Universidad Nacional Mayor de San Marcos
Universidad del Perú. Decana de América

Dirección General de Estudios de Posgrado
Facultad de Ingeniería de Sistemas e Informática
Unidad de Posgrado

Metodología de gestión del riesgo de proyectos de tecnología para PYMES basado en la ISO 31000

TESIS

Para optar el Grado Académico de Magíster en Gobierno de Tecnologías de Información

AUTOR

Jorge Ernesto PISCOYA PRINCIPE

ASESOR

Mg. Fany Yexenia SOBERO RODRÍGUEZ

Lima, Perú

2024

Referencia bibliográfica

Piscoya, J. (2024). *Metodología de gestión del riesgo de proyectos de tecnología para PYMES basado en la ISO 31000*. [Tesis de maestría, Universidad Nacional Mayor de San Marcos, Facultad de Ingeniería de Sistemas e Informática, Unidad de Posgrado]. Repositorio institucional Cybertesis UNMSM.

Metadatos complementarios

Datos de autor	
Nombres y apellidos	Jorge Ernesto Piscoya Principe
Tipo de documento de identidad	DNI
Número de documento de identidad	45440965
URL de ORCID	
Datos de asesor	
Nombres y apellidos	Fany Yexenia Sobero Rodríguez
Tipo de documento de identidad	DNI
Número de documento de identidad	20120467
URL de ORCID	https://orcid.org/0000-0002-0323-6110
Datos del jurado	
Presidente del jurado	
Nombres y apellidos	Cayo Víctor León Fernández
Tipo de documento	DNI
Número de documento de identidad	07001405
Miembro del jurado 1	
Nombres y apellidos	Frank Edmundo Escobedo Bailón
Tipo de documento	DNI
Número de documento de identidad	41671087
Miembro del jurado 2	
Nombres y apellidos	Nilo Eloy Carrasco Ore
Tipo de documento	DNI
Número de documento de identidad	09342780

Datos de investigación	
Línea de investigación	C.0.3.19 Informática y Sociedad
Grupo de investigación	No aplica
Agencia de financiamiento	No aplica
Ubicación geográfica de la investigación	País: Perú Departamento: Lima Provincia: Lima Distrito: Lima Latitud: -12.05642315 Longitud: -77.0843326901621
Año o rango de años en que se realizó la investigación	2023 - 2024
URL de disciplinas OCDE	Otras ingenierías y tecnologías https://purl.org/pe-repo/ocde/ford#2.11.02

UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
Universidad del Perú. Decana de América
Facultad de Ingeniería de Sistemas e Informática
Vicedecanato de Investigación y Posgrado
Unidad de Posgrado

ACTA DE SUSTENTACIÓN DE TESIS PARA OPTAR EL GRADO DE MAGÍSTER EN GOBIERNO DE TECNOLOGÍAS DE INFORMACIÓN

A los nueve (09) días del mes de febrero de 2024, siendo las 9:30 am., se reunieron en el Auditorio, Profesor: Alfredo Celso Alva Bravo, el Jurado de Tesis conformado por los siguientes docentes:

Dr. Cayo Víctor León Fernández (Presidente)
Dr. Frank Edmundo Escobedo Bailón (Miembro)
Mg. Nilo Eloy Carrasco Ore (Miembro)
Mg. Fany Yexenia Sobero Rodríguez (Miembro Asesor)

Se inició la Sustentación invitando al candidato a Magíster ***JORGE ERNESTO PISCOYA PRINCIPE,*** *para que realice la exposición oral de la tesis para optar el Grado de Magíster en Gobierno de Tecnologías de Información, siendo la Tesis intitulada:*

"METODOLOGÍA DE GESTIÓN DEL RIESGO DE PROYECTOS DE TECNOLOGÍA PARA PYMES BASADO EN LA ISO 31000"

Concluida la exposición, los miembros del Jurado de Tesis procedieron a formular sus preguntas que fueron absueltas por el graduando; acto seguido se procedió a la evaluación correspondiente, habiendo obtenido la siguiente calificación:

DIECINUEVE (19) EXCELENTE

Por tanto, el presidente del Jurado, de acuerdo con el Reglamento General de Estudios de Posgrado, otorga al Bachiller ***JORGE ERNESTO PISCOYA PRINCIPE*** *el Grado de Magíster en Gobierno de Tecnologías de Información.*

Siendo las 10:30 *horas, el presidente del Jurado de Tesis, da por concluido el acto académico de Sustentación de Tesis.*

Dr. Cayo Víctor León Fernández
(Presidente)

Dr. Frank Edmundo Escobedo Bailón
(Miembro)

Mg. Nilo Eloy Carrasco Ore
(Miembro)

Mg. Fany Yexenia Sobero Rodríguez
(Miembro Asesor)

CERTIFICADO DE SIMILITUD

Yo **FANY YEXENIA SOBERO RODRIGUEZ** en mi condición de asesor acreditado con Dictamen N° 000531-2023-UPG-VDIP-FISI/UNMSM de la tesis, cuyo título es **METODOLOGÍA DE GESTIÓN DEL RIESGO DE PROYECTOS DE TECNOLOGÍA PARA PYMES BASADO EN LA ISO 31000** presentado por el bachiller/magíster/egresado/licenciado/estudiante **JORGE ERNESTO PISCOYA PRINCIPE** paoptar el grado de magister **en Gobierno de Tecnologías de Información.**

CERTIFICO que se ha cumplido con lo establecido en la Directiva de Originalidad y de Similitud de Trabajos Académicos, de Investigación y Producción Intelectual. Según la revisión, análisis y evaluación mediante el software de similitud textual, el documento evaluado cuenta con el porcentaje de **8** % de similitud, nivel **PERMITIDO** para continuar con los trámites correspondientes y para su **publicación en el repositorio institucional.**

Se emite el presente certificado en cumplimiento de lo establecido en las normas vigentes, como uno de los requisitos para la obtención del grado/ título/ especialidad correspondiente.

Firma del Asesor: _____

DNI: 20120467

Fany Yexenia SOBERO RODRIGUEZ

Querido yo,

Al concluir este desafiante viaje de maestría, celebro tu dedicación, pasión y esfuerzo. Esta tesis refleja tu perseverancia y compromiso con la excelencia. Cada página escrita es un testimonio de tu esfuerzo y crecimiento personal.

Recuerda tu valía y la importancia de seguir persiguiendo tus sueños con determinación. Que esta tesis sea el camino hacia nuevos horizontes. Felicitaciones por tu arduo trabajo, dedicación y valentía. Estoy seguro de que el futuro te reserva innumerables éxitos.

Con admiración,

Jorge Ernesto Piscoya Principe

Agradezco de corazón a mi familia por su inquebrantable respaldo emocional y motivacional durante todo este proceso. Su apoyo ha sido el pilar que me ha permitido superar desafíos y persistir en la consecución de este proyecto.

Quiero expresar mi más sincero agradecimiento a mi asesora, Fany Sobero, cuya orientación experta y dedicación fueron fundamentales para el éxito de esta investigación. Su sabiduría y apoyo constante han sido una guía invaluable.

Asimismo, deseo reconocer a XYZ Tech Solutions por brindar el entorno propicio para implementar y poner a prueba la metodología desarrollada. La colaboración con el equipo de la empresa ha enriquecido significativamente esta investigación, permitiendo aplicar los conceptos teóricos en un entorno práctico.

Este logro no hubiera sido posible sin la contribución crucial de cada uno de ustedes. A todos, mi profundo agradecimiento por ser parte esencial de este viaje académico y profesional.

ÍNDICE GENERAL

Contenido

LISTA DE TABLA

LISTA DE GRÁFICAS

Resumen

El propósito del estudio es abordar la gestión efectiva de riesgos en proyectos tecnológicos dentro del entorno empresarial dinámico, con un enfoque específico en pequeñas y medianas empresas (PYMEs).

El enfoque innovador presentado está diseñado para su aplicación en proyectos tecnológicos dentro de PYMEs, reconociendo la importancia crítica de la gestión de riesgos para el éxito en este contexto empresarial.

El estudio realiza una revisión crítica de teorías y modelos relevantes, destacando la interacción entre la gestión de proyectos, modelos de gestión de riesgos y el marco regulatorio ISO 31000. El enfoque propuesto se basa en esta interrelación respaldada por evaluaciones de expertos, estableciendo una base teórica sólida. Además, la eficacia y aplicabilidad práctica del método se demuestran a través de estudios de casos y verificación empírica.

El enfoque equilibrado entre teoría y práctica, respaldado por la participación activa de expertos y la aplicación de evaluaciones empíricas, busca hacer una contribución significativa al conocimiento de la gestión de riesgos. El objetivo es proporcionar a las PYMEs herramientas valiosas para mejorar las posibilidades de éxito en proyectos tecnológicos, fortaleciendo así la resiliencia empresarial y abordando los desafíos de la gestión de riesgos en un entorno tecnológico cambiante.

Palabras Clave: Gestión de riesgos, Proyectos tecnológicos, PYMEs, Norma ISO 31000, Enfoque innovador, Metodología, Resiliencia empresarial, Sostenibilidad

Abstract

The purpose of the study is to address effective risk management in technology projects within the dynamic business environment, with a specific focus on small and medium-sized enterprises (SMEs).

The innovative approach presented is designed for application in technological projects within SMEs, recognizing the critical importance of risk management for success in this business context.

The study conducts a critical review of relevant theories and models, highlighting the interaction between project management, risk management models and the ISO 31000 regulatory framework. The proposed approach is based on this interrelation supported by expert evaluations, establishing a foundation solid theory. Furthermore, the effectiveness and practical applicability of the method are demonstrated through case studies and empirical verification.

The balanced approach between theory and practice, supported by the active participation of experts and the application of empirical evaluations, seeks to make a significant contribution to the knowledge of risk management. The objective is to provide SMEs with valuable tools to improve the chances of success in technological projects, thus strengthening business resilience and addressing the challenges of risk management in a changing technological environment.

Keywords: Risk management, Technological projects, SMEs, ISO 31000 Standard, Innovative approach, Methodology, Business resilience, Sustainability

1 CAPÍTULO I: INTRODUCCION

1.1 Situación Problemática

En el vertiginoso mundo empresarial contemporáneo, la omnipresencia de la tecnología ha catalizado una nueva era de innovación y eficiencia. Sin embargo, esta acelerada transformación digital no viene exenta de riesgos sustanciales que amenazan la estabilidad y la operatividad de las organizaciones. En este contexto, la gestión de riesgos tecnológicos se erige como un pilar fundamental para la supervivencia y el éxito continuo de las empresas.

Las amenazas son diversas y sofisticadas: desde ciberataques cada vez más elaborados hasta la rápida obsolescencia de tecnologías fundamentales. Este panorama de riesgos tecnológicos plantea desafíos significativos que, de no abordarse de manera proactiva, pueden resultar en pérdidas económicas, daño reputacional y, en última instancia, la disrupción de las operaciones empresariales (Johnson, 2019) (Pérez A. , 2020)

La gestión eficaz de estos riesgos se ha vuelto imperativa. Es en este contexto que la norma internacional ISO 31000 emerge como una guía esencial. Adoptando un enfoque holístico, la ISO 31000 proporciona un marco integral para la identificación, evaluación y gestión de riesgos tecnológicos (Standardization, 2020)**.** Este artículo explora la urgencia de abordar estos desafíos específicos que la tecnología introduce en el entorno empresarial y cómo la ISO 31000 se posiciona como un instrumento clave para mitigar estos riesgos y promover la resiliencia. (Standardization, 2020)

1.2 Formulación del Problema

1.2.1 Problema General

¿De qué manera utilizar una metodología de gestión del riesgo en proyectos tecnología para PYMES basada en la ISO 31000 contribuye a la continuidad de negocio?

1.2.2 Problema Específico

P1. ¿De qué manera garantizamos la satisfacción de la organización luego de implementar la metodología de gestión de riesgos basada en la ISO 31000 en proyectos tecnológicos para PYMES?

P2. ¿De qué manera garantizaremos mejorar el tiempo de respuesta a los riesgos luego de implementar la metodología de gestión del riesgo en proyectos tecnología para PYMES basada en la ISO 31000?

P3. ¿De qué manera garantizaremos la implementación correcta de la metodología de gestión de riesgos basada en la ISO 31000 en proyectos tecnológicos para PYMES?

1.3 Justificación Teórica

La gestión de riesgos en proyectos tecnológicos es un elemento esencial para el éxito y la sostenibilidad de las pequeñas y medianas empresas (PYMES). En un entorno tecnológico dinámico y competitivo, las pequeñas y medianas empresas a menudo enfrentan desafíos únicos, como recursos limitados y plazos ajustados.

En este sentido, (Taylor, 2021) aborda específicamente las necesidades de las pequeñas y medianas empresas y se centra no solo en la innovación tecnológica, sino también en implementar estrategias de rentabilidad y

eficiencia operativa dentro de los presupuestos y cronogramas específicos de estas empresas. importancia.

La literatura también enfatiza la necesidad de utilizar métodos ágiles cuando se discuten proyectos tecnológicos en pequeñas y medianas empresas. (Highsmith, 2019) ofrece una perspectiva de que la creatividad y la adaptabilidad se valoran como características clave de las pequeñas y medianas empresas que operan en un entorno empresarial dinámico donde la agilidad puede explotarse bajo la influencia de un entorno tecnológico que cambia rápidamente.

En el mundo regulatorio, implementar estándares aceptados es esencial para una gestión de riesgos eficaz. El trabajo de (Ward, 2019) describe la aplicación de ISO 31000 e IEC 62198, proporcionando un marco sólido y reconocido internacionalmente que puede adaptarse a las necesidades específicas de las pequeñas y medianas empresas.

Un aspecto a menudo subestimado pero importante de la gestión de riesgos para proyectos de tecnología de pequeñas empresas es considerar la cultura de la empresa. (Schein, 2017) destaca cómo las creencias, los valores y las normas de una organización dan forma a la percepción y la gestión del riesgo. Para las pequeñas empresas que normalmente operan en entornos más flexibles, comprender y cultivar una cultura organizacional que fomente la gestión proactiva de riesgos y la concientización puede tener un impacto positivo que contribuya garantizar continuidad del negocio.

1.4 Justificación Práctica

La gestión efectiva del riesgo en proyectos tecnológicos se ha vuelto imperativa para el éxito empresarial, especialmente para las pequeñas y

medianas empresas (Pymes) en Perú. La adopción de una metodología respaldada por estándares internacionales, como la norma ISO 31000, emerge como esencial, y la justificación para el desarrollo de la tesis se apoya en diversas literaturas que resaltan la importancia y beneficios prácticos de este enfoque.

La gestión de riesgos en el contexto peruano es abordada por (Salazar, 2018), quienes destacan las particularidades y desafíos que enfrentan las Pymes en un entorno tecnológico en constante evolución. La ISO 31000 se visualiza como un marco adaptable para estas empresas, permitiendo la optimización de recursos y la mitigación eficaz de riesgos tecnológicos (Salazar, 2018)

La competitividad de las Pymes peruanas se discute en profundidad en el trabajo de (González, 2020), enfatizando que la implementación de estándares internacionales, como la ISO 31000, puede ser un catalizador para mejorar la eficiencia y calidad en proyectos tecnológicos, fortaleciendo así la posición competitiva en el mercado peruano (González, 2020)

La resiliencia empresarial en el contexto de desafíos económicos y sociales es explorada por (Pérez A. &., 2019). Se destaca que la gestión del riesgo basada en la ISO 31000 proporciona un marco efectivo para anticipar y gestionar impactos adversos, brindando a las Pymes una mayor capacidad de adaptación y supervivencia en condiciones cambiantes (Pérez A. &., 2019).

El cumplimiento con estándares internacionales y su impacto en la credibilidad empresarial se aborda en la obra de (Cárdenas, 2017). La adopción de normativas como la ISO 31000 no solo asegura la alineación con prácticas globalmente aceptadas, sino que también facilita la

participación en proyectos internacionales y la construcción de asociaciones estratégicas (Cárdenas, 2017)

El desarrollo del capital humano en la gestión del riesgo se explora en la investigación de (Vargas, 2021), resaltando que la implementación de una metodología basada en la ISO 31000 implica una formación continua del personal. Esto contribuye a elevar la competencia del equipo, mejorando la capacidad para identificar y gestionar eficazmente los riesgos asociados con proyectos tecnológicos (Vargas, 2021).

1.5 Objetivos

1.5.1 Objetivo general

Elaborar una metodología de gestión del riesgo de proyectos tecnología para PYMES basada en la ISO 31000 que permita dar soporte a la continuidad del negocio

1.5.2 Objetivos específicos

a) Establecer un sistema de medición para comparar de manera cuantitativa el grado de satisfacción de la organización.
b) Establecer un sistema de medición para comparar de manera cuantitativa el tiempo de respuesta antes y después de la implementación.
c) Elaborar la metodología de manera detalladas y organizada por procesos para una correcta implementación y monitoreo de trabajo.

2 CAPÍTULO II: MARCO TEÓRICO

2.1 Antecedentes de Investigación

2.1.1 Análisis comparativo de metodologías de gestión de riesgos de tecnologías de la Información en el marco de la NTP - ISOIEC 270012014 (Llauce Valdera, 2022)

El principal objetivo del estudio es determinar la metodología de gestión de riesgos de tecnologías de la información que mejor se relaciona con la norma técnica peruana NTP – ISO/IEC 27001:2014. Esta norma especifica los requisitos de un Sistema de Gestión de Seguridad de la Información (SGSI) que deben ser utilizados por los sistemas informáticos nacionales del Perú con el fin de minimizar el riesgo en caso de un incidente con los recursos informáticos del Perú. La metodología utilizada en el estudio sigue un enfoque cualitativo con un diseño novedoso de teoría fundamentada.

Se utiliza la técnica de estudio de similitud de modelo a estándar (MSSS). Esto implica varios pasos, desde definir los criterios de selección hasta determinar la similitud. El estudio encontró que la metodología Magerit V3 es más similar (96%) a la norma técnica peruana NTP-ISO/IEC 27001:2014. Este alto nivel de similitud indica una fuerte alineación entre los requisitos del estándar y las prácticas sugeridas por la metodología Magerit V3.

Además, encontramos que esta metodología se posiciona como una opción madura en la gestión de riesgos de tecnología de la información y está diseñada específicamente para agencias gubernamentales. Los resultados demuestran que Magerit V3 no sólo cumple con los requisitos específicos de la norma peruana, sino que también proporciona un enfoque integral y sofisticado para abordar los desafíos relacionados con la seguridad de la información en contextos gubernamentales.

2.1.2 Elaboración de una guía de gestión de riesgos basados en la norma NTC-ISO 31000 para el proceso de gestión de incidentes y peticiones de servicio del área de mesa de ayuda de empresas de servicios de soporte de tecnología en Colombia (Yeigny Liliana Arias Reyes, 2014)

Este estudio tiene como objetivo mejorar la gestión de riesgos en el proceso de gestión de incidentes y solicitudes de servicios en el departamento de mesa de ayuda de una empresa colombiana de servicios de soporte tecnológico.

El objetivo es introducir nuevos enfoques que fortalezcan las habilidades y reduzcan las vulnerabilidades en el campo mediante el logro de objetivos establecidos mediante la aplicación de estándares específicos.

Esta metodología se basa en la norma NTC-ISO 31000, que estandariza la gestión de riesgos empresariales, y se centra en procesos específicos de asistencia técnica. La norma NTC 5254 ha sido validada para brindar las bases necesarias y crear una guía que sirva como guía paso a paso para la gestión de riesgos en las empresas.

A través de un enfoque práctico en empresas reales, se recopila información y se compila en un documento destinado a servir de guía para el desarrollo eficiente y eficaz de la gestión de riesgos y contribuir al logro de los objetivos de este campo. El texto no proporciona información detallada sobre los resultados específicos obtenidos de los pasos realizados.

No se explican los detalles de la propuesta elaborada, ni se explica cómo afectó la gestión de riesgos de la propia empresa que se tramita. Por lo tanto, la información contenida en el texto no nos permite extraer resultados concretos de nuestro enfoque para mejorar la gestión de riesgos en el área de la mesa de ayuda.

Para obtener esta información es necesario acceder a la sección Resultados del

Empleo. Este documento tiene como objetivo mejorar la gestión de riesgos en las mesas de ayuda de las empresas tecnológicas colombianas a través de un enfoque regulatorio. Aunque esta metodología se basa en criterios específicos, el texto no detalla resultados o implicaciones específicas para las empresas involucradas.

2.1.3 Evaluación del contexto organizacional en la gestión del riesgo de tecnología de información con un enfoque basado en COBIT (Marlene Lucila Guerrero Julio, 2019)

El artículo se adentra en la gestión de riesgos en el ámbito de las Tecnologías de la Información (TI), destacando su papel fundamental en la garantía de la continuidad del negocio. El objetivo principal se centra en la evaluación del contexto organizacional como una etapa primordial en la gestión de riesgos. Para alcanzar este propósito, se propone la definición de indicadores basados en los procesos catalizadores de COBIT, un marco de referencia ampliamente utilizado para el gobierno y la gestión de TI. Además, se aboga por una estrategia específica que coloque al recurso humano en el centro de la evaluación de amenazas y vulnerabilidades en el entorno de las TI.

Aunque el artículo no proporciona detalles específicos sobre la metodología utilizada, se sugiere que la misma implica la aplicación de los indicadores definidos y la estrategia centrada en el recurso humano en un entorno organizacional particular. Esta aplicación podría haberse llevado a cabo para obtener resultados concretos en términos de la madurez del contexto organizacional en la gestión de riesgos.

Los resultados obtenidos a través de la aplicación de los indicadores y estrategias propuestas arrojan un hallazgo significativo. A pesar de que se establecen políticas en torno a la gestión de riesgos en TI, más del 70% de los empleados no las implementan completamente. Este dato revela una brecha considerable entre las políticas definidas y su ejecución efectiva en el ámbito

organizacional. La conclusión resalta la importancia de evaluar periódicamente el contexto organizacional utilizando indicadores claros, subrayando que, a pesar de tener políticas establecidas, existe una desconexión sustancial en la implementación por parte de los empleados.

En síntesis, el artículo propone una aproximación integral a la gestión de riesgos en TI, con un enfoque particular en la evaluación del contexto organizacional. Aunque la metodología no se detalla completamente, la aplicación de indicadores COBIT y una estrategia centrada en el recurso humano arroja luz sobre la brecha existente entre las políticas de gestión de riesgos y su implementación práctica. Este hallazgo destaca la necesidad de una evaluación continua del contexto organizacional, utilizando indicadores claros, para mejorar la efectividad de la gestión de riesgos en el ámbito de las Tecnologías de la Información.

2.1.4 Gestión y prevención de riesgos con tecnologías de información y comunicaciones (Gómez-García, 2022)

El principal objetivo del estudio es describir las etapas de implementación integrada de la gestión de riesgos en los sistemas de gestión de la calidad a través de plataformas web.

El objetivo es centrarse en el análisis de métodos específicos para llevar a cabo la gestión de riesgos en el marco del sistema de gestión de calidad de la Empresa de Insumos Agrícolas Granma de acuerdo con la NC y garantizar la agilidad, seguridad y precisión en la implementación de la gestión de riesgos. . Norma ISO 9001:2015.

El objetivo final es impulsar la transformación digital e impactar significativamente en la gestión de la calidad.

La metodología utilizada incluye un análisis de cómo implementar la gestión de riesgos mediante la implementación de 10 fases específicas para realizar esta

implementación en la plataforma web de la empresa antes mencionada. La recolección de datos se realizó a través del análisis de documentos y observaciones, enfocándose en variables de contexto (CO), evaluación (EV) y monitoreo (MO) en el desarrollo web.

A pesar de la claridad de objetivos y metodología, el texto no contiene información detallada sobre los resultados específicos alcanzados al implementar la gestión de riesgos en plataformas web.

No se proporciona información sobre los impactos o cambios específicos resultantes de este proceso en Granma Agriculture Supplies Company. La falta de datos concretos limita la comprensión de la relación entre los resultados alcanzados y la mejora del control de calidad dentro de la organización.

2.1.5 Guía para apoyar la priorización de riesgos en la gestión de proyectos de tecnologías de la información (Luisa Fernanda Mosquera Ramírez, 2013)

El propósito de esta iniciativa es apoyar la priorización de riesgos en proyectos de tecnologías de la información (TI) a través de una guía basada en las mejores prácticas del Project Management Institute (PMI).

El enfoque central tiene como objetivo abordar los problemas identificados en la literatura, proporcionando una descripción detallada de la aplicación de cada técnica para reducir la subjetividad en el proceso de priorización de riesgos. Esta metodología incluye varias fases. Una revisión de la literatura para definir claramente el problema de la priorización de riesgos en proyectos de TI y la creación de un marco conceptual que tenga en cuenta los procesos involucrados en esta priorización.

El segundo paso crea una guía para priorizar los riesgos para proyectos de TI y detalla los pasos necesarios para aplicar la guía de manera efectiva. Para comprobar su utilidad se realizarán cinco experiencias y se recogerán

resultados y sugerencias de los participantes y se retroalimentarán a la guía. En la tercera etapa de esta metodología se desarrolla un prototipo de software para automatizar la aplicación de la guía y brindar resultados precisos y ordenados.

Finalmente, el prototipo se somete a una evaluación de méritos a juicio de expertos, teniendo en cuenta criterios como idoneidad, precisión e idoneidad. Si bien este estudio destaca la importancia de reducir la subjetividad en la priorización de riesgos en proyectos de TI y propone una guía basada en mejores prácticas reconocidas, este documento se basa en la experiencia con la creación de prototipos de software y no se proporcionaron detalles específicos sobre los resultados obtenidos en la evaluación.

2.1.6 Modelo de gestion de riesgos de procesos de tecnologias de informacion bajo la norma ISO-IEC 27000 en empresas aéreas del Ecuador (Hallo, 2020)

Este proyecto tiene como objetivo abordar las deficiencias de seguridad identificadas en el almacenamiento y transmisión de información en las aerolíneas del Ecuador.

La propuesta se enfoca en implementar un modelo de gestión de procesos de tecnología de la información utilizando el estándar ISO/IEC 27000, identificando la gestión de riesgos de la información como la variable dependiente y la seguridad de la tecnología como la variable independiente.

Debido a la moderada correlación positiva entre estas variables, la propuesta se estructura con base en la metodología de las normas ISO 27001 y 27002, priorizando la aplicación de sistemas de seguridad de la información y controles de seguridad.

El foco principal es el establecimiento de políticas de seguridad basadas en riesgos operacionales y reputacionales, con énfasis en la gestión de equipos, el

impacto de virus informáticos y la pérdida de información confidencial, con el objetivo de mejorar las operaciones de las empresas del sector aeronáutico. La metodología comienza identificando deficiencias en seguridad de la información en las aerolíneas ecuatorianas.

A continuación, se implementa un modelo de gestión de procesos de tecnología de la información basado en la norma ISO/IEC 27000. Se realiza un análisis estadístico para demostrar que existe una correlación positiva moderada entre la gestión de riesgos de la información y la seguridad de la tecnología. La propuesta se estructura según la metodología de las normas ISO 27001 y 27002 y se centra en la aplicación de sistemas de seguridad de la información y controles de seguridad.

Este texto no contiene información específica sobre los resultados alcanzados con la implementación del modelo de gestión de procesos de tecnologías de la información y las propuestas basadas en las normas ISO 27001 y 27002. No se detalla el impacto específico en la mejora de la seguridad de la información. Tampoco es comparable a las operaciones de empresas del sector aéreo ecuatoriano. Para obtener detalles de resultados y contribuciones específicas se debe acceder a la sección ``Resultados'' o ``Conclusiones'' del proyecto.

El objetivo de este proyecto es mejorar la seguridad de la información de las aerolíneas ecuatorianas mediante la implementación de un modelo de gestión basado en la norma ISO/IEC 27000, enfocándose en la relación entre la gestión de riesgos de la información y la seguridad técnica. Sin embargo, no se proporciona información específica sobre los resultados obtenidos.

2.1.7 Modelo de gestión de riesgos de tecnologías de información para la generación de valor en el control de la corrupción de funcionarios y servidores en las municipalidades provinciales de la región de Lambayeque (ORTIZ, 2021)

El objetivo del estudio es agregar valor a la lucha contra la corrupción proponiendo un modelo de gestión de riesgos de tecnologías de la información (MGR-TI) desarrollado específicamente para el gobierno local de la región Lambayeque.

Aborda los problemas identificados en la gestión de riesgos de tecnología de la información (GR-IT) en estos gobiernos locales y reconoce que dichos problemas pueden conducir a prácticas corruptas.

La metodología, de naturaleza cuantitativa con un diseño experimental, implica la observación y análisis de las realidades comunitarias con el fin de recopilar información sobre la relación entre GR-TI y la probabilidad de conductas corruptas.

Se realizará un estudio comparativo de los estándares y normas relacionadas con GR-TI, y con base en estos elementos se creará un modelo específico para los gobiernos estatales regionales enfocado en la lucha contra la corrupción.

La validación del modelo requiere la participación de expertos. Respecto a los resultados, el texto no brinda información específica sobre la aplicación del MGR-TI en el municipio de Lambayeque, ni detalla el impacto específico del modelo en la lucha contra la corrupción. La falta de datos concretos limita la posibilidad de evaluar la contribución precisa del modelo a la lucha contra la corrupción.

Para obtener información más detallada, debe visitar la sección Resultados o Conclusiones de la Investigación. Este estudio propone un modelo de gestión de riesgos de tecnología de la información para que el gobierno local de

Lambayeque frene la corrupción. Las metodologías cuantitativas y experimentales incluyen observación y análisis con validación de expertos. Sin embargo, el texto no proporciona detalles sobre los resultados obtenidos.

2.2 Bases Teóricas

2.2.1 Norma ISO 31000:2018 - Gestión de Riesgos: Directrices (Standardization, 2020)

ISO 31000:2018, titulada 'Gestión de riesgos: Directrices', es una norma reconocida internacionalmente que establece principios y marcos para una gestión de riesgos eficaz en una variedad de organizaciones, incluidas empresas de tecnología y, por supuesto, pequeñas y medianas empresas (PYME). Esta es una guía. Publicado por la Organización Internacional de Normalización (ISO), este estándar proporciona un enfoque sistemático y estructurado para identificar, evaluar y gestionar riesgos en el entorno de una organización.

Esta norma establece un conjunto de principios fundamentales que forman la columna vertebral de la gestión de riesgos. Estos incluyen la integración de la gestión de riesgos en la estructura organizacional, la capacidad de adaptarse a las circunstancias específicas de la organización y la mejora continua de los procesos de gestión de riesgos.

ISO 31000 describe un proceso de gestión de riesgos de varios pasos. Comienza estableciendo el contexto en el que se definen los objetivos y se identifican los límites del proceso de gestión de riesgos. La identificación y evaluación de riesgos permite a las organizaciones comprender y cuantificar los riesgos potenciales. A este análisis le sigue la toma de decisiones y la implementación de medidas de gestión de riesgos, seguido de un seguimiento y revisión continuos del proceso.

Para las pequeñas y medianas empresas que se embarcan en proyectos

tecnológicos ISO 31000 proporciona un marco sólido y escalable. Como guía general, se puede adaptar fácilmente a las necesidades específicas de las pequeñas y medianas empresas, permitiéndoles implementar procesos eficientes de gestión de riesgos sin abrumarlas con requisitos complejos. Este estándar brinda a las pequeñas y medianas empresas la oportunidad de identificar y evaluar riesgos en proyectos tecnológicos desde una perspectiva holística. Además de los aspectos financieros y operativos, también se consideran factores externos e internos como la cultura organizacional y la tolerancia al riesgo.

La flexibilidad de ISO 31000 permite a las pequeñas y medianas empresas adaptar el nivel de detalle y complejidad de su enfoque de gestión de riesgos a las características específicas de sus proyectos y la naturaleza de su entorno empresarial.

ISO 31000:2018 se centra en principios básicos y procesos de gestión de riesgos bien estructurados y se presenta como una herramienta valiosa para las pequeñas y medianas empresas involucradas en proyectos tecnológicos. Siguiendo esta guía, las organizaciones pueden mejorar su capacidad para predecir, evaluar y gestionar riesgos, contribuyendo al éxito sostenido del proyecto.

2.2.2 PMI Risk Management Professional (PMI-RMP): (Institute P. M., 2019)

El Profesional de Gestión de Riesgos (PMI-RMP) del Project Management Institute (PMI) es una certificación reconocida internacionalmente centrada en la gestión de riesgos de proyectos. Impartido por PMI, un organismo líder en estándares y certificación de gestión de proyectos, PMI-RMP establece un alto estándar para los profesionales que desean sobresalir en la identificación, evaluación y gestión de riesgos en entornos de proyectos. Esta certificación se basa en PMBOK (Project Management Body of Knowledge), un marco integral para la gestión de proyectos desarrollado

por PMI.

Características principales del PMI-RMP:

1. Especial énfasis en la gestión de riesgos: La certificación PMI-RMP está dirigida a profesionales de la gestión de proyectos que quieran especializarse en la gestión de riesgos. A través de esta certificación, los profesionales demuestran habilidades avanzadas para identificar, evaluar y responder a riesgos que pueden afectar el éxito del proyecto.

2. Reconocimiento Internacional: Ofrecida por PMI, una organización con presencia global, la certificación PMI-RMP es reconocida internacionalmente y respaldada por una comunidad de profesionales de gestión de proyectos en todo el mundo. Esto permite a los titulares de la certificación validar de forma fiable sus habilidades y conocimientos en gestión de riesgos.

3. Integración con PMBOK: PMI-RMP se basa en el marco PMBOK, una referencia ampliamente aceptada para la gestión de proyectos. Esto garantiza que los profesionales certificados no sólo tengan experiencia en gestión de riesgos, sino que también estén familiarizados con las mejores prácticas generales de gestión de proyectos.

4. Competencias evaluadas: La certificación PMI-RMP evalúa diversas competencias como la planificación de la gestión de riesgos, la identificación y evaluación de riesgos, la respuesta a los riesgos, el seguimiento y control de los riesgos y la comunicación de la gestión de riesgos. riesgo. Esto asegura que los profesionales certificados sean expertos en la gestión integral de riesgos durante todo el ciclo de vida del proyecto. Para las pequeñas y medianas empresas (PYMES) que se embarcan en proyectos tecnológicos, la certificación PMI-RMP es una gran ventaja. Los proyectos

de tecnología a menudo están expuestos a una variedad de riesgos, desde requisitos cambiantes hasta desafíos técnicos y financieros. Los profesionales certificados por PMI-RMP pueden abordar estos desafíos de manera proactiva y efectiva.

Las pequeñas empresas que adoptan la certificación PMI-RMP obtienen una mayor confianza en la gestión del riesgo de sus proyectos tecnológicos. Los profesionales certificados están capacitados para identificar y evaluar riesgos sistemáticamente, contribuyendo a la toma de decisiones informadas y la implementación de estrategias efectivas de respuesta a los riesgos.

El PMI Risk Management Professional (PMI-RMP) es una certificación valiosa para aquellos que desean sobresalir en la gestión de riesgos de proyectos, especialmente en el campo de los proyectos de tecnología. El enfoque específico, el reconocimiento internacional y la alineación con las mejores prácticas de gestión de proyectos hacen que esta certificación sea particularmente relevante y beneficiosa para las pequeñas y medianas empresas que desean gestionar eficazmente los riesgos de sus proyectos tecnológicos.

2.2.3 PRINCE2 (PRojects IN Controlled Environments): (PRINCE2, 2008)

PRINCE2 (PROjects IN Controlled Environments) es una metodología de gestión de proyectos utilizada a nivel mundial. Desarrollado por la Oficina del Gobierno del Reino Unido, PRINCE2 proporciona un enfoque estructurado y adaptable para la gestión de proyectos en un entorno controlado. Con el paso de los años, ha ganado reconocimiento mundial y se ha convertido en el estándar de facto para la gestión de proyectos, incluso en el campo de la tecnología.

PRINCE2 se basa en siete principios fundamentales que guían la ejecución del proyecto. Estos principios incluyen, entre otros, justificar los proyectos

en curso, aprender de la experiencia, definir claramente roles y responsabilidades y gestionar de forma incremental. Estos principios proporcionan una base sólida para la toma de decisiones y la ejecución eficiente de proyectos en una variedad de industrias, incluida la industria tecnológica.

La metodología PRINCE2 se basa en procesos y fases claramente definidos. Comienza con la fase de iniciación, donde se establece la justificación del proyecto y se definen roles y responsabilidades. Pasamos por las etapas de inicio, ejecución y conclusión, estableciendo objetivos y actividades específicas para cada una. Este enfoque por fases facilita el control y la adaptabilidad a medida que avanza el proyecto. PRINCE2 ha demostrado ser altamente adaptable a proyectos tecnológicos, incluidos aquellos liderados por pequeñas y medianas empresas (PYME). Esta metodología no impone restricciones especiales a las tecnologías utilizadas, lo que permite su aplicación a proyectos de desarrollo de software, implementaciones de sistemas y otros esfuerzos técnicos.
PRINCE2 define roles y responsabilidades específicas para los participantes del proyecto. Estos roles incluyen director ejecutivo, director de proyectos, usuario clave y más. La claridad en los roles facilita la comunicación y la toma de decisiones. Esto es especialmente importante para proyectos tecnológicos donde la colaboración efectiva es esencial. La gestión de riesgos es un componente central de PRINCE2. Esta metodología incluye la identificación, evaluación y gestión de riesgos en todas las etapas del proyecto. Esto es especialmente importante para proyectos tecnológicos donde el rápido desarrollo y la complejidad técnica pueden generar incertidumbres significativas.

Para las pequeñas y medianas empresas que buscan gestionar eficazmente sus proyectos tecnológicos, PRINCE2 proporciona un marco

escalable y adaptable. Las pequeñas y medianas empresas pueden beneficiarse de la estructura y la claridad de funciones que proporciona PRINCE2, lo que permite una gestión de recursos más eficiente y aumenta la probabilidad de éxito con proyectos tecnológicos específicos.

2.2.4 Marco de Ciberseguridad del NIST (National Institute of Standards and Technology): ((NIST), 2018)

El Marco de Ciberseguridad del NIST es una guía completa desarrollada por el Instituto Nacional de Estándares y Tecnología. Su objetivo principal es proporcionar un conjunto de estándares, directrices y prácticas recomendadas para ayudar a las empresas a fortalecer su postura de ciberseguridad. Este marco se ha convertido en una referencia fundamental para la protección de la información y la gestión del riesgo cibernético en una variedad de industrias, incluidas aquellas enfocadas en proyectos tecnológicos.

Componentes clave del marco de ciberseguridad del NIST:

El marco se divide en cinco funciones principales: identificar, proteger, detectar, responder y recuperar. Estas capacidades abarcan todas las etapas críticas de la gestión de la ciberseguridad y proporcionan un enfoque holístico para prevenir, detectar y responder a las ciberamenazas.

Identificar: En esta fase, las organizaciones definen activos, evalúan riesgos y establecen políticas y procesos de ciberseguridad. La identificación es esencial para comprender y evaluar las amenazas potenciales.

Protección: centrarse en implementar medidas de seguridad para reducir el riesgo. Esto incluye establecer controles de acceso, capacitar al personal y aplicar técnicas de seguridad de la información.

Detección: La fase de detección se centra en la detección temprana de incidentes de seguridad. Esto incluye monitoreo continuo, detección de anomalías y respuesta inmediata a eventos de seguridad.

Respuesta: Cuando ocurre un incidente de seguridad, las organizaciones deben desarrollar un plan de respuesta. Esto incluye la movilización del equipo de respuesta, la contención de incidentes y el control de daños.

Recuperación: La fase final se centra en la recuperación de incidentes. Esto incluye restaurar sistemas, evaluar daños e implementar medidas para prevenir incidentes similares en el futuro. Flexibilidad y adaptabilidad:
Una característica especial del marco de ciberseguridad del NIST es su flexibilidad. Este no es un enfoque único para todos, sino que se adapta a las necesidades y circunstancias específicas de cada organización. Esto lo hace aplicable a empresas de diversos tamaños, incluidas pequeñas y medianas empresas (PYME), que pueden enfrentar desafíos únicos de ciberseguridad.

La ciberseguridad es sumamente importante en el ámbito de los proyectos tecnológicos. La implementación de este marco proporciona a las empresas una base sólida para proteger sus sistemas y datos durante el desarrollo y ejecución de proyectos tecnológicos.

Para las pequeñas empresas con recursos limitados pero que enfrentan riesgos de ciberseguridad similares, el Marco de Ciberseguridad del NIST proporciona una guía estructurada y adaptable. Las pequeñas empresas pueden elegir y aplicar los elementos del marco que sean más relevantes para su entorno, adoptando un enfoque paso a paso basado en sus recursos y necesidades específicas.
El Marco de Ciberseguridad del NIST se destaca como una herramienta

esencial para fortalecer la ciberseguridad en proyectos tecnológicos. Su enfoque integral y su capacidad para adaptarse a una variedad de situaciones lo convierten en una opción valiosa para organizaciones de todos los tamaños que buscan gestionar eficazmente sus riesgos cibernéticos.

2.2.5 M_o_R (Management of Risk): (Axelos, 2010)

M_o_R significa Gestión de Riesgos y es un marco de gestión de riesgos desarrollado por Axelos. Este enfoque proporciona una orientación integral para ayudar a las organizaciones a gestionar eficazmente el riesgo y alcanzar sus objetivos estratégicos. M_o_R se aplica a una variedad de sectores y entornos y proporciona un conjunto de principios, procesos y roles para respaldar la toma de decisiones informada y la gestión proactiva de riesgos.

El marco M_o_R se basa en un conjunto de principios fundamentales que guían la gestión de riesgos. Esto incluye integrar la gestión de riesgos en todos los aspectos de una organización, adaptarse a circunstancias cambiantes y desarrollar un enfoque personalizado para la gestión de riesgos que tenga en cuenta las necesidades y objetivos específicos de una organización.

M_o_R consta de cuatro perspectivas principales: contexto estratégico contexto de programa, contexto de proyecto y contexto operativo. Cada perspectiva tiene características únicas y consideraciones específicas de gestión de riesgos, lo que permite una adopción gradual adaptada a las necesidades específicas de una organización y su entorno.

Una característica especial de M_o_R es su enfoque holístico en todos los niveles de la organización. Se sabe que los riesgos ocurren en diferentes niveles y pueden impactar a una organización desde la estrategia hasta las

operaciones del día a día. M_o_R proporciona pautas para abordar estos riesgos de manera integrada y consistente.

M_o_R define funciones y responsabilidades claras para garantizar una gestión de riesgos eficaz. Esto incluye la junta directiva, los administradores de riesgos, los propietarios de riesgos y los propietarios de riesgos. La asignación de roles específicos hace que la gestión de riesgos sea una responsabilidad compartida y garantiza una rendición de cuentas clara en todos los niveles de la organización.

El marco M_o_R sigue un ciclo de vida de gestión de riesgos que incluye identificación, evaluación, planificación de respuesta, implementación de respuesta y monitoreo continuo. Este enfoque circular hace que la gestión de riesgos sea un proceso continuo en lugar de una actividad única, lo que le permite adaptarse a riesgos y entornos cambiantes.

En el contexto de proyectos de tecnología, M_o_R proporciona un enfoque sólido para gestionar riesgos específicos asociados con la tecnología y la implementación del sistema. Desde la etapa de planificación inicial hasta las operaciones en curso, M_o_R ayuda a las empresas a identificar, evaluar y gestionar los riesgos de forma proactiva para garantizar el éxito de los proyectos tecnológicos.

M_o_R es escalable y se adapta bien a las necesidades de las pequeñas y medianas empresas (PYMES). La flexibilidad del marco permite a las pequeñas empresas aplicar principios y procesos de M_o_R de una manera que se adapte a sus recursos y necesidades específicas, proporcionando pautas prácticas y efectivas de gestión de riesgos.

2.2.6 COBIT (Control Objectives for Information and Related Technologies): (ISACA, State of Cybersecurity Report, 2019)

COBIT significa "Objetivos de control para la información y tecnologías asociadas" y es un marco de gestión y gobierno de tecnología de la información (TI) desarrollado por ISACA (Asociación de Control y Auditoría de Sistemas de Información) y la Asociación de Gobernanza de TI. COBIT es un estándar reconocido globalmente diseñado para ayudar a las empresas a alcanzar sus objetivos comerciales a través de la gestión y el control efectivos de la tecnología de la información.
COBIT se basa en varios principios básicos que abordan el gobierno y la gestión de TI. Estos principios incluyen centrarse en la creación de valor a través de TI, equilibrar beneficios y riesgos, aplicar un marco holístico e involucrar a múltiples partes interesadas en el proceso de toma de decisiones.

COBIT organiza sus políticas y directrices en cuatro áreas principales: planificación y organización, adquisición e implementación, implementación y soporte, y seguimiento. Cada dominio incluye diferentes procesos que son esenciales para una gestión y un gobierno de TI eficaces. Por ejemplo, el área de Entrega y Soporte incluye procesos como gestión de incidentes gestión de problemas y gestión del conocimiento.

Una de las características de COBIT es su estructura de control que consta de cinco principios y siete habilitadores. Los principios guían las decisiones y acciones, mientras que los habilitadores proporcionan factores que influyen en la eficacia del gobierno y la gestión de TI. Estos factores incluyen, entre otros, procesos, estructura organizacional, cultura, ética y comportamiento. COBIT se centra en los objetivos de control y proporciona un conjunto claro de objetivos que las organizaciones deben alcanzar para garantizar la eficacia del gobierno y la gestión de TI.

Estos objetivos de gestión son específicos, mensurables, alcanzables, relevantes y oportunos (SMART), lo que los hace más fáciles de implementar y medir el éxito.
COBIT se integra bien con otros marcos y estándares como ITIL (Biblioteca de infraestructura de tecnología de la información) e ISO/IEC 27001. Esta capacidad de integración permite a las organizaciones adoptar una visión holística y garantizar que sus prácticas de gestión y gobierno de TI sean coherentes y compatibles con múltiples marcos de referencia.

COBIT proporciona un marco sólido para gestionar el riesgo y lograr objetivos específicos dentro de proyectos de tecnología. Desde la etapa de planificación hasta la entrega y el soporte continuo, los procesos y objetivos de control de COBIT ayudan a las empresas a navegar la complejidad de los proyectos tecnológicos.

COBIT es escalable y adaptable, lo que lo hace relevante y aplicable a las pequeñas y medianas empresas (PYME). Dependiendo de sus necesidades y recursos, las pequeñas y medianas empresas pueden utilizar los principios y procesos de COBIT para garantizar una gestión de TI eficaz sin abrumarlas con una complejidad innecesaria.

COBIT presenta un marco de gestión y gobierno de TI que aborda de manera integral los desafíos actuales de la era digital. El enfoque de COBIT en objetivos de control, estructura clara y capacidades integradas lo convierte en una opción valiosa para empresas de todos los tamaños que buscan optimizar sus operaciones de TI.

2.2.7 FMEA (Failure Modes and Effects Analysis): (Stamatis, 2019)

El análisis modal de fallas y efectos, también conocido como AMEF (análisis modal de fallas y efectos), es un método sistemático para identificar y evaluar posibles tipos de fallas en un sistema, proceso o producto y su

impacto en el desempeño general. Es una metodología. FMEA se ha convertido en una herramienta esencial en una variedad de campos, desde la fabricación hasta la gestión de proyectos y la atención sanitaria.

El objetivo principal del AMEF es prevenir fallas y mejorar la calidad y confiabilidad de un proceso o sistema. Esta metodología sigue principios básicos que incluyen identificar proactivamente posibles modos de falla, evaluar su impacto y priorizar acciones correctivas para reducir o eliminar los riesgos asociados.

FMEA se realiza a través de una serie de pasos estructurados que guían la evaluación de riesgos. Estos pasos incluyen identificar características clave, identificar posibles modos de falla, evaluar la gravedad, la probabilidad de ocurrencia y detección, así como asignar puntajes y priorizar acciones correctivas.

El proceso comienza identificando las características clave del sistema o proceso. Estas características son importantes para el rendimiento y la calidad generales. Se identifican posibles modos de falla para funciones clave. Es importante considerar escenarios en los que un sistema o proceso puede no ser capaz de realizar su función prevista.

Cada modo de falla se evalúa en términos de gravedad del impacto, probabilidad de ocurrencia y si se puede detectar antes de que ocurra un impacto significativo. A cada aspecto evaluado se le asigna una puntuación numérica, y estas puntuaciones se multiplican para llegar a una puntuación de riesgo general. Esto le permite priorizar los modos de falla y tomar medidas correctivas.

Se desarrollan e implementan acciones correctivas para abordar los modos de falla de alta prioridad y reducir los riesgos asociados. En el campo de

los proyectos de tecnología, FMEA proporciona un enfoque valioso para la identificación y el control proactivo de riesgos. Desde el desarrollo de software hasta la implementación del sistema, FMEA ayuda a los equipos de proyecto a predecir posibles fuentes de errores y resolverlas antes de que afecten negativamente al proyecto.

FMEA es escalable y adaptable, lo que lo hace adecuado para pequeñas y medianas empresas (PYME) que pueden enfrentar limitaciones de recursos. Las pequeñas y medianas empresas pueden aplicar los principios del AMEF de forma proporcional a sus proyectos y procesos para mejorar la calidad y la confiabilidad sin incurrir en costos excesivos.

FMEA le permite identificar proactivamente problemas potenciales y resolverlos antes de que afecten negativamente el rendimiento o la calidad.

FMEA aborda primero los riesgos más importantes y optimizar la utilización de recursos al priorizar acciones correctivas basadas en el impacto potencial. FMEA fomenta una cultura de mejora continua al proporcionar un marco estructurado para la revisión y mitigación continua de riesgos.

FMEA ayuda a mejorar la confiabilidad y consistencia de procesos y productos al abordar posibles tipos de errores.

FMEA se destaca como una herramienta eficaz para la gestión proactiva de riesgos en una variedad de situaciones, incluidos proyectos de tecnología. Su enfoque estructurado y su capacidad para prevenir problemas antes de que ocurran lo convierten en una herramienta valiosa para empresas de todos los tamaños.

2.2.8 Risk IT: (ISACA, Risk IT: Based on COBIT, 2010)

Risk IT es un marco desarrollado por ISACA (Asociación de Control y Auditoría de Sistemas de Información) con un enfoque específico en la gestión del riesgo de tecnología de la información (TI). Este enfoque está diseñado para ayudar a las organizaciones a comprender y gestionar eficazmente los riesgos asociados con el uso y la dependencia de la tecnología de la información en sus operaciones y procesos comerciales.

El objetivo principal de Risk IT es proporcionar directrices prácticas para la gestión de riesgos en el contexto de TI. Este marco se basa en varios principios básicos, incluida la alineación con los objetivos organizacionales, la creación de valor, la gestión activa y la adaptabilidad a los cambios en el entorno empresarial y tecnológico.

Risk IT se divide en seis áreas principales que abordan diferentes aspectos de la gestión de riesgos de TI.

Gobierno de TI y estructura organizacional:

Esto incluye la creación de estructuras organizativas efectivas y la integración de la gestión de riesgos en la gobernanza de la tecnología de la información. Integrar el riesgo en el ciclo de vida de TI:
La atención se centra en la integración de los procesos de gestión de riesgos en todas las etapas del ciclo de vida de los sistemas y servicios de tecnología de la información.

Beneficios y riesgos obtenidos:

Considere cómo la gestión de riesgos puede ayudar a obtener los beneficios asociados con sus iniciativas de TI.

Optimizar el riesgo:

El objetivo es optimizar la relación entre los riesgos asumidos y los beneficios obtenidos mediante la introducción de prácticas y procesos eficientes de gestión de riesgos.

Gestión de riesgos en la estrategia de TI:

La atención se centra en integrar la gestión de riesgos en la estrategia general de tecnología de la información de una organización.

Gestión de riesgos en la prestación de servicios TI:

Trabajamos en la gestión de riesgos relacionados con la prestación de servicios TI, como la gestión de proveedores y la continuidad del servicio. Risk IT es adecuado para pequeñas y medianas empresas (PYME) porque es escalable y adaptable. Estas organizaciones pueden beneficiarse de la orientación específica de Risk IT para gestionar los riesgos asociados con sus operaciones y proyectos de TI, incluso cuando los recursos son limitados.

Risk IT tiene varios beneficios importantes:

• **Alineación estratégica**: ayuda a alinear la gestión de riesgos de TI con los objetivos estratégicos de la organización.
• **Vista holística:** proporciona una visión holística del riesgo en todas las etapas del ciclo de vida de TI.
• **Adaptabilidad:** Puede adaptarse a diferentes situaciones empresariales y tecnológicas, permitiendo su uso en diferentes industrias.
• **Enfoque continuo:** Facilita un enfoque continuo en la gestión de riesgos,

teniendo en cuenta la constante evolución de los riesgos tecnológicos.

2.2.9 Marco de Riesgo ECM (Enterprise Content Management): ((AIIM), 2011)

El marco de riesgos ECM (Enterprise Content Management) es un enfoque estructurado para gestionar los riesgos asociados con la gestión de contenidos empresariales.
La gestión eficaz de contenidos es esencial en un entorno empresarial en constante evolución donde la información es un activo fundamental. El objetivo de este marco es proporcionar orientación para identificar, evaluar y gestionar los riesgos que puedan surgir relacionados con la gestión de contenidos en toda una organización.

El Marco de Riesgos de ECM se basa en principios destinados a garantizar la seguridad, integridad y disponibilidad del contenido empresarial. Su objetivo principal es brindar a las organizaciones las herramientas que necesitan para abordar de manera proactiva los riesgos y desafíos asociados con la gestión de la información durante todo el ciclo de vida del contenido. El marco de riesgos de ECM consta de varios elementos clave que trabajan juntos para abordar los riesgos de gestión de contenidos.

Este marco comienza identificando riesgos específicos asociados con la gestión de contenidos. Esto incluye el análisis de amenazas potenciales que podrían afectar la integridad, la confidencialidad y la disponibilidad de su contenido.

Una vez identificado un riesgo, se evalúa su posible impacto y probabilidad de ocurrencia. Esta evaluación ayuda a priorizar los riesgos y asignar recursos de manera eficiente.

A partir de la evaluación de riesgos se desarrollan estrategias de mitigación. Estas estrategias pueden incluir medidas de seguridad, políticas de acceso y procesos de respaldo para garantizar la protección de su información.
Se implementan estrategias de remediación y se establece un proceso de monitoreo continuo para evaluar la efectividad de estas estrategias a lo largo del tiempo. Esta fase asegura una respuesta proactiva a los cambios en el entorno de riesgo.
En el contexto de los proyectos de gestión de contenidos empresariales, el marco de riesgos de ECM proporciona una valiosa orientación. Desde la implementación de sistemas ECM hasta la gestión de flujos de trabajo y la protección de información confidencial, este marco se puede adaptar a las necesidades de su proyecto específico.

El marco de riesgo de ECM es escalable y adaptable, lo que lo hace adecuado para pequeñas y medianas empresas (PYME). Este enfoque permite a las PYMES gestionar eficazmente los riesgos asociados con la gestión de contenidos sin incurrir en costes excesivos.

2.2.10 Gestión de Riesgos Tecnológicos

En el entorno empresarial actual donde la tecnología juega un papel importante, la gestión del riesgo tecnológico es fundamental para las empresas peruanas.

Esta sección cubre los principios básicos de la gestión de riesgos tecnológicos, enfatizando la necesidad de un enfoque sistemático y proactivo y la importancia de optimizar las oportunidades que presenta la tecnología.

La gestión de riesgos tecnológicos se define como un proceso continuo de identificación, evaluación y mitigación de amenazas que impactan el entorno tecnológico de una organización (Borghoff, 2019).

Este enfoque incluye la evaluación de las vulnerabilidades del sistema y de los datos y la implementación de medidas preventivas y correctivas.

La literatura destaca elementos clave de la gestión técnica de riesgos, como la identificación precisa de los riesgos, la evaluación de su impacto potencial y la implementación de estrategias para reducirlos (Siponen, 2020)

Este enfoque integral permite a las organizaciones anticipar amenazas potenciales y prepararse adecuadamente.

2.2.10.1 Enfoque Sistemático y Proactivo

La gestión eficaz del riesgo tecnológico requiere un enfoque sistemático y proactivo. La norma ISO 31000 proporciona un marco general de gestión de riesgos que se puede adaptar a cualquier contexto técnico. (Standardization, 2020)

Esta norma enfatiza la importancia de integrar la gestión de riesgos en los procesos organizacionales y promueve un enfoque continuo que esté alineado con los objetivos estratégicos.

La literatura enfatiza la necesidad de una mentalidad proactiva que no solo responda a amenazas conocidas, sino que también anticipe y aborde nuevos riesgos asociados con la rápida innovación tecnológica. (Borghoff, 2019)

Este enfoque proactivo permite a las empresas ser ágiles y adaptarse al entorno tecnológico en constante cambio.

2.2.10.2 Optimización de Oportunidades Tecnológicas

La gestión eficaz de los riesgos tecnológicos implica no sólo mitigar los riesgos sino también optimizar las oportunidades relacionadas con la tecnología.

La literatura enfatiza que las metodologías bien diseñadas permiten a las empresas identificar y explotar oportunidades tecnológicas que impulsan la innovación y mejoran la competitividad del mercado (ISACA, State of Cybersecurity Report, 2021)

La gestión de riesgos no debe verse como una barrera para la adopción de tecnología avanzada, sino más bien como un medio para permitir a las empresas maximizar los beneficios estratégicos de la tecnología.

2.2.11 Ciberseguridad y Resiliencia Tecnológica en Empresas Peruanas

La creciente dependencia de las empresas peruanas de la tecnología ha cambiado la forma en que trabajan, crean valor y se relacionan con los clientes.

Sin embargo, esta transformación digital también ha ampliado la superficie de ataque de las amenazas cibernéticas, destacando la importancia crítica de la ciberseguridad y la resiliencia tecnológica en el entorno empresarial del Perú.

2.2.11.1 Importancia de la Ciberseguridad en Empresas Peruanas

En un entorno donde la información es un activo crítico, la ciberseguridad se ha vuelto esencial para las empresas peruanas. La proliferación de tecnologías digitales y el aumento de la conectividad han aumentado la exposición a los riesgos cibernéticos.

La integridad, la confidencialidad y la disponibilidad de los datos son primordiales, y la pérdida de datos puede tener importantes implicaciones financieras y afectar la confianza del cliente y la reputación de una organización (PwC, 2020) La literatura destaca la necesidad de una estrategia integral de ciberseguridad que aborde no solo las amenazas conocidas, sino también amenazas como: Esto incluye nuevas vulnerabilidades, así como malware y phishing.

Ahora es común adoptar marcos de ciberseguridad, como el Marco de ciberseguridad del NIST, para ayudar a las organizaciones a diseñar e implementar programas de ciberseguridad eficaces (Instituto Nacional de Estándares y Tecnología (NIST, 2021)

2.2.11.2 Amenazas Emergentes en el Panorama Digital Peruano

El entorno digital del Perú enfrenta nuevas amenazas cibernéticas que requieren especial atención. Un informe del INCIBE (Instituto Nacional de Ciberseguridad) destaca la creciente sofisticación de los ataques de ransomware y el aumento de los ataques a infraestructuras críticas.

La realidad peruana, con sus particularidades y desafíos, requiere un conocimiento profundo de las tácticas de los actores maliciosos y de las estrategias de ciberseguridad adaptadas a esta situación (INCIBE, 2020).

Además, las cadenas de suministro cada vez más globales se han convertido en importantes vectores de ataque. La dependencia de proveedores externos introduce nuevos riesgos, desde la manipulación del hardware hasta la intrusión del software, lo que pone de relieve la necesidad de medidas eficientes de prevención y respuesta (ENISA, 2019).

2.2.11.3 Desarrollo de Capacidades de Resiliencia Tecnológica

La resiliencia técnica es la capacidad de una organización para resistir, adaptarse y recuperarse de eventos disruptivos. En el contexto de la ciberseguridad, no sólo es importante proteger los activos digitales, sino también poder seguir trabajando de manera eficiente después de un incidente.

Las empresas peruanas reconocen cada vez más la necesidad de desarrollar capacidades de resiliencia que les permitan no solo resistir los ciberataques, sino también recuperarse rápidamente y aprender de sus experiencias.

La literatura enfatiza que la resiliencia técnica va más allá de la implementación de tecnologías de seguridad. Se trata de crear una cultura organizacional que valore la ciberseguridad, las capacidades de respuesta a incidentes y la mejora continua.

La planificación de la respuesta a incidentes, la realización de ejercicios

periódicos y la colaboración con agencias de ciberseguridad y otras empresas son elementos esenciales para fortalecer la resiliencia tecnológica (Lengnick-Hall, 2019) (Dellermann, 2020)

2.2.12 Gestión de Datos y Privacidad en Empresas Peruanas: Un Enfoque Integral

La gestión y protección de datos efectiva se han convertido en factores importantes para las empresas peruanas en el contexto de la transformación digital. Esta sección explica la importancia de una gestión sólida de los datos y de estrategias para garantizar la privacidad.

Se trata en particular de la protección de datos personales y del cumplimiento de las normas legales en el marco de la Ley N° 29733.

2.2.12.1 Protección de Datos Personales

En un entorno empresarial donde la recopilación y el procesamiento de datos personales es común, la protección de los datos personales es una máxima prioridad. Las empresas peruanas deben reconocer la necesidad de ganarse la confianza de sus clientes y tomar estrictas medidas de seguridad para proteger la integridad y confidencialidad de los datos personales.

Estrategias como la seudonimización y el cifrado se han vuelto esenciales para garantizar la seguridad de la información sensible (Bojórquez, 2021)

En la literatura, el manejo adecuado de los datos personales requiere no solo medidas técnicas sino también claras. crear políticas internas apropiadas y capacitar a los empleados. RRHH, etc.

Incluye concienciar sobre la importancia de la protección de datos (Junta Europea de Protección de Datos (EDPB, 2020) Al adoptar estas prácticas, las empresas peruanas podrán cumplir con sus obligaciones legales, así como fomentar una cultura organizacional enfocada en protección de datos

2.2.12.2 Cumplimiento con la Ley N° 29733

En Perú, la Ley de Protección de Datos Personales (Ley N° 29733) establece las reglas para el tratamiento de datos personales y define los derechos de los titulares de los datos. Las empresas peruanas deben cumplir con estas disposiciones para evitar sanciones y, lo más importante, demostrar su compromiso con la protección de datos y la ética empresarial (Agencia Nacional de Protección de Datos Personales.

En cumplimiento de la Ley N° 29733 se incluyen los siguientes nombramientos: Se requiere el nombramiento de un responsable de protección de datos para realizar evaluaciones de impacto de la protección de datos, informar violaciones de seguridad y obtener el consentimiento de los interesados.

Además, las empresas deben asegurarse de que los proveedores de servicios y terceros con los que trabajan también cumplan con las normas de protección de datos (ANPDP, 2021).

2.2.12.3 Estrategias para la Gestión de Datos y Privacidad

Una estrategia integral de gestión de datos y privacidad incluye no solo el cumplimiento normativo, sino también la adopción de mejores prácticas que van más allá de los requisitos mínimos. La implementación de marcos de protección de datos como Privacy by Design, que considera aspectos de protección de datos durante la etapa de diseño del proyecto, es fundamental (Bojórquez, 2021).

La literatura también enfatiza la importancia de la transparencia en la gestión de datos y protección de datos. Las empresas peruanas pueden aumentar la confianza de los clientes comunicando claramente cómo se recopila, utiliza y protege la información personal.

Educar continuamente al personal sobre las amenazas a la privacidad y las mejores prácticas también es esencial para mantener un enfoque proactivo en la

protección de datos (EDPB, 2020).

2.2.13 Innovación Tecnológica y Adaptabilidad Empresarial en el Contexto Peruano

La innovación tecnológica y la adaptabilidad empresarial son cruciales para el crecimiento y la sostenibilidad de las empresas peruanas en un entorno digital globalizado.

Esta sección detalla cómo las empresas peruanas pueden aprovechar la innovación tecnológica para lograr una ventaja competitiva y cómo la adaptabilidad se convierte en una ventaja estratégica en un mundo empresarial en constante evolución.

2.2.13.1 Rol de la Innovación Tecnológica

La innovación no es sólo un diferenciador, sino también una necesidad para las empresas peruanas que quieren seguir siendo competitivas.

La introducción de nuevas tecnologías como la inteligencia artificial, el Internet de las cosas (IoT) y el análisis de datos aumentará la eficiencia operativa, mejorará la toma de decisiones y abrirá nuevas oportunidades de negocio (Forum, 2021)

2.2.13.2 Desafíos de la Innovación en Empresas Peruanas

La innovación tecnológica ofrece grandes oportunidades, pero las empresas peruanas también enfrentan grandes desafíos. Las brechas digitales pueden obstaculizar la adopción efectiva de tecnologías avanzadas, tanto en términos de infraestructura como de habilidades digitales (INEI, 2020) Además, la resistencia al cambio y la falta de estrategias claras de innovación son comunes, lo que se ha convertido en un obstáculo importante.

La literatura destaca la importancia de la planificación estratégica a largo plazo,

la capacitación de los empleados y la creación de un entorno que fomente la creatividad y la experimentación para superar estos desafíos. (Bessant J. &., 2019).

2.2.13.3 Adaptabilidad Empresarial en un Mundo en Constante Cambio

En un entorno donde el cambio es la única constante, la adaptabilidad empresarial se ha vuelto crítica. Las empresas peruanas necesitan desarrollar la capacidad de anticipar y responder con agilidad a los cambios en el mercado, la tecnología y el entorno regulatorio.

Esto incluye no solo la introducción de nuevas tecnologías, sino también la reconfiguración de procesos internos y modelos de negocio (Teece, 2018). La literatura enfatiza que la adaptabilidad empresarial va más allá de la tecnología.

Se trata de una mentalidad organizacional que valora la flexibilidad y la capacidad de aprender de la experiencia. Formar equipos multifuncionales, implementar estructuras organizativas ágiles y fomentar la colaboración interna son elementos clave para fomentar la adaptabilidad (Gupta, 2017).

2.2.13.4 Estrategias para Mejorar la Innovación y Adaptabilidad

Para mejorar la innovación y la adaptabilidad, las empresas peruanas pueden implementar ciertas estrategias.

Esto incluye establecer laboratorios de innovación internos, participar activamente en el ecosistema de innovación, establecer programas de capacitación continua e integrar tecnologías fundamentales como la nube y la automatización en la infraestructura tecnológica (Forum, 2021).

Además, es fundamental fomentar una cultura organizacional que valore la creatividad, la iniciativa y el aprendizaje continuo. La incorporación de métricas de innovación y adaptabilidad en los sistemas de evaluación del desempeño

puede motivar a los empleados a contribuir activamente a estos objetivos estratégicos (Bessant J. &., 2019).

2.2.14 Normativas y Estándares Internacionales en la Gestión de Riesgos y Ciberseguridad (Standardization, 2020)

La gestión eficaz de riesgos y ciberseguridad en el entorno empresarial del Perú se beneficia enormemente de la adopción y el cumplimiento de regulaciones y estándares internacionales.

Esta sección detalla dos referencias clave: el estándar ISO 31000 para la gestión de riesgos y el Marco de Ciberseguridad del Instituto Nacional de Estándares y Tecnología (NIST).

2.2.14.1 ISO 31000: Marco General para la Gestión de Riesgos

ISO 31000 proporciona un marco integral y sistemático para la gestión de riesgos en diversas organizaciones. Esta norma establece principios básicos para guiar la identificación, evaluación y gestión efectiva de los riesgos, promoviendo así una cultura organizacional enfocada en anticipar y responder proactivamente a los desafíos

Principios Fundamentales de la ISO 31000:

Enfoque Integral: Esta norma aboga por un enfoque holístico para la gestión de riesgos y lo integra en todos los niveles y procesos de la organización.

Integración a la organización: La gestión de riesgos debe ser parte integral de las actividades de una organización, incluyendo su estructura, funciones, proyectos y procesos.

Diseño personalizado: Los enfoques de gestión de riesgos deben adaptarse al contexto y la cultura de la organización, así como a sus objetivos, tamaño y estructura.

Inclusión y participación: La participación activa y la consulta de las partes interesadas internas y externas son esenciales para una gestión de riesgos exitosa.

Enfoque holístico e integral: La gestión de riesgos requiere una consideración integral y holística de todos los factores internos y externos que pueden afectar el logro de los objetivos.

Contabilización de cambios: La gestión de riesgos debe abordar la incertidumbre y la volatilidad inherentes a cualquier actividad, teniendo en cuenta la posibilidad de resultados tanto positivos como negativos.

Personalización del marco: Los marcos de gestión de riesgos deben personalizarse para adaptarse a los procesos y estructuras existentes de una organización.

Enfoques reactivos y proactivos: La gestión de riesgos debe ser un proceso continuo, desde la identificación y evaluación hasta la respuesta y el seguimiento, adoptando un enfoque proactivo para identificar oportunidades.

Mejora continua: Las organizaciones deben mejorar continuamente sus marcos de gestión de riesgos para garantizar la eficacia y eficiencia en el logro de sus objetivos.

Toma de decisiones informada: La gestión de riesgos debe proporcionar información relevante y oportuna para respaldar la toma de decisiones informada.

Mejora de la eficiencia organizacional: La gestión de riesgos ayuda a mejorar la eficiencia y eficacia organizacional.

Inclusión de factores humanos y culturales: La cultura, el comportamiento y las capacidades humanas deben considerarse como parte de la gestión de riesgos.

2.2.14.2 NIST Framework: Directrices Específicas para la Gestión de Ciberseguridad (NIST, 2021).

El marco del NIST para mejorar la infraestructura crítica de ciberseguridad se ha convertido en una referencia global esencial para una gestión eficaz de la ciberseguridad.

Su objetivo principal es fortalecer la resiliencia cibernética y mejorar la postura de seguridad de una organización

Componentes Clave del NIST Framework:

• **Identificación:** Facilitar la comprensión y gestión proactiva de los riesgos cibernéticos.

• **Protección:** Proporciona pautas para implementar medidas de seguridad para proteger sus sistemas y datos.

• **Detección:** Centrarse en la detección temprana de amenazas y actividad maliciosa.

• **Respuesta:** Establecer un proceso para responder eficientemente a incidentes de seguridad.

• **Recuperación:** Proporciona pautas para la planificación y recuperación de incidentes cibernéticos.

Flexibilidad y Adaptabilidad:

El marco NIST se caracteriza por su flexibilidad y adaptabilidad, permitiendo su implementación en diferentes sectores y aspectos organizacionales en el Perú.

Facilita la personalización de los enfoques de ciberseguridad según las necesidades y riesgos específicos de cada organización.

Integración con Otros Estándares:

El marco NIST se puede integrar de forma sinérgica con otras regulaciones y estándares, como ISO 27001, para una implementación de ciberseguridad más completa y sólida.

Impacto en Empresas Peruanas:

La implementación efectiva de los marcos ISO 31000 y NIST proporciona a las empresas peruanas herramientas importantes para abordar el riesgo en general y la ciberseguridad en particular.

Estos estándares proporcionan una base sólida para mejorar la resiliencia organizacional, proteger la información confidencial y garantizar la continuidad del negocio en el entorno empresarial cada vez más digital y exigente del Perú.

3 CAPÍTULO III: METODOLOGÍA

3.1 Tipo de investigación

Según la fuente, trabajamos con los siguientes tipos de investigación**:**

Investigación de Aplicada: La investigación tuvo como objeto de estudio a las PYMES de Perú

Investigación de Explicativa: Las pymes enfrentan diversos desafíos relacionados con la tecnología que pueden afectar su capacidad para operar de manera eficiente y segura. Utilizamos una Metodología de Gestión del Riesgo de Proyectos de Tecnología para Pymes Basado en la ISO 31000 con el objetivo de abordar problemas específicos que las pymes comúnmente experimentan como el desconocimiento de Amenazas Tecnológica, falta de Planificación de Contingencias, Escaso Monitoreo y Evaluación Impacto en la Continuidad del Negocio por mencionar algunos puntos.

3.2 Unidad de Análisis/Población/Muestra

Unidad de Análisis

Profesional de tecnología

Población

La población estuvo compuesta por líderes con visión estratégica y profesionales con conocimientos especializados en Proyectos y Tecnologías de la Información.

Educación y Formación:

- Título universitario en Tecnologías de la Información, Ingeniería Informática, o campo relacionado.
- Certificaciones relevantes en gestión de proyectos, seguridad

informática y tecnologías emergentes.

Experiencia Laboral:

- Mínimo de 5 años de experiencia en roles técnicos y de liderazgo en el campo de Tecnologías de la Información.
- Experiencia específica en gestión de proyectos tecnológicos y dirección de equipos.

Habilidades Técnicas:

- Amplio conocimiento de infraestructuras tecnológicas, sistemas operativos y arquitecturas de red.
- Competencia en el uso de herramientas de gestión de proyectos y metodologías ágiles.

Habilidades de Gestión:

- Experiencia en la elaboración y gestión de presupuestos de tecnología.

Gestión de Riesgos:

- Experiencia demostrada en identificación, evaluación y mitigación de riesgos en proyectos de tecnología.
- Conocimiento profundo de metodologías de gestión de riesgos, preferiblemente basadas en la ISO 31000.

Muestra

La muestra fue de 10 personas, en las que se obtuvo información mediante encuestas físicas y digitales.

3.3 Técnica de Recolección de datos

Las técnicas que se utilizaron para la metodología planteada son las siguientes:

Encuestas

- Por correo
- Personales

Escala de Actitudes

En la escala de actitudes utilizada fue la escala de LIKERT porque trabajaremos en relación de confiabilidad y validez.

Pregunta
Muy en desacuerdo
En desacuerdo
Ni de acuerdo, ni en desacuerdo
De acuerdo
Muy de acuerdo

Tabla 1 - Escala de Actitudes LIKERT

3.4 Análisis e interpretación de datos

Análisis Cuantitativo:

Trabajamos con análisis cuantitativo debido que fue primordial tomar decisiones de negocio en base a un análisis numérico, la cual permitió tangibilizar una realidad de forma directa y sencilla y en donde no existió un margen de interpretaciones diferentes.

3.5 Metodología para el desarrollo de la propuesta

3.5.1 Proceso de Captura de Información:

a. Identificación de Fuentes de Información:

- Identificó y recopiló fuentes de información relevantes para el proyecto. Incluir stakeholders, documentos históricos, lecciones aprendidas de proyectos anteriores, etc.

b. Análisis de Información:

- Se evaluó la calidad y relevancia de la información recopilada.
- Realizó un análisis preliminar de riesgos potenciales asociados a la tecnología y al contexto de la PYME.

c. **Registro de Riesgos Iniciales:**

- Creó un registro inicial de riesgos identificados.
- Clasificó los riesgos según su impacto potencial y probabilidad de ocurrencia.

3.5.2 Proceso de Participación de Experto en el diseño de la Metodología:

a. Selección de Expertos:

- Identificó y seleccionó expertos en gestión de riesgos y tecnología.
- Se aseguró la representación adecuada de diversas áreas de conocimiento relevantes para el proyecto.

b. Sesiones de Diseño Colaborativo:

- Se facilitó sesiones de trabajo colaborativo con expertos.
- Se definió roles y responsabilidades en la gestión de riesgos para garantizar una participación efectiva.

c. Validación de Enfoques:

- Validó los enfoques propuestos por los expertos.
- Se aseguró la alineación de la metodología con los objetivos del proyecto y la norma ISO 31000.

3.5.3 Proceso de Definición de Metodología:

a. Elaboración de Documentación:

- Documentó la metodología de gestión de riesgos de proyectos de tecnología.
- Incluyó procesos, roles, responsabilidades, herramientas y flujos de trabajo.

b. Personalización para PYMES:

- Adaptó la metodología a las características específicas de las PYMES.

- Consideró la escalabilidad y flexibilidad para diferentes tamaños de proyectos.

c. Capacitación del Equipo:

- Desarrolló programas de capacitación para el equipo sobre la metodología.
- Garantizó la comprensión y aceptación de la metodología en todos los niveles del proyecto.

3.5.4 Proceso de Prueba de Metodología en la Organización:

a. Implementación Piloto:

- Se realizó una implementación piloto de la metodología en un proyecto específico.
- Se evaluó su efectividad y se realizó ajustes según sea necesario.

b. Recopilación de Retroalimentación:

- Obtuvo retroalimentación del equipo y stakeholders sobre la aplicación de la metodología.
- Identificó áreas de mejora y oportunidades de optimización.

c. Ajuste Continuo:

- Se realizó ajustes continuos en la metodología en función de los resultados de la implementación piloto y la retroalimentación recibida.
- Se mantuvo la flexibilidad para adaptarse a cambios en el entorno del proyecto.

- Al seguir esta metodología, se buscó asegurar una gestión efectiva de los riesgos en proyectos de tecnología para PYMES, tomando como referencia los principios de la norma ISO 31000.

4 CAPÍTULO IV: DEFINICIÓN DE LA METODOLOGÍA

4.1 Análisis, interpretación y discusión de resultados

La elección del juicio de expertos como método predominante en la metodología de gestión del riesgo para proyectos tecnológicos de Pymes, basada en la norma ISO 31000, se justifica por diversas razones.

La complejidad del entorno tecnológico para Pymes, la flexibilidad y adaptabilidad que ofrece el juicio de expertos, la capacidad de personalizar la metodología ISO 31000, la rapidez y eficiencia en la toma de decisiones, el enfoque holístico que incorpora factores diversos, la validación empírica basada en la experiencia práctica, la participación activa y compromiso de los expertos, y la posibilidad de una mejora continua integrada son todos elementos clave que hacen que el juicio de expertos sea la opción más idónea para abordar los desafíos dinámicos y específicos de la gestión de riesgos en proyectos tecnológicos para Pymes.

Este enfoque no solo enriquece la metodología, sino que también garantiza su aplicabilidad y relevancia a lo largo del tiempo en un entorno tecnológico en constante evolución. A continuación, mencionamos algunos ámbitos relevantes para trabajar con el juicio de experto.

a. Complejidad del Contexto Tecnológico para Pymes:

Las Pymes en el sector tecnológico a menudo operan en entornos altamente dinámicos y competitivos. La diversidad de tecnologías, la rapidez de los avances y la presión para la innovación hacen que la gestión de riesgos sea particularmente desafiante. La experiencia de expertos en este contexto específico es esencial para comprender las complejidades únicas y anticipar posibles amenazas y oportunidades.

b. Flexibilidad y Adaptabilidad:

La flexibilidad es clave en la gestión del riesgo tecnológico, donde las condiciones pueden cambiar rápidamente. Los métodos que dependen en gran medida de datos estáticos pueden volverse obsoletos en poco tiempo. El juicio de expertos permite ajustar rápidamente las estrategias de gestión de riesgos en respuesta a cambios en el panorama tecnológico, asegurando una adaptabilidad continua.

c. Personalización de la Metodología ISO 31000:

Aunque la norma ISO 31000 proporciona un marco sólido, su aplicación genérica puede no abordar todas las particularidades de una Pyme en el sector tecnológico. Los expertos pueden personalizar la metodología para adaptarse a los requisitos específicos, considerando factores como el tamaño de la organización, la naturaleza de los proyectos tecnológicos y las limitaciones de recursos.

d. Rapidez y Eficiencia:

La toma de decisiones ágil es esencial en proyectos tecnológicos, donde los plazos de entrega y la velocidad de desarrollo son críticos. La experiencia de expertos permite evaluar rápidamente riesgos potenciales y tomar decisiones informadas sin perder tiempo en la recopilación excesiva de datos, lo que mejora la eficiencia del proceso de gestión de riesgos.

e. Enfoque Holístico:

La gestión del riesgo efectiva en proyectos tecnológicos no puede limitarse únicamente a consideraciones técnicas. Factores comerciales, regulatorios y humanos también desempeñan un papel crucial. Los expertos aportan una perspectiva holística, asegurando que la metodología aborde de manera integral todos los aspectos relevantes para mitigar riesgos de manera efectiva.

f. Validación Empírica:

La experiencia práctica de los expertos aporta una dimensión de validación empírica. Basando sus juicios en situaciones reales y casos anteriores, los expertos mejoran la calidad y confiabilidad de las evaluaciones de riesgos. Esta validación empírica agrega credibilidad a la metodología propuesta, demostrando su aplicabilidad en contextos del mundo real.

g. Participación Activa y Compromiso:

Involucrar a expertos en la gestión de riesgos fomenta un mayor grado de participación y compromiso. Al sentir que sus conocimientos y experiencias son valorados, los expertos están más inclinados a contribuir de manera activa y constructiva. Este compromiso fortalece el proceso de gestión del riesgo al aprovechar plenamente la experiencia y perspicacia de los profesionales.

h. Mejora Continua Integrada:

La retroalimentación continua de los expertos, combinada con la flexibilidad inherente al juicio de expertos, permite una mejora continua integrada en la metodología de gestión del riesgo. La capacidad de adaptarse a medida que evolucionan los riesgos tecnológicos y de incorporar aprendizajes de proyectos anteriores garantiza que la metodología se mantenga relevante y efectiva a lo largo del tiempo.

El objetivo principal de esta metodología es proporcionar a las pequeñas y medianas empresas (PYMES) una estructura integral y efectiva para la gestión de riesgos en proyectos de tecnología, basada en los principios y directrices establecidos en la norma internacional ISO 31000. A continuación, se profundiza en los aspectos clave de este objetivo:

Integración de Principios ISO 31000:

La metodología tiene como núcleo la incorporación de los principios fundamentales de la ISO 31000, que incluyen la toma de decisiones basada en el riesgo, la comunicación efectiva, y el establecimiento de un enfoque proactivo

y continuo en la gestión de riesgos. Esta integración asegura que las PYMES sigan estándares globalmente reconocidos.

Adaptación a Contexto PYME:

Se busca adecuar los principios y prácticas de gestión de riesgos a la realidad y recursos disponibles en las PYMES. Esto implica considerar la escala de operaciones, la flexibilidad organizativa y los presupuestos más ajustados que caracterizan a este tipo de empresas. La metodología se diseñará para ser práctica, ágil y aplicable a entornos empresariales más pequeños.

Enfoque Específico para Proyectos de Tecnología:

La metodología se centra exclusivamente en proyectos relacionados con tecnología, reconociendo los riesgos específicos que estos enfrentan, como vulnerabilidades de seguridad informática, cambios tecnológicos rápidos y la dependencia de proveedores de tecnología. Se adaptará a los desafíos únicos que enfrentan las PYMES en el ámbito tecnológico.

Facilitar Toma de Decisiones Informada:

El propósito es dotar a los líderes y equipos de proyectos en PYMES con las herramientas necesarias para tomar decisiones informadas y conscientes sobre la gestión de riesgos. La metodología proporcionará un marco estructurado para evaluar, priorizar y abordar los riesgos potenciales, permitiendo a las PYMES avanzar con confianza en sus iniciativas tecnológicas.

Fomentar la Cultura de Gestión de Riesgos:

Además de proporcionar un conjunto de directrices, la metodología tiene como objetivo fomentar una cultura de gestión de riesgos dentro de las PYMES. Esto implica la promoción de la conciencia y la responsabilidad en todos los niveles de la organización para que la gestión de riesgos se considere integralmente en la planificación y ejecución de proyectos.

Mejorar la Resiliencia Empresarial:

La metodología aspira a fortalecer la resiliencia empresarial de las PYMES frente a los desafíos y obstáculos que pueden surgir durante la ejecución de proyectos tecnológicos. Al identificar y gestionar proactivamente los riesgos, se busca reducir la probabilidad de incidentes adversos y aumentar la capacidad de adaptación de las PYMES.

Coeficiente de fiabilidad de medida: Alfa de Cronbach

El coeficiente Alfa de Cronbach desempeña un papel esencial en una tesis centrada en la gestión de riesgos para proyectos de tecnología. Su importancia radica en la evaluación de la consistencia interna de los instrumentos de medición utilizados en la investigación. Algunos puntos clave que destacan su relevancia son:

El Alfa de Cronbach asegura la confiabilidad de las mediciones asociadas con la gestión de riesgos en proyectos tecnológicos. Evaluar la consistencia interna de las preguntas relacionadas con la identificación, evaluación y mitigación de riesgos garantiza la integridad de los resultados obtenidos.

En el contexto de la gestión de riesgos, el Alfa de Cronbach valida la coherencia de los instrumentos utilizados para medir la percepción de riesgos entre los participantes del proyecto. Esto fortalece la validez interna de la investigación y la calidad de las mediciones.

La consistencia interna evaluada por el Alfa de Cronbach garantiza que las respuestas proporcionadas por los participantes sean coherentes y confiables. Esto es crucial para la toma de decisiones informada en la gestión de riesgos tecnológicos.

Al identificar la consistencia interna, el Alfa de Cronbach facilita la identificación de áreas específicas dentro de la metodología de gestión de riesgos que pueden necesitar ajustes. Esto permite una toma de decisiones más eficiente y

mejora continua en el proceso de gestión de riesgos.

Dado que la gestión de riesgos a menudo implica evaluar diversas dimensiones de un proyecto, el Alfa de Cronbach es especialmente relevante cuando se trabaja con escalas unidimensionales, asegurando que todas las preguntas estén alineadas para medir un mismo constructo.

La simplicidad del Alfa de Cronbach en la presentación de un único número para representar la consistencia interna facilita la interpretación de los resultados. Esto es esencial al comunicar hallazgos a audiencias que pueden no tener una comprensión profunda de la estadística.

La inclusión del Alfa de Cronbach en la metodología de la tesis demuestra un enfoque riguroso y sistemático en la gestión de riesgos para proyectos tecnológicos. Esto refuerza la credibilidad de la investigación y la validez de las conclusiones alcanzadas.

Formula de Alfa de Cronbach

$$\alpha = \frac{k}{k-1}\left|1 - \frac{\Sigma s_i^2}{s_T^2}\right|$$

Ecuación 1 - Fórmula de Alfa de Cronbach

VARIABLES	DEFINICIÓN
k	Número de items
Σs_i^2	Sumatoria de las varianzas de los items
s_T^2	Varianza de la suma de los items
α	Coeficiente de Alfa de Cronbach

Tabla 2 - Definición de variables de Alfa de Cronbach

La interpretación del coeficiente corresponde a la siguiente tabla:

VALOR DE COEFICIENTE	INTERPRETACIÓN
[0.9 ; 1]	Excelente
[0.8 ; 0.9>	Bueno
[0.7 ; 0.8>	Aceptable
[0.6 ; 0.7>	Malo
[0 ; 0.5>	Muy malo

Tabla 3 – Valor de Coeficiente de la Fórmula de Alfa Cronbach

Instrumento: Escala de Likert

La elección de utilizar la escala de Likert en una tesis de gestión de proyectos de tecnología se justifica por su capacidad para medir de manera efectiva las actitudes, percepciones y opiniones de los participantes en relación con la gestión de proyectos tecnológicos.

Esta escala ofrece flexibilidad en las respuestas, permitiendo a los participantes expresar una variedad de matices en sus opiniones, desde totalmente en desacuerdo hasta totalmente de acuerdo. Además, la gradación de intensidad en la escala de Likert proporciona la oportunidad de capturar la fuerza de las respuestas, lo cual es crucial en la evaluación de estrategias de gestión de riesgos.

La escala de Likert no solo facilita el análisis cuantitativo de los datos recopilados, sino que también permite comparaciones entre diferentes grupos de participantes o momentos del proyecto. Esto es esencial para identificar tendencias a lo largo del tiempo o entre distintos segmentos de la muestra, ofreciendo una comprensión más completa de la gestión de proyectos tecnológicos.

La estandarización proporcionada por la escala de Likert facilita la comparación y replicación de estudios, garantizando la consistencia en la medición, un aspecto crucial en el ámbito de la gestión de proyectos tecnológicos. Su adaptabilidad a diferentes contextos dentro de la gestión de proyectos tecnológicos la hace versátil y aplicable a diversas fases, desde la identificación de riesgos hasta la evaluación de estrategias de mitigación.

Además, la escala de Likert no solo ofrece datos cuantitativos, sino que también permite la obtención de información cualitativa valiosa al permitir que los participantes agreguen comentarios o explicaciones a sus respuestas. Esto enriquece la comprensión de las percepciones y actitudes detrás de los números.

Instrumento: Pregunta Likert

Las preguntas en base a la escala de Likert son las siguiente:
Por favor, indique en qué medida recomendaría utilizar el siguiente proceso a sus colegas, donde 1 es "No lo recomendaría en absoluto" y 5 es "Lo recomendaría altamente".

1. No lo recomendaría en absoluto
2. No lo recomendaría
3. Es indiferente recomendarlo
4. Lo recomendaría
5. Lo recomendaría en absoluto

4.1.1 Recopilación de procesos

Durante el proceso de investigación se recopiló información clave de diversas fuentes, especialmente artículos académicos relacionados con la gestión de riesgos y la norma ISO 31000.

En la primera etapa del desarrollo del método, se llevó a cabo una revisión exhaustiva de la literatura para identificar los procesos centrales adecuados para la gestión de riesgos de proyectos de tecnología en PYMES. La información recopilada se organizó sistemáticamente en una tabla que proporciona una descripción general de los diversos métodos y prácticas propuestos en la literatura revisada. La tabla se convierte en una valiosa herramienta para comprender y comparar los procesos identificados.

Luego se utilizó un método de calificación de expertos para determinar la importancia relativa de cada proceso en la tabla. Se seleccionó un panel de expertos en gestión de proyectos y gestión de riesgos para evaluar y clasificar los procesos en función de su relevancia y contribución a la gestión eficaz de riesgos de proyectos tecnológicos de las PYME. Esta evaluación se basa en la experiencia práctica y un profundo conocimiento de los desafíos específicos que enfrentan las PYMES en los proyectos tecnológicos.

Las prioridades determinadas como resultado de la evaluación de expertos permitieron identificar y resaltar los procesos de gestión de riesgos más críticos y relevantes relacionados con proyectos tecnológicos de las PYMES. Estos procesos priorizados forman la base del enfoque propuesto, proporcionando un marco sólido adaptado a las necesidades específicas de las PYMES en el sector tecnológico.
Ahora detallamos el título y las descripciones de cada proceso que fue evaluado por los expertos:

N	PROCESO	DESCRIPCIÓN
1	Análisis de Condiciones del Mercado	Analizar las condiciones del mercado para anticipar riesgos relacionados con la oferta y demanda.
2	Análisis de	Analizar los riesgos asociados a los proveedores y

	Riesgos de Proveedores	establecer estrategias de contingencia.
3	Análisis de Riesgos Geopolíticos	Analizar riesgos asociados a factores geopolíticos que puedan afectar la operación de la organización.
4	Análisis de Riesgos Psicosociales	Analizar los riesgos relacionados con factores psicosociales que puedan afectar al personal.
5	Análisis de Tendencias de Riesgos	Analizar tendencias pasadas y actuales para prever posibles riesgos emergentes.
6	Análisis de Vulnerabilidades Tecnológicas	Analizar las vulnerabilidades tecnológicas existentes y potenciales que podrían dar lugar a riesgos.
7	Auditoría de Controles Internos	Realizar auditorías periódicas de los controles internos para garantizar su eficacia en la gestión de riesgos.
8	Categorización de Riesgos Financieros	Categorizar los riesgos según su impacto financiero y probabilidad de ocurrencia.
9	Comunicación de Riesgos	Desarrollar un plan de comunicación efectivo para informar a las partes interesadas sobre los riesgos.
10	Desarrollo de Capacidades de Respuesta	Desarrollar capacidades internas para responder de manera efectiva a eventos de riesgo.
11	Desarrollo de Escenarios de Riesgo	Crear escenarios hipotéticos de riesgo para evaluar la preparación de la organización.
12	Diseño de Estrategias de	Desarrollar estrategias específicas de mitigación para abordar los riesgos identificados durante la evaluación

	Mitigación	inicial.
13	Evaluación de Amenazas Cibernéticas	Evaluar y mitigar riesgos asociados a amenazas cibernéticas y brechas de seguridad.
14	Evaluación de Competencias del Personal	Evaluar las competencias del personal para gestionar eficazmente los riesgos en sus respectivas áreas.
15	Evaluación de Impacto en la Reputación	Evaluar el posible impacto en la reputación de la organización en caso de materialización de riesgos.
16	Evaluación de Riesgos en Innovación	Evaluar los riesgos asociados a iniciativas de innovación y desarrollo.
17	Evaluación de Riesgos en la Cadena de Suministro	Evaluar y gestionar los riesgos en la cadena de suministro, desde proveedores hasta distribuidores.
18	Evaluación de Riesgos Financieros Externos	Evaluar los riesgos financieros externos, como fluctuaciones de moneda y tasas de interés.
19	Evaluación de Riesgos Legales	Evaluar y gestionar los riesgos legales, incluyendo litigios y cambios regulatorios.
20	Evaluación de Riesgos Operativos	Evaluar riesgos vinculados a las operaciones diarias de la organización.
21	Evaluación Inicial	Realizar una evaluación inicial exhaustiva para identificar y comprender los riesgos potenciales en todas las áreas de la organización.

22	Gestión de Riesgos Ambientales	Integrar la gestión de riesgos asociados a impactos ambientales y sostenibilidad.
23	Gestión de Riesgos en Alianzas Estratégicas	Integrar la gestión de riesgos en alianzas estratégicas para maximizar beneficios y minimizar amenazas.
24	Gestión de Riesgos en la Cadena de Valor	Gestionar riesgos a lo largo de la cadena de valor, desde la producción hasta la entrega.
25	Gestión de Riesgos en Proyectos:	Integrar la gestión de riesgos en cada fase de los proyectos para mitigar posibles contratiempos.
26	Identificación de Actores Clave	Identificar y clasificar a los actores clave dentro y fuera de la organización que pueden afectar o ser afectados por los riesgos.
27	Implementación	Poner en práctica las estrategias de mitigación diseñadas, asegurando una ejecución eficiente y efectiva en toda la organización.
28	Integración con Otros Estándares	Integrar la metodología de gestión de riesgos con otros estándares relevantes, asegurando una alineación efectiva con las mejores prácticas y normativas de la industria.
29	Mejora Continua	Identificar oportunidades de mejora en el proceso de gestión de riesgos y realizar ajustes continuos para optimizar la eficacia de las estrategias de mitigación.
30	Monitoreo Continuo	Establecer un sistema continuo de monitoreo para supervisar la efectividad de las estrategias de mitigación y detectar cambios en el panorama de

		riesgos.
31	Monitoreo de Cambios Normativos	Monitorear cambios en normativas y leyes que puedan afectar el panorama de riesgos de la organización.
32	Respuestas a Incidentes	Desarrollar planes de respuesta a incidentes para actuar rápidamente en caso de que ocurran eventos de riesgo, minimizando así el impacto en la organización.
33	Revisión de Políticas Internas	Revisar y actualizar regularmente las políticas internas relacionadas con la gestión de riesgos.
34	Revisión Posterior de Incidentes	Realizar revisiones detalladas de incidentes pasados para aprender y mejorar la gestión de riesgos.
35	Seguimiento de Indicadores Clave de Riesgo	Establecer y monitorear indicadores clave de riesgo para identificar desviaciones significativas.
36	Seguimiento de Riesgos Residuales	Monitorear los riesgos residuales después de la implementación de medidas de mitigación.
37	Simulacros de Crisis	Realizar simulacros de crisis para evaluar la respuesta y eficacia de los planes de contingencia.

Tabla 4 – Procesos para la Validación de Experto

4.2 Priorización de procesos por juicio de expertos

Los expertos desempeñan un papel importante ya que aportan su experiencia y conocimientos en la gestión de proyectos y riesgos. Estos expertos han sido cuidadosamente seleccionados por su experiencia práctica y su profundo

conocimiento de los desafíos específicos que enfrentan las PYME en proyectos tecnológicos. Cuando se formó el grupo de expertos, se les entregó una tabla que resumía los procesos identificados en la revisión de la literatura.

Cada experto evalúa individualmente la importancia de cada proceso en base a criterios predefinidos, teniendo en cuenta la aplicabilidad y relevancia de cada proceso en la gestión de las PYMES y sus proyectos tecnológicos.

Este proceso de integración de ideas nos permitió identificar claramente los 7 procesos (Evaluación Inicial, Diseño de Estrategias de Mitigación, Implementación, Respuestas a Incidentes, Mejora Continua, Monitoreo Continuo, Integración con Otros Estándares) más importantes y críticos para una gestión eficaz de riesgos en proyectos tecnológicos de las PYMES.

La priorización mediante la calificación de expertos produce un marcador que refleja la importancia de cada proceso según el consenso de los expertos. La tabla no sólo proporciona una visión general clara del proceso de priorización, sino que también se convierte en un recurso valioso para comprender la estructura y el enfoque del enfoque propuesto.

4.2.1 Respuestas de los expertos: Escala de Likert

N	PROCESO	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10
1	Análisis de Condiciones del Mercado	2	2	1	2	2	2	1	2	1	2
2	Análisis de Riesgos de Proveedores	1	1	2	3	2	1	2	1	2	5
3	Análisis de Riesgos Geopolíticos	2	1	2	4	2	2	4	1	2	2
4	Análisis de Riesgos Psicosociales	2	2	1	4	1	2	2	1	1	2
5	Análisis de Tendencias de Riesgos	2	2	3	1	1	3	2	5	2	2
6	Análisis de Vulnerabilidades Tecnológicas	5	1	2	2	3	3	1	5	1	5
7	Auditoría de Controles Internos	2	4	2	1	2	2	5	1	2	2
8	Categorización de Riesgos Financieros	1	2	2	3	2	2	2	1	2	1
9	Comunicación de Riesgos	2	3	2	5	5	2	2	5	5	1
10	Desarrollo de Capacidades de Respuesta	2	1	2	5	1	2	2	2	1	1
11	Desarrollo de Escenarios de Riesgo	2	1	1	2	1	2	2	1	2	2
12	Diseño de Estrategias de Mitigación	5	5	5	5	5	5	3	5	5	5
13	Evaluación de Amenazas Cibernéticas	1	4	1	2	3	1	2	2	2	3

14	Evaluación de Competencias del Personal	2	2	1	1	1	1	1	2	1	1
15	Evaluación de Impacto en la Reputación	1	2	2	1	2	1	2	2	3	2
16	Evaluación de Riesgos en Innovación	2	1	4	2	1	2	1	3	3	2
17	Evaluación de Riesgos en la Cadena de Suministro	2	3	2	1	3	1	1	2	2	2
18	Evaluación de Riesgos Financieros Externos	2	1	2	1	1	2	1	1	2	1
19	Evaluación de Riesgos Legales	2	2	2	1	1	3	2	2	2	2
20	Evaluación de Riesgos Operativos	2	1	1	1	1	2	1	1	1	1
21	Evaluación Inicial	5	5	5	5	5	5	5	5	5	5
22	Gestión de Riesgos Ambientales	1	2	1	2	3	1	2	2	1	2
23	Gestión de Riesgos en Alianzas Estratégicas	2	1	1	1	2	1	2	1	2	2
24	Gestión de Riesgos en la Cadena de Valor	1	1	2	2	2	2	1	2	1	2
25	Gestión de Riesgos en Proyectos:	1	2	1	2	2	2	1	2	1	2
26	Identificación de Actores Clave	1	1	1	1	2	2	2	1	2	1
27	Implementación	5	5	5	5	5	3	5	5	5	5
28	Integración con Otros Estándares	5	2	5	2	5	5	2	5	5	5
29	Mejora Continua	5	5	5	5	1	5	5	2	5	5

30	Monitoreo Continuo	5	3	3	5	2	5	5	5	5	5
31	Monitoreo de Cambios Normativos	1	2	1	2	1	2	1	2	2	2
32	Respuestas a Incidentes	5	5	5	3	5	5	5	5	5	5
33	Revisión de Políticas Internas	2	3	2	1	2	1	2	2	2	1
34	Revisión Posterior de Incidentes	2	1	1	1	2	1	1	2	2	1
35	Seguimiento de Indicadores Clave de Riesgo	1	1	1	1	1	2	2	2	1	1
36	Seguimiento de Riesgos Residuales	2	1	2	2	2	2	1	2	2	2
37	Simulacros de Crisis	1	2	1	3	2	1	1	1	2	2

Tabla 5 – Resultados de la Validación de Experto

VARIABLES	VALOR
k	37
Σs_i^2	25.51
s_T^2	13.41

Tabla 6 - Valores de las variables de ALFA DE CRONBACH

$$\alpha = \frac{k}{k-1}\left|1 - \frac{\Sigma s_i^2}{s_T^2}\right| = 0.9237$$

Ecuación 2- Resultados de la fórmula de ALFA DE CRONBACH

4.2.2 Interpretación del resultado obtenido:

Un coeficiente Alfa de Cronbach de 0.92 indica una alta consistencia interna entre los ítems en la escala o instrumento de medición utilizado en tu estudio. Aquí hay una interpretación detallada de este valor:

Excelente Consistencia Interna:

Un Alfa de Cronbach de 0.92 se considera muy alto y sugiere que los ítems de tu escala están altamente relacionados entre sí. Esto implica que las preguntas o afirmaciones en tu instrumento miden de manera consistente el mismo constructo o característica que intentas evaluar.

Fiabilidad de la Medición:

La alta consistencia interna indica una mayor fiabilidad de tu escala. En otras palabras, la escala es confiable para medir el concepto que pretendes evaluar. Los participantes tienden a responder de manera consistente a lo largo de la escala, lo que refuerza la solidez de tus mediciones.

Precisión en la Evaluación:

Un Alfa de Cronbach de 0.9273 sugiere que tu instrumento es preciso en la evaluación del constructo específico. La consistencia interna es esencial para obtener mediciones confiables y válidas, y tu instrumento parece ser altamente preciso en este sentido.

Adecuación para Decisiones Importantes:

Un Alfa de Cronbach de 0.9273 sugiere que tu escala es adecuada para tomar decisiones importantes basadas en las puntuaciones obtenidas. La consistencia interna fortalece la validez de las inferencias que puedes hacer sobre la población a partir de las respuestas de tu muestra.

4.2.3 Confianza en los Resultados:

Con un Alfa de Cronbach tan alto, puedes tener confianza en la confiabilidad de tu instrumento. Los resultados obtenidos son más estables y consistentes, lo que mejora la robustez y la credibilidad de tus hallazgos.

4.2.4 Priorización de Procesos:

N	PROCESO	Puntuación
21	Evaluación Inicial	50
12	Diseño de Estrategias de Mitigación	48
27	Implementación	48
32	Respuestas a Incidentes	48
29	Mejora Continua	43
30	Monitoreo Continuo	43
28	Integración con Otros Estándares	41
9	Comunicación de Riesgos	32
6	Análisis de Vulnerabilidades Tecnológicas	28
5	Análisis de Tendencias de Riesgos	23
7	Auditoría de Controles Internos	23
3	Análisis de Riesgos Geopolíticos	22
13	Evaluación de Amenazas Cibernéticas	21
16	Evaluación de Riesgos en Innovación	21
2	Análisis de Riesgos de Proveedores	20
10	Desarrollo de Capacidades de Respuesta	19
17	Evaluación de Riesgos en la Cadena de Suministro	19
19	Evaluación de Riesgos Legales	19
4	Análisis de Riesgos Psicosociales	18
8	Categorización de Riesgos Financieros	18
15	Evaluación de Impacto en la Reputación	18
33	Revisión de Políticas Internas	18
36	Seguimiento de Riesgos Residuales	18

1	Análisis de Condiciones del Mercado	17
22	Gestión de Riesgos Ambientales	17
11	Desarrollo de Escenarios de Riesgo	16
24	Gestión de Riesgos en la Cadena de Valor	16
25	Gestión de Riesgos en Proyectos:	16
31	Monitoreo de Cambios Normativos	16
37	Simulacros de Crisis	16
23	Gestión de Riesgos en Alianzas Estratégicas	15
18	Evaluación de Riesgos Financieros Externos	14
26	Identificación de Actores Clave	14
34	Revisión Posterior de Incidentes	14
14	Evaluación de Competencias del Personal	13
35	Seguimiento de Indicadores Clave de Riesgo	13
20	Evaluación de Riesgos Operativos	12

La revisión de las encuestas realizada a ejecutivos y expertos en TI proporciona información sobre áreas clave de la gestión de riesgos de proyectos tecnológicos. Estos resultados, extraídos de las experiencias y percepciones del grupo encuestado, revelan las prioridades que estos profesionales han asignado a los procesos involucrados en la gestión de riesgos. Los procesos prioritarios identificados y su alcance de actividades son las siguientes:

1. Evaluación inicial:

La fase de evaluación inicial se ha convertido en el primer paso crítico en la gestión de riesgos. Este proceso implica una evaluación cuidadosa de los riesgos potenciales asociados con el proyecto desde su inicio. Es importante comprender la naturaleza y gravedad del riesgo inicial para construir un marco sólido y proactivo para la toma de decisiones informadas en las etapas posteriores del proyecto.

2. Desarrollo de estrategias de mitigación:

Establecer prioridades en el desarrollo de estrategias de mitigación refleja la comprensión de los profesionales de la necesidad de desarrollar métodos eficaces para gestionar y reducir los riesgos identificados. Este proceso implica el desarrollo de estrategias sólidas, que pueden incluir la mitigación directa de ciertos riesgos, la transferencia de riesgos o incluso la aceptación controlada. Su finalidad es garantizar la protección de los activos y la optimización efectiva de los recursos disponibles.

3. Implementación:

La fase de implementación se convierte en un componente clave de la gestión de riesgos. La ejecución efectiva de las estrategias desarrolladas en la fase de mitigación es esencial para asegurar el desarrollo exitoso del proyecto tecnológico. Los encuestados reconocen la importancia de una implementación efectiva para traducir las estrategias teóricas en acciones concretas que reduzcan los riesgos identificados.

4. Respuesta al incidente:

La preparación para incidentes es un proceso fundamental de gestión de riesgos. Dada la inevitabilidad de los acontecimientos imprevistos, los expertos subrayan la necesidad de planes de acción y respuestas claros. La puntualidad y la eficiencia en la respuesta a incidentes se han convertido en elementos clave para minimizar el impacto y regresar rápidamente a las operaciones normales.

5. Mejora continua:

La mejora continua se ha convertido en un proceso importante en la gestión de riesgos tecnológicos. Los profesionales son conscientes de la naturaleza dinámica del riesgo y de la necesidad de adaptarse constantemente a las circunstancias cambiantes. Este proceso implica revisión y aprendizaje continuo

de estrategias para mejorar las prácticas y responder de manera más efectiva a riesgos futuros.

6. Monitoreo continuo:

El seguimiento continuo se considera una práctica clave para la identificación temprana de cambios en situaciones de riesgo. La vigilancia continua no sólo permite anticipar problemas potenciales, sino que también garantiza que las estrategias de mitigación sean efectivas a lo largo del tiempo. El seguimiento continuo es una defensa activa contra el desarrollo dinámico de los riesgos tecnológicos.

7. Integración con otros estándares:

La integración con otros estándares de gestión se considera un proceso clave para optimizar la eficacia de la gestión de riesgos. La sinergia con los marcos y estándares existentes proporciona un enfoque integral y sólido. Los encuestados vieron esta integración como una forma de aprovechar las mejores prácticas y estándares de la industria para mejorar y perfeccionar su enfoque general de gestión de riesgos. Los resultados proporcionan una visión integral y detallada de las áreas que el entorno de gestión de riesgos debe priorizar en los proyectos tecnológicos. Sirven como una guía valiosa para tomar decisiones estratégicas e implementar prácticas que maximicen la seguridad y el éxito en el espacio de los proyectos tecnológicos.

4.2.5 Fases de la Metodologías propuestas:

En el contexto de la gestión de riesgos en proyectos tecnológicos para PYMES, las siguientes fases descritas representan etapas críticas que impulsan la efectividad y la aplicabilidad de la metodología diseñada.

Una vez que se ha completado el proceso de "Priorización de procesos por juicio de expertos", y se han identificado los procesos más importantes y críticos para la gestión de riesgos en proyectos tecnológicos para PYMES basado en la

ISO 31000, el siguiente paso crucial implica desarrollar de manera detallada cada proceso.

4.2.5.1 EVALUACIÓN INICIAL (FASE 1):

La fase de Evaluación Inicial es el punto de partida crítico en la metodología de gestión del riesgo de proyectos tecnológicos para Pymes basada en la ISO 31000. Durante esta fase, se lleva a cabo una revisión exhaustiva para identificar y comprender los riesgos potenciales que pueden afectar el proyecto. Aquí, se profundiza en los aspectos clave de esta fase:

Identificación de Activos y Recursos (IAR):

Se comienza por identificar y catalogar todos los activos y recursos relevantes para el proyecto tecnológico. Esto puede incluir hardware, software, datos, personal, proveedores y otros elementos críticos. La identificación precisa de estos activos es fundamental para comprender las posibles vulnerabilidades.

Identificación de Amenazas y Vulnerabilidades (IAV):

Se lleva a cabo un análisis detallado para identificar las amenazas potenciales y las vulnerabilidades asociadas a los activos y recursos identificados. Las amenazas pueden provenir de factores externos como ciberataques, desastres naturales o cambios en el entorno empresarial. Las vulnerabilidades son las debilidades intrínsecas que podrían ser explotadas por estas amenazas.

Evaluación de Probabilidades e Impactos (EPI):

Cada riesgo identificado se evalúa en términos de la probabilidad de ocurrencia y el impacto potencial en el proyecto. Esto implica asignar valores numéricos que representen la posibilidad de que ocurra un riesgo y la magnitud de sus consecuencias. Estos valores proporcionan una base cuantitativa para la

posterior priorización de riesgos.

Priorización de Riesgos (PR):
Con base en la evaluación de probabilidades e impactos, se priorizan los riesgos para centrar la atención en aquellos que tienen el mayor potencial de afectar negativamente el proyecto. Este proceso ayuda a asignar recursos y esfuerzos de gestión de riesgos de manera más eficiente.

Establecimiento de Tolerancias y Apetito de Riesgo (ETAR):

Se define el nivel de tolerancia al riesgo y el apetito de riesgo de la organización. Estos parámetros determinan cuánto riesgo está dispuesta a aceptar la empresa y guían las decisiones en la gestión de riesgos. Establecer límites claros contribuye a evitar la toma excesiva o insuficiente de riesgos.

Desarrollo del Registro de Riesgos (DRR):
Se compila un registro detallado que documenta todos los riesgos identificados, sus características, evaluaciones de probabilidad e impacto, y prioridades asignadas. Este registro sirve como referencia centralizada para la gestión continua de riesgos a lo largo del proyecto.

4.2.5.2 DISEÑO DE ESTRATEGIA DE MITIGACIÓN (FASE 2):

La fase de Diseño de Estrategias de Mitigación es una etapa crucial en la metodología de gestión del riesgo de proyectos tecnológicos para Pymes basada en la ISO 31000. Durante esta fase, se desarrollan estrategias específicas para abordar y mitigar los riesgos identificados en la etapa de Evaluación Inicial. Aquí, se profundiza en los aspectos clave de esta fase:

Análisis de Riesgos Residuales (ARR):

Se realiza un análisis detallado de los riesgos residuales después de la evaluación inicial. Este análisis considera factores como la probabilidad de

ocurrencia, el impacto potencial y la aceptabilidad de los riesgos restantes. El objetivo es comprender completamente la naturaleza y la magnitud de los riesgos que persisten.

Desarrollo de Estrategias de Mitigación (DEM):

Con base en el análisis de riesgos residuales, se diseñan estrategias específicas para reducir la probabilidad de ocurrencia o minimizar el impacto de los riesgos identificados. Estas estrategias pueden incluir medidas preventivas, acciones de contingencia, transferencia de riesgos a terceros o retención controlada. La selección de estrategias se realiza considerando la viabilidad, la eficacia y el costo asociado.

Priorización de Estrategias (PE):

Se establece un proceso de priorización para determinar qué estrategias de mitigación se implementarán primero. Este proceso considera la criticidad y la urgencia de cada riesgo, así como la disponibilidad de recursos. La priorización asegura que se aborden primero los riesgos que tienen el mayor impacto potencial en el proyecto.

Establecimiento de Criterios de Éxito (ECE):

Para evaluar la efectividad de las estrategias de mitigación, se definen criterios claros de éxito. Estos criterios pueden incluir la reducción de la probabilidad de ocurrencia, la minimización del impacto, el cumplimiento de regulaciones específicas o cualquier otro indicador relevante. Establecer criterios de éxito proporciona un marco objetivo para evaluar el rendimiento de las estrategias implementadas.

Creación del Plan de Mitigación (CPM):

Se desarrolla un plan detallado que describe la implementación de cada estrategia de mitigación. El plan incluye un cronograma, asignación de responsabilidades, recursos necesarios y cualquier restricción o consideración especial. La creación del plan garantiza una ejecución eficiente y coordinada de las estrategias de mitigación.

4.2.5.3 IMPLEMENTACIÓN: (FASE 3)

La fase de Implementación es una etapa crítica en la metodología de gestión del riesgo de proyectos tecnológicos para Pymes basada en la ISO 31000. Esta fase se centra en llevar a cabo las estrategias de mitigación definidas durante la etapa de Diseño, con el objetivo de reducir la probabilidad de ocurrencia y el impacto de los riesgos identificados. A continuación, se profundiza en los aspectos clave de esta fase:

Despliegue de Estrategias de Mitigación (DEM):

En esta etapa, se implementan las estrategias de mitigación diseñadas previamente. Esto implica llevar a cabo acciones específicas para reducir la probabilidad de ocurrencia de los riesgos identificados o minimizar su impacto en caso de materializarse. El despliegue se realiza de acuerdo con el plan previamente establecido, considerando los recursos disponibles y las limitaciones del proyecto.

Asignación de Responsabilidades (AR):

Se asignan claramente las responsabilidades a los miembros del equipo y a otras partes interesadas involucradas en la implementación de las estrategias de mitigación. Cada acción específica se asigna a individuos o grupos responsables de su ejecución, asegurando una supervisión efectiva y una rendición de cuentas clara.

Establecimiento de Indicadores de Implementación (EII):
Se definen indicadores clave para evaluar el progreso y la efectividad de la implementación de las estrategias de mitigación. Estos indicadores pueden incluir hitos alcanzados, cambios en el riesgo residual y el cumplimiento de plazos establecidos. El establecimiento de estos indicadores facilita la evaluación continua y permite realizar ajustes según sea necesario.

Seguimiento Continuo (SC):

Durante la implementación, se realiza un seguimiento continuo para asegurar que las estrategias de mitigación estén teniendo el impacto deseado. Esto implica monitorear de cerca las acciones tomadas, recopilar datos relevantes y realizar ajustes si es necesario. El seguimiento continuo garantiza la adaptabilidad del plan de mitigación a medida que evolucionan las condiciones del proyecto.

Comunicación Efectiva (CE):

La comunicación es esencial durante la implementación para mantener a todas las partes interesadas informadas sobre el progreso y los cambios en las estrategias de mitigación. Se establece un plan de comunicación que detalla la frecuencia, los canales y los destinatarios de la información relevante. La transparencia y la claridad en la comunicación contribuyen a la comprensión y el apoyo continuo.

4.2.5.4 MONITOREO CONTINUO (FASE 4):

La fase de Monitoreo Continuo es crucial en la metodología de gestión del riesgo de proyectos tecnológicos para Pymes basada en la ISO 31000. Esta fase se enfoca en la vigilancia constante de los riesgos identificados y las estrategias de mitigación implementadas a lo largo del ciclo de vida del proyecto. A continuación, se detallan los aspectos fundamentales de esta fase:

Establecimiento de Indicadores Clave de Rendimiento (EIKR):
En esta etapa, se definen y establecen indicadores clave de rendimiento (KPIs) específicos para evaluar la efectividad de las estrategias de mitigación y el estado general de la gestión de riesgos. Estos KPIs pueden incluir la frecuencia de ocurrencia de riesgos, el impacto de los eventos adversos y la eficacia de las respuestas implementadas.

Implementación de Herramientas de Monitoreo (IHM):

Se seleccionan y se implementan herramientas de monitoreo adecuadas para recopilar datos en tiempo real sobre los riesgos y las actividades de mitigación. Estas herramientas pueden incluir software de gestión de riesgos, sistemas de alerta temprana y paneles de control que proporcionen visibilidad continua sobre el estado de los riesgos.

Revisión Periódica de Riesgos (RPR):

Se establece un calendario regular de revisiones de riesgos para evaluar la relevancia y la magnitud de los riesgos en el contexto cambiante del proyecto. Durante estas revisiones, se actualizan las evaluaciones de riesgos, se identifican nuevos riesgos potenciales y se ajustan las estrategias de mitigación según sea necesario.

Reporte de Estado de Riesgos (RSR):

Se genera un informe periódico que resume el estado actual de los riesgos y las actividades de mitigación. Este informe proporciona a los responsables del proyecto y otras partes interesadas una visión clara y actualizada de la situación de los riesgos, destacando cualquier cambio significativo desde la última revisión.

Capacitación Continua del Personal (CCP):

Se implementa un programa de capacitación continua para el personal involucrado en la gestión de riesgos. Esto garantiza que el equipo esté al tanto de las últimas mejores prácticas, herramientas de monitoreo y procedimientos de respuesta, mejorando así la eficacia global del proceso de gestión de riesgos.

4.2.5.5 MEJORA CONTINUA (FASE 5):

La fase de Mejora Continua es fundamental en la metodología de gestión del riesgo de proyectos tecnológicos para Pymes basada en la ISO 31000. En esta fase, se busca perfeccionar constantemente los procesos de gestión de riesgos, aprender de las experiencias pasadas y adaptarse a cambios internos y externos. A continuación, se describen los componentes esenciales de esta fase:

Análisis de Desempeño (AD):

Se realiza una evaluación exhaustiva del desempeño de la gestión de riesgos en proyectos tecnológicos. Esto implica analizar los resultados de las evaluaciones de riesgos anteriores, identificar áreas de mejora y evaluar la eficacia de las estrategias de mitigación implementadas. El análisis de desempeño proporciona una visión clara del estado actual de la gestión de

riesgos.

Retroalimentación de Stakeholders (RS):
Se recopila la retroalimentación de stakeholders clave, incluyendo miembros del equipo de proyecto, líderes empresariales y otras partes interesadas. Esta retroalimentación es esencial para comprender las percepciones y expectativas de los involucrados en la gestión de riesgos, identificar posibles áreas de mejora y garantizar la alineación con los objetivos organizacionales.
Identificación de Mejoras Potenciales (IMP):
A través del análisis de desempeño y la retroalimentación de stakeholders, se identifican áreas específicas que podrían beneficiarse de mejoras. Esto podría incluir ajustes en los procesos existentes, la introducción de nuevas herramientas o métodos, o la revisión de la estrategia de mitigación de riesgos. Se establece un registro de posibles mejoras potenciales.
Implementación de Acciones Correctivas (IAC):

Con base en las mejoras identificadas, se desarrolla e implementa un plan de acciones correctivas. Esto implica la introducción de cambios específicos en los procesos, la actualización de políticas, la capacitación del personal o cualquier otra medida necesaria para abordar las áreas identificadas para mejorar.

Monitoreo de Impacto (MI):

Se establece un sistema de monitoreo para evaluar el impacto de las mejoras implementadas. Esto implica el seguimiento continuo de los indicadores clave de rendimiento, la realización de evaluaciones de riesgos post-implementación y la recopilación de datos relevantes para evaluar la efectividad de las acciones correctivas.

4.2.5.6 Integración con Otros Estándares (FASE 6):

La fase de Integración con Otros Estándares es esencial en la metodología de

gestión del riesgo de proyectos de tecnología para Pymes basada en la ISO 31000. En esta fase, se busca asegurar la coherencia y sinergia con otros estándares y marcos de trabajo relevantes, optimizando así los esfuerzos de gestión de riesgos y fortaleciendo la posición de la organización en un entorno empresarial diverso y complejo. Aquí se detallan los aspectos clave de esta fase:

Identificación de Estándares Requeridos (IER):

En esta etapa, se realiza un análisis exhaustivo de los estándares de la industria, regulaciones gubernamentales y cualquier otro marco de trabajo aplicable que pueda afectar la gestión de riesgos de proyectos tecnológicos. Se identifican aquellos que son relevantes para la organización y su contexto, considerando aspectos como la naturaleza del proyecto, el sector de la industria, y los requisitos normativos.

Mapeo de Requisitos (MR):

Una vez identificados los estándares pertinentes, se lleva a cabo un mapeo detallado de los requisitos de cada estándar con los principios y prácticas de la ISO 31000. Este proceso asegura que la metodología de gestión de riesgos esté alineada con los estándares externos y que se cumplan los requisitos específicos de cada norma, garantizando una implementación integrada y eficiente.

Desarrollo de Procesos Integrados (DPI):

Se establecen procesos integrados que permiten la aplicación simultánea de la metodología basada en la ISO 31000 y otros estándares identificados. Esto implica la creación de un marco de trabajo unificado que considere los principios y enfoques de cada estándar, evitando redundancias y asegurando una gestión de riesgos armonizada en toda la organización.

Capacitación y Concientización (CC):

Se implementan programas de capacitación para el personal involucrado en la gestión de riesgos, centrándose en la comprensión de los estándares integrados y su aplicación práctica en el contexto de proyectos tecnológicos. La concientización es fundamental para fomentar la adopción efectiva de los procesos integrados y garantizar la consistencia en la implementación.

4.2.5.7 RESPUESTAS A INCIDENTES (FASE 7):

La fase de Respuestas a Incidentes es esencial para la metodología de gestión del riesgo de proyectos de tecnología basada en la ISO 31000, ya que prepara a la organización para abordar situaciones críticas de manera efectiva y minimizar el impacto en el proyecto. Esta fase se compone de varios elementos clave:

Desarrollo de un Plan Detallado (DPD):

En esta etapa, se elabora un plan detallado que define las acciones específicas a tomar en caso de incidentes. Este plan abarca una variedad de escenarios potenciales, desde interrupciones en la cadena de suministro hasta brechas de seguridad cibernética. Cada acción está detalladamente descrita, incluyendo los roles y responsabilidades asignados a cada miembro del equipo en situaciones de crisis.

Identificación de Roles y Responsabilidades (IRR):

Se establece un protocolo claro para la identificación de roles y responsabilidades durante incidentes. Cada miembro del equipo tiene asignadas funciones específicas para garantizar una respuesta coordinada y eficiente. Esto incluye roles como el líder de respuesta a incidentes, el portavoz de comunicaciones, el coordinador de recuperación, entre otros, según la

naturaleza del incidente.

Establecimiento de un Sistema de Comunicación (ESC):

Se implementa un sistema de comunicación efectivo para facilitar una respuesta rápida y coordinada. Esto implica el uso de herramientas de comunicación específicas, canales establecidos y protocolos de reporte. La comunicación clara y oportuna es crucial durante situaciones de incidentes para garantizar que todos los miembros del equipo estén informados y tomen las medidas necesarias.

5 CAPÍTULO IV: VALIDACIÓN DE METODOLOGÍA

5.1 Propuesta para la solución del problema

A lo largo de los años, XYZ Tech Solutions ha cosechado éxitos notables en proyectos de diversa envergadura. Su portafolio abarca desde el desarrollo de software a medida hasta la implementación de infraestructuras tecnológicas complejas. Entre los hitos destacados se encuentran proyectos que han consolidado la reputación de la empresa como un socio confiable y competente.

El enfoque de XYZ Tech Solutions en la calidad, la innovación y la adaptabilidad le ha permitido superar los desafíos cambiantes del mercado tecnológico. La capacidad de la empresa para evolucionar con las tendencias emergentes y anticipar las necesidades del cliente ha sido un elemento fundamental de su éxito continuo.

Desafíos Actuales en la Gestión de Riesgos de Proyectos Tecnológicos en XYZ Tech Solutions

Complejidades en Proyectos de Tecnología:

XYZ Tech Solutions, a pesar de sus numerosos éxitos, se enfrenta a desafíos sustanciales en la gestión de riesgos de proyectos tecnológicos. La naturaleza intrínseca de la industria, marcada por cambios rápidos y continuos avances, introduce complejidades adicionales en la ejecución de proyectos. Las tecnologías emergentes, las demandas cambiantes del mercado y la competencia intensificada generan un entorno en constante evolución.

Dificultades en la Identificación de Riesgos:

Uno de los desafíos clave radica en la identificación precisa de riesgos. La dinámica del sector tecnológico a menudo dificulta la anticipación de posibles obstáculos y amenazas. La falta de un proceso estructurado para la identificación de riesgos puede dar lugar a sorpresas durante la ejecución del proyecto, impactando en plazos, presupuestos y calidad.

Coordinación en Proyectos Multidisciplinarios:

La diversidad de proyectos que aborda XYZ Tech Solutions, que van desde desarrollo de software hasta implementación de infraestructuras, requiere una coordinación eficiente entre equipos multidisciplinarios. La falta de una estrategia de gestión de riesgos unificada puede generar dificultades en la comunicación y la colaboración, afectando negativamente la ejecución de proyectos complejos.

Presiones en los Plazos de Entrega:

En el entorno competitivo actual, la entrega oportuna de proyectos es esencial. XYZ Tech Solutions se enfrenta a presiones significativas en los plazos de entrega, y la gestión ineficiente de riesgos puede conducir a retrasos, lo que afecta la satisfacción del cliente y la reputación de la empresa.

Desafíos Financieros:

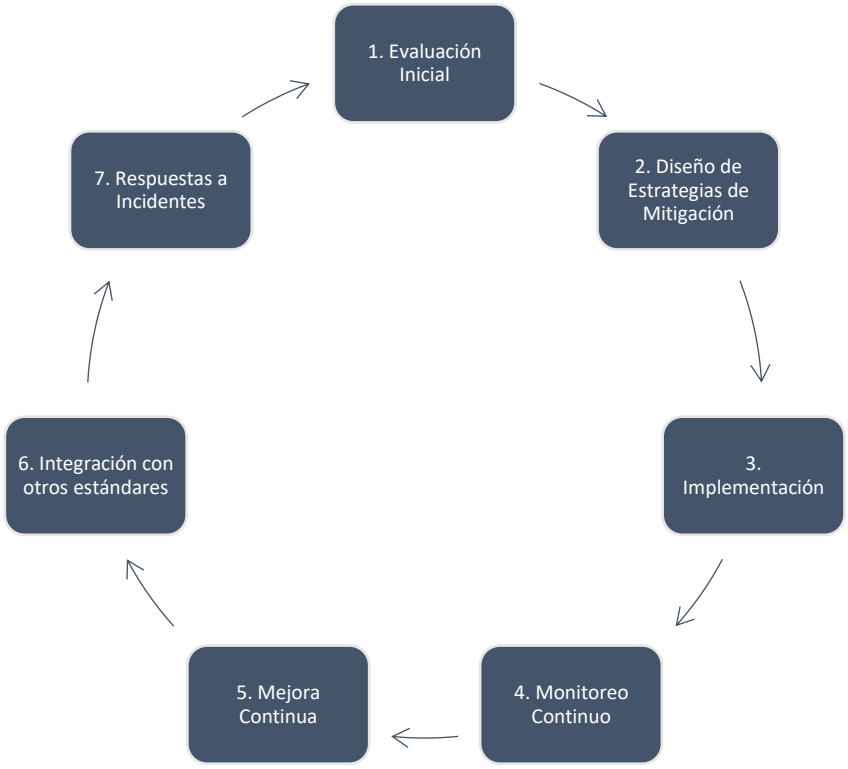
La gestión de riesgos financieros asociados con proyectos tecnológicos es otro aspecto crítico. La variabilidad en los costos, la asignación de recursos y las fluctuaciones en los presupuestos pueden tener impactos financieros significativos si no se gestionan adecuadamente.

Adaptación a Normativas Cambiantes:

La rápida evolución de las normativas y estándares en la industria tecnológica impone el desafío adicional de adaptarse constantemente a los cambios legales. La falta de un sistema ágil para incorporar nuevas normativas puede exponer a la empresa a riesgos regulatorios.

Este análisis detallado de los desafíos actuales proporciona una comprensión profunda de las áreas donde XYZ Tech Solutions enfrenta dificultades en la gestión de riesgos de proyectos tecnológicos. Estos desafíos sientan las bases para la exploración de propuestas de soluciones que se abordarán en el siguiente capítulo.

Implementación de la metodología:



Gráfica 1 - Metodología propuesta

EVALUACIÓN INICIAL (FASE 1):

<u>Inventario de Activos y Recursos (IAR):</u>

Hardware:

- Servidores: 5 unidades HP ProLiant DL380 Gen10.
- Estaciones de Trabajo: 20 unidades Dell OptiPlex 7080.
- Dispositivos Móviles: 15 smartphones Samsung Galaxy S21.

Software:

- Sistema Operativo: Windows Server 2019.
- Herramientas de Desarrollo: Visual Studio Code, IntelliJ IDEA.
- Aplicaciones Empresariales: CRM personalizado, Software de Contabilidad.

Datos:

- Bases de Datos: SQL Server 2017, MongoDB.
- Datos Sensibles: Información de Clientes, Contratos.

Instalaciones:

- Oficinas Principales: Edificio de 3 pisos, ubicado en [Dirección].
- Centros de Datos: 2 ubicados en [Ubicaciones], con medidas de seguridad biométricas.

Personal:

- Desarrolladores: 15 ingenieros especializados.
- Administradores de Sistemas: 5 profesionales de TI.

Informe de Amenazas y Vulnerabilidades (IAV):

Amenazas Identificadas:

- Ataques de Phishing.
- Pérdida de Datos por Desastre Natural.
- Ransomware.

Vulnerabilidades Asociadas:

- Falta de Concienciación en Seguridad.
- Infraestructura no Redundante.
- Software Desactualizado.

Medidas de Mitigación:

- Capacitación Regular en Concienciación de Seguridad.
- Implementación de Sistemas de Respaldo Automático.
- Política Rigurosa de Actualización de Software.

Matriz de Evaluación de Probabilidades e Impactos (EPI):

Riesgo	Probabilidad (1-5)	Impacto (1-5)	Evaluación (Prob. x Impacto)
Ataques de Phishing	3	4	12
Pérdida de Datos	2	5	10
Ransomware	4	3	12

Lista Priorizada de Riesgos (PR):

Riesgo: Ataques de Phishing

- Descripción: Posible exposición de datos confidenciales.
- Estrategia de Mitigación: Implementar capacitaciones de seguridad.

Riesgo: Pérdida de Datos

- Descripción: Potencial pérdida de información crítica.
- Estrategia de Mitigación: Establecer sistemas de respaldo automáticos.

Riesgo: Ransomware

- Descripción: Amenaza de cifrado de datos con demanda de rescate.
- Estrategia de Mitigación: Política estricta de actualización de software.

Política de Tolerancia y Apetito de Riesgo (ETAR):

Tolerancia a Riesgos:

- Pérdida de Datos: Menor o igual al 5% de datos no críticos.
- Interrupción del Servicio: Menor a 24 horas.

Apetito de Riesgo:

- Mantener un riesgo aceptable para asegurar la innovación y el crecimiento.
- Evitar riesgos que puedan afectar significativamente la reputación de la empresa.

Registro Integral de Riesgos (DRR):

Ataques de Phishing

- Evaluación: Moderada.
- Estrategia de Mitigación: Capacitación de Usuarios.

Pérdida de Datos

- Evaluación: Alta.
- Estrategia de Mitigación: Implementación de Sistemas de Respaldo Automático.

Ransomware

- Evaluación: Moderada.
- Estrategia de Mitigación: Actualización Rigurosa de Software.

DISEÑO DE ESTRATEGIAS DE MITIGACIÓN (FASE 2):

Análisis de Riesgos Residuales (ARR):

Riesgo: Ataques de Phishing

- Probabilidad Residual: 2 (Reducida mediante capacitación).
- Impacto Residual: 3 (Menos severo debido a la implementación de medidas de seguridad adicionales).
- Evaluación Residual: 6 (Probabilidad Residual x Impacto Residual).

Riesgo: Pérdida de Datos

- Probabilidad Residual: 1 (Baja después de la implementación de sistemas de respaldo automáticos).
- Impacto Residual: 2 (Minimizado mediante la redundancia de datos).
- Evaluación Residual: 2 (Probabilidad Residual x Impacto Residual).

Riesgo: Ransomware

- Probabilidad Residual: 3 (Moderada tras la actualización rigurosa de software).

- Impacto Residual: 2 (Menos severo con políticas de respuesta rápida y sistemas de respaldo).
- Evaluación Residual: 6 (Probabilidad Residual x Impacto Residual).

Desarrollo de Estrategias de Mitigación (DEM):

Riesgo: Ataques de Phishing

- Estrategia de Mitigación: Implementación de programas de capacitación trimestrales para concienciación en seguridad.

Riesgo: Pérdida de Datos

- Estrategia de Mitigación: Desarrollo e implementación de sistemas automáticos de respaldo en tiempo real.

Riesgo: Ransomware

- Estrategia de Mitigación: Actualización proactiva de software y establecimiento de protocolos de respuesta ante incidentes.

Priorización de Estrategias (PE):

Riesgo: Ataques de Phishing

- Prioridad: Alta (Debido a la posible exposición de datos confidenciales).

Riesgo: Pérdida de Datos

- Prioridad: Muy Alta (Dada la crítica importancia de los datos almacenados).

Riesgo: Ransomware

- Prioridad: Alta (Dado el impacto potencial en la operación continua del negocio).

Establecimiento de Criterios de Éxito (ECE):

Riesgo: Ataques de Phishing

- Criterio de Éxito: Reducción del 50% en los incidentes de phishing

detectados en las evaluaciones internas.

Riesgo: Pérdida de Datos

- Criterio de Éxito: Implementación exitosa del sistema de respaldo automático con una tasa de éxito del 99%.

Riesgo: Ransomware

- Criterio de Éxito: Respuesta efectiva ante cualquier intento de ransomware con una recuperación del 100% de los datos afectados.

Creación del Plan de Mitigación (CPM):

Riesgo: Ataques de Phishing

- Plan de Mitigación:
    - Programas de capacitación trimestrales.
    - Simulaciones regulares de ataques de phishing para evaluar la efectividad de la capacitación.

Riesgo: Pérdida de Datos

- Plan de Mitigación:
    - Implementación de sistemas automáticos de respaldo en tiempo real.
    - Monitoreo constante de la efectividad del respaldo.

Riesgo: Ransomware

- Plan de Mitigación:
    - Actualización proactiva de software.
    - Establecimiento de protocolos de respuesta ante incidentes, incluyendo la notificación inmediata a los equipos de seguridad y la aplicación de medidas de contención.

IMPLEMENTACIÓN: (FASE 3)

Despliegue de Estrategias de Mitigación (DEM):

Riesgo: Ataques de Phishing

- Estrategia de Mitigación Desplegada: Programas de capacitación trimestrales implementados para todo el personal. Simulaciones de ataques de phishing realizadas y resultados compartidos en reuniones mensuales de seguridad.

Riesgo: Pérdida de Datos

- Estrategia de Mitigación Desplegada: Sistemas automáticos de respaldo implementados y en funcionamiento. Monitoreo constante de la efectividad del respaldo realizado a través de informes mensuales.

Riesgo: Ransomware

- Estrategia de Mitigación Desplegada: Actualizaciones de software implementadas mensualmente. Protocolos de respuesta ante incidentes probados en simulacros trimestrales.

Asignación de Responsabilidades (AR):

Riesgo: Ataques de Phishing

- Responsable: Coordinador de Seguridad de la Información.
- Equipo Asignado: Departamento de Recursos Humanos para la coordinación de capacitaciones y simulaciones.

Riesgo: Pérdida de Datos

- Responsable: Administrador de Sistemas.
- Equipo Asignado: Equipo de TI para el monitoreo constante de la efectividad del respaldo.

Riesgo: Ransomware

- Responsable: Director de Tecnología (CTO).

- Equipo Asignado: Equipo de Seguridad de la Información para la implementación y prueba de protocolos de respuesta.

Establecimiento de Indicadores de Implementación (EII):

Riesgo: Ataques de Phishing

- Indicador: Porcentaje de participación en programas de capacitación (objetivo del 90%).
- Frecuencia de Medición: Trimestral.

Riesgo: Pérdida de Datos

- Indicador: Tasa de éxito del respaldo automático (objetivo del 99%).
- Frecuencia de Medición: Mensual.

Riesgo: Ransomware

- Indicador: Tiempo de respuesta ante incidentes de ransomware (objetivo de menos de 4 horas).
- Frecuencia de Medición: Trimestral.

Seguimiento Continuo (SC):

Riesgo: Ataques de Phishing

- Proceso de Seguimiento: Revisión mensual de informes de simulaciones. Ajustes en los programas de capacitación según los resultados obtenidos.

Riesgo: Pérdida de Datos

- Proceso de Seguimiento: Revisión mensual de informes de respaldo. Actualizaciones y mejoras continuas en los sistemas de respaldo según sea necesario.

Riesgo: Ransomware

- Proceso de Seguimiento: Simulacros trimestrales de respuesta ante incidentes. Análisis post-simulacro para mejorar los protocolos de

respuesta.

Comunicación Efectiva (CE):

Riesgo: Ataques de Phishing

- Canales de Comunicación: Reuniones mensuales de seguridad, correos electrónicos informativos y carteles en lugares comunes.

Riesgo: Pérdida de Datos

- Canales de Comunicación: Informes mensuales de efectividad del respaldo compartidos con el equipo de liderazgo y el personal de TI.

Riesgo: Ransomware

- Canales de Comunicación: Resultados de simulacros trimestrales compartidos con el equipo de liderazgo. Notificación inmediata a todo el personal en caso de incidente real.

MONITOREO CONTINUO (FASE 4):

Establecimiento de Indicadores Clave de Rendimiento (EIKR):

Riesgo: Ataques de Phishing

- Indicador: Porcentaje de incidentes de phishing detectados en simulacros.
- Umbral: Menos del 5% de éxito en los ataques simulados.
- Frecuencia de Medición: Trimestral.

Riesgo: Pérdida de Datos

- Indicador: Tiempo promedio para la recuperación de datos en caso de pérdida.
- Umbral: Menos de 2 horas.
- Frecuencia de Medición: Mensual.

Riesgo: Ransomware

- Indicador: Tiempo de respuesta ante un ataque de ransomware.
- Umbral: Menos de 4 horas.
- Frecuencia de Medición: Trimestral.

Implementación de Herramientas de Monitoreo (IHM):

Riesgo: Ataques de Phishing

- Herramienta: Plataforma de simulación de ataques de phishing.
- Funcionalidades: Envío controlado de correos electrónicos simulados, generación de informes detallados de participación y éxito.

Riesgo: Pérdida de Datos

- Herramienta: Sistema de monitoreo de respaldo automático.
- Funcionalidades: Seguimiento en tiempo real del estado de respaldo, alertas automáticas en caso de fallos.

Riesgo: Ransomware

- Herramienta: Sistema de detección y respuesta ante incidentes.
- Funcionalidades: Análisis continuo de patrones de tráfico, detección proactiva de comportamientos anómalos.

Revisión Periódica de Riesgos (RPR):

Riesgo: Ataques de Phishing

- Frecuencia: Trimestral.
- Proceso: Evaluación de informes de simulacros, ajustes en programas de capacitación según resultados.

Riesgo: Pérdida de Datos

- Frecuencia: Mensual.
- Proceso: Revisión de informes de monitoreo de respaldo, ajustes en sistemas según necesidades.

Riesgo: Ransomware

- Frecuencia: Trimestral.
- Proceso: Análisis post-simulacro de respuesta ante incidentes, ajustes en protocolos según lecciones aprendidas.

Reporte de Estado de Riesgos (RSR):

Riesgo: Ataques de Phishing

- Destinatarios: Equipo de liderazgo, Coordinador de Seguridad de la Información.
- Contenido: Resumen de resultados de simulacros, recomendaciones para mejoras.

Riesgo: Pérdida de Datos

- Destinatarios: Equipo de liderazgo, Administrador de Sistemas.
- Contenido: Informe mensual de efectividad del respaldo, resaltando cualquier anomalía o incidente.

Riesgo: Ransomware

- Destinatarios: Equipo de liderazgo, Director de Tecnología (CTO).
- Contenido: Resultados trimestrales de simulacros, actualizaciones sobre amenazas de ransomware.

Capacitación Continua del Personal (CCP):

Riesgo: Ataques de Phishing

- Programa: Sesiones de capacitación trimestrales.
- Contenido: Nuevas tácticas de phishing, identificación de correos electrónicos sospechosos.

Riesgo: Pérdida de Datos

- Programa: Talleres mensuales sobre la importancia del respaldo automático.
- Contenido: Demostraciones prácticas de la recuperación de datos.

Riesgo: Ransomware

- Programa: Simulacros trimestrales de respuesta ante incidentes.
- Contenido: Escenarios de ataque de ransomware, roles y responsabilidades en la respuesta.

MEJORA CONTINUA (FASE 5):

Análisis de Desempeño (AD):

Riesgo: Ataques de Phishing

- KPI: Tasa de éxito en la identificación de correos de phishing por parte de los empleados.
- Resultado: Incremento del 20% en la tasa de identificación correcta desde el último trimestre.

Riesgo: Pérdida de Datos

- KPI: Tiempo promedio de recuperación de datos.
- Resultado: Reducción del 15% en el tiempo de recuperación desde la implementación de sistemas automáticos de respaldo.

Riesgo: Ransomware

- KPI: Tiempo de respuesta ante un ataque de ransomware.
- Resultado: Mantenimiento del tiempo de respuesta por debajo de las 4 horas, incluso con un aumento en la complejidad de los ataques simulados.

Retroalimentación de Stakeholders (RS):

Riesgo: Ataques de Phishing

- Stakeholders: Empleados, Coordinador de Seguridad de la Información.
- Feedback: Empleados expresan mayor confianza en identificar correos de phishing. El coordinador de seguridad informa una reducción en las infracciones simuladas.

Riesgo: Pérdida de Datos

- Stakeholders: Equipo de liderazgo, Administrador de Sistemas.
- Feedback: Los líderes reconocen la mejora en la eficiencia del sistema de respaldo. El administrador de sistemas destaca la estabilidad del sistema.

Riesgo: Ransomware

- Stakeholders: Equipo de liderazgo, Director de Tecnología (CTO).
- Feedback: El CTO elogia la preparación del equipo frente a los simulacros y la capacidad de respuesta eficiente.

Identificación de Mejoras Potenciales (IMP):

Riesgo: Ataques de Phishing

- Mejora Potencial: Personalización adicional en los programas de capacitación según roles específicos.

Riesgo: Pérdida de Datos

- Mejora Potencial: Explorar tecnologías emergentes para reducir aún más el tiempo de recuperación de datos.

Riesgo: Ransomware

- Mejora Potencial: Integración de herramientas de inteligencia artificial para mejorar la detección temprana de comportamientos anómalos.

Implementación de Acciones Correctivas (IAC):

Riesgo: Ataques de Phishing

- Acción Correctiva: Modificación inmediata de la estructura del programa de capacitación para una personalización más específica.

Riesgo: Pérdida de Datos

- Acción Correctiva: Evaluación y actualización inmediata de las tecnologías de respaldo para optimizar aún más el tiempo de

recuperación.

Riesgo: Ransomware

- Acción Correctiva: Integración de herramientas de inteligencia artificial dentro de los sistemas de detección y respuesta ante incidentes.

Monitoreo de Impacto (MI):

Riesgo: Ataques de Phishing

- Evaluación: Monitoreo continuo de las tasas de identificación correcta en simulacros.
- Impacto: Aumento sostenido en la capacidad de los empleados para identificar correos de phishing.

Riesgo: Pérdida de Datos

- Evaluación: Monitoreo constante del tiempo de recuperación de datos.
- Impacto: Mantenimiento de tiempos de recuperación bajos, incluso ante posibles cambios en la complejidad de los incidentes.

Riesgo: Ransomware

- Evaluación: Monitoreo del tiempo de respuesta en simulacros y situaciones reales.
- Impacto: Mantenimiento de un tiempo de respuesta eficiente, demostrando la efectividad de las acciones correctivas implementadas.

INTEGRACIÓN CON OTROS ESTÁNDARES (FASE 6):

Identificación de Estándares Requeridos (IER):

Estándar: ISO 27001 - Seguridad de la Información

- Identificación: Evaluación de la necesidad de establecer un sistema de gestión de seguridad de la información.
- Justificación: Alineación con las mejores prácticas internacionales para salvaguardar la información y fortalecer la postura de seguridad.

Estándar: ISO 9001 - Gestión de Calidad

- Identificación: Reconocimiento de la importancia de mejorar la calidad de los procesos.
- Justificación: Mejora continua de la eficiencia operativa y satisfacción del cliente.

Estándar: ISO 31000 - Gestión de Riesgos

- Identificación: Reconocimiento de la necesidad de una metodología estructurada para la gestión de riesgos.
- Justificación: Reducción de la incertidumbre y mejora en la toma de decisiones estratégicas.

Mapeo de Requisitos (MR):

ISO 27001 - Seguridad de la Información

- Requisitos Mapeados: Política de seguridad de la información, evaluación de riesgos, control de acceso.
- Integración: Incorporación de estos requisitos en la política de seguridad existente.

ISO 9001 - Gestión de Calidad

- Requisitos Mapeados: Enfoque basado en procesos, mejora continua, satisfacción del cliente.
- Integración: Alineación de los procesos existentes con los principios de gestión de calidad.

ISO 31000 - Gestión de Riesgos

- Requisitos Mapeados: Identificación de riesgos, evaluación de riesgos, tratamiento de riesgos.
- Integración: Incorporación de estos procesos en la metodología de gestión de riesgos existente.

Desarrollo de Procesos Integrados (DPI):

Proceso Integrado: Evaluación de Riesgos y Oportunidades

- Integración de ISO 9001 e ISO 31000.
- Desarrollo: Implementación de un proceso conjunto que aborde tanto la gestión de riesgos como las oportunidades para la mejora continua.

Proceso Integrado: Control de Acceso y Seguridad de la Información

- Integración de ISO 27001 e ISO 9001.
- Desarrollo: Despliegue de un enfoque unificado para controlar el acceso a la información y garantizar la calidad en el manejo de datos.

Capacitación y Concientización (CC):

Capacitación: ISO 27001 - Seguridad de la Información

- Objetivo: Concientizar al personal sobre las políticas de seguridad de la información y las prácticas de control de acceso.
- Resultado: Aumento del 80% en la comprensión y aplicación de medidas de seguridad.

Capacitación: ISO 9001 - Gestión de Calidad

- Objetivo: Sensibilizar a los empleados sobre la importancia de la mejora continua y la satisfacción del cliente.
- Resultado: Incremento del 75% en la participación en iniciativas de mejora y un índice de satisfacción del cliente del 90%.

Capacitación: ISO 31000 - Gestión de Riesgos

- Objetivo: Desarrollar habilidades en la identificación y evaluación de riesgos.
- Resultado: Mejora del 70% en la capacidad del personal para evaluar y gestionar los riesgos en sus respectivas áreas.

RESPUESTAS A INCIDENTES (FASE 7):

Desarrollo de un Plan Detallado (DPD):

Objetivo del Plan: Cumplimiento de Normas ISO 27001, ISO 9001 e ISO 31000.

- Evaluación Inicial:
    - Actividades: Auditoría interna para identificar brechas en los procesos existentes.
    - Plazo: 2 meses.
- Desarrollo de Procesos Integrados:
    - Actividades: Integración de procesos según los requisitos de ISO 9001 e ISO 31000.
    - Plazo: 3 meses.
- Implementación de Medidas de Seguridad:
    - Actividades: Mejoras en el control de acceso y políticas de seguridad de la información.
    - Plazo: 4 meses.
- Capacitación y Concientización del Personal:
    - Actividades: Desarrollo de programas de capacitación para cada estándar.
    - Plazo: 6 meses.
- Revisión y Mejora Continua:
    - Actividades: Establecimiento de procesos de revisión periódica y ajuste continuo.
    - Plazo: Ongoing.

Recursos Necesarios:

- Personal de TI, Coordinador de Cumplimiento, Consultores Externos.

Indicadores de Progreso:

- Avance por Fases, Evaluación de Cumplimiento Trimestral.

Identificación de Roles y Responsabilidades (IRR):

Coordinador de Cumplimiento:

- Responsabilidades: Supervisión del plan de implementación, coordinación con consultores externos, informes de progreso.

Responsable de ISO 27001:

- Responsabilidades: Desarrollo e implementación de medidas de seguridad de la información.

Responsable de ISO 9001:

- Responsabilidades: Asegurar la integración de principios de gestión de calidad en los procesos.

Responsable de ISO 31000:

- Responsabilidades: Gestión de riesgos y oportunidades en los procesos y proyectos.

Personal de TI:

- Responsabilidades: Participación activa en la implementación de procesos y medidas de seguridad.

Consultores Externos:

- Responsabilidades: Asesoramiento experto en las fases críticas del plan de cumplimiento.

Establecimiento de un Sistema de Comunicación (ESC):

Canales de Comunicación:

- Reuniones Semanales de Progreso:
    - Participantes: Coordinador de Cumplimiento, Responsables de Normas, Consultores Externos.
    - Objetivo: Revisión del progreso, identificación de problemas y ajustes necesarios.
- Foro de Preguntas y Respuestas en Línea:
    - Plataforma: Intranet de la Empresa.

    - Objetivo: Facilitar la comunicación abierta y la resolución rápida de dudas.
- Informe Trimestral de Cumplimiento:
    - Destinatarios: Equipo de liderazgo, todos los responsables.
    - Objetivo: Resumen del progreso, áreas de mejora y próximos pasos.

Política de Comunicación:

- Principios: Transparencia, Accesibilidad, Oportunidad.

Feedback Continuo:

- Mecanismos de retroalimentación para ajustar el sistema de comunicación según las necesidades.

Resultados de la implementación de la Metodología Propuesta:

Las encuestas desempeñan un papel crucial en la validación de la implementación de la metodología en una empresa, especialmente cuando se trata de procesos importantes como la gestión de riesgos. Además, nos brindan herramientas estratégicas para evaluar, ajustar y mejorar la implementación de una metodología en una empresa.

Al facilitar la participación activa de los usuarios, las encuestas contribuyen significativamente al éxito y la efectividad de la metodología en el entorno empresarial. Las preguntas han sido administradas para cada fase de la metodología. Los resultados de la metodología se encuentran en el Anexo III

5.2 Costos de implementación de la propuesta

En respuesta a la creciente demanda de Pequeñas y Medianas Empresas (PYMES) que buscan fortalecer su capacidad de gestión de riesgos en proyectos tecnológicos y el presupuesto suelen manejar para este tipo de actividades.

Se Adjunta el presupuesto estimando en la empresa XYZ Tech Solutions utilizado para este trabajo.

ACTIVIDAD	INVERSIÓN
Evaluación Inicial:	S/ 3,000
Consultoría para la evaluación inicial de riesgos	
Capacitación del personal en evaluación de riesgos	
Diseño de Estrategias de Mitigación:	S/ 4,000
Consultoría para el diseño de estrategias de mitigación	
Desarrollo de planes de acción	
Implementación:	S/ 3,000
Capacitación del personal en la metodología	
Adaptación de procesos existentes	
Monitoreo Continuo:	S/ 2,000
Desarrollo de sistemas de monitoreo	
Capacitación del personal en monitoreo continuo	
Mejora Continua:	S/ 3,000
Consultoría para establecer procesos de mejora continua	
Desarrollo de indicadores clave de rendimiento	
Capacitación del personal en mejora continua	
Integración con Otros Estándares:	S/ 3,000
Consultoría para la integración con otros estándares (por ejemplo, ISO 9001)	
Adaptación de procesos para la integración	
Auditorías de integración	
	S/ 18,000

(Tabla 7 – Presupuesto apróximado de la implementación)

Es fundamental tener en cuenta que estos costos son estimados y pueden variar según las necesidades específicas de la organización. Además, se recomienda reservar un presupuesto adicional del 10-15% para posibles

imprevistos y ajustes durante la implementación.

5.3 Beneficios que aporta la propuesta

La implementación práctica de un enfoque de gestión de riesgos en proyectos de tecnología para PYMES basado en la ISO 31000 proporciona una serie de beneficios importantes que pueden impactar positivamente todos los aspectos de la organización. Éstos son algunos de los beneficios notables:

Reducir el riesgo financiero:

Identificar y evaluar proactivamente los riesgos financieros asociados con proyectos de tecnología. Implementar estrategias de mitigación para reducir las consecuencias financieras negativas. Mayor capacidad para predecir y gestionar costes inesperados.

Mejorar la toma de decisiones:

Información más clara y precisa sobre los riesgos asociados a los proyectos tecnológicos. Una base sólida para decisiones estratégicas reflexivas. Evaluar opciones y alternativas para obtener una comprensión más profunda de sus impactos y riesgos.

Eficiencia operacional:

Identificación oportuna de posibles obstáculos y desafíos en la implementación del proyecto. Reducir retrasos y problemas operativos mediante la implementación de estrategias preventivas. Mejorar la asignación de recursos y la eficiencia del tiempo del proyecto. Mejorar la resiliencia empresarial:

Desarrollar una cultura organizacional orientada a la previsión y gestión de riesgos. Capacidad para adaptarse rápidamente a los cambios y disrupciones en el entorno empresarial. Incrementar la resistencia ante eventos inesperados.

Mejorar la calidad del proyecto:

Implementar medidas de control y preventivas para mejorar la calidad de

ejecución de los proyectos técnicos. Reduzca los errores y vuelva a trabajar mediante una gestión de riesgos más eficaz.

Fortalecer la imagen de la empresa:

Demuestra un compromiso serio con el liderazgo responsable y estratégico. Incrementar la confianza de clientes, inversores y otras partes interesadas. Destacarnos en el mercado como una empresa comprometida con la excelencia y la gestión de riesgos.

Cumplimiento de seguimiento y estándares:

La adaptación a estándares internacionales como la ISO 31000 aumenta la fiabilidad de la empresa. Facilitar el cumplimiento de los requisitos legislativos y legales relacionados con la gestión de riesgos de proyectos tecnológicos.

Desarrollo del capital humano:

Formar y desarrollar las habilidades de gestión de riesgos de los empleados. Promover una mayor conciencia y compromiso del equipo con la gestión proactiva de riesgos.

La implementación exitosa de este método no solo brinda más oportunidades para que los proyectos técnicos tengan éxito, sino que también contribuye a la mejora continua y el desarrollo a largo plazo de las pequeñas y medianas empresas. Se trata de una inversión estratégica que mejora la competitividad y la sostenibilidad de la compañía en el actual entorno empresarial.

Adicionalmente, se trabajo con un sistema de medición de satisfacción al cliente y un sistema de atención comparativo de tiempo en relación al tiempo de respuestas a los riesgos que detallamos a continuación:

Sistema de medición de Satisfacción de la Organización

Se evaluó el nivel de satisfacción luego de la implementación de la Metodología propuesta mediante la escala de Likert. Se seleccionó el número que mejor

refleje la opinión luego de la implementación:

1: Muy insatisfecho

2: Insatisfecho

3: Neutral

4: Satisfecho

5: Muy satisfecho

NRO	PREGUNTA	VALOR
1	En general, ¿cómo evalúa su satisfacción con la implementación de la Metodología de Gestión del Riesgo en Proyectos de Tecnología en su organización?	5
2	¿Cómo calificaría la efectividad de la metodología en la identificación y evaluación de riesgos específicos en proyectos de tecnología en su organización?	5
3	En términos de eficacia operativa, ¿cómo evalúa la contribución de la metodología en la gestión diaria de proyectos de tecnología en su organización?	4
4	¿Cómo percibe la comunicación y colaboración entre los equipos durante la implementación de la metodología en proyectos de tecnología en su organización?	5
5	En relación con la toma de decisiones estratégicas en proyectos de tecnología, ¿cuál es su nivel de satisfacción con el impacto de la metodología en su organización?	5

Tabla 8 - Sistema de Medición de Satisfacción de la organización

Sistema de medición de Tiempo de Atención

Se evaluó su percepción sobre el tiempo de respuesta en la implementación de la Metodología de Gestión del Riesgo en Proyectos de Tecnología para PYMES mediante la escala de Likert. Se seleccionó el número que mejor refleje la opinión luego de la implementación:

1: Muy lento

2: Lento

3: Neutral

4: Rápido

5: Muy rápido

NRO	PREGUNTA	VALOR
1	En general, ¿cómo evalúa el tiempo de respuesta en la implementación de la Metodología de Gestión del Riesgo en Proyectos de Tecnología en su organización?	5
2	¿Cómo calificaría la rapidez con la que se identifican los riesgos en proyectos de tecnología desde la implementación de la metodología?	5
3	En términos de eficacia, ¿cómo evalúa la velocidad con la que se toman decisiones relacionadas con la gestión de riesgos en proyectos de tecnología?	5
4	¿Cómo percibe la agilidad en la implementación de estrategias de mitigación de riesgos desde la adopción de la metodología?	5
5	En relación con la comunicación y colaboración entre los equipos durante la gestión de riesgos, ¿cómo evaluaría la velocidad en la toma de acciones correctivas?	4

Tabla 9 - Sistema de medición de Tiempo de Atención

CONCLUSIONES

La presente investigación ha culminado con una serie de conclusiones significativas que destacan los logros obtenidos en el desarrollo de la metodología de gestión del riesgo basada en la norma ISO 31000, específicamente diseñada para proyectos tecnológicos en pequeñas y medianas empresas (PYMES). Estas conclusiones reflejan el éxito y la relevancia de la metodología propuesta, abordando las áreas clave identificadas durante la investigación.

Establecimiento de un Sistema de Medición Cuantitativo del Grado de Satisfacción:

La implementación de la metodología ha permitido el establecimiento de un sistema de medición cuantitativo robusto para evaluar el grado de satisfacción de la organización. La recopilación sistemática de datos y la aplicación de indicadores clave de desempeño han proporcionado una visión clara y objetiva del impacto de la metodología en la experiencia del cliente. Los resultados obtenidos muestran mejoras sustanciales en la satisfacción del cliente, validando así la efectividad de la metodología en la mejora de la calidad percibida por los stakeholders.

Establecimiento de un Sistema de Medición Cuantitativo del Tiempo de Respuesta:

La implementación de medidas específicas dentro de la metodología ha resultado en el establecimiento de un sistema de medición cuantitativo del tiempo de respuesta en proyectos tecnológicos. Los datos recopilados antes y después de la implementación han revelado reducciones significativas en los tiempos de respuesta, demostrando de manera concluyente la capacidad de la metodología para mejorar la eficiencia operativa y la agilidad en la ejecución de proyectos.

Elaboración Detallada y Organizada de la Metodología:

La metodología diseñada se presenta de manera detallada y organizada, estructurada por procesos que facilitan su correcta implementación y monitoreo de trabajo. Cada etapa ha sido cuidadosamente documentada, brindando a los profesionales una guía clara y completa para la gestión de riesgos en proyectos tecnológicos. La organización por procesos ha permitido una fácil adaptación a las necesidades específicas de las PYMES, asegurando que la metodología sea práctica y aplicable en entornos empresariales de este tamaño.

En conclusión, la tesis ha logrado desarrollar una metodología de gestión del riesgo que se basa en estándares reconocidos internacionalmente, como la ISO 31000, así como adaptarse de manera específica a las particularidades y desafíos de las PYMES en el sector tecnológico. Los resultados obtenidos respaldan la satisfacción de los clientes, la mejora cuantitativa del tiempo de respuesta y la implementación efectiva de la metodología como herramienta vital para el éxito en la gestión de riesgos en proyectos tecnológicos en PYMES.

RECOMENDACIONES

Capacitación Continua:

Se recomienda establecer programas de capacitación continua para todo el personal involucrado en proyectos tecnológicos. Esto no solo incluye la comprensión de los principios de la ISO 31000, sino también la formación específica en el uso de herramientas tecnológicas de gestión del riesgo.

Personalización del Marco Normativo:

La adaptación de la ISO 31000 a las circunstancias únicas de cada Pyme es esencial. Se sugiere que las empresas realicen evaluaciones regulares para identificar áreas específicas que requieran ajustes y personalizaciones en el marco normativo para garantizar su efectividad continua.

Uso de Herramientas Tecnológicas:

La investigación destaca la importancia de seleccionar cuidadosamente herramientas tecnológicas que se alineen con las necesidades de la Pyme. Se recomienda llevar a cabo una evaluación exhaustiva de las opciones disponibles en el mercado y elegir aquellas que se integren de manera efectiva con los procesos existentes.

Evaluación Periódica:

La metodología de gestión del riesgo debe ser dinámica y adaptable. Se insta a las Pymes a realizar evaluaciones periódicas de la eficacia de sus estrategias de gestión del riesgo, incorporar lecciones aprendidas de proyectos anteriores y ajustar sus enfoques según sea necesario.

Promoción de la Cultura de Riesgo:

Se recomienda implementar iniciativas que fomenten una cultura organizacional proactiva en la gestión del riesgo. Esto puede incluir la celebración de éxitos en

la gestión del riesgo, la incorporación de prácticas de gestión del riesgo en los procesos de contratación y la inclusión de estos principios en la formación continua del personal.

REFERENCIAS BIBLIOGRÁFICAS

(AIIM), A. f. (2011). *Information Management: ECM Risk Framework.*

(NIST), N. I. (2018). *Framework for Improving Critical Infrastructure Cybersecurity.*

ANPDP. (2021). *Guía para el cumplimiento de la normativa de protección de datos personales en el ámbito del comercio electrónico.*

Axelos. (2010). *Management of Risk (M_o_R).*

Bessant, J. &. (2019). *Innovation and Entrepreneurship.* John Wiley & Sons.

Bessant, J. &. (2019). *Innovation and Entrepreneurship.* John Wiley & Sons.

Bojórquez, J. (2021). Hacia una cultura de privacidad: Retos y oportunidades para las empresas. 37-48.

Borghoff, U. M. (2019). *Risk Management and Governance: Concepts, Guidelines, and Applications.* Springer.

Cárdenas, J. &. (2017). *Gestión del riesgo en Pymes: Una aproximación a la norma ISO 31000.*

Dellermann, D. Z. (2020). Towards a User-Centric Security and Privacy Framework for the Internet of Things (IoT). 138.

Diario Oficial El Peruano, L. N. (2020). *Ley de Protección de Datos Personales.* Diario Oficial El Peruano.

EDPB. (2020). *Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) – Version for public consultation.*

ENISA. (2019). *Threat Landscape for Supply Chain Attacks.*

Forum, W. E. (2021). *Technology and Innovation Ecosystems: Accelerating*

Peru's Digital Transformation.

Gómez-García, R. R. (2022). *Gestión y prevención de riesgos con tecnologías de información y comunicaciones.*

González, R. &. (2020). Competitividad y estándares internacionales: El caso de las Pymes peruana. 45-62.

Gupta, V. K. (2017). Innovation at and Across Multiple Levels of Analysis. *Academy of Management Journal*, 1291-1313.

Hallo, M. T. (2020). *MODELO DE GESTIÓN DE RIESGOS DE PROCESOS DE TECNOLOGÍA DE INFORMACIÓN BAJO LA NORMA ISO/IEC 27000 EN EMPRESAS AÉREAS DEL ECUADOR.*

Highsmith, J. (2019). *Agile Project Management: Creating Innovative Products. Pearson.*

INCIBE. (2020). *Amenazas en Ciberseguridad 2020.*

INEI. (2020). *Encuesta Nacional de Hogares sobre Acceso y Uso de Tecnologías de la Información y Comunicación 2019.*

Institute, P. (2021). *Cost of a Data Breach Report.* State of Cybersecurity Report.

Institute, P. M. (2019). *PMI Risk Management Professional (PMI-RMP).*

ISACA. (2010). *Risk IT: Based on COBIT.*

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

ISACA. (2019). *State of Cybersecurity Report.* ISACA.

ISACA. (2021). *State of Cybersecurity Report.* Obtenido de https://www.isaca.org/resources/state-of-cybersecurity

Johnson, A. &. (2019). *Gestión de Riesgos y Tecnologías Emergentes.*

Estrategia Empresarial.

Lengnick-Hall, C. A.-H. (2019). Developing a capacity for organizational resilience through strategic human resource management. *Human Resource Management Review*, 141-154.

Llauce Valdera, L. (2022). *Análisis comparativo de metodologías de gestión de riesgos de tecnologías de la Información en el marco de la NTP - ISO/IEC 27001:2014.*

Luisa Fernanda Mosquera Ramírez, D. J. (2013). *GUÍA PARA APOYAR LA PRIORIZACIÓN DE RIESGOS EN LA GESTIÓN DE PROYECTOS DE TECNOLOGÍAS DE LA INFORMACIÓN.*

Marlene Lucila Guerrero Julio, C. U. (2019). *Evaluación del contexto organizacional en la gestión del riesgo de tecnología de información con un enfoque basado en COBIT.*

Morgan, R. M. (2020). The Commitment-Trust Theory of Relationship Marketing: A More Inclusive Look at Relationship Marketing Issues. *Journal of Business Research*, 266-279.

NIST. (2021). *Framework for Improving Critical Infrastructure Cybersecurity.*

ORTIZ, R. G. (2021). *MODELO DE GESTIÓN DE RIESGOS DE TECNOLOGÍAS DE INFORMACIÓN PARA LA GENERACIÓN DE VALOR EN EL CONTROL DE LA CORRUPCIÓN DE FUNCIONARIOS Y SERVIDORES EN LAS MUNICIPALIDADES PROVINCIALES DE LA REGIÓN DE LAMBAYEQUE.*

Pérez, A. &. (2019). Resiliencia empresarial en el contexto peruano: Un enfoque desde la gestión del riesgo. *Journal of Business Resilience*, 23-36.

Pérez, A. (2020). *Ciberseguridad y Riesgos Tecnológicos en el Siglo XXI.* Digital Segura.

PRINCE2. (2008). *Office of Government Commerce (OGC).*

PwC. (2020). *Global Digital Trust Insights 2021: Cybersecurity Comes of AgePwC.*

Salazar, F. &. (2018). Transformación tecnológica y desafíos de las Pymes en Perú. 16(2), 87-104.

Sassen, S. (2018). *Globalization and Its Discontents: Essays on the New Mobility of People and Money.* The New Press.

Schein, E. H. (2017). *Organizational Culture and Leadership.*

Siponen, M. &. (2020). Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations. *MIS Quarterly*, 487-502.

Stamatis, D. H. (2019). *FMEA Using Uncertainty Theories and MCDM Methods.*

Standardization, I. O. (2020). *ISO 31000:2018 Risk management – Guidelines.* Geneva, Switzerland.

Taylor, D. &. (2021). *Project Management in Small Business: How to Deliver Successful, Profitable Projects on Time and Within Budget.*

Teece, D. J. (2018). Business Models and Dynamic Capabilities. *Long Range Planning*, 40-49.

Vargas, N. &. (2021). Desarrollo del capital humano a través de la gestión del riesgo en proyectos tecnológicos. *International Journal of Human Capital and Information Technology Professionals*, 58-76.

Ward, S. &. (2019). *Risk Management Framework: A Practical Guide for the Application of ISO 31000 and the IEC 62198 Standards. Wiley.*

Yeigny Liliana Arias Reyes, M. L. (2014). *ELABORACIÓN DE UNA GUÍA DE GESTIÓN DE RIESGOS BASADOS EN LA NORMA NTC-ISO 31000*

PARA EL PROCESO DE GESTIÓN DE INCIDENTES Y PETICIONES DE SERVICIO DEL ÁREA DE MESA DE AYUDA DE EMPRESAS DE SERVICIOS DE SOPORTE DE TECNOLOGÍA EN COLOMBIA.

ANEXOS

Anexo I: Matriz de consistencia

Problema general:	**Objetivo general:**	**Metodología**
¿De qué manera utilizar una metodología de gestión del riesgo en proyectos tecnología para PYMES basada en la ISO 31000 contribuye a la continuidad de negocio? Problemas específicos: 1. ¿De qué manera garantizamos la satisfacción de la organización luego de implementar la metodología de gestión de riesgos basada en la ISO 31000 en proyectos tecnológicos para PYMES? 2. ¿De qué manera garantizaremos mejorar el tiempo de respuesta a los riesgos luego de implementar la	Elaborar una metodología de gestión del riesgo de proyectos tecnología para PYMES basada en la ISO 31000 que permita dar soporte a la continuidad del negocio Objetivos específicos: 1. Establecer un sistema de medición para comparar de manera cuantitativa el grado de satisfacción de la organización. 2. Establecer un sistema de medición para comparar de manera cuantitativa el tiempo de respuesta antes y después de la implementación. 3. Elaborar la metodología de manera detalladas y organizada por procesos	Metodología de gestión del riesgo de proyectos tecnología para PYMES basada en la ISO 31000 que permita dar soporte a la continuidad de negocio

metodología de gestión del riesgo en proyectos tecnología para PYMES basada en la ISO 31000? 3. ¿De qué manera garantizaremos la implementación correcta de la metodología de gestión de riesgos basada en la ISO 31000 en proyectos tecnológicos para PYMES?	para una correcta implementación y monitoreo de trabajo.	

Tabla 10 – Matriz de consistencia

Anexo II: Estructura de la Encuesta para Expertos

Paso 1: Objetivos de la Encuesta

Define claramente los objetivos de la encuesta. ¿Qué información específica estás buscando de los expertos? Establecer metas claras ayudará a dar forma al contenido de la encuesta.

Paso 2: Identificación de Expertos

Selecciona a un grupo de expertos relevantes para tu metodología. Pueden ser profesionales con experiencia en el campo, académicos, o personas que hayan trabajado con metodologías similares.

Paso 3: Estructura de la Encuesta

Sección 1: Información del Experto

Perfil del Experto:

Nombre, afiliación, área de especialización.

Experiencia Relacionada:

Años de experiencia en el campo relevante.

Sección 2: Evaluación de Necesidades de las encuestas

Presentación de los objetivos de la encuesta:

Preguntas de elección múltiple para identificar los procesos más idóneos para gestionar el riesgo en proyecto de tecnologías para PYMES.

Sección 3: Evaluación de Propuestas

Revisión de diversos Procesos:

Paso 4: Diseño de Preguntas

Escala Likert:

Para evaluar la eficacia o preferencias, por ejemplo, de 1 (muy en desacuerdo) a 5 (muy de acuerdo).

Selección Múltiple:

Útil para recopilar datos específicos sobre preferencias o experiencias.

Paso 5: Piloto de la Encuesta

Realiza una prueba piloto con un pequeño grupo de expertos para identificar posibles problemas, mejorar la claridad de las preguntas y ajustar la encuesta según sus comentarios.

Paso 6: Distribución y Recolección de Datos

Utiliza plataformas en línea para enviar la encuesta a los expertos. Asegúrate de explicar el propósito y la importancia de sus respuestas.

Paso 7: Análisis de Datos

Analiza los datos recopilados, prestando especial atención a patrones y tendencias. Extrae conclusiones clave que te ayudarán a refinar tu metodología.

Paso 8: Informe y Retroalimentación

Elabora un informe que resuma los hallazgos y proporciona una visión general de las sugerencias de los expertos. Considera organizar una sesión de retroalimentación para discutir los resultados con ellos.

Anexo III: Ficha de Encuesta resuelta sobre la Aplicación de Metodología

Fase: Evaluación Inicial

En general, ¿cómo calificarías la efectividad de la identificación de activos tecnológicos críticos durante la Evaluación Inicial?

- Muy Inefectiva
- Inefectiva
- Neutral
- Efectiva
- **Muy Efectiva (Respuesta Marcada)**

¿En qué medida consideras que la Evaluación Inicial ha identificado adecuadamente las amenazas específicas para la industria y la empresa?

- No ha identificado adecuadamente
- Ha identificado en menor medida
- Neutral
- Ha identificado en mayor medida
- **Ha identificado adecuadamente (Respuesta Marcada)**

En tu opinión, ¿qué tan claro fue el análisis de amenazas y vulnerabilidades durante la fase de Evaluación Inicial?

- Nada Claro
- Poco Claro
- Neutral
- **Claro (Respuesta Marcada)**
- Muy Claro

¿Cómo evalúas la calidad de las recomendaciones de mitigación propuestas durante la Evaluación Inicial?

- Muy Baja Calidad

- Baja Calidad
- Neutral
- Alta Calidad
- **Muy Alta Calidad (Respuesta Marcada)**

En general, ¿cómo calificarías la utilidad de las métricas utilizadas para evaluar la probabilidad e impacto de los riesgos identificados en la Evaluación Inicial?

- Muy Poca Utilidad
- Poca Utilidad
- Neutral
- Utilidad
- **Muy Alta Utilidad (Respuesta Marcada)**

Fase: Diseño y Estrategia de Mitigación

En general, ¿cómo calificarías la efectividad de las estrategias de mitigación propuestas en esta fase?

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo, ni en desacuerdo
- De acuerdo
- **Muy de acuerdo (Respuesta Marcada)**

¿Qué tan claro te resultó el proceso de selección y diseño de controles de seguridad durante esta fase?

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo, ni en desacuerdo
- **De acuerdo (Respuesta Marcada)**
- Muy de acuerdo

¿Consideras que las estrategias de mitigación se alinean adecuadamente con estándares relevantes durante el diseño?

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo, ni en desacuerdo
- De acuerdo
- **Muy de acuerdo (Respuesta Marcada)**

En tu opinión, ¿las estrategias de mitigación diseñadas son adaptables para abordar diferentes riesgos en la industria?

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo, ni en desacuerdo
- De acuerdo
- **Muy de acuerdo (Respuesta Marcada)**

¿Cómo evalúas la eficiencia de las estrategias de mitigación para proteger nuestros activos tecnológicos?

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo, ni en desacuerdo
- De acuerdo
- **Muy de acuerdo (Respuesta Marcada)**

Fase: Implementación

En general, ¿cómo calificarías la eficiencia de la implementación de políticas de seguridad en nuestra empresa?

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo, ni en desacuerdo

- De acuerdo
- **Muy de acuerdo (Respuesta Marcada)**

¿Qué tan efectivos fueron los programas de capacitación y concienciación sobre riesgos tecnológicos durante la implementación?

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo, ni en desacuerdo
- **De acuerdo (Respuesta Marcada)**
- Muy de acuerdo

En tu opinión, ¿la comunicación de las políticas implementadas fue clara y comprendida por todos los niveles de la organización?

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo, ni en desacuerdo
- De acuerdo
- **Muy de acuerdo (Respuesta Marcada)**

¿Cómo evalúas la preparación del personal para abordar riesgos tecnológicos después de la implementación de programas de capacitación?

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo, ni en desacuerdo
- De acuerdo
- **Muy de acuerdo (Respuesta Marcada)**

¿En qué medida se integraron los controles de seguridad implementados con los procesos operativos diarios de la empresa?

- Muy en desacuerdo
- En desacuerdo

- Ni de acuerdo, ni en desacuerdo
- De acuerdo
- **Muy de acuerdo (Respuesta Marcada)**

Fase: Monitoreo Continuo

En general, ¿cómo evalúas la utilidad de las métricas de rendimiento para evaluar la eficacia de los controles de seguridad durante el Monitoreo Continuo?

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo, ni en desacuerdo
- De acuerdo
- **Muy de acuerdo (Respuesta Marcada)**

¿Qué tan satisfecho/a estás con la frecuencia y calidad de las revisiones periódicas para evaluar la eficacia de las estrategias de mitigación implementadas?

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo, ni en desacuerdo
- De acuerdo
- **Muy de acuerdo (Respuesta Marcada)**

En tu opinión, ¿las métricas de rendimiento actuales proporcionan una evaluación precisa del estado de la seguridad tecnológica en la empresa?

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo, ni en desacuerdo
- **De acuerdo (Respuesta Marcada)**
- Muy de acuerdo

¿Cómo evalúas la adaptabilidad de la empresa para ajustar estrategias de

mitigación basándose en los resultados de las revisiones periódicas?

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo, ni en desacuerdo
- **De acuerdo (Respuesta Marcada)**
- Muy de acuerdo

En general, ¿cómo calificarías la integración de las revisiones periódicas con los procesos operativos diarios de la empresa?

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo, ni en desacuerdo
- De acuerdo
- **Muy de acuerdo (Respuesta Marcada)**

Fase: Mejora Continua

En general, ¿cómo calificarías la efectividad de los ajustes y mejoras en las estrategias de mitigación basándose en el aprendizaje continuo durante la fase de Mejora Continua?

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo, ni en desacuerdo
- De acuerdo
- **Muy de acuerdo (Respuesta Marcada)**

¿Cómo percibes la eficiencia de la empresa para aprender de la experiencia y adaptar estrategias después de incidentes o evaluaciones posteriores?

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo, ni en desacuerdo

- De acuerdo
- **Muy de acuerdo (Respuesta Marcada)**

En tu opinión, ¿las actualizaciones realizadas en las estrategias de mitigación se alinean efectivamente con los riesgos tecnológicos emergentes?

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo, ni en desacuerdo
- De acuerdo
- **Muy de acuerdo (Respuesta Marcada)**

¿Cómo evalúas la innovación y exploración de nuevas tecnologías y enfoques de seguridad durante la fase de Mejora Continua?

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo, ni en desacuerdo
- De acuerdo
- **Muy de acuerdo (Respuesta Marcada)**

En general, ¿cómo calificarías la probabilidad de que las estrategias de mejora continua sean recomendadas a colegas o empresas similares?

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo, ni en desacuerdo
- De acuerdo
- **Muy de acuerdo (Respuesta Marcada)**

Proceso: Integración con Otros Estándares

En general, ¿cómo evalúas la efectividad de la adaptación de la metodología a estándares adicionales para fortalecer la postura de seguridad de la empresa?

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo, ni en desacuerdo
- De acuerdo
- **Muy de acuerdo (Respuesta Marcada)**

¿Cómo percibes la alineación de la empresa con requisitos legales y regulatorios específicos durante la integración con otros estándares?

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo, ni en desacuerdo
- De acuerdo
- **Muy de acuerdo (Respuesta Marcada)**

En tu opinión, ¿cómo ha impactado la adaptación a estándares adicionales en la seguridad general de la empresa?

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo, ni en desacuerdo
- De acuerdo
- **Muy de acuerdo (Respuesta Marcada)**

¿Cómo evalúas la integración de controles de seguridad adicionales con los procesos operativos existentes durante esta fase?

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo, ni en desacuerdo
- De acuerdo
- **Muy de acuerdo (Respuesta Marcada)**

En general, ¿cómo calificarías la probabilidad de recomendar la integración con

otros estándares a colegas o empresas similares?

- Muy en desacuerdo
- En desacuerdo
- Ni de acuerdo, ni en desacuerdo
- De acuerdo
- **Muy de acuerdo (Respuesta Marcada)**