanzado	No aplica.
	El proceso se mide y se gestiona utilizando datos cuantitativos y métricas establecidas.	No	No Alcanzado	No aplica.
	Las métricas recolectadas son analizadas y utilizadas para la toma de decisiones informadas.	No	No Alcanzado	No aplica.

Nivel de Capacidad del Proceso	Criterios	¿Criterios logrados? Sí / No	Resultado	Evidencia
	Las desviaciones en el rendimiento del proceso son identificadas y corregidas de manera proactiva.	No	No Alcanzado	No aplica.
	Se utilizan herramientas avanzadas para el análisis de datos y la optimización del proceso.	No	No Alcanzado	No aplica.
5 - Optimizado	El proceso es continuamente mejorado a través de mediciones cuantitativas y análisis de tendencias.	No	No Alcanzado	No aplica.
	Existe un enfoque sistemático para la mejora continua del proceso basado en lecciones aprendidas y resultados de rendimiento.	No	No Alcanzado	No aplica.
	Se aplican técnicas innovadoras y mejores prácticas para optimizar el proceso.	No	No Alcanzado	No aplica.
	El proceso se ajusta rápidamente a los cambios en el entorno y las necesidades del negocio.	No	No Alcanzado	No aplica.
	Las mejoras se documentan y se implementan consistentemente en toda la organización.	No	No Alcanzado	No aplica.

P. Apéndice P: Minuta de aceptación de la metodología por parte de la contraparte

MINUTA DE REUNIÓN			
Reunión #4	**Fecha: 11/10/2024**	**Inicio: 13:00**	**Fin: 14:00**
Lugar:	Reunión por medio de Google Meets		
Objetivo:	Validación de la metodología creada en el Trabajo Final de Graduación		
Participantes:	Fabiana Herrera Madriz, Ingeniero Carlos Daniel Calderón Salazar (Administrador de TI)		

Temas Tratados			
#	**Asunto**	**Comentarios**	**Acuerdos**
1	Evaluación de los artefactos creados	Se le enseñan los artefactos creados para la implementación de la metodología propuesta	
2	Aceptación de la metodología	Se explica el uso conjunto de los artefactos y la integración general de la metodología	Carlos Calderón aprueba la metodología propuesta y su alineación con las necesidades de la empresa.

Observaciones
Firma por parte del Ingeniero Carlos Calderón Salazar. 

10. Anexos

I. Carta de revisión filológica

Revisiones Filológicas PalmaM.

Carta de Aprobación del Filólogo

24 de octubre de 2024

Señores
Tecnológico de Costa Rica
Escuela de Administración de Tecnologías de Información
Carrera de Administración de Tecnología de Información
Presente

Estimados señores:

La suscrita, Karen Elena Palma Monge, mayor, soltera, filóloga, incorporada a la Asociación Costarricense de Filólogos con el número de carné 271, portadora del número de cédula 1-1410-0933, da fe de que el documento titulado: **"Propuesta de Metodología para la Gestión de Riesgos de TI Basada en las Mejores Prácticas Internacionales para la Empresa Information Evolution Costa Rica."**, elaborado por la estudiante **Fabiana Herrera Madriz** para optar por el grado de **Licenciatura en Administración de Tecnología de Información,** fue sometido a revisión filológica y corrección de estilo.

Se han realizado las modificaciones pertinentes en los distintos niveles textuales, a saber, macro y microestructura, intención comunicativa, coherencia y cohesión, puntuación y ortografía, así como de otros vicios del lenguaje que se pudieron trasladar al texto; además de seguir los protocolos que dicta APA7 y los lineamientos de la universidad. Por tanto, desde ese punto de vista y especificando que la validez del contenido, así como la originalidad del escrito son responsabilidad de la autora, considero que está listo para ser presentado como Proyecto Profesional de Graduación, por cuanto cumple con los requisitos establecidos por la Universidad.

Suscribe de Ustedes cordialmente,

KAREN ELENA PALMA MONGE (FIRMA)
Firmado digitalmente por KAREN ELENA PALMA MONGE (FIRMA)
Fecha: 2024.10.24 18:22:14 -06'00'

Karen E. Palma Monge
Filóloga
Universidad de Costa Rica
Código ACFIL No. 271