Escuela de Administración de Tecnologías de Información

Propuesta de un Proceso Formal de Gestión de Riesgos de Tecnologías de Información para la Municipalidad de Turrialba

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

Modalidad Proyecto de Graduación

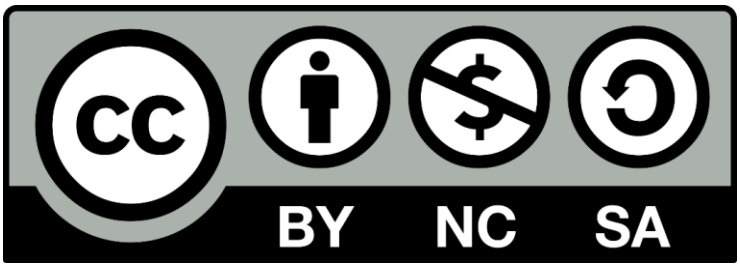
Elaborado por: Pablo Alonso Chaves Rivera

Prof. Tutor: M.Ed., Ing Luis Pablo Soto Chaves

Cartago, Costa Rica

Semestre II

Noviembre, 2024



Hoja de Aprobación

INSTITUTO TECNOLÓGICO DE COSTA RICA

ESCUELA DE ADMINISTRACIÓN DE TECNOLOGÍAS DE INFORMACIÓN

GRADO ACADÉMICO: LICENCIATURA

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

LUIS PABLO SOTO CHAVES (FIRMA)

Digitally signed by LUIS PABLO SOTO CHAVES (FIRMA)
Date: 2024.11.29 18:49:02 -06'00'

M.Ed., Ing Luis Pablo Soto Chaves

Profesor Tutor

Marco Salazar Vega

Lic. Marco Salazar Vega

Lector externo

LAURA CRISTINA ALPIZAR CHAVES (FIRMA)

Firmado digitalmente por LAURA CRISTINA ALPIZAR CHAVES (FIRMA)
Fecha: 2024.11.30 15:33:35 -06'00'

Ing. Laura Alpízar Chaves

Lector académico

TEC | Tecnológico de Costa Rica

Firmado digitalmente por YARIMA TATIANA SANDOVAL SANCHEZ (FIRMA)
Fecha: 2024.11.29 16:32:19 -06'00'

Ing. Yarima Sandoval Sánchez

Coordinadora de Trabajo Final de Graduación

CARTA DE LA FILÓLOGA

30 de octubre de 2024

Señores
Escuela de Administración de Tecnologías de Información
Licenciatura en Administración de Tecnología de Información
Instituto Tecnológico de Costa Rica
Presente

Estimados señores:

La suscrita da fe de que la tesis titulada *Propuesta de un Proceso Formal de Gestión de Riesgos de Tecnologías de Información para la Municipalidad de Turrialba*, del estudiante Pablo Alonso Chaves Rivera, fue sometida a revisión filológica.

Se han realizado las modificaciones pertinentes en los distintos niveles textuales, a saber, macro y microestructura, intención comunicativa, construcción sintáctica, precisión léxica, coherencia y cohesión, puntuación y ortografía.

Con todo respeto,

Karina R.S.

Bach. Karina Romero Solano
Filóloga
Asociada No. 408
Cédula 305270350

Dedicatoria

A mis padres, por ser los pilares de mi vida, apoyarme en mis decisiones
y estar para mí siempre que los necesito.
A mi hermana, por acompañarme desde mis primeros pasos
hasta la conclusión de este proceso.

Resumen

Chaves Rivera, Pablo Alonso. (2024). Propuesta de un Proceso Formal de Gestión de Riesgos de Tecnologías de Información para la Municipalidad de Turrialba. (Trabajo Final de Graduación). Escuela de Administración de Tecnología de Información. Instituto Tecnológico de Costa Rica.

Este Trabajo Final de Graduación propone un proceso formal de gestión de riesgos de tecnologías de información para la Municipalidad de Turrialba. El objetivo general es proponer un proceso formal de gestión de riesgos de tecnologías de información en la Municipalidad de Turrialba para la identificación, evaluación y tratamiento de riesgos tecnológicos y cumplimiento normativo a partir de la Norma Técnica del MICITT y las buenas prácticas de la industria, en el segundo semestre del año 2024. La propuesta se desarrolló tomando en cuenta las limitaciones del personal de TI en la municipalidad y la infraestructura tecnológica existente, con un enfoque práctico que permita al único encargado de TI gestionar eficazmente los riesgos.

El análisis incluyó una evaluación detallada del proceso actual de gestión de amenazas de TI, que reveló la falta de formalización y documentación del proceso. En respuesta a estos hallazgos, se diseñó un marco de gestión de riesgos sencillo y efectivo, alineado con estándares como ISO 27005, ISO 3100, COBIT 2019 e ITIL, que engloba políticas y procedimientos detallados para la identificación y tratamiento de los riesgos. Asimismo, se propuso un plan de comunicación y una estrategia de monitoreo continuo para asegurar la conformidad con la norma técnica del MICITT.

Finalmente, el proyecto concluye que la propuesta de implementación del proceso formal propuesto mejorará la capacidad de la municipalidad para gestionar sus riesgos tecnológicos, reducir la frecuencia y severidad de incidentes y cumplir con las normativas regulatorias, fortaleciendo así su infraestructura y la confianza ciudadana.

Palabras clave: Gestión de riesgos de TI, Norma Técnica MICITT, ISO 27005, ISO 31000, COBIT 2019, ITIL, Evaluación de riesgos, Tratamiento de riesgos.

Abstract

Chaves Rivera, Pablo Alonso. (2024). Proposal for a Formal IT Risk Management Process for the Municipalidad de Turrialba. (Final Graduation Project). School of Information Technology Management. Instituto Tecnológico de Costa Rica.

This Final Graduation Project proposes a formal IT risk management process for the Municipalidad de Turrialba. The general objective is to propose a formal process for the identification, evaluation, and treatment of technological risks, ensuring regulatory compliance based on the MICITT Technical Standard and industry best practices during the second semester of 2024. The proposal was developed considering the limitations of the municipality's IT personnel and its existing technological infrastructure, with a practical approach that allows the sole IT officer to effectively manage risks.

The analysis included a detailed evaluation of the current IT threat management process, revealing a lack of formalization and documentation. In response to these findings, a simple and effective risk management framework was designed, aligned with standards such as ISO 27005, ISO 31000, COBIT 2019, and ITIL, including detailed policies and procedures for risk identification and treatment. In addition, a communication plan and a continuous monitoring strategy were proposed to ensure compliance with the MICITT technical standard.

The project concludes that implementing the proposed formal process will enhance the municipality's ability to manage technological risks, reduce the frequency and severity of incidents, and ensure regulatory compliance, thereby strengthening its infrastructure and building public trust.

Keywords: IT risk management, MICITT Technical Standard, ISO 27005, ISO 31000, COBIT 2019, ITIL, Risk assessment, Risk treatment.

Tabla de Contenidos

Página

1 Introducción 1
1.1 Descripción General 1
1.2 Antecedentes 1
1.2.1 Descripción de la Organización 1
1.2.2 Trabajos Similares Realizados Dentro y Fuera de la Organización 6
1.3 Planteamiento del Problema 7
1.3.1 Situación Problemática 7
1.3.2 Justificación del Proyecto 9
1.3.3 Impacto Positivo en la Municipalidad 10
1.3.4 Beneficios Esperados o Aportes del Trabajo Final de Graduación 11
1.4 Objetivos del Trabajo Final de Graduación 12
1.4.1 Objetivo General 12
1.4.2 Objetivos Específicos 12
1.5 Alcance 12
1.5.1 Recolección y Análisis de Información: 13
1.5.2 Diseño del Marco de Gestión de Riesgos de TI: 13
1.5.3 Verificación de conformidad 13
1.6 Supuestos 14
1.7 Entregables 14
1.7.1 Entregables del producto 14
1.7.2 Entregables Académicos 16
1.8 Limitaciones 16
2 Marco Conceptual 17
2.1 Riesgo 18
2.1.1 Gestión de Riesgos 18
2.1.2 Partes Interesadas 18
2.1.3 Fuente de Riesgo 18
2.1.4 Evento 18
2.1.5 Consecuencia 18
2.1.6 Probabilidad 18

2.1.7 Control 19
2.1.8 Gestión de riesgos de TI 19
2.2 Norma Técnica de Gestión de TI del MICITT 20
2.2.1 Responsabilidades 21
2.2.2 Principio de Cumplimiento 21
2.2.3 Perfil del Proceso 21
2.2.4 Proceso de Gestión de Riesgos Tecnológicos según la normal del MICITT 23
2.3 Buenas prácticas internacionales 24
2.3.1 ISO 31000 24
2.3.2 NIST 800-30 30
2.3.3 COBIT 2019 31
2.3.4 ITIL 4 36
2.3.5 ISO 27005 39
2.3.6 ISO 9001 50
2.4 Procesos de Negocio 52
2.4.1 Business Process Management 52
2.4.2 Procesos BPM 52
3 Marco Metodológico 54
3.1 Tipo de Investigación 54
3.2 Enfoque y Diseño de la Investigación 55
3.2.1 Enfoque Cualitativo 55
3.2.2 Diseño de la Investigación 56
3.3 Fuentes de Datos e Información 57
3.3.1 Fuentes Primarias 58
3.3.2 Fuentes secundarias 60
3.4 Sujetos de Investigación 60
3.5 Variables o Categorías de la Investigación 61
3.6 Técnicas e Instrumentos de Recolección de Datos 63
3.7 Procedimiento Metodológico de la Investigación 64
3.7.1 Fase 1: Recolección y Análisis de Información 65
3.7.2 Fase 2: Diseño del Marco de Gestión de Riesgos de TI 65
3.7.3 Fase 3: Verificación de Conformidad 66

3.8 Operacionalización de las Variables o Categorías 67
4 Análisis de Resultados 70
4.1 Fase 1: Recolección y Análisis de Información 70
4.1.1 Revisión Documental 70
4.2 Análisis de Datos Recopilados 72
4.2.1 Responsabilidad en la Gestión de Amenazas de TI 72
4.2.2 Falta de Documentación Formal 72
4.2.3 Tareas o actividades del proceso existente 73
4.2.4 Tareas o actividades que requiere el proceso formal de gestión de riesgos 74
4.2.5 Externalización de Servicios de TI 77
4.2.6 Marcos Internacionales 77
4.2.7 Desafíos Anticipados para la Implementación de un Marco Formal 77
4.2.8 Estado del Apetito de Riesgo 77
4.3 Modelado del proceso as-is 78
4.3.1 Inicio del proceso 78
4.3.2 Evaluación inicial 78
4.3.3 Respuestas a las amenazas 79
4.3.4 Fin del proceso 79
4.3.5 Evaluación del Nivel de Madurez del Proceso Actual 80
4.4 Identificación de brechas y áreas de mejora 80
4.4.1 Comparativa con la norma técnica del MICITT 82
4.4.2 Comparativa con COBIT 2019 83
4.4.3 Comparativa con la ISO 27005 85
4.4.4 Comparativa con la NIST SP 800-30 86
5 Propuesta de Solución 89
5.1 Diseño de Solución 89
5.1.1 Desarrollo de Políticas de Gestión de Riesgos de TI 89
5.1.2 Elaboración de Procedimientos de Gestión de Riesgos de TI 98
5.1.3 Diseño de una Herramienta Integral de Gestión de Riesgos 103
5.1.4 Plan de Comunicaciones 108
5.2 Verificación de Conformidad 111
5.2.1 Revisión de Conformidad Normativa 111

5.2.2 Estrategia de Implementación 121
5.2.3 Informe de Resultados: 123
5.3 Análisis de la viabilidad de la propuesta 123
5.3.1 Costo por hora del encargado de TI 124
5.3.2 Costo del encargado de TI para la implementación 124
5.3.3 Costo de Office 365: 124
5.3.4 Costo total de implementación: 124
5.3.5 Ahorro en horas por semana: 124
5.3.6 Ahorro total durante la implementación: 124
5.3.7 Cálculo del Retorno sobre la Inversión (ROI) 124
5.3.8 Cálculo del Período de Recuperación de la Inversión 125
5.3.9 Cumplimiento Normativo y Beneficios Asociados 126
6 Conclusiones 127
6.1 Objetivo General 127
6.2 Objetivo Específico 1 127
6.3 Objetivo Específico 2 128
6.4 Objetivo Específico 3 128
7 Recomendaciones 129
7.1 Objetivo General 129
7.2 Objetivo específico 1 130
7.3 Objetivo Específico 2 130
7.4 Objetivo Específico 3 131
8 Referencias 132
9 Apéndices 134
9.1 Apéndice A Plantilla de Minuta 134
9.2 Apéndice B Plantilla Gestión de Cambios 135
9.3 Apéndice C Minuta 01 | Reunión inicial con la organización 136
9.4 Apéndice D Minuta reunión 02 | Reunión con el profesor Tutor 137
9.5 Apéndice E Minuta reunión 03 | Reunión con la organización 138
9.6 Apéndice F Bitácora Revisión Documental 139
9.7 Apéndice G Entrevista Situación Actual 139
9.8 Apéndice H Entrevista Miembro Comisión de Control Interno 140

9.9 Apéndice I Cuestionario Situación Actual 141
9.10 Apéndice J Resultados Cuestionario Situación Actual 143
9.11 Apéndice K Plantilla Lista de Comprobación del Proceso de Gestión de Riesgos 145
9.12 Apéndice L Minuta de Reunión 04 – Aplicación de Entrevista 149
9.13 Apéndice M Resultados Entrevista Situación Actual 150
9.14 Apéndice N Resultados Entrevista Miembro de la Comisión de Control Interno 152
9.15 Apéndice O Transcripción de Entrevistas 153
9.16 Apéndice P Plantilla Perfil del Proceso 155
9.17 Apéndice Q Modelado to-be 157
9.1 Apéndice R Política para la Gestión de Riesgos de Tecnologías de Información 158
9.2 Apéndice S Procedimientos para la gestión de Riesgos de TI 186
10 Anexos 210
10.1 Anexo I BPMN Guía de Referencia 210
10.2 Anexo II Actividades EDM03 — Asegurar la optimización del riesgo. 211
10.3 Anexo III Actividades APO12-Gestionar el riesgo. 213
10.4 Anexo IV Proceso de gestión de riesgos ISO 27005 215
11 Glosario 216

Índice de Figuras

Figura No Descripción Página

Figura 1 Organigrama de la Municipalidad de Turrialba 5
Figura 2 Organigrama del proyecto 6
Figura 3 Árbol del Problema 7
Figura 4 Árbol de conceptos 17
Figura 5 Principios ISO 31000 24
Figura 6 Proceso de gestión de Riesgo ISO 31000 26
Figura 7 Modelo Core de COBIT 32
Figura 8 Niveles de capacidad para los procesos 35
Figura 9 Cadena de Valor del Servicio 36
Figura 10 Proceso de gestión de riesgos para la seguridad de la información 41
Figura 11 Proceso cualitativo 55
Figura 12 Fases de la metodología del proyecto 64
Figura 13 Efectividad del proceso actual de gestión de amenazas de TI 73
Figura 14 Marcos internacionales de gestión de riesgos de TI está familiarizado 77
Figura 15 Proceso as-is de Gestión de Amenazas de TI 78

Figura 16 Modelado del Proceso to-be 100
Figura 17 Plantilla lista de activos 104
Figura 18 Plantilla Registro de riesgos 105
Figura 19 Plantilla Lista de Procesos de Negocio 106
Figura 20 Plantilla Matriz de Riesgos 107
Figura 21 Informe de resultados 123

Índice de Tablas

Tabla No Descripción Página

Tabla 1 Conceptos de la Gestión de Riesgos de TI 19
Tabla 2 EDM03 — Asegurar la optimización del riesgo 33
Tabla 3 APO12—Gestionar el riesgo 33
Tabla 4 Conceptos de la ISO 27005 39
Tabla 5 Ejemplo de escala de consecuencias 42
Tabla 6 Ejemplo de escala de probabilidad 43
Tabla 7 Ejemplo de enfoque cualitativo de los criterios de riesgo 44
Tabla 8 Ejemplo de Análisis de Riesgos 46
Tabla 9 Ejemplo del proceso de tratamiento de riesgos 47
Tabla 10 Fuentes primarias 58
Tabla 11 Fuentes Secundarias 60
Tabla 12 Sujetos de investigación 60
Tabla 13 Cuadro de variables de investigación 61
Tabla 14 Instrumentos de recolección de datos 63
Tabla 15 Operacionalización de las variables 68
Tabla 16 Bitácora de Revisión Documental 71
Tabla 17 Brechas estado actual y estado ideal del proceso de gestión de amenazas de TI 80
Tabla 18 Apartados de la política de gestión de riesgos de TI 89
Tabla 19 Creación de Inventarios 93
Tabla 20 Escala para determinar el Impacto 95
Tabla 21 Escala de Probabilidad 96
Tabla 22 Mapa de Calor Nivel de Riesgo 97
Tabla 23 Apartados de Procedimientos de gestión de riesgos de TI 98
Tabla 24 Grupos de Interés 108
Tabla 25 Matriz de comunicaciones 110
Tabla 26 Perfil del proceso 111
Tabla 27 Lista de comprobación del Proceso de Gestión de Riesgos Tecnológicos 113
Tabla 28 Cronograma de Implementación 122
Tabla 29 Cálculo del Período de Recuperación de la Inversión 125

1 Introducción

En este primer capítulo se mencionan los aspectos generales sobre el Trabajo Final de Graduación (TFG). El capítulo contiene información sobre la Municipalidad de Turrialba, organización en la que se realiza el proyecto. Así mismo, el documento proporciona un contexto más claro sobre la problemática en la que se encuentra la organización, así como los desafíos y las oportunidades que se presentan. Por otra parte, se definen los objetivos del TFG y el alcance y los beneficios que se esperan obtener al finalizar el proyecto.

1.1 Descripción General

La gestión de riesgos de Tecnologías de Información (TI) es un aspecto crítico en la administración de organizaciones públicas y privadas. Su pertinencia radica en la necesidad de proteger la información y cumplir con las normativas internas, externas y leyes vigentes. El caso de la Municipalidad de Turrialba, sujeto de este trabajo, es el mismo de muchas otras instituciones gubernamentales, pues enfrenta, desafíos significativos relacionados con la seguridad de la información y la eficiencia operativa en sus sistemas de TI.

El problema empresarial que aborda este trabajo es un proceso ineficiente de la gestión de riesgos de la Municipalidad de Turrialba, lo cual puede poner en riesgo la seguridad, eficiencia y cumplimiento normativo de sus sistemas de información. Existen antecedentes relevantes en la literatura y en las normativas nacionales e internacionales, tales como COBIT 2019, ITIL, UNE-ISO 31000, y NIST 800-30, que proporcionan marcos y directrices para una gestión efectiva de estos riesgos. Sin embargo, la aplicación específica de estas normativas en el contexto de una municipalidad costarricense requiere un análisis y adaptación cuidadosa. Es por esta razón que en este trabajo se estudiará la gestión de riesgos de TI en la Municipalidad de Turrialba, ya que el objetivo es proponer un proceso formal de gestión que se alinee con la Norma Técnica para la Gestión de las Tecnologías de Información del MICITT y las mejores prácticas internacionales.

La organización de este informe es la siguiente: en la sección dos se presenta una revisión de la organización y proyectos similares; en la sección tres se plantea el problema de investigación; en la sección cuatro los objetivos; en la sección cinco se justifica el problema dentro del ámbito de un administrador de TI; en la sección seis se define el alcance del proyecto; y en la sección siete la metodología que se utilizará en el desarrollo del proyecto.

1.2 Antecedentes

En el siguiente apartado se brinda una descripción detallada de la organización, en donde se incluyen las características generales de la empresa, su misión, su visión, sus valores y un esquema del equipo de trabajo del departamento.

1.2.1 *Descripción de la Organización*

La Municipalidad de Turrialba, ubicada en la provincia de Cartago, Costa Rica, se erige como una entidad administrativa fundamental para el desarrollo local. Su labor se centra en la gestión eficiente y eficaz de los recursos y en los servicios públicos del cantón, con el objetivo

primordial de mejorar la calidad de vida de sus habitantes. En este contexto, la realización del Trabajo Final de Graduación (TFG) en la Municipalidad de Turrialba presenta una valiosa oportunidad para vincular el conocimiento académico con las necesidades reales del cantón, lo cual permite contribuir de manera significativa al progreso social y económico del mismo.

Los orígenes de Turrialba se remontan al año 1786, cuando Juan de Dios Zeledón fundó la localidad. Su nombre proviene del vocablo indígena tarasco *turrialba*, que significa «río de fuego», en clara alusión al volcán homónimo que domina la región. El municipio, por su parte, se estableció en 1848, hecho a partir del cual se sentaron las bases para la organización y administración del cantón.

Turrialba goza de una ubicación estratégica, pues se sitúa en el corazón de la provincia de Cartago. Limita con cantones como Alvarado, Jiménez, Paraíso y Juan Viñas, consolidando una zona de gran dinamismo comercial y cultural. Su extensión territorial abarca 360.13 km² y cuenta con una densidad de población de 44.77 habitantes por kilómetro cuadrado (INEC, 2022).

La Municipalidad de Turrialba, como ente rector del cantón, se estructura en torno a un sistema de gobierno democrático; un alcalde, electo por votación popular para un período de cuatro años, lidera la administración municipal. El Concejo Municipal, conformado por cinco miembros también electos popularmente, ejerce como órgano legislativo, aprobando el presupuesto y las ordenanzas municipales que rigen el cantón.

La Municipalidad de Turrialba, al igual que las demás municipalidades de Costa Rica, desempeña un rol fundamental en el ámbito del gobierno local, tal como lo establece el Código Municipal de la República de Costa Rica (Ley n.° 7794). Este instrumento legal define las funciones y competencias que les corresponden a los gobiernos municipales como entes rectores del desarrollo cantonal, abarcando un amplio espectro de áreas que impactan directamente en la vida de los ciudadanos.

Dentro de las funciones y competencias de la Municipalidad de Turrialba se encuentran las siguientes:

- Gestión de servicios públicos esenciales:
    - Abastecimiento de agua potable: garantiza el acceso a agua potable de calidad a toda la población del cantón, mediante la captación, tratamiento, distribución y mantenimiento del sistema de agua potable.
    - Alcantarillado sanitario: la entidad se encarga de la recolección, tratamiento y disposición final de las aguas residuales generadas en el cantón, asegurando un manejo adecuado de estas para proteger el medio ambiente y la salud pública.
    - Recolección de residuos sólidos: se implementan programas eficientes de recolección y disposición final de los residuos sólidos generados en el cantón, incluyendo iniciativas de reciclaje y compostaje con el fin de reducir la cantidad de desechos enviados a vertederos.
    - Alumbrado público: vela por la instalación, mantenimiento y operación del sistema de alumbrado público del cantón, lo cual garantiza la iluminación adecuada de

calles y espacios públicos que, a su vez, promueve la seguridad y el bienestar de la comunidad.
    - Mantenimiento de vías públicas: la entidad se encarga de la construcción, mantenimiento y reparación de las vías públicas del cantón, asegurando la transitabilidad vehicular y peatonal en todo el territorio.
    - Administración de parques y áreas recreativas: la municipalidad crea, mantiene y administra parques, plazas y áreas recreativas para el disfrute y esparcimiento de los habitantes del cantón, fomentando así la cohesión social y el bienestar general.
- Gestión administrativa eficiente y transparente:
    - Administración de recursos públicos: administra de manera eficiente y transparente los recursos públicos del cantón, medida con la cual se asegura su uso adecuado y responsable para el cumplimiento de sus funciones y el bien común de la comunidad.
    - Gestión del recurso humano: la entidad administra eficientemente el recurso humano del cantón, contratando, capacitando y evaluando al personal con el fin de garantizar la prestación de servicios públicos de calidad y el cumplimiento de sus objetivos.
    - Relaciones con la comunidad: mantiene una comunicación fluida y transparente con la comunidad, de manera que promueve la participación ciudadana en la toma de decisiones, la rendición de cuentas y la construcción de una relación de confianza entre la entidad y los habitantes del cantón.
- Cumplimiento normativo y regulatorio:
    - La municipalidad es responsable de cumplir con todas las leyes y reglamentos aplicables a su funcionamiento, para garantizar un accionar legal, ético y responsable en el ejercicio de sus funciones y competencias. Algunas de estas leyes son:
        - Código Municipal (Ley n.º 7794): esta es la ley fundamental que regula la organización, funcionamiento, competencias y atribuciones de las municipalidades en Costa Rica.
        - Ley de Contratación Administrativa (Ley n.º 7494): regula los procesos de contratación pública que las municipalidades deben seguir para garantizar la transparencia y legalidad en la adquisición de bienes, servicios y obras.
        - Ley General de la Administración Pública (Ley n.º 6227): establece principios y normas básicas sobre el funcionamiento de la administración pública, incluyendo el de las municipalidades.
        - Norma Técnica de Gestión de Tecnologías de Información (NTG-001): emitida por el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT). Esta norma establece lineamientos para la gestión efectiva de las tecnologías de información, asegurando que las

entidades públicas, (incluidas las municipalidades) implementen buenas prácticas en la administración, seguridad y uso de sus recursos tecnológicos.

1.2.1.1 **Misión.**

A continuación, se indica la misión de la organización:

> Brindar la eficiente y oportuna prestación de los servicios locales y promover el desarrollo local, con participación plena y organizada de la población que interviene, apoya y fiscaliza la gestión municipal, buscando que Turrialba sea un cantón competitivo en que sus ciudadanos vivan con orgullo, dignidad y respeto al medio ambiente. (Municipalidad de Turrialba, 2021)

1.2.1.2 Visión.

A continuación, se define la visión de la organización:

> La Municipalidad de Turrialba, será una empresa comprometida y competitiva, de alta productividad, de reconocido prestigio, que contribuya a mejorar permanentemente la condición de vida de los turrialbeños. La gestión se sustentará en el ordenamiento jurídico vigente, una estructura orgánica y funcional adecuada, la prestación de servicios de calidad, el trabajo en equipo, la sostenibilidad presupuestaria, la protección al ambiente, la participación ciudadana la comunicación efectiva y capacidad de sus recursos humanos. (Municipalidad de Turrialba, 2021)

1.2.1.3 Valores.

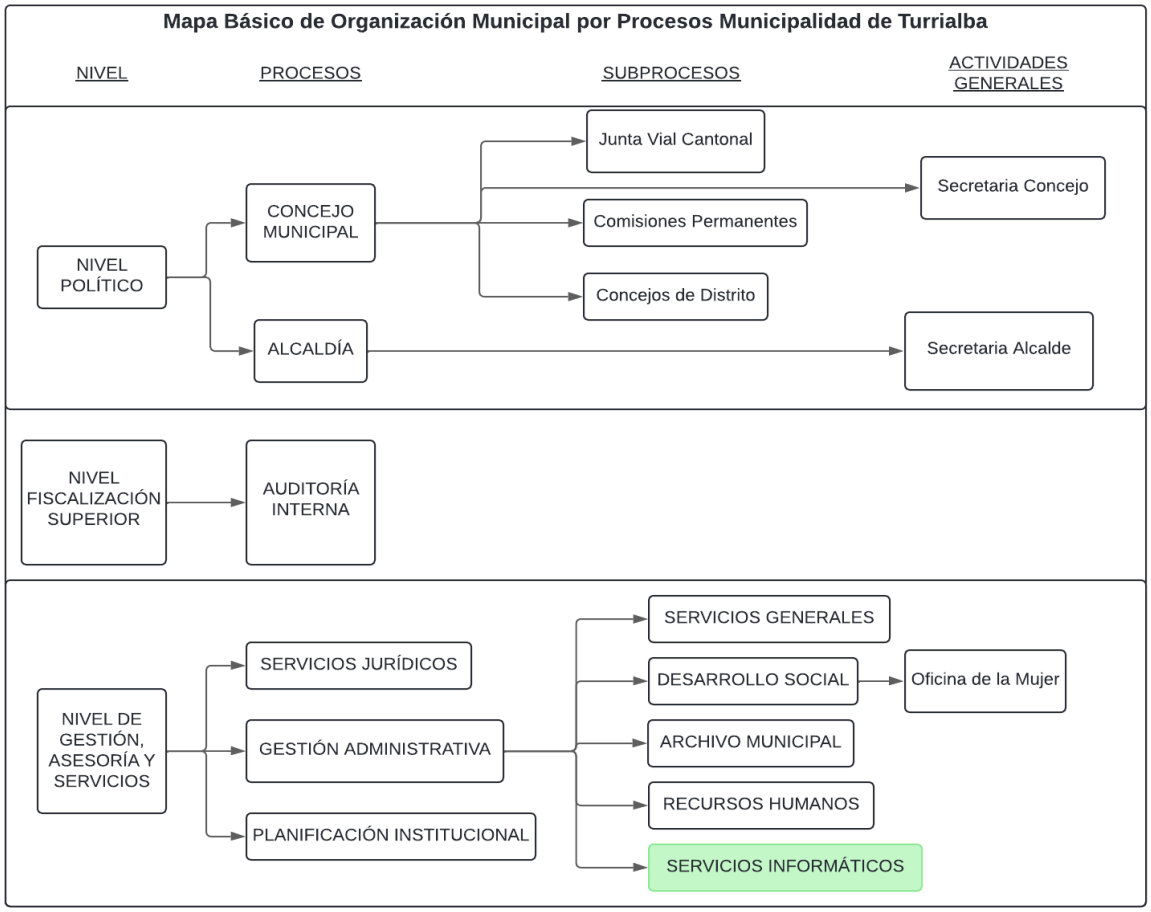
Los valores de la Municipalidad de Turrialba son los siguientes:

- Fe en Dios
- Amor por Turrialba
- Trabajo en equipo
- Visión empresarial
- Diálogo permanente
- Espíritu de servicio al cliente
- Comunicación efectiva
- Respeto ambiente
- Rendición de cuentas
- Respeto a las leyes (Municipalidad de Turrialba, 2021).

1.2.1.4 Equipo de Trabajo.

A continuación, en la Figura 1 Organigrama de la Municipalidad de Turrialba se muestra la estructura organizativa actual que relaciona órganos.

Figura 1 *Organigrama de la Municipalidad de Turrialba*



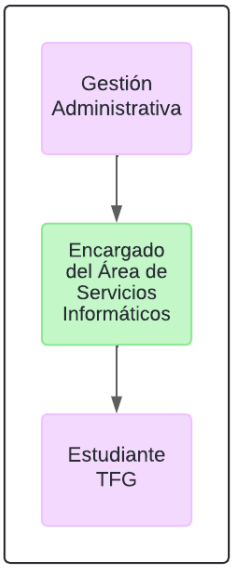
Nota. Adaptado de Depto Tecnologías de Información de la Municipalidad de Turrialba, 2021.

El organigrama de la Municipalidad de Turrialba está diseñado por los procesos que realiza la municipalidad. El proyecto en cuestión se desarrolla en el área de Servicios Informáticos, subproceso de la Gestión Administrativa, área que se deriva de Gestión de Asesoría y Servicios. El equipo de trabajo para el desarrollo del proyecto TFG está conformado por las siguientes personas:

- Encargado del Área de Servicios Informáticos: es el responsable de los procesos del área y único trabajador asignado a los servicios informáticos de la Municipalidad de Turrialba. Es el encargado de supervisar el trabajo del estudiante.
- Estudiante: Es el responsable de desarrollar el proyecto TFG bajo la supervisión del encargado del Área de Servicios Informáticos.

En la **Figura *2*** Organigrama del proyecto se muestra gráficamente la ubicación del estudiante dentro del organigrama de la Municipalidad de Turrialba:

Figura 2 *Organigrama del proyecto*



1.2.2 Trabajos Similares Realizados Dentro y Fuera de la Organización

Para establecer un contexto adecuado y justificar la relevancia del presente proyecto de graduación, es importante analizar trabajos similares que se han realizado tanto dentro de la Municipalidad de Turrialba como en otras organizaciones que enfrentan desafíos relacionados con la gestión de riesgos de tecnologías de información.

1.2.2.1 Proyectos Internos.

Según información proporcionada por el encargado del Área de Servicios Informáticos, la Municipalidad de Turrialba no cuenta con proyectos documentados previos relacionados con la gestión de riesgos de TI.

1.2.2.2 Proyectos Similares Externos.

Trabajo Final de Graduación: Metodología para la gestión de riesgos de TI basada en COBIT 5 (Alfaro, 2017). Este proyecto se centra en la implementación de las mejores prácticas y de estándares globales para la gestión de riesgos de TI en Deloitte. El objetivo es ofrecer servicios de gestión de riesgos de TI que se ajustaran a las necesidades y tendencias en vigencia de los clientes.

Asesoría para el diseño del mapa de riesgos de TIC: Informe del mapa de riesgos del centro de cómputo de la municipalidad de Tibás (PwC Costa Rica, 2019). Este trabajo tiene como objetivo identificar los principales riesgos a los que estaba expuesto el centro de cómputo de la Municipalidad de Tibás. El mapa de riesgos sigue la metodología de gestión de riesgos de TIC y se utilizaron estándares internacionales como ISO/IEC 27001, ISO/IEC 27005 e ISO/IEC 31000.

Estructura de Riesgos: Portafolio de Riesgos de la Municipalidad de Santo Domingo de Heredia. Este proyecto consiste en la elaboración de un portafolio de riesgos para la Municipalidad de Santo Domingo de Heredia. El portafolio de riesgos incluye una descripción de cada riesgo, su impacto potencial y las medidas de control existentes.

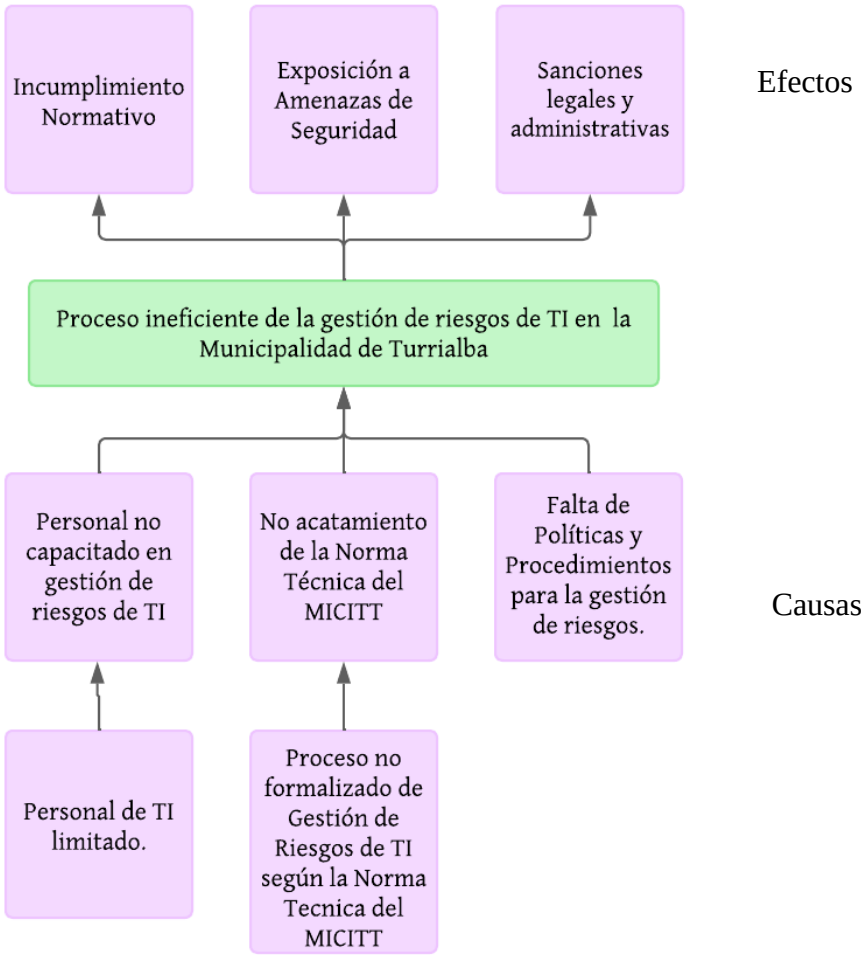
1.3 Planteamiento del Problema

La correcta gestión de los riesgos de TI es crucial para el funcionamiento eficiente y seguro de las instituciones públicas, especialmente en un entorno regulado como el de la Municipalidad de Turrialba. Esta sección aborda la situación problemática que motiva el desarrollo de este proyecto y los beneficios esperados de su implementación.

1.3.1 Situación Problemática

En esta sección se describe detalladamente la situación problemática de este TFG, presentada por la organización en la primera reunión**, Apéndice C Minuta 01 | Reunión inicial con la organización**. Para una mejor percepción del problema, se utiliza la herramienta del árbol del problema en la **Figura *3*** Árbol del Problema

Figura 3 *Árbol del Problema*



La Municipalidad de Turrialba, en su labor como entidad administrativa, enfrenta desafíos significativos en la gestión de tecnologías de información y comunicación (TIC). Como parte del sector público, está sujeta a normas y regulaciones estrictas que buscan garantizar la eficiencia, transparencia y seguridad en el uso de estos recursos. En este contexto, se ha identificado una situación problemática relacionada con el proceso de la gestión de riesgos de TI que requiere atención urgente.

En 2021, el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT) emitió normas técnicas para la gestión y el control de las tecnologías de información (Solís García et al, 2021), estableciendo un marco de gestión de TI obligatorio para las instituciones públicas que se encuentran fiscalizadas por la Contraloría General de la República. Este marco de gestión incluye catorce procesos esenciales, entre los cuales se encuentra el proceso de la gestión de riesgos de TI.

El incumplimiento de estos procesos puede tener graves consecuencias. Según el artículo 99 del Código Municipal (Ley n.° 7794), la falta de acatamiento de las normativas de gestión de TI puede resultar en la no aprobación del presupuesto municipal por parte de la Contraloría General de la República. Por lo tanto, es imperativo que la Municipalidad de Turrialba implemente estas normativas para asegurar su funcionamiento continuo y evitar sanciones administrativas.

Actualmente, según indica el encargado del área de TI, la Municipalidad de Turrialba se encuentra en las primeras etapas de implementación de las normas técnicas emitidas por el MICITT. Ha avanzado en la gobernanza, la gestión y la planificación estratégica de TI. Sin embargo, la Gestión de Riesgos de TI, el cuarto proceso estipulado por el marco de gestión de TI, aún no se ha implementado.

La ausencia de un proceso formal de gestión de riesgos de TI crea una serie de vulnerabilidades significativas para la Municipalidad. Entre estas vulnerabilidades se incluyen:

- Interrupciones en los servicios críticos que la Municipalidad proporciona, afectando la calidad de vida de los habitantes de Turrialba.
- La información manejada por la Municipalidad puede estar expuesta a accesos no autorizados, alteraciones o pérdida.
- Sanciones legales y administrativas, afectando la operación y reputación de la municipalidad.

El encargado del área de TI ha señalado que la Municipalidad aún no ha implementado un proceso estandarizado de gestión de riesgos de TI; este es un aspecto crítico que debe ser abordado para proteger la infraestructura tecnológica. El marco de gestión de TI estipula lo siguiente:

> La institución debe establecer un proceso formal de gestión de riesgos para responder a las amenazas que puedan afectar el logro de los objetivos institucionales. Este proceso debe estar integrado al sistema de valoración del riesgo institucional y considerar el marco de gestión de riesgos aplicable. La Unidad de TI debe aplicar este marco para identificar, valorar, priorizar y gestionar los riesgos en el ámbito de TI, abarcando escenarios que

puedan afectar la continuidad operacional y la integridad y confidencialidad de la información. (Solís García et al, 2021)

Actualmente, la Municipalidad de Turrialba se encuentra en un estado de incumplimiento de la norma técnica del MICITT sobre el proceso de Gestión de Riesgos de TI. El estandarizar dicho proceso permite a la Municipalidad de Turrialba cumplir con las normas establecidas, proteger su infraestructura tecnológica y evitar sanciones legales o administrativas.

1.3.2 Justificación del Proyecto

El proyecto TFG propuesto se alinea de manera integral con el perfil profesional de un administrador de tecnologías de información en diversos aspectos:

- **Auditoría de TI:** la gestión de riesgos de TI implica la realización de un análisis profundo y sistemático de los riesgos en los sistemas de información, similar a una auditoría de TI en términos de evaluación, identificación y documentación de riesgos.
- **Seguridad de TI:** la gestión de riesgos de TI es fundamental para establecer e implementar estrategias de seguridad de la información efectivas, lo que permite identificar, prevenir y mitigar amenazas y vulnerabilidades que afectarían la confidencialidad, integridad y disponibilidad de los datos y sistemas de la organización.
- **Administración de servicios de TI:** la implementación de un marco de gestión de riesgos de TI contribuye a la mejora continua de los servicios de TI al garantizar la continuidad operativa, la eficiencia y la calidad de los servicios prestados.
- **Administración de Procesos de TI:** la gestión de riesgos de TI requiere la integración de políticas, procedimientos y prácticas dentro de los procesos de TI existentes, asegurando que todos los componentes de los sistemas de TI estén alineados con los objetivos estratégicos y operacionales de la organización. Esto implica la estandarización de procesos para la identificación, evaluación, tratamiento y monitoreo de riesgos, lo cual es esencial para mantener la resiliencia y efectividad de los servicios de TI.

1.3.2.1 Tecnologías, Buenas Prácticas y Marcos de Referencia.

El proyecto contempla la aplicación de diversas tecnologías, buenas prácticas y marcos de referencia reconocidos en la industria para la gestión de riesgos de TI, incluyendo:

- COBIT 2019: desarrollado por Information Systems Audit and Control Association (ISACA), se presenta como un marco de referencia completo para la gestión de TI, incluyendo un enfoque integral para la gestión de riesgos.
- NIST Cybersecurity Framework: creado por el National Institute of Standards and Technology (NIST), ofrece un enfoque integral para la gestión de riesgos cibernéticos, ayudando a las organizaciones a proteger sus sistemas de información contra amenazas cada vez más sofisticadas.
- A diferencia de otros marcos de referencia, el NIST Cybersecurity Framework se caracteriza por su flexibilidad y adaptabilidad, aspecto que permite a las organizaciones

personalizarlo de acuerdo con sus necesidades y contexto específicos, asegurando una implementación efectiva y alineada con su realidad particular.

- ISO 31000:2018 Gestión del riesgo - Principios y directrices: la norma ISO 31000:2018, desarrollada por la Organización Internacional de Normalización (ISO), ofrece un conjunto de principios y directrices para la gestión del riesgo en cualquier contexto, incluyendo la gestión de riesgos de TI. Su enfoque universal la convierte en una herramienta valiosa para organizaciones de diversos sectores y tamaños.
- ITIL 4: desarrollado por Axelos, es un conjunto de buenas prácticas para la gestión de servicios de TI que incluye recomendaciones específicas para la gestión de riesgos. Su enfoque, basado en el valor, ayuda a las organizaciones a optimizar sus servicios de TI y a alinearlos con las necesidades del negocio.
- Metodología BPM de Dumas: actúa como un catalizador en este proceso**.** Al modelar y optimizar los procesos de negocio, la BPM permite identificar las áreas más expuestas a riesgos y diseñar controles más efectivos. La combinación de BPM con los marcos mencionados garantiza una gestión de riesgos proactiva y alineada con las estrategias de la organización.

1.3.3 Impacto Positivo en la Municipalidad

La implementación de un proceso de gestión de riesgos de TI en la Municipalidad de Turrialba generará un impacto positivo y significativo en la organización en los siguientes aspectos:

- **Continuidad operacional:** se reducirá la probabilidad de incidentes de seguridad que afecten la disponibilidad de los sistemas y servicios de TI, garantizando la continuidad de las operaciones municipales y la prestación oportuna de servicios a los ciudadanos.
- **Protección de la información:** se fortalecerá la protección de la confidencialidad, integridad y disponibilidad de la información sensible de la Municipalidad, incluyendo datos personales, financieros y administrativos. De esta manera, se minimiza el riesgo de filtraciones, pérdidas o alteraciones no autorizadas.
- **Cumplimiento normativo:** al cumplir con las normativas y regulaciones relacionadas con la seguridad de la información y la gestión de riesgos de TI, se evitarán sanciones y multas por parte de las entidades reguladoras, con lo cual se asegura el cumplimiento legal y se fortalece la imagen institucional.
- **Eficiencia en la gestión de TI:** se optimizarán los recursos y esfuerzos destinados a la seguridad de la información, al contar con un enfoque sistemático y preventivo para la gestión de riesgos. De esta manera, se da una asignación más efectiva de recursos y una mejor planificación de inversiones en seguridad.
- **Fortalecimiento al ambiente de control interno de TI:** se mejorará el ambiente de control interno de TI mediante la implementación de políticas y procedimientos claros y consistentes para la identificación, evaluación y mitigación de riesgos. Esto no solo aumentará la capacidad de la municipalidad para detectar y responder a posibles amenazas,

sino que también promoverá una cultura de seguridad y responsabilidad entre los empleados.

- **Mejora de la imagen institucional:** se fortalecerá la imagen de la municipalidad como una entidad responsable, comprometida con la seguridad de la información, la protección de los datos de los ciudadanos y el cumplimiento de las normativas legales, mejorando la confianza y credibilidad ante la comunidad.

1.3.4 Beneficios Esperados o Aportes del Trabajo Final de Graduación

Este proyecto ofrece una serie de beneficios que serán puntualmente listados según su categoría, ya sean beneficios directos o indirectos.

1.3.4.1 Beneficios Directos.

La implementación de un proceso formal de gestión de riesgos de TI permitirá a la Municipalidad de Turrialba:

- Identificar proactivamente los riesgos potenciales que afectarían sus sistemas de información, datos y operaciones, mediante la realización de análisis de amenazas y vulnerabilidades, evaluaciones de impacto y análisis de probabilidad.
- Evaluar cada riesgo identificado, utilizando metodologías cuantitativas y cualitativas para determinar su prioridad y asignar recursos de manera eficiente a cada riesgo identificado.
- Contribuir en la generación de estrategias de tratamiento de los riesgos identificados mediante la implementación de medidas de control técnicas, organizativas y físicas, de acuerdo con los estándares y buenas prácticas de la industria.
- Reducir los incidentes de seguridad: una gestión adecuada de riesgos de TI permitirá disminuir la frecuencia y severidad de incidentes de seguridad como ataques cibernéticos, pérdida de datos o interrupciones del servicio.
- Continuidad operativa: se asegura el funcionamiento continuo de los servicios municipales críticos, contribuyendo a la implementación de planes de recuperación ante desastres y continuidad del negocio.
- Cumplimiento normativo: la Municipalidad de Turrialba estará en cumplimiento del cuarto proceso de la Norma Técnica del MICITT, gestión de riesgos de TI en el sector público, que proporciona guías y recomendaciones para la implementación de un sistema de gestión de riesgos de TI en las entidades del sector público. El cumplimiento normativo permitirá:
    - Evitar sanciones: multas y penalizaciones por parte de las entidades reguladoras debido al incumplimiento de las normativas y regulaciones relacionadas con la seguridad de la información y la gestión de riesgos de TI.
    - Aprobar el presupuesto: facilitar la aprobación de la Contraloría General de la República para el presupuesto municipal, al probar el cumplimiento de los requisitos mínimos de seguridad de la información y gestión de riesgos de TI.
    - Fortalecer la reputación: demostrar a la ciudadanía y a otras entidades el compromiso de la municipalidad con la seguridad de la información, la protección

de datos y el cumplimiento de las normativas legales, lo cual fomenta la idea de la municipalidad como una entidad responsable y transparente.

- Protección de la información: la implementación de medidas de gestión de riesgos de TI protegerá la información confidencial y sensible de la municipalidad.

1.3.4.2 Beneficios Indirectos.

- Aumentar la confianza ciudadana: la mejora en la gestión de riesgos de TI y la garantía de la seguridad y eficiencia en la prestación de servicios públicos por parte de la municipalidad contribuirán a aumentar la confianza de los ciudadanos en la capacidad de la institución para proteger su información y brindar servicios confiables, transparentes y eficientes.
- Mejorar la legitimidad institucional: esto se logrará reforzando la imagen de la municipalidad como una entidad responsable, comprometida con la seguridad de la información y el bienestar de la comunidad.

1.4 Objetivos del Trabajo Final de Graduación

En el presente apartado se establece el objetivo general y los objetivos específicos del proyecto.

1.4.1 Objetivo General

Proponer un proceso formal de gestión de riesgos de tecnologías de información en la Municipalidad de Turrialba para la identificación, evaluación y tratamiento de riesgos tecnológicos y cumplimiento normativo a partir de la Norma Técnica del MICITT y las buenas prácticas de la industria en el segundo semestre del año 2024.

1.4.2 Objetivos Específicos

- Analizar la situación actual del proceso de gestión de amenazas de TI que afectarían a la Municipalidad de Turrialba para la identificación de oportunidades de mejora del proceso existente contra las buenas prácticas de la industria.
- Diseñar un marco de gestión de riesgos de TI basado en la norma técnica del MICITT y las mejores prácticas de la industria para la estandarización de las actividades del proceso.
- Verificar la conformidad del proceso de gestión de riesgos de TI con los requisitos establecidos en la norma técnica del MICITT para el cumplimiento regulatorio y la protección de los activos de información.

1.5 Alcance

Este trabajo se desarrollará durante el segundo semestre del año 2024, tiene como objetivo proponer un proceso formal de gestión de riesgos de TI para la Municipalidad de Turrialba, enfocado en la identificación, evaluación y tratamiento de los riesgos tecnológicos y en garantizar el cumplimiento normativo según la Norma Técnica del MICITT y las mejores prácticas de la industria.

1.5.1 Recolección y Análisis de Información:

En la fase inicial, se llevará a cabo una recolección exhaustiva de información que permita comprender el estado actual del proceso de gestión de amenazas de TI en la Municipalidad de Turrialba. Esta etapa incluirá la revisión documental interna con el fin de analizar los procedimientos y prácticas vigentes. Se realizarán entrevistas y cuestionarios dirigidos al encargado del área de servicios de TI y a otros miembros del personal relevante para obtener una visión integral de cómo se identifican, evalúan y gestionan las amenazas en la práctica diaria. Este proceso permitirá la construcción de un modelo as-is del proceso actual, con el cual se identificarían tanto las fortalezas como las debilidades del sistema existente y las oportunidades de mejora tomando como referencia las mejores prácticas de la industria.

1.5.2 Diseño del Marco de Gestión de Riesgos de TI:

Con base en la información recopilada y el análisis del estado actual, se procederá al diseño de un marco formal de gestión de riesgos de TI. En esta fase, se desarrollarán las siguientes componentes:

- **Políticas de gestión de riesgos de TI:** se definirán las políticas que establecerán los principios y directrices generales para la gestión de riesgos de TI. Estas políticas establecerán los roles y responsabilidades, los criterios para la identificación y evaluación de riesgos, y las directrices para el tratamiento y monitoreo de riesgos.
- **Procedimientos de gestión de riesgos de TI:** se elaborarán procedimientos que describan los pasos para la implementación de las prácticas de gestión establecidas. Estos procedimientos cubrirán aspectos como la identificación de riesgos, la priorización de riesgos, y el seguimiento y revisión de los riesgos.
- **Prácticas basadas en la Norma Técnica del MICITT y mejores prácticas internacionales:** el marco propuesto incorporará las mejores prácticas internacionales, tales como COBIT 2019, ITIL 4, UNE-ISO 31000 UNE-ISO 27005, UNE-ISO 9001 y NIST 800-30. Se adaptarán estas prácticas a las necesidades y al contexto específico de la Municipalidad de Turrialba con el objetivo de asegurar su efectividad y relevancia.
- **Herramienta Integral de Gestión de Riesgos:** se creará un Herramienta Integral que incluirá una estrategia de monitoreo y seguimiento de riesgos que detallará el método de supervisión de los riesgos identificados. También se desarrollará un plan de comunicación que garantice que todas las partes interesadas estén informadas y comprometidas con el proceso de gestión de riesgos.

1.5.3 Verificación de conformidad

Una vez diseñado el marco de gestión de riesgos de TI, se llevará a cabo una revisión para verificar la conformidad del proceso con los requisitos establecidos en la Norma Técnica del MICITT, utilizando una lista de comprobación con las actividades que indica la norma, con el propósito de corroborar que se lleve a cabo cada una de las actividades del proceso de gestión de riesgos de TI. Esta revisión asegurará que el marco propuesto cumpla con las regulaciones y estándares aplicables y garantice la protección adecuada de los activos de información de la Municipalidad de Turrialba. La verificación incluirá la evaluación de las políticas, procedimientos

y prácticas desarrolladas en relación con los requisitos normativos y las expectativas de cumplimiento regulatorio.

El resultado final de este proyecto será un documento integral que integre el marco de gestión de riesgos de TI propuesto. Dicho documento proporcionará un enfoque estandarizado para la identificación, evaluación y tratamiento de riesgos tecnológicos, asegurando el cumplimiento regulatorio y la protección de los activos de información de la Municipalidad de Turrialba. De este modo, el marco propuesto funcionará como una base sólida para la implementación de un proceso formal de gestión de riesgos de TI en la organización.

1.6 Supuestos

Se asume que lo siguiente será cierto durante la ejecución del proyecto:

- Provisión de información y recursos: la Municipalidad de Turrialba proporcionará toda la información y los recursos necesarios para completar el proyecto de manera oportuna y eficiente.
- Cooperación del personal: los empleados de la municipalidad estarán dispuestos a cooperar y a proporcionar la información requerida.
- Ausencia de interrupciones mayores: no habrá interrupciones significativas en el proyecto producto de eventos externos imprevistos.

1.7 Entregables

En esta sección se describen los entregables que tendrá el proyecto, tomando en cuenta los entregables académicos y los entregables del producto solicitados por la organización.

1.7.1 Entregables del producto

- **Objetivo 1: analizar la situación actual del proceso de gestión de amenazas de TI que afectarían a la Municipalidad de Turrialba para la identificación de oportunidades de mejora del proceso existente contra las buenas prácticas de la industria.**
    - **Entregable 1:** Informe de la situación actual
        - Este informe documentará la evaluación detallada del estado actual del proceso de gestión de amenazas de TI en la Municipalidad de Turrialba. Incluirá un análisis de los procedimientos y prácticas vigentes de la gestión de amenazas, así como una identificación de fortalezas, debilidades y oportunidades de mejora, tomando como referencia las mejores prácticas de la industria.
        - El documento incluirá:
            - Descripción y evaluación del proceso actual de gestión de riesgos de TI
            - Identificación de brechas y áreas de mejora
            - Modelo as-is del proceso actual

- **Objetivo 2: diseñar un marco de gestión de riesgos de TI basado en la normas técnica del MICITT y las mejores prácticas de la industria para la estandarización de las actividades del proceso.**
    - **Entregable 2:** Marco de gestión de riesgos de TI
        - Este documento presentará el marco formal de gestión de riesgos de TI propuesto, basado en la norma técnica del MICITT y las mejores prácticas internacionales. Incluirá políticas, procedimientos y prácticas diseñadas para la identificación, evaluación y tratamiento de riesgos tecnológicos.
        - El marco incluirá:
            - Políticas de gestión de riesgos de TI, detallando principios y directrices generales.
            - Procedimientos operativos, describiendo los pasos específicos para implementar las prácticas de gestión.
            - Una Herramienta Integral de gestión de riesgos, que abarca el monitoreo, seguimiento y comunicación de riesgos.
            - Plan de comunicación.
- **Objetivo 3: verificar la conformidad del proceso de gestión de riesgos de TI con los requisitos establecidos en la norma técnica del MICITT para el cumplimiento regulatorio y la protección de los activos de información.**
    - **Entregable 3:** Informe de Verificación de Conformidad
        - Este informe evaluará la conformidad del marco de gestión de riesgos de TI con los requisitos de la Norma Técnica del MICITT. Asegurará que el marco propuesto cumpla con las regulaciones y estándares aplicables para garantizar la protección adecuada de los activos de información.
        - El documento incluirá:
            - Análisis de la alineación del marco propuesto con la norma técnica del MICITT mediante una lista de comprobación de las actividades del proceso.
            - Identificación de cualquier desviación o área que requiera ajuste.
            - Recomendaciones para asegurar el cumplimiento normativo y mejorar el proceso de gestión de riesgos de TI.

1.7.2 Entregables Académicos

En esta sección se describen los artefactos asociados a los entregables académicos del Trabajo Final de Graduación. Los resultados académicos que se desarrollan son los siguientes:

- Capítulo 1: Introducción
- Capítulo 2: Marco conceptual
- Capítulo 3. Marco metodológico
- Capítulo 4: Análisis de resultados
- Capítulo 5: Propuesta de Solución
- Capítulo 6: Conclusiones
- Capítulo 7: Recomendaciones

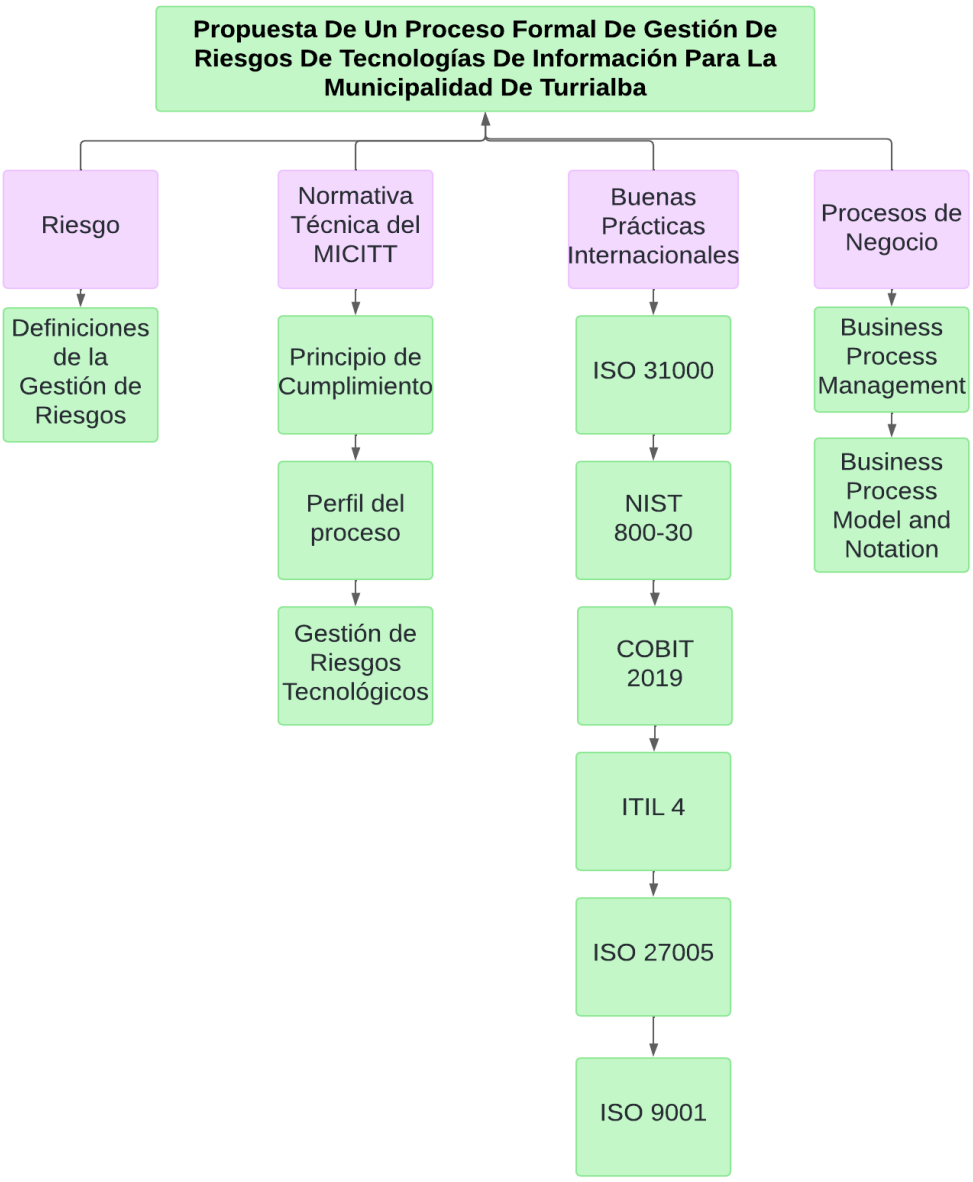
1.8 Limitaciones

- **Recursos humanos limitados:** el área de servicios informáticos de la Municipalidad de Turrialba cuenta actualmente con un único encargado, quien es el único del personal con conocimiento de los servicios y procesos de TI del área. Esta limitación en el personal podría afectar la disponibilidad de información y la capacidad de obtener perspectivas diversas sobre el proceso de gestión de riesgos.
- **Ámbito de aplicación restringido:** El proyecto se centrará exclusivamente en el área de servicios de TI de la Municipalidad de Turrialba. No se considerarán otros departamentos o áreas que puedan tener interacciones o impactos relacionados con la gestión de riesgos de TI, lo que podría limitar la exhaustividad del análisis en el contexto global de la organización.
- **Exclusión de implementación:** la fase de implementación del marco de gestión de riesgos de TI no está incluida en el alcance de este proyecto. El objetivo se limita a la propuesta y diseño del marco, y no abarca la aplicación práctica, puesta en marcha o ejecución de las políticas, procedimientos y prácticas desarrolladas.

2 Marco Conceptual

El marco conceptual, también conocido como marco referencial, tiene el propósito de dar a la investigación un sistema coordinado y coherente de conceptos y definiciones con el cual se va a abordar el problema. En este capítulo se describen los conceptos teóricos y prácticos que sustentan el desarrollo del estudio. Por ende, a partir de la **Figura *4*** Árbol de conceptos se explora la norma técnica del MICITT, las buenas prácticas internacionales como ISO 31000, NIST 800-30, ITIL y COBIT 2019.

Figura 4 *Árbol de conceptos*



2.1 Riesgo

La ISO 3100 define el riesgo como el «efecto de la incertidumbre sobre los objetivos» (Asociación Española de Normalización, 2018). En este contexto, un efecto es una desviación respecto a lo previsto, que crea oportunidades o amenazas si el desvío es positivo, negativo o ambos. La Norma Técnica del MICITT dentro de su glosario define el riesgo como:

> La exposición a una situación donde hay una posibilidad de sufrir un daño o de estar en peligro. Es la vulnerabilidad o amenaza a que ocurra un evento y sus efectos sean negativos y que alguien o algo puedan verse afectados por él. Cuando se dice que un elemento está en riesgo es porque se considera que se encuentra en desventaja frente a algo más, bien sea por su ubicación o posición; además de ser susceptible a recibir una amenaza sin importar cuál sea su índole. (MICITT, 2021)

2.1.1 Gestión de Riesgos

Las actividades coordinadas para dirigir y controlar el riesgo tomadas por la organización se conocen como *gestión del riesgo.* Este es un proceso integral y sistemático que permite a las organizaciones identificar, evaluar y responder a los riesgos que podrían afectar el logro de sus objetivos. En el contexto de las tecnologías de la información (TI), la gestión de riesgos se centra en proteger los activos de información de las amenazas que puedan comprometer su confidencialidad, integridad y disponibilidad (Asociación Española de Normalización, 2018).

2.1.2 Partes Interesadas

«Las partes interesadas son aquellas personas u organizaciones que puede afectar, verse afectada o percibirse como afectada por una decisión o actividad» (Asociación Española de Normalización, 2018).

2.1.3 Fuente de Riesgo

«El elemento que, por si solo o en combinación con otros, tiene el potencial de generar riesgos» es conocido como una fuente de riesgo (Asociación Española de Normalización, 2018).

2.1.4 Evento

Según la Asociación Española de Normalización (2018), un evento es «una ocurrencia o cambio de un conjunto particular de circunstancias» y tiene una o varias causas y consecuencias. Un evento también es algo previsto que no llega a ocurrir o algo no previsto que ocurre y ser una fuente de riesgo.

2.1.5 Consecuencia

Una consecuencia es el «resultado de un evento que afecta a los objetivos» (Asociación Española de Normalización, 2018). Esta tiene efectos positivos o negativos y directos o indirectos. Las consecuencias se expresan de manera cualitativa o cuantitativa, y puede darse el caso de incrementarse por un efecto cascada y efectos acumulativos.

2.1.6 Probabilidad

La probabilidad es «la posibilidad de que algo suceda». Según la definición, se «utiliza para indicar la posibilidad de que un evento suceda, esté definida, medida o determinada objetiva o

subjetivamente, cualitativa o cuantitativamente y descrita utilizando términos generales o matemáticos» (Asociación Española de Normalización, 2018).

2.1.7 Control

El control es la «medida que mantiene y/o modifica un riesgo» (Asociación Española de Normalización, 2018). Estos incluyen procesos, políticas, prácticas o acciones que modifiquen un riesgo, pero no siempre producen el efecto de modificación previsto.

2.1.8 Gestión de riesgos de TI

La gestión de riesgos de TI se refiere a la aplicación de los principios y procesos de gestión de riesgos específicamente al ámbito de las tecnologías de la información. Este proceso tiene como objetivo proteger los sistemas de TI, los datos y las infraestructuras críticas contra las amenazas que puedan comprometer su funcionamiento (NIST, 2012).

2.1.8.1 Definiciones claves.

En el contexto de la gestión de riesgos de tecnologías de información (TI), es fundamental comprender con precisión una serie de conceptos clave que sustentan la identificación, evaluación y mitigación de riesgos. En la **Tabla *1*** se presentan las definiciones de los términos más relevantes para asegurar una adecuada comprensión y aplicación de los principios de seguridad de la información.

Tabla 1 *Conceptos de la Gestión de Riesgos de TI.*

Concepto	Definición
Amenaza	Cualquier circunstancia o evento con el potencial de impactar negativamente las operaciones organizacionales mediante acceso no autorizado, destrucción, divulgación o modificación de la información y/o denegación de servicio.
Ataque	Cualquier tipo de actividad maliciosa que intente recolectar, interrumpir, negar, degradar o destruir los recursos del sistema de información o la propia información.
Autenticación	Verificar la identidad de un usuario, proceso o dispositivo, a menudo como requisito previo para permitir el acceso a los recursos en un sistema de información.
Autenticidad	La propiedad de ser genuino y ser verificado y confiable. Confianza en la validez de una transmisión, un mensaje o el origen de un mensaje.
Autorización	La decisión de gestión oficial otorgada por un funcionario organizacional superior para autorizar la operación de un sistema de información y aceptar explícitamente el riesgo para las operaciones organizacionales (incluyendo misión, funciones, imagen o reputación), activos organizacionales, individuos, otras organizaciones y la nación.
Confidencialidad	Preservar las restricciones autorizadas sobre el acceso y la divulgación de información, incluyendo medios para proteger la privacidad personal e información propietaria.
Criticidad	Una medida del grado en el que una organización depende de la información o del sistema de información para el éxito de una misión o función comercial.

Concepto	Definición
Disponibilidad	Asegurar el acceso oportuno y confiable a la información y su uso.
Enfoque de evaluación	El enfoque utilizado para evaluar el riesgo y sus factores de contribución, incluyendo cuantitativa, cualitativa o semicuantitativamente.
Entorno de operación	El entorno físico, técnico y organizacional en el que opera un sistema de información, que incluye ―pero que no se limita a― varios factores que influyen en la seguridad y el riesgo del sistema.
Evaluación de amenaza	Proceso de evaluación formal del grado de amenaza a un sistema de información o empresa y descripción de la naturaleza de la amenaza.
Evaluación de vulnerabilidad	Examen sistemático de un sistema de información o producto para determinar la adecuación de las medidas de seguridad, identificar deficiencias de seguridad y predecir la efectividad de las medidas propuestas.
Información	Cualquier comunicación o representación de conocimientos tales como hechos, datos u opiniones en cualquier medio o forma, incluyendo textual, numérico, gráfico, cartográfico, narrativo o audiovisual.
Integridad	Protección contra la modificación o destrucción indebida de la información. Incluye asegurar el no repudio y la autenticidad de la información.
Riesgo de seguridad de la información	El riesgo para las operaciones organizacionales, activos, individuos, otras organizaciones y la nación debido a la posibilidad de acceso, uso, divulgación, interrupción, modificación o destrucción no autorizados de información y/o sistemas de información.
Seguridad de la información	La protección de la información y de los sistemas de información contra el acceso, uso, divulgación, interrupción, modificación o destrucción no autorizado con el fin de proporcionar confidencialidad, integridad y disponibilidad.
Sistema de información	Conjunto discreto de recursos de información organizados para la recolección, procesamiento, mantenimiento, uso, intercambio, difusión o disposición de información.
Tecnología de la información	Cualquier equipo o sistema interconectado o subsistema de equipos utilizado en la adquisición automática, almacenamiento, manipulación, gestión, movimiento, control, visualización, transmisión o recepción de datos o información.
Vulnerabilidad	Debilidad en un sistema de información, procedimientos de seguridad del sistema, controles internos o implementación que podría ser explotada por una fuente de amenaza.

Nota. Adaptado de la NIST 800-30 por NIST, 2012.

2.2 Norma Técnica de Gestión de TI del MICITT

El Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT), en el año 2021, estableció la Norma Técnica para la Gestión y el Control de las Tecnologías de Información, con una dirección más ajustada a la realidad en el entorno tecnológico actual. Esta norma tiene el siguiente alcance:

> Este Marco de Gestión de TI es de acatamiento obligatorio para las instituciones y órganos sujetos a la fiscalización de la Contraloría General de la República, y su inobservancia generará las responsabilidades que correspondan de conformidad con el marco jurídico que resulte aplicable. (MICITT, 2021)

2.2.1 Responsabilidades

La norma establece la responsabilidad de la norma para cada organización de la siguiente manera:

> La responsabilidad de las instancias institucionales en materia de Tecnologías de Información y comunicaciones como ente rector dentro de la organización, es velar por la implementación y seguimiento del Marco de Gestión de TI para la aplicación de sanas prácticas y adecuar su realidad basándose en este documento como referencia. (MICITT, 2021)

En el caso de la Municipalidad de Turrialba, la responsabilidad de cumplir con estos lineamientos recae en el encargado del área de TI. Este profesional es el responsable de liderar y supervisar la implementación del marco de gestión de TI en la municipalidad, asegurando que las prácticas adoptadas no solo cumplan con los estándares establecidos, sino que también estén alineadas con las necesidades operativas y estratégicas de la organización.

2.2.2 Principio de Cumplimiento

Sobre el principio de cumplimiento y la obligatoriedad de la norma, se indica lo siguiente:

> El Marco de Gestión de TI de Gobierno y Gestión de las Tecnologías de Información orienta a la institución en la implementación de buenas prácticas que permiten la adecuada gestión de los procesos requeridos para brindar de forma oportuna y efectiva los servicios brindados a través del uso y administración de los recursos tecnológicos de forma tal que garanticen la continuidad de las operaciones institucionales, la salvaguarda de la información gestionada, la entrega de valor y el cumplimiento normativo. (MICITT, 2021)

Se indica que el proceso de implementación «puede ser progresivo, debidamente planificado, de acuerdo con las prioridades institucionales, criticidad de los procesos y riesgos asociados al uso de recursos tecnológicos y los servicios» (MICITT, 2021).

2.2.3 Perfil del Proceso

La norma técnica, para asegurar que se realiza una adecuada implementación de cada proceso, establece las siguientes características para el perfil:

1. Debe estar formalmente definido a través de la disposición de un objetivo claro y metas específicas, que sean ejecutables, reales, orientadas a resultados y medibles.

2. La propiedad del proceso debe estar claramente establecida en relación con el diseño, interacción con otros procesos, rendición de cuentas de los resultados finales, medición del desempeño e identificación de mejora.

3. Debe estar claramente establecida la secuencia de actividades de forma lógica, consecuente, flexible y escalable, de manera tal que produzca los resultados esperados, considerando el manejo de excepciones y emergencias.

4. Los roles y responsabilidades deben estar exactamente asignados para la ejecución efectiva de las actividades clave y su documentación, además de la rendición de cuentas sobre los entregables finales asociados.

5. Debe disponer de lineamientos y planes debidamente formalizados, revisados, actualizados, aprobados, almacenados, comunicados, publicados y utilizados en forma consecuente, que establezcan las directrices y acciones requeridas. Los lineamientos deben ser accesibles y asegurar el claro entendimiento tanto de los responsables de su aplicación como de las partes interesadas. Los lineamientos se constituyen por:

    - Planes de gestión, de trabajo y de acción que permitan establecer las actividades y tareas para un período específico y el logro de resultados.

    - Políticas y directrices que brinden la información necesaria en el más amplio nivel de detalle sobre las normas y mecanismos que se deben cumplir.

    - Normas que definan los propósitos generales dentro de un marco o política regulatoria, indicando lo que debe hacerse para su cumplimiento de acuerdo con el entorno de gestión y alcances establecidos por la organización.

    - Procedimientos para tareas específicas de tipo operativo-administrativo que indiquen la manera en la que se lleva a cabo una actividad o un proceso. Estos procedimientos deben describir con alto grado de detalle el modo de realizar las actividades principales y la parametrización de los componentes e integrantes del proceso que describen.

    - Estándar técnico, desarrollado como una guía para la configuración de valores, reglas, condiciones o características en los productos de *hardware* y *software* que integran la arquitectura de procesos alcanzados por los requerimientos normativos, regulatorios y legales relacionados con las actividades institucionales.

    - Instructivos, listas de comprobación y formularios, documentación anexa a los procedimientos y que sirven como guía de paso a paso, documento de control y/o registros que presentan resultados obtenidos o proporcionan evidencia de actividades realizadas.

6. Debe contar con indicadores de desempeño que permitan identificar el porcentaje de logro de las metas. Deben establecerse las formas de recopilación de datos asociados y la presentación de los resultados y acciones para tratar las desviaciones según aplique. (MICITT, 2021).

Este perfil lo debe cumplir cada uno de los procesos establecidos por la norma, los cuales son los siguientes:

1. Gobernanza de TI
2. Gestión de TI
3. Planificación tecnológica institucional
4. Gestión de riesgos tecnológicos
5. Arquitectura empresarial
6. Calidad de los procesos tecnológicos
7. Recursos humanos
8. Contratación y adquisiciones de bienes y servicios tecnológicos
9. Gestión de proyectos que implementan recursos tecnológicos
10. Desarrollo, implementación y mantenimiento de sistemas de información
11. Seguridad y ciberseguridad
12. Administración de infraestructura tecnológica
13. Continuidad y disponibilidad operativa de los servicios tecnológicos
14. Aseguramiento

La norma dentro de su glosario define un proceso como la «secuencia de acciones que se llevan a cabo para lograr un fin determinado» (Solís García et al, 2021).

2.2.4 Proceso de Gestión de Riesgos Tecnológicos según la normal del MICITT

El MICITT (2021) define el proceso de gestión de riesgos tecnológicos como:

> Un proceso formal de gestión de riesgos [que la institución debe establecer] que responda a las amenazas que puedan afectar el logro de los objetivos institucionales, basado en una gestión continua de riesgos que esté integrada al sistema específico de valoración del riesgo institucional y considerando el Marco de Gestión de TI que le resulte aplicable.

Establece que la Unidad de TI, «el sector responsable de la administración de los recursos tecnológicos», debe aplicar el marco de gestión de riesgo tecnológico, con el fin de

> Identificar, valorar, priorizar y gestionar los riesgos al nivel de TI en cualquiera de sus escenarios, que impliquen una eventual afectación a la continuidad operacional, así como la integridad y confidencialidad de la información y el cumplimiento regulatorio de la institución. (MICITT, 2021)

La ISO 27005 define el proceso de gestión de riesgos como la «aplicación sistemática de políticas, procedimientos y prácticas de gestión a las actividades de comunicación, consulta, establecimiento del contexto e identificación, análisis, evaluación, tratamiento, seguimiento y revisión del riesgo» (Asociación Española de Normalización, 2024).

2.3 Buenas prácticas internacionales

Las buenas prácticas internacionales proporcionan un marco estructurado para gestionar los riesgos asociados con las tecnologías de la información (TI). Estos marcos son esenciales para asegurar que los procesos de gestión de riesgos estén alineados con los estándares globales, ayudando a las organizaciones a identificar, evaluar, mitigar y monitorear los riesgos de TI de manera efectiva. A continuación, se explora la relación de cuatro de las principales buenas prácticas internacionales con la gestión de riesgos de TI.

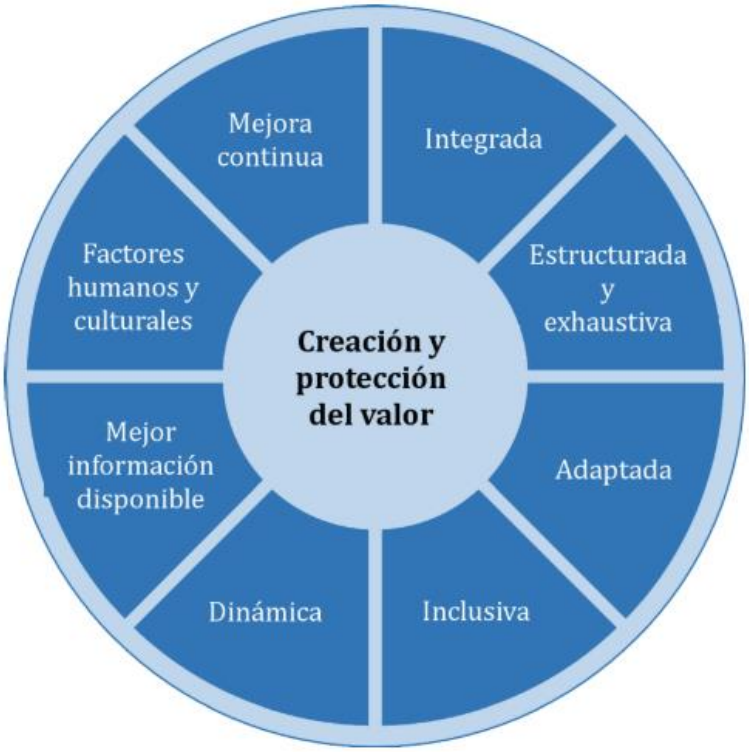
2.3.1 ISO 31000

La UNE-**ISO 31000:2018** es un estándar internacional que ofrece directrices generales para la gestión de riesgos. Aunque no está diseñado específicamente para TI, sus principios y procesos son aplicables a cualquier tipo de riesgo, incluyendo los tecnológicos.

2.3.1.1 Principios.

El propósito de la gestión del riesgo es «la creación y la protección del valor». Por esta razón, se proponen ocho principios que son «el fundamento de la gestión del riesgo y [que] se deberían considerar cuando se establecen el marco de referencia y los procesos de la gestión del riesgo de la organización» (Asociación Española de Normalización, 2018). En la **Figura *5*** se muestran los principios:

Figura 5 *Principios ISO 31000*



Nota. Adaptado de UNE-ISO 31000 Gestión del Riesgo Directrices, 2018.

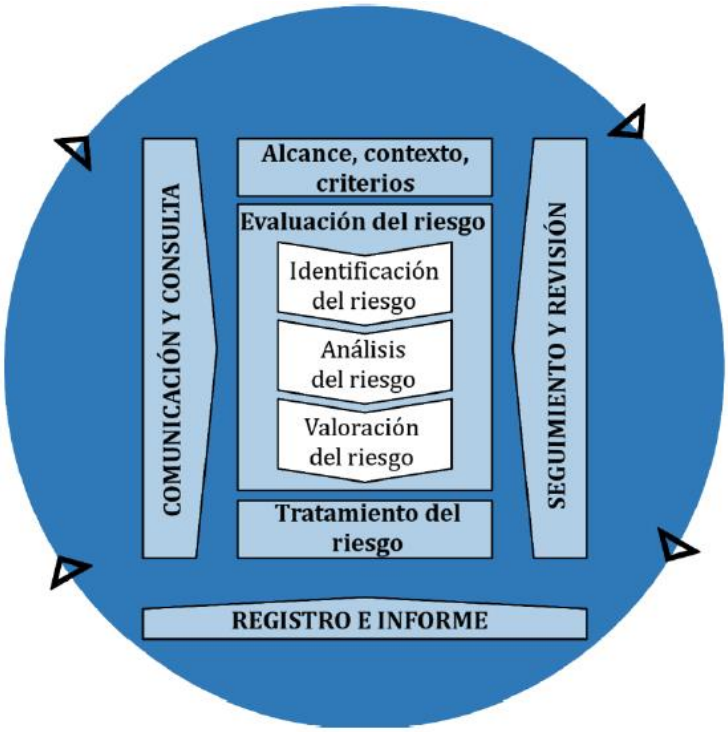
Estos principios se explican a continuación:

a) Integrada: la gestión del riesgo es parte integral de todas las actividades de la organización.
b) Estructurada y exhaustiva: un enfoque estructurado y exhaustivo hacia la gestión del riesgo contribuye a resultados coherentes y comparables.
c) Adaptada: el marco de referencia y el proceso de la gestión del riesgo se adaptan y son proporcionales a los contextos externo e interno de la organización relacionados con sus objetivos.
d) Inclusiva: la participación apropiada y oportuna de las partes interesadas permite que se consideren su conocimiento, puntos de vista y percepciones. Esto resulta en una mayor toma de conciencia y en una gestión del riesgo informada.
e) Dinámica: los riesgos pueden aparecer, cambiar o desaparecer con los cambios de los contextos externo e interno de la organización. La gestión del riesgo anticipa, detecta, reconoce y responde a esos cambios y eventos de una manera apropiada y oportuna.
f) Mejor información disponible: las entradas a la gestión del riesgo se basan en información histórica y actualizada, así como en expectativas. La gestión del riesgo tiene en cuenta explícitamente cualquier limitación e incertidumbre asociada con tal información y expectativas. La información debería ser oportuna, clara y disponible para las partes interesadas pertinentes.
g) Factores humanos y culturales: el comportamiento humano y la cultura influyen considerablemente en todos los aspectos de la gestión del riesgo en todos los niveles y etapas.
h) Mejora continua: la gestión del riesgo mejora continuamente mediante aprendizaje y experiencia.

2.3.1.2 Proceso.

El proceso de la gestión del riesgo implica la aplicación sistemática de políticas, procedimientos y prácticas a las actividades de comunicación y consulta, establecimiento del contexto y evaluación, tratamiento, seguimiento, revisión, registro e informe del riesgo. Este proceso se ilustra en la **Figura *6***.

***Figura* 6** *Proceso de gestión de Riesgo ISO 31000*



Nota. UNE-ISO 31000 Gestión del riesgo Directrices, 2018.

El proceso de la gestión del riesgo, como una parte integral de la gestión y de la toma de decisiones, debe estar integrado por la estructura, las operaciones y los procesos de la organización. Puede aplicarse a nivel estratégico, operacional, de programa o de proyecto. Por otro lado, puede haber muchas aplicaciones del proceso de la gestión del riesgo dentro de la organización, adaptadas para lograr objetivos, y apropiadas a los contextos externo e interno en los cuales se aplican.

2.3.1.2.1 Comunicación y Consulta.

La ISO (2018) establece que el propósito de la comunicación y consulta es asistir a las partes interesadas pertinentes en comprender el riesgo, las bases con las que se toman decisiones y las razones por las que son necesarias acciones específicas. La comunicación y consulta con las partes interesadas apropiadas, externas e internas, se debería realizar en todas y cada una de las etapas del proceso de la gestión del riesgo.

La comunicación y consulta pretende:

- Reunir diferentes áreas de experiencia para cada etapa del proceso de la gestión del riesgo.

- Asegurar que se tomen en cuenta de manera apropiada los diferentes puntos de vista al momento de definir los criterios del riesgo y la valoración de los riesgos.
- Proporcionar suficiente información para facilitar la supervisión del riesgo y la toma de decisiones.
- Construir un sentido de inclusión y propiedad entre las personas afectadas por el riesgo.

2.3.1.2.2 Alcance, Contexto y Criterios.

La ISO (2018) establece que el propósito del establecimiento del alcance, contexto y criterios es adaptar el proceso de la gestión del riesgo para permitir una evaluación del riesgo eficaz y un tratamiento apropiado del riesgo. El alcance, el contexto y los criterios implican la definición del alcance del proceso y la comprensión de los contextos externo e interno.

Como el proceso de la gestión del riesgo puede aplicarse a niveles distintos, es importante tener claro el alcance considerado, los objetivos pertinentes por analizar y su alineamiento con los objetivos de la organización. En la planificación del enfoque se incluyen las siguientes consideraciones:

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

Los contextos externo e interno son el entorno en el cual la organización busca definir y lograr sus objetivos. El contexto del proceso de la gestión del riesgo se debería establecer a partir de la comprensión de los entornos externo e interno en los cuales opera la organización, y debería reflejar el entorno específico de la actividad en la cual se va a aplicar el proceso de la gestión del riesgo. La comprensión del contexto es importante porque:

- La gestión del riesgo tiene lugar en el contexto de los objetivos y las actividades de la organización.
- Los factores organizacionales pueden ser una fuente de riesgo.
- El propósito y alcance del proceso de la gestión del riesgo pueden estar interrelacionados con los objetivos de la organización como un todo.

La organización debería precisar la cantidad y el tipo de riesgo que puede o no puede tomar con relación a los objetivos. También debería definir los criterios para valorar la importancia del riesgo y para apoyar los procesos de toma de decisiones. Para establecer los criterios del riesgo, se debería considerar lo siguiente:

- La naturaleza y los tipos de las incertidumbres que pueden afectar a los resultados y objetivos.
- La manera en la que se definirán y medirán las consecuencias (tanto positivas como negativas) y la probabilidad.

- Los factores relacionados con el tiempo.
- La coherencia en el uso de las mediciones.
- La manera en la que se determinará el nivel de riesgo.
- El modo en el que se tendrán en cuenta las combinaciones y las secuencias de múltiples riesgos.
- La capacidad de la organización.

2.3.1.2.3 Evaluación del Riesgo.

La ISO establece la evaluación del riesgo como «el proceso global de identificación del riesgo, análisis del riesgo y valoración del riesgo» (2018); la evaluación del riesgo se debería llevar a cabo de manera sistemática, iterativa y colaborativa, basándose en el conocimiento y los puntos de vista de las partes interesadas.

Identificación del riesgo: el propósito de la identificación del riesgo es «encontrar, reconocer y describir los riesgos que pueden ayudar o impedir a una organización lograr sus objetivos» (Asociación Española de Normalización, 2018). Se deberían considerar los factores siguientes y la relación entre ellos:

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

La organización debería identificar los riesgos, indiferentemente de si sus fuentes están o no bajo su control. Se debería considerar que puede haber más de un tipo de resultado, que puede dar lugar a una variedad de consecuencias tangibles o intangibles.

Análisis del riesgo: el objetivo del análisis del riesgo es «comprender la naturaleza del riesgo y sus características incluyendo, cuando sea apropiado, el nivel del riesgo» (Asociación Española de Normalización, 2018). El análisis del riesgo implica una consideración detallada de incertidumbres, fuentes de riesgo, consecuencias, probabilidades, eventos, escenarios, controles y su eficacia. Dicho análisis debería considerar factores tales como:

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

- Los niveles de sensibilidad y de confianza

Los resultados proporcionan un entendimiento profundo para tomar decisiones cuando se está eligiendo entre distintas alternativas y las opciones implican diferentes tipos y niveles de riesgo.

Valoración del riesgo: el propósito de la valoración del riesgo es «apoyar a la toma de decisiones» (Asociación Española de Normalización, 2018), lo cual implica comparar los resultados del análisis del riesgo con los criterios del riesgo establecidos para determinar cuándo se requiere una acción adicional. Esto puede conducir a una decisión de:

- No hacer nada más.
- Considerar opciones para el tratamiento del riesgo.
- Realizar un análisis adicional para comprender mejor el riesgo.
- Mantener los controles existentes.
- Reconsiderar los objetivos.

Los resultados de la valoración del riesgo se deberían registrar, comunicar y luego validar a los niveles apropiados de la organización.

2.3.1.2.4 Tratamiento del Riesgo.

La ISO (2018) establece el tratamiento del riesgo como el acto de «seleccionar e implementar opciones para abordar el riesgo». El tratamiento del riesgo implica un proceso iterativo de:

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

La selección de las opciones más apropiadas para el tratamiento del riesgo implica «hacer un balance entre los beneficios potenciales, derivados del logro de los objetivos contra costos, esfuerzo o desventajas de la implementación» (Asociación Española de Normalización, 2018). Las opciones para tratar el riesgo pueden implicar una o más de las siguientes:

- Evitar el riesgo, decidiendo no iniciar o continuar con la actividad que genera el riesgo.
- Aceptar o aumentar el riesgo en busca de una oportunidad.
- Eliminar la fuente de riesgo.
- Modificar la probabilidad.
- Modificar las consecuencias.
- Compartir el riesgo (por ejemplo: a través de contratos, compra de seguros).
- Retener el riesgo con base en una decisión informada.

La selección de las opciones para el tratamiento del riesgo debería realizarse de acuerdo con «los objetivos de la organización, los criterios del riesgo y los recursos disponibles»

(Asociación Española de Normalización, 2018). Al seleccionar opciones para el tratamiento del riesgo, la organización debería considerar los valores, las percepciones, el involucramiento potencial de las partes interesadas y los medios más apropiados para comunicarse con ellas y consultarlas.

2.3.1.2.5 Seguimiento y Revisión.

La ISO (2018) establece el seguimiento y la revisión para «asegurar y mejorar la calidad y la eficacia del diseño, la implementación y los resultados del proceso». El seguimiento continuo y la revisión periódica del proceso de la gestión del riesgo y sus resultados deberían ser dos partes planificadas del proceso de la gestión del riesgo, con responsabilidades claramente definidas.

2.3.1.2.6 Registro e Informe.

La ISO (2018) establece el proceso de la gestión del riesgo y sus resultados como el acto de «documentar e informar a través de los mecanismos apropiados». El registro e informe pretenden:

- Comunicar las actividades de la gestión del riesgo y sus resultados a lo largo de la organización.
- Proporcionar información para la toma de decisiones.
- Mejorar las actividades de la gestión del riesgo.
- Asistir la interacción con las partes interesadas, incluyendo a las personas que tienen la responsabilidad y la obligación de rendir cuentas de las actividades de la gestión del riesgo.

El informe es una parte integral de la gobernanza de la organización y debería mejorar la calidad del diálogo con las partes interesadas, además de brindar apoyo a la alta dirección y a los órganos de supervisión para facilitar el cumplimiento de sus responsabilidades. Los factores que se deben considerar en el informe incluyen:

- Las diferentes partes interesadas, sus necesidades y requisitos específicos de información.
- El costo, la frecuencia y los tiempos del informe.
- El método del informe.
- La pertinencia de la información con respecto a los objetivos de la organización y la toma de decisiones.

2.3.2 NIST 800-30

El NIST 800-30 es una guía clave para la evaluación de riesgos dentro de las organizaciones, desarrollada por el Instituto Nacional de Estándares y Tecnología (NIST). Esta publicación es parte del marco más amplio de gestión de riesgos de seguridad de la información, que abarca tanto las operaciones y los activos organizacionales como a los individuos y la nación en su conjunto (NIST, 2012).

2.3.2.1 Proceso de Evaluación de Riesgos.

La guía NIST 800-30 (NIST, 2012) describe un proceso sistemático para llevar a cabo evaluaciones de riesgos que incluye:

1. **Preparación para la evaluación**: esta fase implica la definición del alcance, el contexto y los criterios que se utilizarán para la evaluación, incluyendo la identificación de las amenazas, las vulnerabilidades y el impacto potencial.

2. **Conducción de la evaluación de riesgos**: se lleva a cabo la identificación de riesgos, análisis y valoración. Esto incluye la identificación de amenazas y vulnerabilidades, la estimación de la probabilidad de ocurrencia y la evaluación del impacto de las amenazas si llegan a materializarse.

3. **Comunicación y compartición de la información de la evaluación de riesgos**: los resultados de la evaluación se comunican a los tomadores de decisiones clave dentro de la organización con el fin de apoyar la gestión de riesgos.

4. **Mantenimiento de la evaluación de riesgos**: las evaluaciones de riesgos no son eventos únicos, sino actividades continuas que deben actualizarse regularmente para reflejar los cambios en el entorno de amenazas, las operaciones y los sistemas.

La NIST 800-30 establece un modelo de riesgo que incluye factores como amenazas, vulnerabilidades, impacto y probabilidad. Estos factores se combinan para determinar el nivel de riesgo (NIST, 2012). La guía permite tanto enfoques cualitativos como cuantitativos para evaluar el riesgo, dependiendo de la información disponible y el contexto de la evaluación. Además, las evaluaciones de riesgos se aplican en diferentes niveles de la organización, desde la misión y los procesos de negocio hasta los sistemas de información específicos.

2.3.3 COBIT 2019

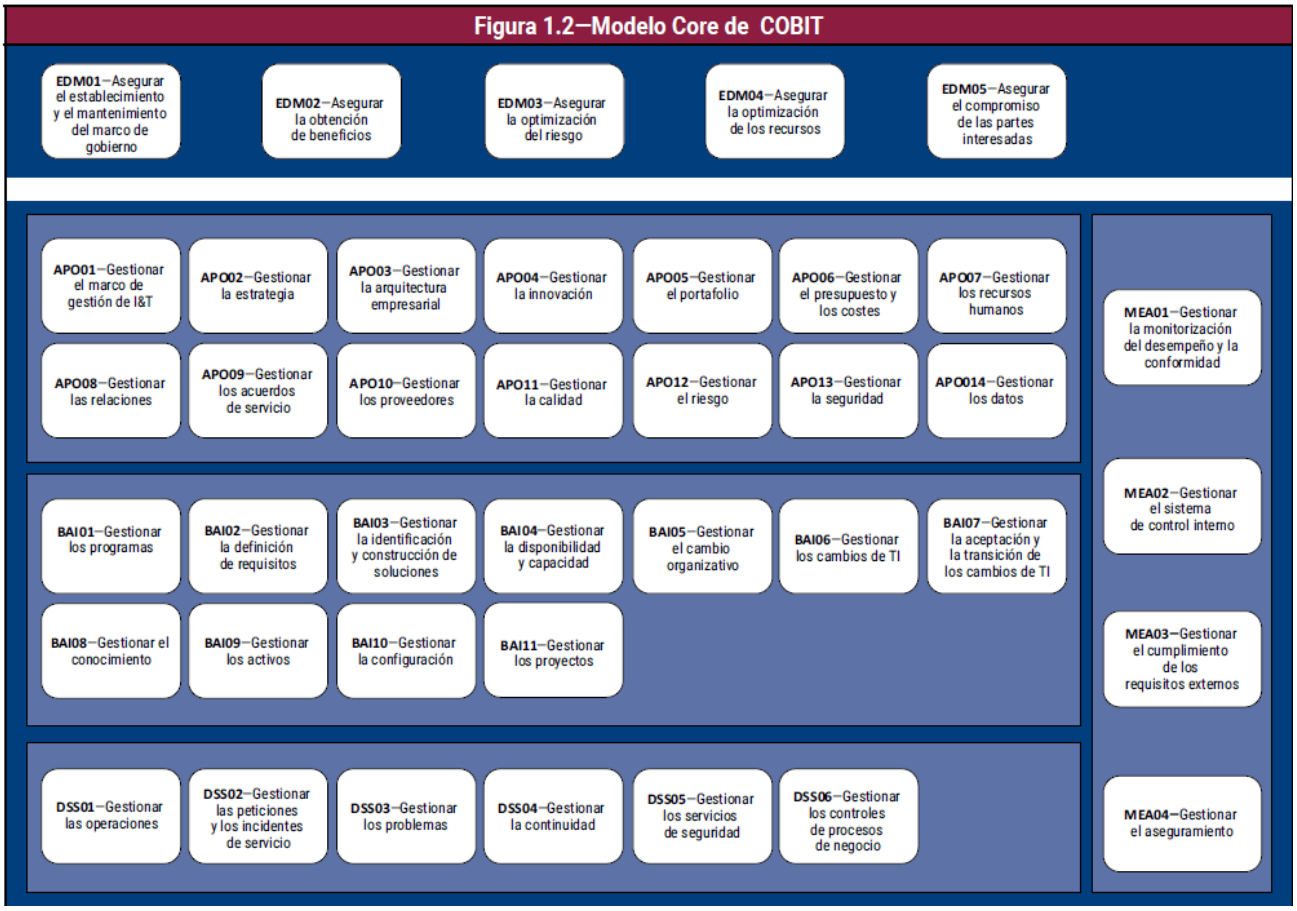
COBIT 2019 Marco De Referencia Objetivos de gobierno y gestión es un marco de gobierno y gestión de TI que proporciona un conjunto integral de herramientas, modelos y prácticas para ayudar a las organizaciones a gestionar y mitigar los riesgos de TI de manera efectiva. Desarrollado por ISACA, COBIT 2019 es ampliamente reconocido por su enfoque en el gobierno de TI y en la alineación de la TI con los objetivos de negocio. COBIT 2019 «incluye 40 objetivos de gobierno y gestión, organizados en cinco dominios» (ISACA, 2018):

- Dominio de gobierno:
    - Evaluar, dirigir y monitorizar (EDM por sus siglas en inglés): el órgano de gobierno evalúa las opciones estratégicas, guía a la alta gerencia con respecto a las opciones estratégicas elegidas y monitoriza el logro de la estrategia.
- Dominios de gestión:
    - Alinear, planificar y organizar (APO): aborda la organización general, la estrategia y las actividades de apoyo para la información y la tecnología (TI).
    - Construir, adquirir e implementar (BAI): se encarga de la definición, adquisición e implementación de soluciones y su integración en los procesos de negocio.

- Entregar, dar servicio y soporte (DSS): aborda la entrega operativa y el soporte de los servicios de información y tecnología (TI), incluida la seguridad.
- Monitorizar, evaluar y valorar (MEA): aborda la monitorización del rendimiento y la conformidad de TI con los objetivos de rendimiento internos, los objetivos de control interno y los requisitos externos.

Estos dominios y sus objetivos se ilustran en la **Figura *7*** Modelo Core de COBIT.

Figura 7 *Modelo Core de COBIT*



Nota. Adaptado de ISACA, 2018.

2.3.3.1 EDM03 - Asegurar la optimización del riesgo

Dentro del dominio evaluar, dirigir y monitorear, se encuentra el EDM03 — Asegurar la optimización del riesgo, el cual se detalla en la **Tabla 2**:

Tabla 2 *EDM03 — Asegurar la optimización del riesgo*

Descripción	Asegurar que el apetito y la tolerancia al riesgo de la empresa se entiendan, articulen y comuniquen, y que se identifique y gestione el riesgo para el valor de negocio relacionado con el uso de TI.
Propósito	Asegurarse de que el riesgo de negocio relacionado con la TI no exceda el apetito y tolerancia al riesgo de la empresa, que se identifique y gestione el impacto del riesgo de TI para el valor de negocio y que se minimicen los posibles fallos de cumplimiento.
Prácticas de gobierno	
EDM03.01 Evaluar la gestión de riesgos.	Examinar y evaluar continuamente el efecto del riesgo sobre el uso actual y futuro de las I&T en la empresa. Considerar si el apetito al riesgo de la empresa es apropiado, y que se identifique y gestione el riesgo para el valor de la empresa relacionado con el uso de I&T.
EDM03.02 Dirigir la gestión de riesgos.	Dirigir el establecimiento de prácticas de gestión de riesgos para ofrecer una seguridad razonable de que las prácticas de gestión de riesgos de I&T son apropiadas y que el riesgo de I&T actual no sobrepasa al apetito al riesgo del consejo de administración.
EDM03.03 Monitorizar la gestión de riesgos.	Monitorizar r las metas y las métricas clave de los procesos de gestión de riesgos. Establecer cómo las desviaciones o los problemas se identificarán, se les dará seguimiento y se comunicarán para su solución.

Nota. Adaptado de ISACA, 2018.

Cada una estas prácticas de gestión, mencionadas en la **Tabla 2** se compone por una serie de actividades. Se asigna un nivel de capacidad a todas las actividades del dominio, permitiendo una clara definición de los procesos con distintos niveles de capacidad. Finalmente, para una mejor comprensión las actividades del EDM03, se encuentran en el Anexo II.

2.3.3.2 APO12 - Gestionar el riesgo

Dentro del dominio alinear, planificar y organizar, se encuentra el APO12-Gestionar el riesgo, el cual se detalla en la **Tabla *3***, con sus seis prácticas de gestión:

Tabla 3 *APO12—Gestionar el riesgo*

Descripción	Identificar, evaluar y reducir continuamente los riesgos relacionados con TI dentro de los niveles de tolerancia establecidos por la gerencia ejecutiva de la empresa.
Propósito	Integrar la gestión del riesgo empresarial relacionado con la TI y con la gestión del riesgo empresarial global (ERM), y equilibrar los costes y beneficios de la gestión del riesgo empresarial relacionado con las TI.

Prácticas de gestión	
APO12.01 Recopilar datos	Identificar y recopilar datos relevantes para habilitar una efectiva identificación, análisis y reporte de los riesgos relacionados con TI.
APO12.02 Analizar el riesgo	Desarrollar una visión fundamentada del riesgo de TI vigente que soporte las decisiones de riesgo.
APO12.03 Mantener un perfil de riesgo	Mantener un inventario de los riesgos conocidos y los atributos de riesgo, incluidos la frecuencia esperada, impacto potencial y respuestas. Documentar los recursos, capacidades y actividades de control actuales relacionados con elementos de riesgo.
APO12.04 Articular el riesgo	Comunicar de manera oportuna información sobre el estado actual de las exposiciones y oportunidades relacionadas con TI a todas las partes interesadas requeridas para obtener una respuesta apropiada.
APO12.05 Definir un portafolio con acciones de gestión de riesgos	Gestionar las oportunidades para reducir el riesgo a un nivel aceptable como un portafolio.
APO12.06 Responder al riesgo	Responder a eventos de riesgo materializados de manera oportuna con medidas eficaces para limitar la magnitud de las pérdidas.

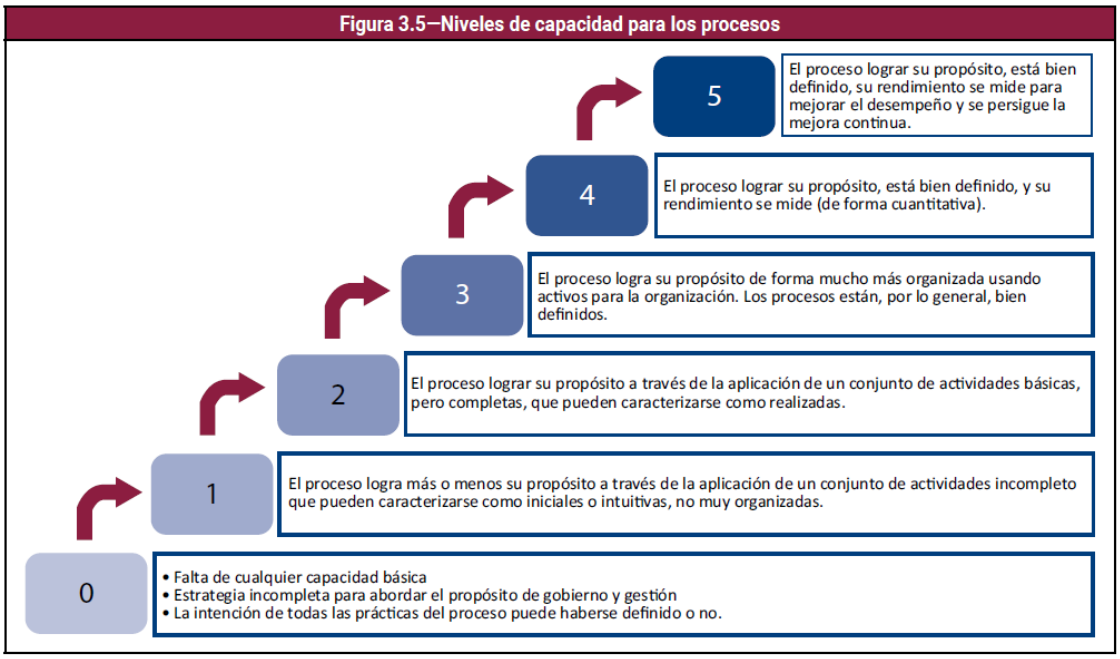
Nota. Adaptado de ISACA, 2018.

Cada una de las practicas mencionadas en la **Tabla *3*** se compone por una serie de actividades. Se asigna un nivel de capacidad a todas las actividades del proceso, permitiendo una clara definición de los procesos con distintos niveles de capacidad. Finalmente, para una mejor comprensión las actividades del APO 12, se encuentra en el Anexo III.

2.3.3.3 Modelo de Madurez de la Capacidad (CMMI®)

Cuando un proceso ejecuta de forma satisfactoria todas las actividades de un nivel, indica que ha alcanzado dicho nivel de capacidad. COBIT 2019 respalda la Integración del Modelo de Madurez de la Capacidad (CMMI®), basado en un esquema de capacidad de los procesos que va de cero a cinco. El nivel de capacidad es «una medida de lo bien que un proceso se ha implementado y funciona» (ISACA, 2018). La **Figura *8*** muestra el modelo, los niveles de capacidad incrementales y las características generales de cada uno.

Figura 8 *Niveles de capacidad para los procesos*



Nota. Adaptado de ISACA, 2018.

Este modelo de niveles de madurez describe cómo los procesos pueden ser evaluados y clasificados en función de su capacidad para cumplir con los objetivos organizacionales. En el esquema, los niveles de capacidad van del cero al cinco, donde:

- **Nivel cero:** indica que no existe capacidad o estrategia clara en el proceso.
- **Nivel uno:** muestra que el proceso tiene algunas actividades básicas, pero es incompleto y poco organizado.
- **Nivel dos:** implica que el proceso está compuesto por actividades completas, aunque aún básicas.
- **Nivel tres:** sugiere que el proceso está bien definido y organizado, utilizando activos que lo hacen útil para la organización.
- **Nivel cuatro:** describe un proceso que no solo está bien definido, sino que también se mide su rendimiento de manera cuantitativa.

- **Nivel cinco:** representa el nivel más alto, donde el proceso está optimizado, mide su rendimiento de manera continua y busca constantemente mejorar el desempeño.

Este modelo permite a las organizaciones evaluar la madurez de sus procesos y determinar en qué nivel se encuentran, lo cual es fundamental para gestionar el desempeño y alinearse con objetivos estratégicos. A medida que una organización avanza por los niveles, mejora la formalidad, efectividad y eficiencia de sus procesos.

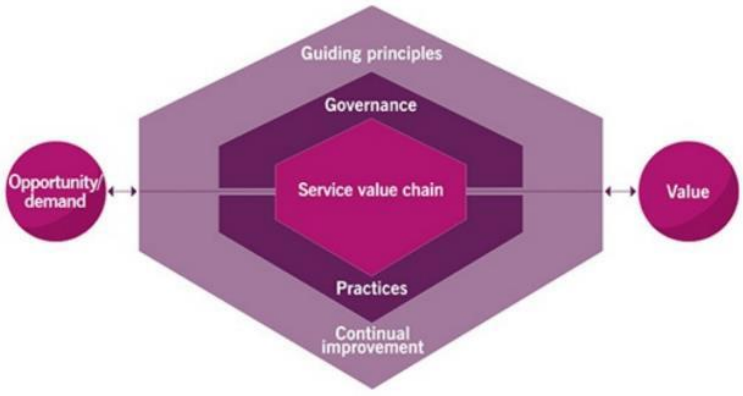
2.3.4 ITIL 4

ITIL® 4 Foundation: IT Infrastructure Library presenta el concepto fundamental de *gestión de servicios*, término que se refiere a un conjunto de capacidades organizacionales que permiten brindar valor a los clientes a través de servicios especializados mediante su sistema de valor de servicio (SVS). Axelos, (2019) explica que:

> La cadena de valor del servicio de ITIL proporciona un modelo operativo para la creación, entrega y mejora continua de servicios. Es un modelo flexible que define seis actividades clave que se combinan de diversas formas, tomando múltiples flujos de valor.

El enfoque innovador que ITIL presenta al crear el sistema de valor del servicio (SVS) supone un cambio significativo en la perspectiva del ciclo de vida del servicio. El principal objetivo del SVS es representar de manera integral todos los componentes, factores y actividades involucrados en la gestión de servicios, con el propósito de favorecer la integración y coordinación de los valores organizacionales. Esta nueva aproximación busca proporcionar una visión más holística y coherente de cómo los servicios se integran en la estructura de la organización y contribuyen a su éxito general. A continuación, se muestra la **Figura *9*** Cadena de Valor del Servicio.

Figura 9 *Cadena de Valor del Servicio*



Nota. Adaptado de Axelos, 2019.

Seguidamente, se detallan los componentes principales del SVS, que se explican en Axelos (2019) en ITIL® 4 Foundation: IT Infrastructure Library:

- Propósito: es el componente central del SVS y establece la razón de ser de la organización de TI. Define la dirección estratégica y los objetivos para entregar valor a los clientes y partes interesadas.

- Gobernanza: es responsable de la toma de decisiones y asegura que las políticas, estrategias y objetivos se cumplan en toda la organización de TI.
- Cadena de valor del servicio: representa las actividades clave involucradas en la creación y entrega de servicios. Estas actividades son planificar, mejorar, diseñar, transaccionar, entregar y apoyar.
- Prácticas de gestión: son conjuntos de actividades organizadas que se emplean para llevar a cabo trabajos o lograr un objetivo particular.
- Resultados: representan los logros obtenidos a través de la aplicación de las prácticas de gestión. Los resultados se dividen en tres dimensiones: resultados de rendimiento, resultados de conformidad y resultados de resistencia.

2.3.4.1 Práctica de Gestión de Riesgos.

Axelos (2019), en el marco de referencia de ITIL® 4 Foundation: IT Infrastructure Library, habla sobre la práctica de gestión de riesgos, la cual tiene como objetivo.

> Garantizar que la organización comprenda y maneje eficazmente los riesgos. La gestión de riesgos es esencial para asegurar la sostenibilidad continua de una organización y crear valor para sus clientes. La gestión de riesgos es una parte integral de todas las actividades organizacionales y, por lo tanto, es central en el SVS de la organización. (Axelos, 2019)

Según Axelos (2019), «el riesgo normalmente se percibe como algo que debe evitarse debido a su asociación con amenazas, y aunque esto generalmente es cierto, el riesgo también está asociado con oportunidades». Según lo anterior, no aprovechar las oportunidades puede ser un riesgo en sí mismo. Los costos de oportunidad de espacios de mercado desatendidos y la demanda no satisfecha son un riesgo que debe evitarse.

Sobre el portafolio de la organización, Axelos indica lo siguiente:

> Puede mapearse a un portafolio subyacente de riesgos que deben ser gestionados. Cuando la gestión de servicios es efectiva, los productos y servicios en el catálogo de servicios y en la línea de desarrollo representan oportunidades para crear y capturar valor para los clientes, la organización y otros interesados. (Axelos, 2019)

En caso de no realizar esta práctica, esos productos y servicios pueden representar amenazas. La implementación de la estrategia a menudo requiere cambios en el portafolio de productos y servicios, lo que significa gestionar los riesgos asociados.

Axelos (2019) indica que para que la gestión de riesgos sea efectiva, los riesgos deben ser:

- **Identificados**: las incertidumbres que afectarían el logro de los objetivos dentro del contexto de una actividad organizacional particular deben considerarse y luego describirse para garantizar que haya un entendimiento común.

- **Evaluados**: se debe estimar la probabilidad, el impacto y la proximidad de los riesgos individuales para que puedan priorizarse y comprenderse el nivel general de riesgo (es decir, exposición al riesgo) asociado con la actividad organizacional.
- **Tratados:** se deben planificar respuestas apropiadas a los riesgos, asignando responsables y ejecutores, y luego implementarlas, monitorearlas y controlarlas.

Los siguientes principios de ITIL se aplican específicamente a la práctica de gestión de riesgos:

- El riesgo es parte del negocio. La organización debe asegurarse de que los riesgos se gestionen adecuadamente; esto no significa que se deban evitar todos los riesgos, por el contrario, asumir riesgos es necesario para garantizar la sostenibilidad a largo plazo. Sin embargo, los riesgos deben ser identificados, comprendidos y evaluados en función de los niveles de riesgo que la organización está dispuesta a asumir (es decir, el apetito de riesgo), y gestionados y monitoreados adecuadamente (Axelos, 2019).
- La gestión de riesgos debe ser coherente en toda la organización. Es vital que la práctica de gestión de riesgos se maneje de manera holística para lograr coherencia en toda la organización. Para asegurar la efectividad, debe haber una consulta continua con los interesados y una flexibilidad adecuada para las diferentes partes de la organización. Esta flexibilidad permitirá el desarrollo de procedimientos de gestión de riesgos personalizados para abordar circunstancias específicas de las unidades organizacionales y/o de los clientes.
- La cultura y los comportamientos en la gestión de riesgos: una cultura y comportamientos adecuados demostrados por todos los niveles del personal de la organización son críticos y deben integrarse como parte de «la forma en que hacemos las cosas». Esto se demostrará mediante comportamientos y creencias como:
    - Comprender que la gestión efectiva de riesgos es vital para la sostenibilidad de la organización y apoya el logro de los objetivos comerciales.
    - Utilizar comportamientos proactivos de gestión de riesgos.
    - Asegurar la transparencia y claridad de los procedimientos de gestión de riesgos, roles, responsabilidades y rendición de cuentas.
    - Fomentar y dar seguimiento activamente a la comunicación de riesgos, incidentes y oportunidades.
    - Asegurar que las estructuras de remuneración apoyen los comportamientos deseados (es decir, esto no debe desalentar la notificación de incidentes ni fomentar la sobre notificación).
    - Fomentar activamente el aprendizaje y el crecimiento en madurez a partir de las experiencias de la organización y las experiencias de otras organizaciones. (Axelos, 2019).

2.3.5 ISO 27005

La UNE-EN ISO 27005 (2024), titulado «Seguridad de la información, ciberseguridad y protección de la privacidad. Guía para la gestión de los riesgos de seguridad de la información» proporciona orientación para ayudar a las organizaciones a hacer frente a los riesgos de seguridad de la información y a realizar actividades de gestión de riesgos de seguridad de la información, específicamente la evaluación y el tratamiento de riesgos de seguridad de la información. Este documento es aplicable a todas las organizaciones, independientemente de su tipo, tamaño o sector.

2.3.5.1 Términos y Definiciones.

La ISO 27005 contempla una serie de términos y definiciones para comprender la norma, los cuales se encuentran en la **Tabla *4*** Conceptos de la ISO 27005:

Tabla 4 *Conceptos de la ISO 27005*

Término	Definición
Aceptación del riesgo	Decisión informada de asumir un determinado riesgo.
Amenaza	Causa potencial de un incidente de seguridad de la información que puede dañar un sistema o perjudicar a una organización.
Análisis de riesgos	Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.
Apetito de riesgo	Cantidad y tipo de riesgo que una organización está dispuesta a perseguir o retener.
Comunicación y consulta de riesgos	Conjunto de procesos continuos e iterativos que una organización lleva a cabo para proporcionar, compartir u obtener información y para entablar un diálogo con las partes interesadas en relación con la gestión de riesgos.
Consecuencia	Resultado de un acontecimiento que afecta a los objetivos.
Contexto externo	Entorno externo en el que la organización pretende alcanzar sus objetivos. El contexto externo puede incluir el entorno social, cultural, político, jurídico, normativo, financiero, tecnológico, económico y geológico, ya sea internacional, nacional, regional o local. También contempla los principales impulsores y tendencias que afectan a los objetivos de la organización, las relaciones, percepciones, valores, necesidades y expectativas de las partes interesadas externas, las relaciones y compromisos contractuales y la complejidad de las redes y dependencias.
Contexto interno	Entorno interno en el que la organización trata de alcanzar sus objetivos.
Criterios de riesgo	Términos de referencia con los que se evalúa la importancia de un riesgo.
Escenario de riesgo	Secuencia o combinación de acontecimientos que conducen de la causa inicial a la consecuencia no deseada.
Evaluación del riesgo	Proceso global de identificación, análisis y evaluación del riesgo.

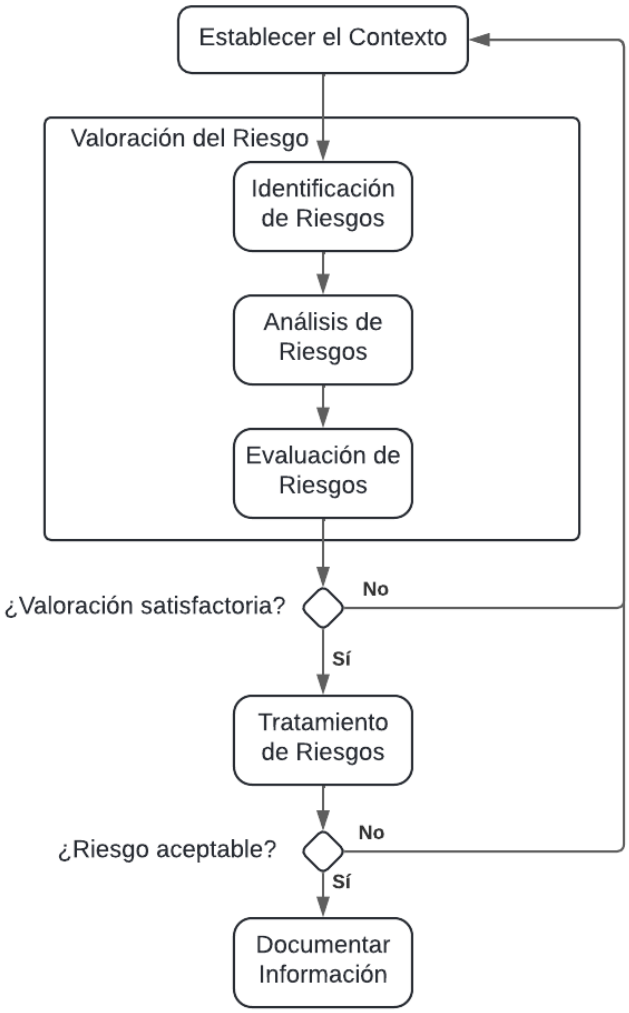
Término	Definición
Evaluación del riesgo	Proceso de comparación de los resultados del análisis del riesgo con los criterios de riesgo para determinar si este y/o su importancia son aceptables o tolerables.
Evento	Ocurrencia o cambio de un conjunto particular de circunstancias.
Fuente de riesgo	Elemento que por sí solo o en combinación tiene el potencial de dar lugar a un riesgo.
Identificación de riesgos	Proceso de búsqueda, reconocimiento y descripción de riesgos.
Incidente de seguridad de la información	Suceso único o serie de sucesos de seguridad de la información no deseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones de la empresa y amenazar la seguridad de la información.
Nivel de riesgo	Importancia de un riesgo, expresada en términos de la combinación de consecuencias y su probabilidad.
Proceso de gestión de riesgos	Aplicación sistemática de políticas, procedimientos y prácticas de gestión a las actividades de comunicación, consulta, establecimiento del contexto, e identificación, análisis, evaluación, tratamiento, seguimiento y revisión del riesgo.
Propietario del riesgo	Persona o entidad con responsabilidad y autoridad para gestionar un riesgo.
Retención del riesgo	Aceptación temporal del beneficio potencial de ganancia o de la carga de pérdida de un riesgo concreto.
Riesgo	Efecto de la incertidumbre sobre los objetivos.
Riesgo compartido	Forma de tratamiento del riesgo que implica la distribución acordada del riesgo con otras partes.
Riesgo residual	Riesgo que permanece tras el tratamiento del riesgo.
Tratamiento del riesgo	Proceso para modificar el riesgo.
Vulnerabilidad	Debilidad de un activo o control que puede ser explotada para que se produzca un evento con consecuencias negativas.

Nota. Adaptado de Asociación Española de Normalización, 2024.

2.3.5.2 Proceso de Gestión de Riesgos para la Seguridad de la Información.

El proceso de gestión de riesgos para la seguridad de la información se presenta el Anexo IV Proceso de gestión de riesgos ISO 27005. Para una comprensión simplificada del proceso, en la **Figura 10**, mediante un diagrama de actividad, se presenta el proceso:

Figura 10 *Proceso de gestión de riesgos para la seguridad de la información*



Nota. Adaptado de la Asociación Española de Normalización, 2024.

Como se muestra en la Figura 10, el proceso de gestión de riesgos para la seguridad de la información puede ser iterativo para las actividades de evaluación y/o tratamiento de riesgos. Establecer el contexto significa reunir el contexto interno y externo para la gestión de riesgos de seguridad de la información o para una evaluación de riesgos de seguridad de la información. Si la evaluación de riesgos proporciona información suficiente para determinar eficazmente las acciones necesarias para modificar los riesgos hasta un nivel aceptable, la tarea se habrá completado y se procederá al tratamiento de los riesgos. Por otro lado, si la información es insuficiente, debe realizarse otra iteración de la evaluación de riesgos. De este modo, el tratamiento del riesgo implica un proceso iterativo de:

- Formulación y selección de opciones de tratamiento del riesgo
- Planificación y aplicación del tratamiento del riesgo
- Evaluación de la eficacia de dicho tratamiento
- Toma de decisiones sobre si el riesgo restante es aceptable
- Adopción de nuevos tratamientos en caso de que no sean aceptables

Hay casos en los que el tratamiento del riesgo no conduce inmediatamente a un nivel aceptable de riesgos residuales; en esta situación, puede realizarse otro intento para encontrar otro tratamiento del riesgo o puede haber otra iteración de la evaluación del riesgo, ya sea en su conjunto o por partes.

2.3.5.3 Establecimiento del Contexto.

La ISO 27005 define una organización como «una persona o grupo de personas que tiene sus propias funciones con responsabilidades, autoridades y relaciones para alcanzar sus objetivos» (Asociación Española de Normalización, 2024). Es importante entender que el apetito de riesgo, definido como la cantidad de riesgo que una organización está dispuesta a perseguir o aceptar, puede variar considerablemente de una organización a otra. La organización debe asegurarse de que el papel del propietario del riesgo se determina en función de las actividades de gestión relativas a los riesgos identificados. Es por esta razón que los propietarios de los riesgos deben tener la responsabilidad y la autoridad adecuadas para gestionar los riesgos identificados.

La evaluación de riesgos debe ayudar a la organización a tomar decisiones sobre la gestión de los riesgos que afectan a la consecución de sus objetivos. Por lo tanto, debe dirigirse a aquellos riesgos y controles que, si se gestionan con éxito, mejorarán la probabilidad de que la organización alcance sus objetivos.

2.3.5.3.1 Criterios de Aceptación de Riesgos.

En la evaluación del riesgo, los criterios de aceptación del riesgo deben «utilizarse para determinar si un riesgo es aceptable o no» (Asociación Española de Normalización, 2024). En el tratamiento del riesgo, los criterios de aceptación del riesgo pueden utilizarse para determinar si el tratamiento del riesgo propuesto es suficiente para alcanzar un nivel de riesgo aceptable o si es necesario un tratamiento adicional del riesgo.

2.3.5.3.2 Criterios para Realizar Evaluaciones de Riesgos para la Seguridad de la Información.

La ISO 27005 especifica que los criterios de evaluación de riesgos se determinan en términos de sus consecuencias, probabilidad y nivel de riesgo. Los criterios de evaluación de riesgos o una base formal para definirlos deben estandarizarse en toda la organización para todos los tipos de evaluación de riesgos, ya que esto puede facilitar la comunicación, comparación y agregación de riesgos asociados con múltiples dominios de negocio.

Los criterios de consecuencia deben desarrollarse y especificarse en términos del alcance del daño o pérdida o bien del perjuicio para una organización o individuo resultante de la pérdida de confidencialidad, integridad y disponibilidad de la información. En la **Tabla *5***, se muestra el ejemplo que brinda la ISO 27005 en relación con la escala de consecuencias.

Tabla 5 *Ejemplo de escala de consecuencias*

Consecuencias	Descripción
1 - Menor	Consecuencias insignificantes para la organización. Sin consecuencias en las operaciones o el desempeño de la actividad o en la seguridad de las personas y la propiedad. La organización superará la situación sin muchas dificultades (se consumirán los márgenes).
2 - Significativo	Consecuencias significativas pero limitadas para la organización. Degradación en el desempeño de la actividad, sin consecuencias en la seguridad de las personas y la propiedad. La organización superará la situación a pesar de algunas dificultades (operación en modo degradado).
3 - Serio	Consecuencias sustanciales para la organización. Alta degradación en el desempeño de la actividad, con posibles consecuencias significativas en la seguridad de las personas y la propiedad. La organización superará la situación con serias dificultades (operación en modo altamente degradado), sin impacto en el sector o en el Estado.
4 - Crítico	Consecuencias desastrosas para la organización. Incapacidad de la organización para asegurar todo o parte de su actividad, con posibles consecuencias graves en la seguridad de las personas y la propiedad. Es poco probable que la organización supere la situación (su supervivencia está amenazada), ya que los sectores de actividad o del Estado en los que opera probablemente se verán ligeramente afectados sin consecuencias duraderas.
5 - Catastrófico	Consecuencias regulatorias o sectoriales más allá de la organización. Ecosistema(s) sectorial(es) sustancialmente impactado(s), con consecuencias que pueden ser duraderas. Y/o: dificultad para el Estado e incluso, una incapacidad para asegurar una función reguladora o una de sus misiones de vital importancia. Y/o: consecuencias críticas en la seguridad de las personas y la propiedad (crisis sanitaria, contaminación ambiental, destrucción de infraestructuras esenciales, etc.).

Nota. Adaptado de la Asociación Española de Normalización, 2024.

La probabilidad puede expresarse en términos probabilísticos (la posibilidad de que se produzca un suceso en un plazo determinado) o frecuentistas (el número medio teórico de ocurrencias en un plazo determinado). La probabilidad expresada en términos relacionados con la frecuencia suele utilizarse cuando se comunica, aunque solo la probabilidad expresada en términos probabilísticos puede utilizarse cuando se realiza la agregación de probabilidades. En la **Tabla *6***, la ISO 27005 brinda el ejemplo de escala de probabilidad:

Tabla 6 *Ejemplo de escala de probabilidad*

Probabilidad	Descripción
1 - Improbable	La fuente de riesgo tiene muy pocas posibilidades de alcanzar su objetivo utilizando uno de los métodos de ataque considerados. La probabilidad es muy baja.
2 - Poco probable	La fuente de riesgo tiene relativamente pocas posibilidades de alcanzar su objetivo utilizando uno de los métodos de ataque considerados. La probabilidad es baja.

Probabilidad	Descripción
3 - Probable	La fuente de riesgo es capaz de alcanzar su objetivo utilizando uno de los métodos de ataque considerados. La probabilidad del escenario de riesgo es significativa.
4 - Muy probable	La fuente de riesgo probablemente alcanzará su objetivo utilizando uno de los métodos de ataque considerados. La probabilidad del escenario de riesgo es alta.
5 - Casi seguro	La fuente de riesgo casi con certeza alcanzará su objetivo utilizando uno de los métodos de ataque considerados. La probabilidad del escenario de riesgo es muy alta.

Nota. Adaptado de la Asociación Española de Normalización, 2024.

El propósito de las escalas para el nivel de riesgo, ejemplificada por la ISO 27005 en la **Tabla *7***, es ayudar a los propietarios del riesgo a decidir sobre la retención o el tratamiento de los riesgos y a priorizarlos para su tratamiento. La organización debe elaborar una clasificación de los riesgos teniendo en cuenta lo siguiente:

- Los criterios de consecuencia y probabilidad.
- Las consecuencias que los eventos de seguridad de la información pueden tener a nivel estratégico, táctico y operativo (esto puede definirse como el peor de los casos o, en otros términos, siempre que se utilice la misma base de forma coherente).
- Requisitos legales y reglamentarios y obligaciones contractuales.
- Los riesgos que aparecen más allá de los límites del ámbito de la organización, incluidos los efectos imprevistos sobre terceros.

***Tabla* 7** *Ejemplo de enfoque cualitativo de los criterios de riesgo*

Probabilidad	Consecuencia				
	Catastrófico	**Crítico**	**Serio**	**Significativo**	**Menor**
Casi seguro	Muy alto	Muy alto	Alto	Alto	Medio
Muy probable	Muy alto	Alto	Alto	Medio	Bajo
Probable	Alto	Alto	Medio	Bajo	Bajo
Poco probable	Medio	Medio	Bajo	Bajo	Muy bajo
Improbable	Bajo	Bajo	Bajo	Muy bajo	Muy bajo

Nota. Adaptado de la Asociación Española de Normalización, 2024.

2.3.5.4 Proceso de Valoración de Riesgos para la Seguridad de la Información.

La organización debe utilizar el proceso de valoración de riesgos de la organización para definir un proceso de evaluación de riesgos para la seguridad de la información, según lo indica la ISO 27005. La valoración de riesgos consta de las siguientes actividades:

Identificación del riesgo: definido como «el proceso de encontrar, reconocer y describir los riesgos. Esto implica la identificación de fuentes y eventos de riesgo» (Asociación Española de Normalización, 2024). El objetivo de la identificación de riesgos es generar una lista de riesgos basada en aquellos sucesos que pueden impedir, afectar o retrasar la consecución de los objetivos

de seguridad de la información. Los riesgos identificados deben ser aquellos que si se materializan pueden tener un efecto sobre la consecución de los objetivos.

Análisis de riesgos: es un proceso para cada riesgo identificado, que se solicita que «se base en la evaluación de las consecuencias derivadas del riesgo y en la evaluación de la probabilidad del riesgo para determinar un nivel de riesgo» (Asociación Española de Normalización, 2024). Las técnicas de análisis de riesgos basadas en las consecuencias y la probabilidad pueden ser:

- Cualitativas, utilizando una escala de atributos calificativos (alto, medio, bajo).
- Cuantitativas, utilizando una escala con valores numéricos.
- Semicuantitativos, utilizando escalas cualitativas con valores asignados.

El análisis de riesgos debe centrarse en aquellos riesgos y controles que, si se gestionan con éxito, mejoran la probabilidad de que la organización alcance sus objetivos.

Evaluación del riesgo: una vez identificados los riesgos y analizados, las organizaciones deben «aplicar sus criterios de aceptación de riesgos para determinar si pueden aceptarse o no; si no se pueden aceptar, se debe dar prioridad a su tratamiento» (Asociación Española de Normalización, 2024). Para evaluar los riesgos, las organizaciones deben comparar los riesgos evaluados con los criterios de riesgo definidos durante el establecimiento del contexto.

2.3.5.4.1 Ejemplo del Proceso de Valoración de Riesgos.

Para entender mejor el proceso de valoración de riesgos, consideremos una entidad gubernamental local encargada de gestionar los servicios básicos de una comunidad de tamaño medio. Esta entidad maneja una gran cantidad de datos sensibles, como información personal de los ciudadanos, registros financieros y proyectos de desarrollo.

El primer paso es la identificación de los riesgos. se identificó una serie de riesgos basados en aquellos sucesos que pueden impedir, afectar o retrasar los servicios de la entidad, los cuales fueron enlistados sin un orden particular:

- Pérdida o corrupción de datos: mediante incendios, inundaciones, fallas en los sistemas de almacenamiento o errores humanos al manipular datos.
- Acceso no autorizado: por ataques cibernéticos (*phishing* o *malware)*, empleados descontentos o contratistas externos sin los permisos adecuados.
- Interrupción de los servicios: por fallas en el suministro eléctrico, ataques de denegación de servicio (DDoS) o errores en la configuración de los sistemas.
- Pérdida de la confidencialidad de la información: debido a divulgación accidental de datos personales, espionaje industrial o robo de dispositivos móviles.
- Incumplimiento de normativas: por el no cumplimiento de leyes de protección de datos, sanciones económicas y pérdida de reputación.

El segundo paso es el análisis de riesgos basado en las consecuencias y la probabilidad. Utilizando las escalas cualitativas de ejemplo de la **Tabla *5*** y **Tabla *6***, se analizaron los riesgos listados en el paso anterior y se muestran en la Tabla 8.

Tabla 8 *Ejemplo de Análisis de Riesgos*

ID	Riesgo	Consecuencias	Probabilidad	Nivel de Riesgo
R-01	Pérdida o corrupción de datos	Crítico	Probable	**Alto**
R-02	Acceso no autorizado	Crítico	Muy probable	**Alto**
R-03	Interrupción de los servicios	Serio	Probable	**Medio**
R-04	Pérdida de la confidencialidad de la información	Crítico	Probable	**Alto**
R-05	Incumplimiento de normativas	Crítico	Poco probable	**Medio**

En el tercer paso, una vez identificados los riesgos y analizados, la entidad debe aplicar sus criterios de aceptación de riesgos para determinar si pueden aceptarlos o no; si no se pueden aceptar, se debe pasar a su tratamiento. Dentro del contexto de la entidad, se definió que los riesgos con un nivel de riesgo igual o inferior a *bajo* son riesgos aceptables.

De acuerdo con el análisis, los cinco riesgos identificados tienen un nivel de riesgo *medio* o *alto*, por lo que todos deben ser tratados con prioridad según su nivel de riesgo. El tratamiento puede incluir la implementación de controles adicionales, políticas de seguridad o la adopción de medidas correctivas para mitigar estos riesgos.

2.3.5.5 Proceso de Tratamiento de Riesgos para la Seguridad de la Información.

La ISO 27005 plantea diversas opciones de tratamiento del riesgo:

- Evitar el riesgo: se decide no iniciar o continuar con la actividad que da lugar al riesgo.
- Modificar el riesgo: se cambia la probabilidad de que se produzca un suceso o una consecuencia o se cambia la gravedad de la consecuencia.
- Retener el riesgo: mediante una elección informada.
- Compartir el riesgo: se reparten las responsabilidades con otras partes, ya sea interna o externamente.

Cada riesgo que necesite un tratamiento debe ser tratado en uno de los planes de tratamiento de riesgos. Una organización puede optar por tener varios planes de tratamiento de riesgos que en conjunto implementen todos los aspectos requeridos del tratamiento de riesgos. Estos planes pueden organizarse en función del lugar en el que reside la información, por activos o por eventos.

2.3.5.5.1 Ejemplo del proceso de tratamiento de riesgos.

En la **Tabla *9*** se detalla una propuesta de tratamiento para cada riesgo identificado en el ejemplo anterior, considerando las distintas opciones que ofrece la ISO 27005.

Tabla 9 *Ejemplo del proceso de tratamiento de riesgos*

ID	Riesgo	Tratamiento	Acciones
R-01	Pérdida o corrupción de datos	Modificar el riesgo	Mejorar la infraestructura de almacenamiento implementando sistemas de respaldo automatizados y redundantes, como copias de seguridad en la nube y fuera de las instalaciones. Capacitar a los empleados en la manipulación adecuada de los datos, minimizando así el riesgo de errores humanos. Establecer planes de contingencia que incluyan simulacros, para asegurarse que los sistemas de recuperación de datos funcionen correctamente en caso de desastre (incendios e inundaciones).
R-02	Acceso no autorizado	Modificar el riesgo	Implementar autenticación multifactor (MFA) en todos los sistemas que manejen datos sensibles. Actualizar y fortalecer las políticas de acceso, limitando estrictamente los permisos según los roles de cada empleado, y realizar auditorías periódicas de los accesos a los sistemas. Organizar talleres de concienciación para que el personal sea capaz de identificar y prevenir ataques de *phishing* o *malware*.
R-04	Pérdida de la confidencialidad de la información	Modificar el riesgo	Aplicar cifrado de extremo a extremo a todos los datos sensibles que se almacenan y transmiten. Establecer controles físicos y digitales para evitar el robo de dispositivos móviles, como políticas de uso de dispositivos personales, y asegurarse de que toda la información se borre de forma segura en los dispositivos que ya no estén en uso. Un monitoreo constante del sistema para detectar brechas o intentos de acceso no autorizado en tiempo real es crucial.

ID	Riesgo	Tratamiento	Acciones
R-03	Interrupción de los servicios	Compartir el riesgo	Externalizar ciertos servicios de infraestructura crítica a proveedores especializados que garanticen alta disponibilidad y tiempos de respuesta rápidos en caso de fallos. Negociar contratos de nivel de servicio (SLA) con proveedores de servicios tecnológicos que aseguren la continuidad de operaciones ante caídas o ataques, como DDoS. Contar con planes de continuidad del negocio bien definidos, respaldados por acuerdos con empresas de servicios esenciales.
R-05	Incumplimiento de normativas	Modificar el riesgo	Cumplir con todas las leyes de protección de datos, como la Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales. Implementar un proceso continuo de auditorías y revisiones legales, asegurándose de que las políticas internas y los sistemas tecnológicos se alineen con las normativas. La creación de un equipo de cumplimiento normativo que supervise y actualice regularmente las políticas y procedimientos será clave para evitar sanciones y mejorar la reputación de la organización.

2.3.5.6 Operación.

El proceso de evaluación de riesgos para la seguridad de la información «debe integrarse en las operaciones de la organización y debe realizarse a intervalos planificados o cuando se propongan o se produzcan cambios significativos» (Asociación Española de Normalización, 2024). A la hora de planificar las evaluaciones rutinarias de riesgos, las organizaciones deben tener en cuenta cualquier calendario que se aplique a sus procesos empresariales generales y a los ciclos presupuestarios asociados.

2.3.5.6.1 Ejemplo de Operación.

Integrar el proceso de evaluación de riesgos para la seguridad de la información en las operaciones diarias de una organización requiere una planificación estratégica que vincule este proceso con las actividades clave y los ciclos de la organización. A continuación, se presentan algunas ideas para integrar el riesgo y sus dimensiones en el proceso operativo de la entidad gubernamental mencionada en el ejemplo anterior:

- Vinculación con los ciclos de planificación presupuestaria
    - El proceso de evaluación de riesgos puede planificarse en función del ciclo presupuestario anual de la organización. Antes de aprobar presupuestos, se realizarían evaluaciones de riesgos para identificar posibles inversiones necesarias en infraestructura tecnológica, formación de personal o soluciones de seguridad.
    - Los riesgos con niveles mayores a *bajo* pueden ser priorizados durante la planificación presupuestaria para asignar fondos de forma eficiente. Esto puede incluir la actualización de sistemas de respaldo de datos (R-01), la implementación de autenticación multifactor (R-02) o la contratación de servicios externos para garantizar la continuidad del negocio (R-03).
- Evaluaciones periódicas integradas en el ciclo operativo
    - Las evaluaciones rutinarias de riesgos deben alinearse con los ciclos operativos de la organización, como revisiones trimestrales o semestrales de desempeño.
    - El proceso de evaluación de riesgos debe activarse automáticamente tras cambios importantes, como la implementación de un nuevo sistema de gestión de datos, la expansión de servicios a nuevos ciudadanos o el uso de proveedores externos para servicios críticos.
- Integración con procesos de gestión de proyectos
    - Cualquier proyecto de tecnología, como la implementación de nuevas plataformas o la actualización de infraestructura, debe incluir una evaluación de riesgos como parte de su fase inicial. Esto garantiza que los proyectos consideren aspectos como la seguridad, disponibilidad y confidencialidad de los datos desde el principio (R-01, R-02).
    - Los sistemas operativos y tecnológicos implementados deben tener un seguimiento continuo del riesgo a lo largo de su ciclo de vida. Esto permite que cualquier fallo o vulnerabilidad emergente sea gestionado en tiempo real, minimizando el impacto en los servicios.
- Evaluaciones de riesgos relacionadas con cumplimiento normativo
    - Las evaluaciones de riesgo deben planificarse en línea con las auditorías de cumplimiento normativo, asegurando que las obligaciones legales estén integradas en las operaciones diarias. Cualquier incumplimiento normativo identificado (R-05) deberá generar acciones correctivas.
    - Las organizaciones deben establecer un calendario de revisiones de las normativas vigentes y cómo estas impactan las operaciones. Esto permitirá anticipar cambios en las leyes y ajustar los controles de seguridad a tiempo.
- Capacitación continua del personal
    - Dado que muchos riesgos están relacionados con errores humanos (R-01) o accesos no autorizados (R-02), las evaluaciones de riesgos deben incluir capacitaciones regulares para empleados. Estas deben alinearse con los ciclos operativos y presupuestarios de la organización para que todo el personal esté actualizado en medidas preventivas.

Los planes de tratamiento del riesgo deben incluir simulacros anuales de incidentes de seguridad, como ataques cibernéticos o desastres naturales, para evaluar la capacidad de respuesta de la organización y ajustar los controles según sea necesario.

2.3.6 ISO 9001

Esta Norma Internacional se basa en los principios de la gestión de la calidad descritos en la Norma ISO 9000. Las descripciones incluyen una declaración de cada principio, una base racional de por qué el principio es importante para la organización, algunos ejemplos de los beneficios asociados con el principio y ejemplos de acciones típicas para mejorar el desempeño de la organización cuando se aplique el principio. Estos son enfoque al cliente, liderazgo, compromiso de las personas, enfoque a procesos, mejora, toma de decisiones basada en la evidencia y gestión de las relaciones (Asociación Española de Normalización, 2015).

El enfoque a procesos implica la definición y gestión sistemática de los procesos y sus interacciones, con el fin de alcanzar los resultados previstos de acuerdo con la política de la calidad y la dirección estratégica de la organización. La gestión de los procesos y el sistema en su conjunto puede alcanzarse utilizando el ciclo PHVA con un enfoque global de pensamiento basado en riesgos dirigido a aprovechar las oportunidades y prevenir resultados no deseados. (Asociación Española de Normalización, 2015).

El ciclo PHVA puede describirse brevemente como sigue:

- Planificar: establecer los objetivos del sistema y sus procesos, y los recursos necesarios para generar y proporcionar resultados de acuerdo con los requisitos del cliente y las políticas de la organización, e identificar y abordar los riesgos y las oportunidades;
- Hacer: implementar lo planificado;
- Verificar: realizar el seguimiento y la medición de los procesos y los productos y servicios resultantes respecto a las políticas, los objetivos, los requisitos y las actividades planificadas, e informar sobre los resultados;
- Actuar: tomar acciones para mejorar el desempeño, cuando sea necesario.

El pensamiento basado en riesgos es esencial para lograr un sistema de gestión de la calidad eficaz. El concepto de pensamiento basado en riesgos ha estado implícito en ediciones anteriores de esta Norma Internacional, incluyendo, por ejemplo, llevar a cabo acciones preventivas para eliminar no conformidades potenciales, analizar cualquier no conformidad que ocurra, y tomar acciones que sean apropiadas para los efectos de la no conformidad para prevenir su recurrencia. (Asociación Española de Normalización, 2015).

2.3.6.1 Política

La ISO 9001 (Asociación Española de Normalización, 2015), indica que la alta dirección debe establecer, implementar y mantener una política de la calidad que:

a) sea apropiada al propósito y contexto de la organización y apoye su dirección estratégica;
b) proporcione un marco de referencia para el establecimiento de los objetivos de la calidad;
c) incluya un compromiso de cumplir los requisitos aplicables;
d) incluya un compromiso de mejora continua del sistema de gestión de la calidad.
e) estar disponible y mantenerse como información documentada;
f) comunicarse, entenderse y aplicarse dentro de la organización;
g) estar disponible para las partes interesadas pertinentes, según corresponda.

2.3.6.1.1 Roles, Responsabilidades y Autoridades en la Organización

La ISO 9001 (Asociación Española de Normalización, 2015), indica que la alta dirección debe asegurarse de que las responsabilidades y autoridades para los roles pertinentes se asignen, se comuniquen y se entiendan en toda la organización. La alta dirección debe asignar la responsabilidad y autoridad para:

a) asegurarse de que el sistema de gestión de la calidad es conforme con los requisitos de esta Norma Internacional;
b) asegurarse de que los procesos están generando y proporcionando las salidas previstas;
c) informar, en particular, a la alta dirección sobre el desempeño del sistema de gestión de la calidad y sobre las oportunidades de mejora;
d) asegurarse de que se promueve el enfoque al cliente en toda la organización;
e) asegurarse de que la integridad del sistema de gestión de la calidad se mantiene cuando se planifican e implementan cambios en el sistema de gestión de la calidad.

2.3.6.2 No conformidad y acción correctiva

La ISO 9001 (Asociación Española de Normalización, 2015), indica que cuando ocurra una no conformidad, incluida cualquiera originada por quejas, la organización debe:

a) reaccionar ante la no conformidad y, cuando sea aplicable: tomar acciones para controlarla y corregirla o hacer frente a las consecuencias;
b) b) evaluar la necesidad de acciones para eliminar las causas de la no conformidad, con el fin de que no vuelva a ocurrir ni ocurra en otra parte, mediante: la revisión y el análisis de la no conformidad; la determinación de las causas de la no conformidad; y la determinación de si existen no conformidades similares, o que potencialmente puedan ocurrir;
c) implementar cualquier acción necesaria;
d) revisar la eficacia de cualquier acción correctiva tomada;
e) si fuera necesario, actualizar los riesgos y oportunidades determinados durante la planificación;
f) y si fuera necesario, hacer cambios al sistema de gestión de la calidad. Las acciones correctivas deben ser apropiadas a los efectos de las no conformidades encontradas.

g) La organización debe conservar información documentada como evidencia de la naturaleza de las no conformidades y cualquier acción tomada posteriormente; y los resultados de cualquier acción correctiva.

2.4 Procesos de Negocio

Los procesos de negocio son una serie de actividades o tareas interrelacionadas que, en conjunto, producen un servicio o producto que cumple con los objetivos de la organización. En el contexto de la gestión de riesgos de TI, los procesos de negocio bien definidos y gestionados son esenciales para garantizar que las operaciones de TI se realicen de manera eficiente, segura y alineada con los objetivos estratégicos de la organización (Dumas et al., 2018).

2.4.1 Business Process Management

La administración de procesos de negocios (*business process management* o BPM por sus siglas en inglés) es un enfoque de gestión que se centra en alinear todos los aspectos de una organización con los deseos y necesidades de los clientes. El BPM promueve la eficiencia organizacional a través de la mejora continua de los procesos de negocio, utilizando un ciclo de modelado, ejecución, monitoreo y optimización (Dumas et al., 2018).

El BPM, como señalan Dumas et al. (2018), tiene como objetivo mejorar la eficiencia y eficacia operativa de una organización mediante la automatización y optimización de sus procesos. Esta disciplina se enfoca en identificar, diseñar, implementar, monitorear y mejorar continuamente los procesos de negocio para alcanzar los objetivos empresariales.

El BPM se ha consolidado como una herramienta clave en la gestión de recursos y activos, ya que permite a las empresas optimizar sus operaciones internas (Dumas y La Rosa, 2018). Además, ofrece un enfoque estructurado, promoviendo flujos de trabajo bien definidos y una mejora continua.

2.4.2 Procesos BPM

Según Bizagi (2024), un proceso se refiere a un «grupo de acciones y pasos ejecutados para lograr un objetivo particular. En BPMN, un proceso contiene todas las formas o elementos de modelado, que cumplen la lógica para lograr el objetivo». Esta por esta razón que el desarrollo del presente proyecto utilizará la Notación de Gestión de Procesos de Negocio (BPMN 2.0), la cual define las pautas para el modelado de procesos que se acepta como la norma en la industria.

Con el fin de obtener un mayor entendimiento la notación del marco de referencia BPMN 2.0, se utiliza el Anexo I, en donde Bizagi muestra todos los elementos necesarios para el modelo de procesos y una definición de cada uno de dichos componentes.

El BPMN busca generar la representación gráfica del proceso tanto en su estado actual (as-is) como en su estado rediseñado (to-be), y apoyar en la identificación de problemas dentro del proceso. El uso de esta metodología ofrece diversas ventajas al personal de la organización, tales como claridad y comunicación, así como el alineamiento empresarial.

Proceso as-is (Estado Actual): Se refiere al modelo que representa cómo se ejecuta el proceso actualmente dentro de la organización. Este modelo proporciona una visión detallada de la situación actual, incluyendo todos los pasos, actividades y flujos que forman parte del proceso. El análisis del proceso as-is permite identificar ineficiencias, cuellos de botella, y áreas de mejora en la operación actual.

Proceso to-be (Estado Futuro): Representa el modelo del proceso una vez que ha sido optimizado o rediseñado. Este diagrama describe la manera en la que se espera que el proceso funcione después de la implementación de mejoras o cambios propuestos. El objetivo del proceso to-be es establecer una estructura más eficiente y alineada con las metas estratégicas de la organización, buscando mejorar la productividad, reducir costos y optimizar el uso de recursos.

Claridad y Comunicación: BPMN ofrece un lenguaje gráfico estándar y altamente comprensible que facilita la comunicación entre diferentes partes interesadas. Los símbolos y elementos visuales utilizados en BPMN permiten representar de manera clara y precisa las etapas, actividades, flujos y decisiones en un proceso, lo que ayuda a evitar malentendidos y ambigüedades en la interpretación de los procesos.

Alineación con la Lógica Empresarial: BPMN permite capturar no solo la secuencia de actividades, sino también la lógica y las condiciones que guían el flujo del proceso. Esto garantiza que el diagrama refleje con precisión las reglas y requerimientos del negocio, lo que contribuye a una implementación más acorde con la realidad operativa y reduce la posibilidad de errores.

Documentación Integral: Utilizar BPMN para diagramar procesos brinda la ventaja de crear una documentación detallada y completa de los flujos de trabajo empresariales. Esta documentación actúa como un recurso valioso para el aprendizaje organizacional, la formación de nuevos empleados y la comprensión general de cómo se llevan a cabo las operaciones. Además, proporciona un punto de referencia sólido para la revisión, la auditoría y la mejora continua de los procesos a lo largo del tiempo.

3 Marco Metodológico

El capítulo presenta información sobre el tipo de investigación seleccionado, el enfoque adoptado, el alcance del estudio, el diseño utilizado, las fuentes de información consultadas, los sujetos y variables de investigación; así como las técnicas empleadas para la recolección de datos. Además, se describen las diferentes etapas que conformaron el proceso de investigación establecido para el trabajo de graduación.

3.1 Tipo de Investigación

Según Hernández et al. (2014), «la investigación es un conjunto de procesos sistemáticos, críticos y empíricos que se aplican al estudio de un fenómeno o problema». En el ámbito de la investigación, existen diversos enfoques que permiten abordar los problemas desde distintas perspectivas: cuantitativo, cualitativo y mixto.

Enfoque cuantitativo: este enfoque, definido por Hernández et al. (2014), es secuencial y probatorio. Parte de una idea que se va delimitando progresivamente, estableciendo objetivos y preguntas de investigación claras. Para su elaboración, se revisa la literatura existente, se construye un marco teórico y se derivan hipótesis que se pretenden probar. Además, se determinan variables, se traza un diseño para probar las hipótesis, se recolectan y miden datos en un contexto específico, y se analizan estos datos utilizando métodos estadísticos para extraer conclusiones.

Enfoque cualitativo: en este enfoque, las preguntas de investigación y las hipótesis pueden desarrollarse antes, durante o después de la recolección y el análisis de los datos (Hernández et al., 2014). Dicho enfoque es más flexible y dinámico, lo cual permite que la acción indagatoria se mueva entre los hechos y su interpretación de manera circular. La secuencia de actividades no es fija, sino que varía según las necesidades del estudio y permite una mayor adaptabilidad al contexto y a los datos emergentes.

Enfoque mixto: este enfoque combina elementos de los enfoques anteriores: cuantitativo y cualitativo. Se utiliza cuando es necesario integrar métodos de recolección y análisis de datos cuantitativos y cualitativos para proporcionar una comprensión más completa del fenómeno estudiado. De este modo, permite aprovechar las fortalezas de ambos enfoques y compensar sus debilidades.

Para el desarrollo de este Trabajo Final de Graduación sobre la gestión de riesgos de TI en la Municipalidad de Turrialba, se emplea un enfoque **cualitativo**. Este enfoque es el más adecuado debido a que el proyecto requiere una comprensión profunda y contextualizada de los riesgos de TI específicos de la municipalidad. El enfoque cualitativo permite explorar detalladamente los distintos riesgos, sus causas y posibles consecuencias, así como seleccionar las metodologías de gestión de riesgos más apropiadas y adaptadas al entorno particular de la municipalidad. Además, este enfoque facilita el análisis de la norma técnica del MICITT y las mejores prácticas internacionales, asegura que el marco propuesto sea efectivo y relevante para las necesidades y circunstancias específicas de la organización.

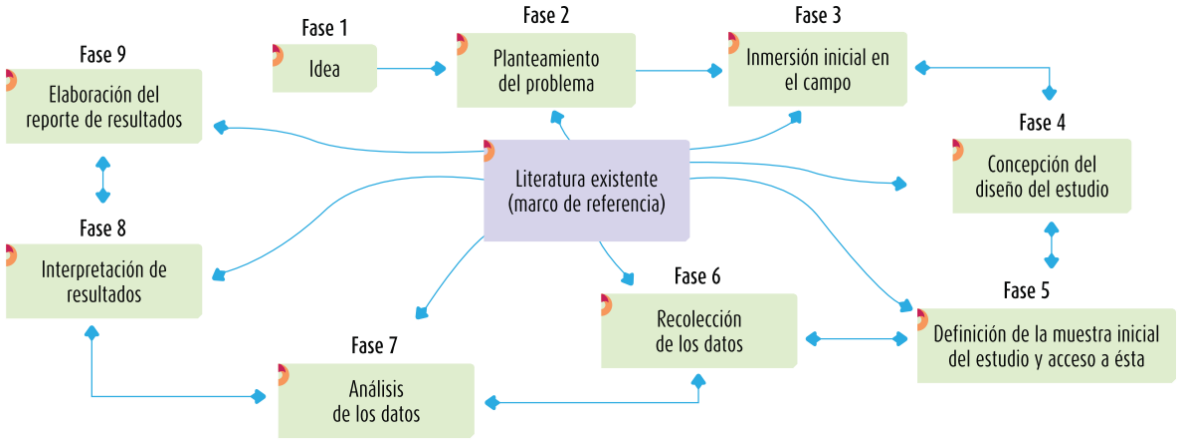
3.2 Enfoque y Diseño de la Investigación

Para el desarrollo del presente proyecto se ha seleccionado un enfoque cualitativo. A continuación, se describe el enfoque seleccionado y los diferentes diseños de investigación considerados, más la justificación de la elección del diseño específico para este proyecto.

3.2.1 Enfoque Cualitativo

El enfoque cualitativo se centra en la comprensión profunda y contextualizada de los fenómenos estudiados, a diferencia del enfoque cuantitativo, que busca medir variables y probar hipótesis de manera secuencial y probatoria. Hernández et al. (2014) representan el proceso cualitativo como se muestra en la Figura 11.

Figura 11 *Proceso cualitativo*



Nota. Adaptado de *Metodología de la investigación*, por Hernández et al., 2014.

Para comprender la Figura 11, Hernández et al. (2014) señalan los siguientes puntos:

a) Revisión de la literatura: aunque hay una revisión inicial de la literatura, esta puede retomarse en cualquier etapa del estudio, con lo cual apoya desde el planteamiento del problema hasta la elaboración del reporte de resultados. La vinculación entre la teoría y las etapas del proceso se representa con flechas curvadas.
b) Regreso a etapas previas: en la investigación cualitativa, a veces es necesario regresar a etapas anteriores. Por eso las flechas de las fases que van desde la inmersión inicial en el campo hasta el reporte de resultados son bidireccionales.
c) Inmersión inicial en el campo: implica sensibilizarse con el entorno del estudio, identificar informantes clave y verificar la factibilidad del estudio.
d) Simultaneidad de fases: en el proceso cualitativo, la muestra, la recolección y el análisis de datos se realizan prácticamente de manera simultánea. Además, el enfoque cualitativo tiene las siguientes características:
    - Planteamiento del problema: el investigador plantea un problema, pero no sigue un proceso definido claramente. Las preguntas de investigación pueden desarrollarse durante el estudio.

- Desarrollo de teoría: en lugar de iniciar con una teoría para probar con datos, el investigador examina los hechos y desarrolla una teoría basada en los resultados observados, siguiendo un proceso inductivo.
- Generación de hipótesis: en la mayoría de los estudios cualitativos no se prueban hipótesis desde el inicio, sino que estas se generan y perfeccionan durante el proceso.
- Métodos de recolección: la recolección de datos no es completamente estandarizada ni predeterminada. Esta consiste en obtener las perspectivas y puntos de vista de los participantes, incluyendo sus emociones, experiencias y significados. Se enfoca en las interacciones entre individuos y grupos, utilizando métodos como entrevistas abiertas y observaciones no estructuradas.
- Empatía y doble perspectiva: el investigador empatiza con los participantes y mantiene una doble perspectiva, analizando tanto los aspectos explícitos como los implícitos de las experiencias de los participantes.
- Observación de procesos: observa los procesos sociales sin alterarlos, percibiéndolos tal como los actores los experimentan.
- Manejo de complejidades: es capaz de manejar paradojas, incertidumbres, dilemas éticos y ambigüedades, y reconoce sus propias tendencias personales, enfocándose en las vivencias de los participantes tal como fueron sentidas y experimentadas.

3.2.2 Diseño de la Investigación

En el siguiente apartado se define el diseño de la presente investigación, para lo cual se utilizarán los diseños de investigación definidos por Hernández et al. (2014). Estos diseños tienen cinco perspectivas o abordajes diferentes. A continuación, se describen cada uno de ellos según lo indicado por los autores:

- Teoría fundamentada: este diseño se encarga de explicar el proceso o fenómeno de investigación. Se utiliza para conocer objetos de estudio como procesos, acciones o interacciones entre individuos. Su objetivo principal es desarrollar una teoría basada en los datos recopilados durante la investigación.
- Etnográfico: el diseño etnográfico busca estudiar un sistema social como un todo, con el fin de brindar descripciones y justificaciones de la composición de elementos y grupos dentro de la estructura social en cuestión. Se centra en la comprensión profunda de la cultura y de las prácticas de un grupo específico.
- Narrativo: este diseño pretende definir el objeto de estudio alrededor de una o más personas y sus biografías o contemplar varios relatos de un evento. Se utiliza para explorar y narrar experiencias individuales, proporcionando una visión detallada y personal de los fenómenos estudiados.
- Fenomenológico: el diseño fenomenológico se encarga de estudiar individuos que hayan compartido una experiencia o fenómeno de estudio. Su objetivo es comprender cómo las

personas perciben y experimentan un determinado fenómeno desde su perspectiva subjetiva.

- Investigación/acción: su finalidad es comprender y resolver problemáticas específicas de una colectividad vinculadas a un ambiente particular. Su principio fundamental es influir en el cambio y, como resultado, incorporarlo al propio proceso de investigación. Este diseño se caracteriza por la colaboración activa entre el investigador y los participantes, y por su enfoque en la aplicación práctica de los hallazgos para mejorar la situación estudiada.

La selección del diseño de investigación cuantitativo para el desarrollo del presente proyecto se basa en el abordaje investigación/acción que, de acuerdo con Hernández et al. (2014), está respaldado por la capacidad inherente de identificar y abordar problemas prácticos que sean contextualmente relevantes, como la gestión insuficiente del proceso de gestión de vulnerabilidades.

La finalidad de la investigación-acción, explican Hernández et al. (2014), es comprender y resolver problemáticas específicas de una colectividad vinculadas a un ambiente, como la problemática que tiene la Municipalidad de Turrialba, frecuentemente aplicando la teoría y mejores prácticas de acuerdo con el planteamiento. Asimismo, se centra en aportar información que guíe la toma de decisiones para proyectos, procesos y reformas estructurales que, en el caso de este proyecto, giran en torno al proceso de gestión de riesgos de TI.

Este abordaje tiene tres fases esenciales: observar (construir un árbol del problema y recolectar datos), pensar (analizar e interpretar los datos recolectados) y actuar (resolver la problemática observada). Estas etapas se dan de manera cíclica, una y otra vez, hasta que la totalidad del problema es resuelto (Hernández et al., 2014).

3.3 Fuentes de Datos e Información

Existe variedad de fuentes de datos e información que generan ideas de investigación, tales como materiales escritos, información disponible en Internet, conversaciones personales, observación de hechos, experiencias individuales, entre otros (Hernández et al., 2014). Así mismo, los autores Hernández et al. (2014) brinda una clasificación para las fuentes de información en dos categorías:

- Fuentes de información viva: personas que no son parte de la muestra, pero que suministran información en una investigación de campo.
- Fuentes de información documentales: son documentos impresos, digitales, audiovisuales o de audio que están autorizados o validados.

3.3.1 Fuentes Primarias

Las fuentes primarias corresponden a todas las fuentes de datos e información de primera mano, dado que incorporan resultados de los estudios correspondientes (Hernández et al., 2014). Las fuentes de información primaria que se usan en el documento son publicaciones académicas, libros, marcos de referencia y otros medios que contengan esta información. En la Tabla 10 Fuentes primarias se visualizan las fuentes primarias que serán utilizadas en este proyecto.

Tabla 10 *Fuentes primarias*

Documento	Tipo de documento	Importancia del documento para la investigación
Normas técnicas para la gestión y el control de las tecnologías de Información	Directrices de políticas	Proporcionan los requerimientos y las directrices esenciales para garantizar que las prácticas de gestión y control de TI, incluyendo el proceso de gestión de riesgos de TI para que se alineen con la norma técnica del MICITT.
Políticas de seguridad en materia de tecnologías de información y comunicación TICS de la Municipalidad de Turrialba	Directrices de políticas	Este documento presenta en forma clara y coherente los elementos que conforman la política de seguridad que debe conocer y cumplir la gerencia municipal (alcalde y Concejo Municipal), directores, jefes de departamento, colaboradores en general, funcionarios contratistas y terceros que presten sus servicios o tengan algún tipo de relación con el Departamento de Tecnologías de Información de la Municipalidad de Turrialba.
Marco de Referencia COBIT® 2019: objetivos de gobierno y gestión	Marco de referencia	Es crucial para seleccionar los enfoques y metodologías más adecuados para la gestión de riesgos de TI, ya que ofrece un marco integral para la gobernanza y gestión de TI que se puede adaptar al contexto específico de la Municipalidad de Turrialba.
Portafolio de riesgos de la Normativa Tecnologías De La Información – MICITT.	Portafolio de riesgos	Este documento identifica y clasifica posibles riesgos de TI que pueden afectar la seguridad, la eficiencia y el cumplimiento normativo, proporcionando una referencia para el análisis y clasificación de riesgos de la Municipalidad de Turrialba.

Documento	Tipo de documento	Importancia del documento para la investigación
ITIL Foundation 4	Marco de referencia	Proporciona un marco de mejores prácticas para la gestión de servicios de TI, ayudando a seleccionar y justificar las metodologías de gestión de riesgos que mejor se alinean con las necesidades operativas y estratégicas de la municipalidad.
UNE-ISO 31000 Gestión del Riesgo Directrices	Buenas prácticas de la industria	Ofrece directrices esenciales para diseñar un marco de gestión de riesgos de TI robusto y efectivo, asegurando que se incluyan todas las etapas, desde la identificación hasta el tratamiento de riesgos.
UNE-EN ISO/IEC 27005:2024 Seguridad de la información, ciberseguridad y protección de la privacidad. Guía para la gestión de los riesgos de seguridad de la información	Buenas prácticas de la industria	Proporciona directrices sobre la gestión de riesgos de seguridad de la información. Esta norma apoya el proceso de implementación de un sistema de gestión de seguridad de la información (SGSI) basado en la ISO/IEC 27001. Se centra específicamente en el análisis y gestión de riesgos que pueden comprometer la confidencialidad, integridad y disponibilidad de la información.
NIST 800-30: Guide for Conducting Risk Assessments	Buenas prácticas de la industria	Proporciona un enfoque estandarizado y detallado para la evaluación de riesgos, que es crucial para realizar un análisis exhaustivo de los riesgos de TI y diseñar un marco de gestión de riesgos bien fundamentado y específico para la Municipalidad de Turrialba.
Fundamentals of Business Process Management	Marco de referencia	El documento permite dar una perspectiva holística, que se centra en la eficiencia, la calidad y la mejora continua en las operaciones organizacionales.
Instrumentos de investigación	Instrumentos de investigación	Las herramientas de investigación son fundamentales: son los dispositivos y procedimientos que se emplean para recopilar datos y conocer los detalles pertinentes sobre el problema que está investigando.

3.3.2 Fuentes secundarias

Corresponde a las fuentes que «contienen información primaria, sintetizada y reorganizada, las cuales facilitan el acceso a las fuentes de datos primarias» (Soberón y Acosta, 2008). En la **Tabla *11*** Fuentes Secundarias es posible visualizar las fuentes secundarias utilizadas.

Tabla 11 *Fuentes Secundarias*

Documento	Tipo de documento	Importancia del documento para la investigación
Repositorio Académicos TEC	Tesis universitarias y Trabajos Finales de Graduación	Proporciona acceso a trabajos académicos previos y materiales de referencia que aseguran que el documento cumpla con los estándares y contenidos requeridos para un Trabajo de Fin de Grado.
Sitios web con artículos y revistas tecnológicas	Artículos	Ofrecen información actualizada sobre las tendencias, innovaciones y desarrollos más recientes en ciberseguridad y gestión de vulnerabilidades, lo cual es esencial para abordar los riesgos de TI de manera efectiva y con una perspectiva actualizada.

3.4 Sujetos de Investigación

Los sujetos de investigación son definidos por Mata (2021) como aquellos grupos de personas que son parte del colectivo en el que sus opiniones, características o experiencias cobran interés para las investigaciones. En la **Tabla *12*** se muestran los sujetos de investigación, las características e importancia del sujeto en el presente trabajo.

Tabla 12 *Sujetos de investigación*

Rol del sujeto	Tiempo en el Rol	Caracterización del sujeto	Justificación de la importancia de este sujeto para su investigación
Encargado del Área de Servicios Informáticos	10 años.	- Responsable de todas las funciones relacionadas con las tecnologías de información (TI) dentro de la Municipalidad de Turrialba. - Gestiona y supervisa los servicios y procesos de TI, incluyendo la infraestructura, sistemas, seguridad y cumplimiento normativo. - Coordina y colabora con otros departamentos para garantizar la eficiencia y seguridad de los sistemas de información municipales.	La importancia de este sujeto radica en su posición central en la gestión de las tecnologías de información dentro de la Municipalidad de Turrialba. Como responsable de todas las funciones de TI, tiene un conocimiento exhaustivo de los riesgos, procesos y necesidades de seguridad de la información en la organización. Su participación es fundamental para comprender los desafíos específicos y las necesidades de gestión de riesgos de TI en la municipalidad.

Rol del sujeto	Tiempo en el Rol	Caracterización del sujeto	Justificación de la importancia de este sujeto para su investigación
Miembro de la Comisión de Control Interno	4 años.	- Participa en la identificación, análisis y mitigación de riesgos dentro de la municipalidad. - Colabora en la elaboración de políticas y procedimientos relacionados con la gestión de riesgos. - Representa a diversas áreas de la municipalidad en el proceso de toma de decisiones sobre la gestión de riesgos.	Este sujeto es clave para la investigación porque su rol en el consejo de gestión de riesgos le proporciona una visión integral de los riesgos que enfrenta la municipalidad, incluyendo aquellos relacionados con las tecnologías de información. Su participación es crucial para validar y adaptar las políticas de seguridad y gestión de riesgos de TI al contexto específico de la organización.

3.5 Variables o Categorías de la Investigación

Hernández (2014) resalta que las variables representan una característica que puede cambiar en magnitud y cuya alteración posible cuantificar y observar. Por lo tanto, las variables que son utilizadas para esta investigación son especificadas en la Tabla 13 Cuadro de variables de investigación.

Tabla 13 *Cuadro de variables de investigación*

Objetivo especifico	Nombre de la variable	Concepto	Indicador	Instrumento
Objetivo 1: Analizar la situación actual del proceso de gestión de amenazas de TI en la Municipalidad de Turrialba.	Responsables del proceso	Identificación de los roles responsables en la gestión de amenazas de TI.	- Cantidad de personas responsables identificadas - Claridad en la asignación de responsabilidades	Entrevistas
	Documentación del proceso	Estado y disponibilidad de la documentación relacionada con el proceso actual de gestión de amenazas.	- Existencia de documentos actualizados - Accesibilidad de la documentación	Revisión documental y entrevistas
	Tareas o actividades del proceso existente	Actividades que se realizan en el proceso actual de gestión de amenazas de TI.	- Número de actividades manuales	Revisión documental, entrevistas, cuestionario

Objetivo especifico	Nombre de la variable	Concepto	Indicador	Instrumento
Objetivo 2: Diseñar un marco de gestión de riesgos de TI basado en la norma técnica del MICITT y las mejores prácticas.	Tareas o actividades que requieren el proceso formal de gestión de riesgos	Actividades y tareas necesarias para la implementación del proceso formal de gestión de riesgos.	- Cantidad de actividades requeridas. - Nivel de capacidad de las actividades - Listado de riesgos - Escala de consecuencias - Escala de probabilidad - Tratamientos	Revisión documental, entrevistas
	Responsables del proceso formal de gestión de riesgos	Identificación de los roles y responsabilidades dentro del nuevo proceso formal.	- Cantidad de responsables identificados	Entrevistas y revisión documental
	Documentación requerida para el proceso formal	Documentos necesarios para implementar el marco formal de gestión de riesgos de TI.	- Número de documentos requeridos - Estado de preparación de la documentación	Revisión documental y entrevistas
Objetivo 3: Verificar la conformidad del proceso de gestión de riesgos de TI con la norma técnica del MICITT.	Tareas o actividades que cumple el proceso formal	Actividades del proceso formal de gestión de riesgos alineadas con los requisitos del MICITT.	- Porcentaje de actividades que cumplen con los requisitos del MICITT	Lista de comprobación, revisión documental
	Fortalezas del proceso	Aspectos positivos del proceso formal que contribuyen a la gestión efectiva de riesgos.	- Número de fortalezas identificadas - Impacto positivo en la gestión de riesgos	Revisión documental
	Oportunidades de mejora del proceso	Áreas dentro del proceso formal que se pueden optimizar o mejorar.	- Número de oportunidades de mejora identificadas - Impacto potencial de las mejoras	Revisión documental

Objetivo especifico	Nombre de la variable	Concepto	Indicador	Instrumento
	Limitaciones del proceso	Factores que limitan la efectividad del proceso formal de gestión de riesgos.	- Número de limitaciones identificadas - Impacto de las limitaciones en el proceso	Revisión documental
	Amenazas que posee el proceso	Riesgos o amenazas que pueden afectar el éxito del proceso formal de gestión de riesgos de TI.	- Número de amenazas identificadas - Probabilidad de que se materialicen	Revisión documental

3.6 Técnicas e Instrumentos de Recolección de Datos

La siguiente sección permite definir los instrumentos de recolección de datos que se utilizarán para el desarrollo del presente proyecto de graduación. Estas herramientas se consideran los medios a través de los cuales se obtendrá la información requerida, que servirá como materia prima para llevar a cabo un análisis pertinente a la situación problemática de la organización.

Hernández et al. (2014) explican que la «recolección de datos cualitativos es el acopio de datos narrativos en los ambientes naturales y cotidianos de los participantes o unidades de muestreo». La **Tabla 14** proporciona una descripción detallada de cada uno de los instrumentos que serán empleados en el proceso.

Tabla 14 *Instrumentos de recolección de datos*

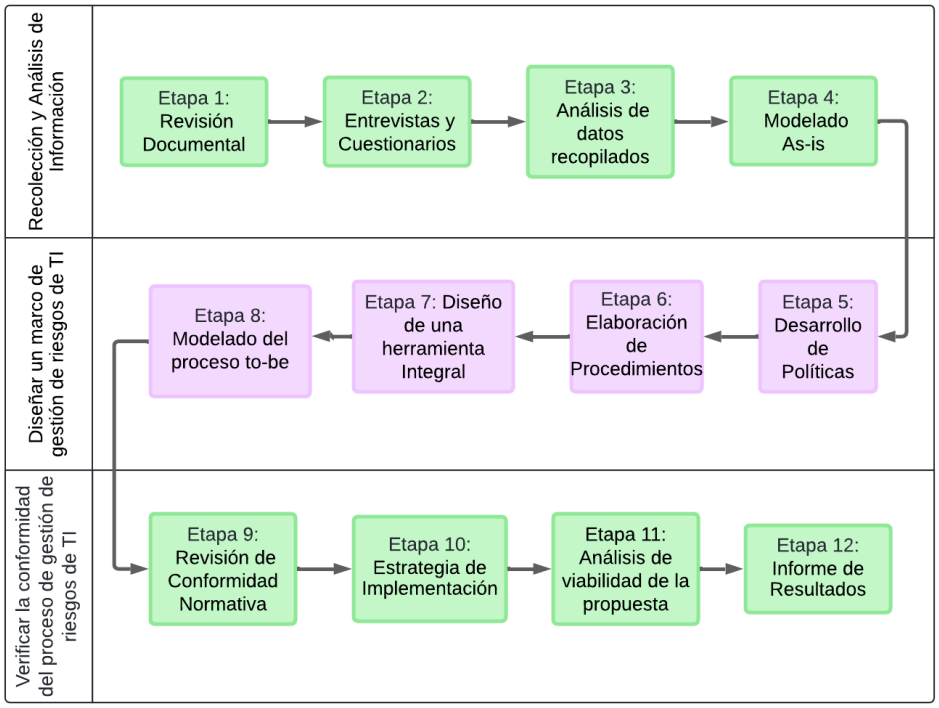
Instrumento	Justificación del uso del instrumento	Apéndice
Revisión documental	La revisión documental es esencial para entender el contexto fundamental del tema de estudio. Este tipo de análisis es útil para conocer los orígenes de un contexto, las experiencias previas y las circunstancias actuales, y cómo estos factores influyen en su funcionamiento tanto diario como excepcional (Hernández et al., 2014).	Apéndice F Bitácora Revisión Documental
Entrevista	Las entrevistas cualitativas permiten explorar experiencias individuales, perspectivas, valores, creencias, emociones, sentimientos, hechos concretos, narrativas de vida y otras dimensiones subjetivas y contextuales, proporcionando una comprensión profunda y matizada del tema de estudio (Hernández et al., 2014).	Apéndice G Entrevista Situación Actual Apéndice H Entrevista Miembro Comisión de Control Interno

Instrumento	Justificación del uso del instrumento	Apéndice
Cuestionario	El uso de cuestionarios facilita la recolección de datos estructurados y cuantificables de un grupo más amplio de participantes. Es un instrumento eficaz para obtener información específica sobre actitudes, opiniones y conocimientos relacionados con la gestión de riesgos de TI dentro de la organización (Hernández et al., 2014).	Apéndice I Cuestionario Situación Actual
Lista de comprobación	La lista de comprobación es una herramienta práctica que permite verificar de manera sistemática la presencia o ausencia de elementos clave durante la revisión de procesos o la implementación de normativas. Es útil para asegurar que todos los aspectos críticos del proceso de gestión de riesgos de TI estén alineados con los estándares establecidos (Hernández et al., 2014).	Apéndice K Plantilla Lista de Comprobación del Proceso de Gestión de Riesgos

3.7 Procedimiento Metodológico de la Investigación

En esta sección se desglosan las distintas etapas que se llevan a cabo para alcanzar el cumplimiento del objetivo general del proyecto. En conformidad con lo expuesto en la sección del alcance, estas etapas están estrechamente vinculadas con los objetivos específicos. La Figura 12 permite visualizar cada objetivo y las etapas que se engloban y alinean con el proceso de investigación para la solución del presente trabajo de graduación.

Figura 12 *Fases de la metodología del proyecto*



3.7.1 Fase 1: Recolección y Análisis de Información

Objetivo: Analizar la situación actual del proceso de gestión de amenazas de TI en la Municipalidad de Turrialba.

3.7.1.1 Etapa 1: Revisión Documental.

Se lleva a cabo una recolección de documentos internos que describan los procesos actuales relacionados con la gestión de riesgos de TI. Esta etapa es crucial para entender cómo la municipalidad aborda la gestión de amenazas tecnológicas y para establecer una base para el análisis. Los documentos son recopilados desde las bases de datos internas, archivos físicos y digitales, y se asegura que estén completos y actualizados.

3.7.1.2 Etapa 2: Entrevistas y Cuestionarios.

Se lleva a cabo entrevistas semiestructuradas y se aplicarán cuestionarios a los encargados del área de servicios de TI y al personal relevante. Esto permite obtener una comprensión detallada sobre la manera de gestionar las amenazas tecnológicas en la práctica. Se analizan las respuestas para identificar patrones, puntos críticos y discrepancias con las prácticas documentadas.

3.7.1.3 Etapa 3: Análisis de Datos Recopilados.

Los datos obtenidos son analizados para identificar fortalezas, debilidades y oportunidades de mejora en el proceso actual de gestión de amenazas de TI. Se compararán los hallazgos con las mejores prácticas de la industria y los requisitos normativos para identificar áreas de mejora. Finalmente, se sintetizan los resultados para crear un panorama claro del estado actual del proceso de gestión de amenazas.

3.7.1.4 Etapa 4: Modelado as-is.

Se desarrolla un modelo as-is que representa el proceso actual de gestión de riesgos de TI en la municipalidad. Este modelo ayuda a visualizar el flujo actual de actividades y a identificar las brechas con respecto a las mejores prácticas. Se utilizan los datos recopilados para construir un diagrama detallado del proceso existente que muestre las etapas del proceso, los flujos de información y los puntos de control.

3.7.2 Fase 2: Diseño del Marco de Gestión de Riesgos de TI

Objetivo: Diseñar un marco de gestión de riesgos de TI alineado con la norma técnica del MICITT y las mejores prácticas de la industria.

3.7.2.1 Etapa 5: Desarrollo de Políticas de Gestión de Riesgos de TI.

Se definen políticas claras que establezcan los principios y directrices generales para la gestión de riesgos de TI. Se estudian la norma técnica del MICITT y las mejores prácticas como COBIT 2019, ITIL 4, UNE-ISO 31000 y NIST 800-30, a partir de las cuales se redactan las políticas que definen los roles y responsabilidades, los criterios de identificación y evaluación de riesgos, y las directrices para el tratamiento de riesgos.

3.7.2.2 Etapa 6: Elaboración de Procedimientos de Gestión de Riesgos de TI.

Se elaboran procedimientos detallados que describen cómo se deben implementar las políticas definidas. Estos procedimientos especifican los pasos operativos para cada actividad de gestión de riesgos. Se detallan, además, los pasos para la identificación, evaluación, priorización y tratamiento de riesgos. También se incluirán procedimientos para el monitoreo y revisión continua. Y, por último, se documentarán los procedimientos en un formato accesible y comprensible para todos los miembros del personal de TI.

3.7.2.3 Etapa 7: Diseño del Herramienta Integral de Gestión de Riesgos.

Se desarrolla una Herramienta Integral que incluya mecanismos de monitoreo y seguimiento de riesgos. Por otro lado, se desarrolla un plan de comunicación que garantice que todas las partes interesadas estén informadas sobre el estado de los riesgos y las medidas de mitigación. Para finalizar, se desarrolla una matriz de riesgos que permita la visualización y el seguimiento continuo de los riesgos identificados.

3.7.2.4 Etapa 8: Modelado del proceso to-be

Se diseña un modelo detallado que representa cómo debería funcionar el proceso formal de gestión de riesgos de TI después de implementar el marco propuesto. Este modelo incluye los flujos de trabajo optimizados, las actividades específicas y los responsables asignados. El modelo to-be se presenta mediante un diagrama BPMN y descripciones textuales que permiten una visualización clara del proceso mejorado.

3.7.3 Fase 3: Verificación de Conformidad

Objetivo: Verificar la conformidad del marco propuesto con la norma técnica del MICITT.

3.7.3.1 Etapa 9: Revisión de Conformidad Normativa.

Se realiza una revisión exhaustiva para asegurar que el marco de gestión de riesgos cumple con los requisitos de la Norma Técnica del MICITT, utilizando una lista de comprobación con las actividades del proceso de gestión de riesgos de TI de la norma.

3.7.3.2 Etapa 10: Estrategia de Implementación

Se diseña una estrategia para implementar el marco de gestión de riesgos en la Municipalidad de Turrialba, asegurando una transición ordenada y eficiente desde el modelo actual (as-is) al modelo propuesto (to-be). Esta estrategia incluye un cronograma de implementación y recursos necesarios.

3.7.3.3 Etapa 11: Análisis de viabilidad de la propuesta

Se lleva a cabo un análisis costo-beneficio que evalúa los recursos requeridos frente a los beneficios esperados al implementar el marco de gestión de riesgos de TI. Este análisis incluye estimaciones financieras detalladas de los costos de implementación y mantenimiento, así como los beneficios relacionados con la mitigación de riesgos, cumplimiento normativo, y mejora de la seguridad de la información. También se consideran las limitaciones de presupuesto y personal en la Municipalidad para garantizar que la propuesta sea práctica y sostenible.

3.7.3.4 Etapa 12: Informe de Resultados.

Se consolidan todos los hallazgos y recomendaciones en un informe final, que servirá como guía para la implementación del proceso formal de gestión de riesgos de TI en la Municipalidad de Turrialba.

3.8 Operacionalización de las Variables o Categorías

En esta sección se describe la relevancia de comprender cómo se relacionan y se ponen en práctica las variables en el contexto de este estudio. El enfoque de este trabajo se basa en la observación para lograr una contextualización adecuada de la función de estas variables. En la **Tabla *15*** se presentan las etapas y el funcionamiento de estas variables.

Tabla 15 *Operacionalización de las variables*

Objetivo especifico	Instrumento	Variables	Sujeto	Indicadores
Fase 1				
Analizar la situación actual del proceso de gestión de amenazas de TI que afectarían a la Municipalidad de Turrialba para la identificación de oportunidades de mejora del proceso existente contra las buenas prácticas de la industria.	Revisión documental (Apéndice F Bitácora Revisión Documental) Entrevistas (Apéndice G Entrevista Situación Actual, Apéndice H Entrevista Miembro Comisión de Control Interno) Cuestionarios (Apéndice I Cuestionario Situación Actual)	Responsables del proceso	- Encargado del Área de Servicios Informáticos - Miembro de la Comisión de Control Interno	- Cantidad de personas responsables identificadas - Claridad en la asignación de responsabilidades
		Documentación del proceso	- Encargado del Área de Servicios Informáticos	- Existencia de documentos actualizados - Accesibilidad de la documentación
		Tareas o actividades manuales del proceso existente	- Encargado del Área de Servicios Informáticos - Miembro de la Comisión de Control Interno	Tareas o actividades manuales del proceso existente
Fase 2				
Diseñar un marco de gestión de riesgos de TI basado en la norma técnica del MICITT y las mejores prácticas de la industria para la estandarización de	Revisión documental. (Apéndice F Bitácora Revisión Documental) Cuestionarios. (Apéndice I Cuestionario Situación Actual Apéndice I Cuestionario Situación Actual)	Tareas o actividades que requiere el proceso formal de gestión de riesgos	- Encargado del Área de Servicios Informáticos	- Cantidad de actividades requeridas - Nivel de capacidad de las actividades - Listado de riesgos - Escala de consecuencias - Escala de probabilidad - Tratamientos

Objetivo especifico	Instrumento	Variables	Sujeto	Indicadores
las actividades del proceso		Responsables del proceso formal de gestión de riesgos	- Encargado del Área de Servicios Informáticos - Miembro de la Comisión de Control Interno	- Cantidad de responsables identificados - Responsabilidades definidas
		Documentación requerida para el proceso formal	- Encargado del Área de Servicios Informáticos	- Número de documentos requeridos - Estado de preparación de la documentación
Fase 3				
Verificar la conformidad del proceso de gestión de riesgos de TI con los requisitos establecidos en la norma técnica del MICITT para el cumplimiento regulatorio y la protección de los activos de información.	Lista de Comprobación (Apéndice K Plantilla Lista de Comprobación del Proceso de Gestión de Riesgos)	Tareas o actividades que cumple el proceso formal	- Encargado del Área de Servicios Informáticos	- Porcentaje de actividades que cumplen con los requisitos del MICITT

4 Análisis de Resultados

En este capítulo se presenta el análisis de resultados de las variables de investigación del proyecto. Dicha sección detalla los resultados de la puesta en práctica de los instrumentos de recolección de información desarrollados para cada variable descrita, de modo que permita conocer la situación actual y la deseada para el cumplimiento de la Municipalidad de Turrialba.

4.1 Fase 1: Recolección y Análisis de Información

4.1.1 Revisión Documental

En esta primera etapa, se realizó una recolección exhaustiva de los documentos internos que describen los procesos relacionados con la gestión de riesgos de TI en la Municipalidad de Turrialba. El propósito de este análisis documental es ofrecer una visión clara de la manera en la que la entidad aborda actualmente la identificación, evaluación y mitigación de riesgos tecnológicos. Sin embargo, de acuerdo con lo expresado por el encargado de TI durante la entrevista sobre la situación actual, "no existe una documentación formal que describa el proceso de gestión de amenazas de TI. Todo se gestiona de manera reactiva y no hay un sistema formalizado de documentación accesible" (ver Apéndice L).

A pesar de la carencia en la documentación específica para la gestión de riesgos, el departamento de TI cuenta con las Políticas de Seguridad en Materia de Tecnologías de Información y Comunicación (Gamboa Calderón, 2022), elaboradas por el encargado de TI. Estas políticas están basadas en estándares internacionales como la ISO 27001, que establece los requisitos para los sistemas de gestión de la seguridad de la información (SGSI), y la ISO 27002, que proporciona directrices para la implementación de controles de seguridad. Además, se utilizan el marco COBIT 2019, que apoya en el control y la auditoría de la tecnología de información, y las buenas prácticas definidas por ITIL, que permiten gestionar de manera efectiva los servicios de TI dentro de la organización. Estos instrumentos brindan un marco general de seguridad, aunque no abordan de manera exhaustiva el proceso de gestión de amenazas de TI. En la **Tabla 16** se detallan los hallazgos derivados del análisis de dicho documento, que permiten identificar áreas clave para la mejora en la formalización y sistematización del proceso de gestión de riesgos en la municipalidad.

Tabla 16 *Bitácora de Revisión Documental*

Nombre del documento	Hallazgo
Políticas de Seguridad en Materia de Tecnologías de Información y Comunicación -TICS	▪ **Documentación actualizada**: el documento fue aprobado por el alcalde municipal en agosto de 2022, lo que indica que está actualizado. Sin embargo, se observó que algunas revisiones periódicas no están definidas. ▪ **Amplia cobertura de políticas**: el documento cubre múltiples aspectos clave de la seguridad, como la política de clasificación de la información; el uso de Internet, redes sociales y mensajería instantánea; y la seguridad de los recursos humanos y contratistas. Esto proporciona un marco robusto, sin embargo, algunas áreas, como la capacitación de personal y el monitoreo continuo, podrían fortalecerse para asegurar el cumplimiento de las políticas. ▪ **Falta de automatización**: el documento describe varios procedimientos manuales, especialmente los que se ejecutan en el respaldo de información y en la gestión de claves de acceso. ▪ **Seguridad física y lógica**: se incluyen directrices claras para la protección del centro de datos y la seguridad de la infraestructura de red. ▪ **Política de retención de datos**: se define la importancia de la retención y archivo de información, que justifica la relevancia de la protección de datos a largo plazo. ▪ **Definición de riesgos y gestión de riesgos**: el documento menciona la **gestión de riesgos** como un enfoque estructurado que maneja la incertidumbre relativa a las amenazas, incluyendo actividades como la evaluación, el desarrollo de estrategias para manejar riesgos y la mitigación mediante controles. Sin embargo, no se detalla un **proceso formal de identificación y tratamiento de riesgos.** ▪ **Políticas de seguridad y evaluación de riesgos**: el documento señala que todo *software* y *hardware* debe cumplir con los controles de seguridad (4.1.8 Política de Adquisición, Desarrollo y Mantenimiento de Sistemas de Información). Esta política está alineada con las prácticas recomendadas de gestión de riesgos; no obstante, **no se especifican herramientas automatizadas** ni metodologías formales para evaluar los riesgos en estas adquisiciones. ▪ **Riesgo en la protección de información y activos**: las políticas incluyen mecanismos para la protección de la información mediante clasificación (4.1.2 Política de Clasificación de la Información) y controles de acceso (4.1.16 Políticas de Seguridad del Centro de Datos y Cableado). Sin embargo, **es necesaria una política clara sobre el tratamiento de riesgos residuales.** ▪ **Capacitación y concientización en riesgos**: el documento aborda la capacitación de personal en relación con la seguridad de la información (4.1.3 Políticas de Seguridad para Recursos Humanos).

Lo encontrado en la columna de hallazgos de la **Tabla 16** revela varios aspectos fundamentales definidos en las políticas de seguridad actuales, que deberán servir como base para el desarrollo de una política formal de gestión de riesgos de TI. Estos puntos proporcionan directrices importantes, aunque actualmente no están alineados ni formalizados dentro de un marco específico para la gestión de riesgos de TI. La ausencia de una documentación estructurada y formal en este ámbito subraya la necesidad de integrar estos aspectos en una política coherente y sistemática que garantice una gestión proactiva y eficaz de las amenazas tecnológicas.

4.2 Análisis de Datos Recopilados

Para complementar la revisión documental, se realizaron entrevistas semiestructuradas y un cuestionario con los responsables del área de servicios de TI y un miembro de la comisión de control interno (ver Apéndices L y Apéndice M). Los encuentros tuvieron como objetivo profundizar en la comprensión práctica de la gestión de riesgos en la municipalidad, con un enfoque en la manera en la que las amenazas tecnológicas son tratadas en el día a día.

Este análisis proporciona una base sólida para formular propuestas de mejora que alineen el proceso con las mejores prácticas internacionales, como COBIT 2019 e ISO 27005, y con la norma técnica del MICITT. El proceso de gestión de riesgos de TI en la municipalidad ha sido, hasta el momento, mayormente reactivo, sin una estructura formal que permita una identificación y mitigación proactiva de las amenazas. A continuación, se detallan los resultados obtenidos a partir de los datos recopilados, centrándose en los aspectos clave del proceso, los hallazgos más relevantes y las áreas de mejora.

4.2.1 Responsabilidad en la Gestión de Amenazas de TI

Actualmente, la gestión de amenazas de TI en la Municipalidad de Turrialba recae sobre una sola persona: el encargado de TI. La ausencia de un equipo o una estructura formal dedicada a esta tarea genera una sobrecarga de responsabilidades y limita la capacidad de gestionar las amenazas eficiente y eficazmente. Por otro lado, la falta de personal especializado también implica que el encargado no tenga la posibilidad de delegar tareas, lo que reduce la efectividad general del proceso y deja a la organización vulnerable ante incidentes imprevistos. Además, como encargado de TI, este empleado cuenta con otras responsabilidades aparte de la gestión de amenazas.

4.2.2 Falta de Documentación Formal

Uno de los hallazgos más relevantes durante la entrevista al encargado de TI fue la ausencia de documentación formal sobre el proceso de gestión de amenazas de TI. El propio encargado manifestó que «no existe una documentación formal que describa el proceso de gestión de amenazas de TI» y que todo se gestiona de manera reactiva, sin un sistema estructurado y accesible para registrar o compartir información relevante sobre amenazas y riesgos.

La falta de documentación es un factor crítico, ya que un proceso de gestión de riesgos que no esté documentado no puede ser evaluado ni mejorado adecuadamente. Sin documentación formal, las acciones y decisiones tomadas en respuesta a las amenazas tecnológicas quedan en manos de las personas involucradas en ese momento, lo que genera un riesgo significativo si ese personal clave no está disponible.

4.2.3 Tareas o actividades del proceso existente

En el análisis del proceso actual de gestión de amenazas de TI en la Municipalidad de Turrialba, se consultó en primera instancia al encargado de TI, cuyas respuestas se pueden consultar en el cuestionario Apéndice I Cuestionario Situación Actual, sobre la efectividad del proceso actual; la respuesta se muestra en la Figura 13.

Figura 13 *Efectividad del proceso actual de gestión de amenazas de TI*

La opinión del encargado de TI sobre la efectividad del proceso actual de gestión de amenazas de TI en la municipalidad es neutra, pues, tal como se observa, la mayor parte de las actividades se gestionan de manera reactiva y manual. Durante la aplicación de la entrevista Apéndice M Resultados Entrevista Situación Actual, se identificaron las siguientes actividades del proceso actual de gestión de amenazas:

- **Identificación de amenazas:** actualmente, las amenazas se gestionan cuando se presentan, lo que significa que no hay un sistema formal para la identificación proactiva de riesgos. El encargado de TI actúa como único responsable de identificar y priorizar las amenazas que surgen en el entorno operativo; para ello, utiliza herramientas limitadas de monitoreo, ya que no existe un sistema documentado para el seguimiento y análisis de riesgos. Este proceso sigue un flujo informal en el cual los usuarios reportan directamente cualquier problema al encargado de TI, ya sea por correo electrónico o en persona. De esta manera, se evidencia la falta de un sistema centralizado para la notificación y gestión de incidentes.
- **Respuesta a las amenazas:** una vez identificada una amenaza, el encargado de TI evalúa su gravedad y determina las acciones correctivas necesarias, que pueden implicar la reconfiguración de equipos o el contacto con proveedores externos en caso de fallos en servicios contratados, como el suministro de internet. Las decisiones y acciones dependen completamente del juicio y experiencia del encargado, lo que introduce un alto grado de informalidad y falta de estandarización en las respuestas.
- **Monitoreo y seguimiento:** aunque existen algunas herramientas automatizadas de monitoreo, gran parte del seguimiento de las amenazas se hace de forma manual. El encargado de TI recibe alertas automáticas de algunas plataformas y realiza acciones correctivas según lo dictado por esas alertas. Sin embargo, no existe un sistema formal de registro de incidentes, por lo que las acciones no se documentan de manera sistemática. Esto impide realizar un análisis posterior o identificar patrones recurrentes de amenazas.

Las actividades del proceso actual de gestión de riesgos de TI son mayoritariamente manuales y reactivas, con escasa documentación formal y una dependencia excesiva en el único responsable de TI. Esto dificulta una respuesta rápida y eficiente ante múltiples amenazas simultáneas o emergentes.

4.2.4 Tareas o actividades que requiere el proceso formal de gestión de riesgos

Para el establecimiento del proceso formal de gestión de riesgos en la Municipalidad de Turrialba, se tomaron como referencia las mejores prácticas definidas en el marco COBIT 2019, específicamente dentro del objetivo de gestión APO12, enfocado en la gestión de riesgos.

A lo largo de la entrevista realizada con el encargado de TI (Apéndice L Minuta de Reunión 04 – Aplicación de Entrevista), se identificó la necesidad de estructurar un proceso formal que permita no solo la identificación y respuesta a los riesgos de TI, sino también la documentación y monitoreo continuo de dichos riesgos. El encargado manifestó su interés en implementar las actividades correspondientes a los niveles de capacidad dos y tres del APO12 de COBIT 2019, con el fin de avanzar hacia una mayor madurez en la gestión de riesgos dentro de la institución. No obstante, se concluyó que no se realizarán las actividades de nivel cuatro y cinco, ya que estas requieren una base sólida para su ejecución, la cual se obtiene mediante las actividades de los niveles dos y tres, como, por ejemplo, el desarrollo de un histórico de los riesgos.

A continuación, se describen las actividades, agrupadas por su respectiva práctica de gestión, que debe incluir este proceso formal.

4.2.4.1 Recopilar datos

Esta primera práctica busca identificar y recopilar datos relevantes para habilitar una efectiva identificación, análisis y reporte de los riesgos. Incluye las siguientes actividades:

- Establecer y mantener un método para la recolección, clasificación y análisis de datos relacionados con el riesgo de TI. Este método debe asegurar que la información vinculada con los riesgos, tanto internos como externos, sea consistentemente recopilada y analizada.
- Registrar datos relevantes y significativos relacionados con los riesgos de TI en el entorno operativo.
- Adoptar o definir una taxonomía de riesgo para las definiciones consistentes de escenarios de riesgo y categorías de impacto y probabilidad.
- Registrar datos de eventos de riesgo que han causado o podrían causar impacto en el negocio, conforme a las categorías de impacto definidas en la taxonomía de riesgo. Este registro se obtiene mediante la captura de datos relevantes de cuestiones, incidentes, problemas e investigaciones.

4.2.4.2 Analizar el riesgo

El análisis de los riesgos de TI busca desarrollar una visión fundamentada del riesgo de TI vigente, que soporte las decisiones de riesgo. Las actividades que deben realizarse son:

- Definir el alcance adecuado de los esfuerzos en análisis de riesgos, considerando todos los factores de riesgo y/o la criticidad de los activos para el negocio.

- Crear y actualizar regularmente los escenarios de riesgo de TI, las exposiciones a pérdidas relacionadas con TI y los escenarios asociados con el riesgo reputacional, incluidos escenarios compuestos de tipos de amenazas y eventos en cascada y/o coincidentes. Para esto, es necesario desarrollar previsiones para actividades de control específicas y capacidades de detección.
- Estimar la frecuencia (o probabilidad) y la magnitud de la pérdida o ganancia asociada con escenarios de riesgos de TI. Esta actividad requiere tener en cuenta todos los factores de riesgo aplicables y evaluar controles operativos conocidos.
- Comparar el riesgo actual (exposición a pérdidas de TI) con el apetito al riesgo y la tolerancia de riesgo aceptable. Para lograr lo anterior, se debe identificar el riesgo inaceptable o elevado.
- Proponer respuestas al riesgo para riesgos que excedan el apetito al riesgo y los niveles de tolerancia.
- Especificar los requisitos de alto nivel para los proyectos o programas que implementarán las respuestas a los riesgos seleccionados. Esta actividad implica la identificación de los requisitos y expectativas para los controles clave adecuados con el fin de proporcionar respuestas de mitigación de riesgos.

4.2.4.3 Mantener un perfil de riesgo

Dicha práctica busca mantener un inventario de los riesgos conocidos y los atributos de riesgo, incluidos la frecuencia esperada, impacto potencial y respuestas. Al mismo tiempo, documenta los recursos, capacidades y actividades de control actuales relacionados con elementos de riesgo. Las actividades que deben realizarse son:

- Realizar un inventario de los procesos de negocio y documentar su dependencia con los procesos de gestión de servicios de TI y los recursos de infraestructura de TI. Para su concreción, se debe identificar el personal de apoyo, aplicaciones, infraestructura, instalaciones, registros manuales críticos, contratistas, proveedores y terceros.
- Determinar y acordar qué servicios de TI y recursos de infraestructura de TI son esenciales para sostener el funcionamiento de los procesos de negocio. Por esta razón, se deben analizar las dependencias e identificar los eslabones débiles.
- Agregar los escenarios de riesgos actuales por categoría, línea de negocio y área funcional.
- Capturar regularmente toda la información del perfil de riesgo y consolidarla en un perfil de riesgo agregado.
- Capturar información sobre el estado del plan de acción de riesgos para su inclusión en el perfil de riesgo de TI de la empresa.

4.2.4.4 Articular el riesgo

En esta práctica se procura comunicar de manera oportuna información sobre el estado actual de las exposiciones y oportunidades relacionadas con TI a todas las partes interesadas requeridas para obtener una respuesta apropiada. Las actividades necesarias son:

- Informar sobre los resultados del análisis de riesgo a todas las partes interesadas y afectadas en términos y formatos útiles para soportar las decisiones empresariales. Siempre que sea

posible, se deben incluir las probabilidades y rangos de pérdidas o ganancias, junto con los niveles de confianza, para permitir que la gerencia haga balance del retorno del riesgo.

- Proporcionar a los responsables de la toma de decisiones la comprensión de los escenarios peores y más probables; exposiciones a pérdidas de TI y consideraciones significativas de reputación, legales y regulatorias o cualquier otra categoría de impacto conforme a la taxonomía de riesgos.
- Informar sobre el perfil de riesgo actual a todas las partes interesadas. Se debe incluir información sobre la eficacia del proceso de gestión de riesgos, eficacia del control, brechas, inconsistencias, redundancias, estado de remediación y sus impactos en el perfil de riesgo.
- De forma periódica, en áreas con riesgos relativos y capacidades de riesgo similares, identificar oportunidades relacionadas con TI que permitirían la aceptación de un riesgo mayor y un mayor crecimiento y retorno.

4.2.4.5 Definir un portafolio con acciones de gestión de riesgos

Para mitigar los riesgos de TI y responder efectivamente a ellos, se requiere gestionar las oportunidades para reducir el riesgo a un nivel aceptable. Las actividades en este ámbito incluyen:

- Mantener un inventario de las actividades de control que se han implantado para mitigar el riesgo y que permiten que se tomen riesgos alineados con el apetito y la tolerancia al riesgo. Clasificando las actividades de control y asignarlas a escenarios de riesgos de TI específicos y escenarios de riesgos de TI agregados.
- Determinar si cada entidad organizativa monitoriza el riesgo y acepta la responsabilidad de actuar dentro de los niveles de tolerancia individuales y del portafolio.
- Definir un conjunto de propuestas de proyectos equilibradas y diseñadas para reducir el riesgo y/o proyectos que permitan oportunidades empresariales estratégicas, teniendo en consideración los costes, beneficios y el efecto en el perfil de riesgo actual y en las regulaciones.

4.2.4.6 Responder al riesgo

A través de esta actividad se pretende responder de manera oportuna y con medidas eficaces para limitar la magnitud de las pérdidas a eventos de riesgo materializados. Para esto, se deben implementar las respuestas claras y específicas ante incidentes de riesgo mostradas a continuación:

- Preparar, mantener y probar planes que documenten los pasos específicos que deben darse cuando un evento de riesgo pudiera causar un incidente significativo de desarrollo u operativo con un impacto grave para el negocio. Por esta razón, se debe asegurar que los planes incluyan vías de escalamiento en la empresa.
- Aplicar el plan de respuesta adecuado para minimizar el impacto cuando ocurren incidentes de riesgo.

El proceso formal de gestión de riesgos propuesto permitirá a la Municipalidad de Turrialba avanzar hacia una gestión proactiva de riesgos, en lugar de simplemente responder a los problemas a medida que se presentan. Esta estructura ayudará a mejorar la resiliencia organizacional frente a los desafíos tecnológicos y garantizará una mayor seguridad y control sobre los activos de TI.

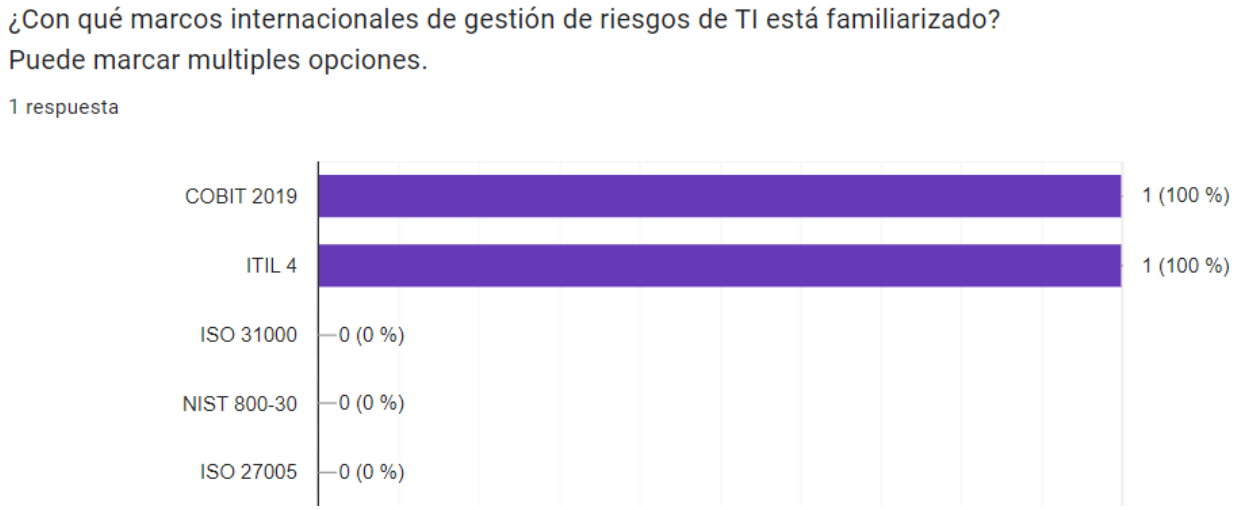
4.2.5 Externalización de Servicios de TI

La Municipalidad de Turrialba externaliza ciertos servicios de TI, como la provisión de Internet y la gestión de bases de datos, lo que introduce una nueva capa de complejidad en la gestión de riesgos. Sin embargo, no existen mecanismos formales para garantizar que los proveedores externos cumplan con las políticas de seguridad establecidos por la Municipalidad. Esto representa un riesgo considerable, ya que cualquier incidente relacionado con los proveedores puede tener un impacto negativo en las operaciones de la organización.

4.2.6 Marcos Internacionales

Se realizó la consulta mediante el cuestionario Apéndice I Cuestionario Situación Actual al encargado de TI sobre su conocimiento de los marcos internacionales relacionados con la gestión de riesgos; en la Figura 14 se muestra el gráfico de la respuesta.

Figura 14 *Marcos internacionales de gestión de riesgos de TI está familiarizado*



El encargado de TI menciona tener conocimiento de marcos internacionales como COBIT 2019 e ITIL 4, lo cual es positivo. Sin embargo, no se mencionan marcos relevantes a la gestión de riesgos de TI, como ISO 27005 o ISO 31000, que son cruciales para una gestión integral de riesgos de TI. La falta de familiaridad con estos marcos podría limitar la capacidad de la municipalidad para adoptar un enfoque más amplio y alineado con las mejores prácticas internacionales.

4.2.7 Desafíos Anticipados para la Implementación de un Marco Formal

Uno de los principales desafíos anticipados para la implementación de un nuevo marco formal de gestión de riesgos de TI es la falta de tiempo y de recursos financieros. La implementación de políticas y procedimientos formales, la adquisición de herramientas de automatización y la capacitación del personal requieren una inversión significativa en términos de tiempo y dinero.

4.2.8 Estado del Apetito de Riesgo

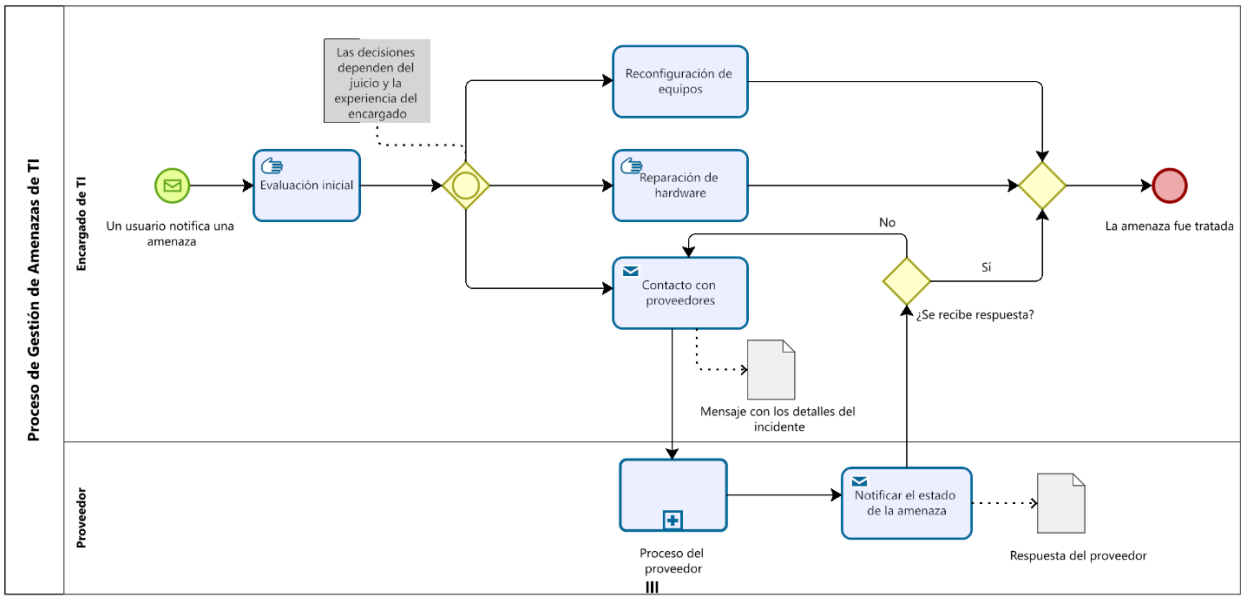
Se identificó que no existe un apetito de riesgo formalmente definido ni comunicado en la Municipalidad de Turrialba. Esto implica que las decisiones relacionadas con los riesgos se toman

en el momento en el que se presentan las amenazas al juicio del encargado de cada departamento, sin un marco claro que guíe las acciones del departamento de TI y otros responsables.

4.3 Modelado del proceso as-is

Para visualizar el estado actual del proceso de gestión de amenazas de TI, se modeló el proceso as-is que representa las actividades y flujos de información dentro de la Municipalidad de Turrialba. El modelo (Figura 15) se construyó a partir de los datos recopilados en las etapas anteriores, mediante el **Apéndice M** Resultados Entrevista Situación Actual. Dicho modelo permite identificar las brechas y puntos de control dentro del proceso actual.

Figura 15 *Proceso as-is de Gestión de Amenazas de TI*



Nota. Elaboración propia usando el modelador de Bizagi, 2024.

El diagrama mostrado en la Figura 15 utiliza la notación **BPMN 2.0** para describir el **proceso actual de gestión de amenazas de TI** en la Municipalidad de Turrialba. A continuación, se explica detalladamente cada parte del proceso.

4.3.1 Inicio del proceso

El proceso comienza cuando un usuario de la municipalidad detecta una posible amenaza o incidente en el sistema de TI. Esta amenaza puede incluir fallos en los sistemas, ciberataques, problemas de *hardware* o cualquier otra amenaza relacionada con las tecnologías de la información. La notificación se realiza directamente al encargado de TI a través de medios informales, como el correo electrónico o la comunicación personal.

4.3.2 Evaluación inicial

Una vez que el encargado de TI recibe la notificación de la amenaza, procede a evaluarla. En este paso, el encargado utiliza su experiencia y juicio personal para determinar la gravedad de la amenaza y las acciones correctivas necesarias. No existe un sistema formalizado ni una guía para llevar a cabo esta evaluación, lo que introduce una alta variabilidad en la toma de decisiones.

4.3.3 Respuestas a las amenazas

Después de la evaluación inicial, el encargado debe decidir cuál es la mejor respuesta para gestionar la amenaza. Existen tres posibles caminos en este punto:

- Reconfiguración de equipos: si la amenaza está relacionada con una mala configuración del sistema o algún fallo que pueda corregirse mediante ajustes en la configuración de los equipos, el encargado procede con esta tarea.
- Reparación de *hardware*: si la amenaza es de naturaleza física, como el fallo de un equipo, se procede a la reparación o reemplazo de los componentes dañados.
- Contacto con proveedores: si la amenaza está relacionada con un servicio externo, como la conectividad a internet o la funcionalidad de un sistema que depende de un proveedor externo, el encargado se comunica con el proveedor.

4.3.3.1 Proceso con el proveedor

- Envío de mensaje con detalles del incidente: si se decide contactar al proveedor, el encargado de TI envía un mensaje con los detalles de la amenaza o incidente. Este mensaje contiene la información relevante para que el proveedor pueda actuar sobre el problema.
- Proceso del proveedor: una vez que el proveedor recibe el mensaje, lleva a cabo sus propios procedimientos internos para resolver el problema. Este proceso puede implicar el soporte técnico o la activación de soluciones específicas en función del contrato de servicios con la municipalidad.
- Notificar el estado de la amenaza: después de que el proveedor ha actuado sobre el problema, informa al encargado de TI sobre el estado del incidente.

4.3.3.2 Decisión: ¿se recibe respuesta del proveedor?

Si el proveedor responde a tiempo con una solución adecuada, se considera que la amenaza fue gestionada correctamente y el proceso concluye. Si no se recibe una respuesta o la solución es insuficiente, el encargado de TI puede tomar nuevas acciones, ya sea escalando el problema o realizando otras tareas correctivas.

4.3.4 Fin del proceso

- La amenaza fue tratada: una vez que la amenaza ha sido gestionada, ya sea mediante reconfiguración, reparación o intervención del proveedor, el proceso se da por concluido. En este punto, no se realiza un registro formal del incidente, lo cual es una de las principales limitaciones del proceso actual.
- Decisiones basadas en juicio personal: a lo largo del proceso, las decisiones dependen en gran medida de la experiencia del encargado de TI; esto introduce un alto nivel de informalidad.
- Falta de estandarización y documentación: no existe un sistema formal para documentar el incidente ni un protocolo claro para gestionar las amenazas, lo que impide un análisis posterior y dificulta la mejora del proceso a largo plazo.

4.3.5 Evaluación del Nivel de Madurez del Proceso Actual

De acuerdo con el Modelo de Madurez de la Capacidad (CMMI), el proceso actual de gestión de amenazas de TI en la Municipalidad de Turrialba se clasifica en Nivel 1: Inicial. Este nivel indica que el proceso tiene algunas actividades básicas en funcionamiento, pero carece de organización formal, estandarización y consistencia en su ejecución. Los procesos dependen en gran medida de la iniciativa y el conocimiento individual del encargado de TI, lo que genera una alta variabilidad y vulnerabilidad en la gestión de amenazas.

4.4 Identificación de brechas y áreas de mejora

En la Tabla 17 se identifican las principales brechas en la gestión de riesgos de TI en la Municipalidad de Turrialba con un estado ideal que debería cumplir según la norma técnica del MICITT y mejores prácticas de la industria.

Tabla 17 *Brechas estado actual y estado ideal del proceso de gestión de amenazas de TI*

Variable	Concepto	Estado actual	Estado ideal
Responsables del proceso	Identificación de los roles responsables en la gestión de amenazas de TI.	El encargado de TI actúa como único responsable de la identificación y gestión de amenazas. No existe una clara asignación de responsabilidades entre diferentes roles.	Definición de roles y responsabilidades claras para gestionar amenazas, con un proceso formalizado y distribuido entre los actores clave.
Documentación del proceso	Estado y disponibilidad de la documentación relacionada con el proceso actual de gestión de amenazas.	No hay documentación formal ni procedimientos documentados. La gestión de amenazas se realiza de manera informal sin registros.	Procesos formalmente documentados con políticas, procedimientos y registros históricos de incidentes para futuras evaluaciones.
Tareas o actividades del proceso existente	Actividades que se realizan en el proceso actual de gestión de amenazas de TI.	Las actividades actuales son reactivas: los usuarios notifican al encargado de TI quien evalúa y responde según su juicio, sin estandarización.	Implementación de actividades estructuradas y proactivas.
Tareas o actividades que requiere el proceso formal de gestión de riesgos	Actividades y tareas necesarias para la implementación del proceso formal de gestión de riesgos.	No existen tareas formalizadas; las actividades dependen del juicio del encargado de TI y las alertas automáticas de herramientas de monitoreo limitadas.	Un proceso formal que incluya las prácticas de gestión del APO12-Gestionar los Riesgos de COBIT 2019.

Variable	Concepto	Estado actual	Estado ideal
Responsables del proceso formal de gestión de riesgos	Identificación de los roles y responsabilidades dentro del nuevo proceso formal.	Actualmente solo el encargado de TI gestiona los riesgos, sin roles distribuidos ni apoyo institucional.	Definir roles específicos para cada etapa del proceso, incluyendo responsables para la identificación, evaluación, respuesta y seguimiento de riesgos de TI.
Documentación requerida para el proceso formal	Documentos necesarios para implementar el marco formal de gestión de riesgos de TI.	No existe documentación sistemática del proceso.	Contar con políticas y procedimientos de gestión de riesgos de TI, una herramienta integral de gestión de riesgos que abarca el monitoreo, seguimiento y comunicación de riesgos.
Tareas o actividades que cumplen el proceso formal	Actividades del proceso formal de gestión de riesgos alineadas con los requisitos del MICITT.	El proceso actual no cumple con los estándares del MICITT, ya que no hay formalidad ni documentación en la gestión de amenazas.	Un proceso que cumpla completamente con la norma técnica del MICITT y con procedimientos bien definidos, documentados y monitoreados regularmente.
Fortalezas del proceso	Aspectos positivos del proceso formal que contribuyen a la gestión efectiva de riesgos.	El encargado de TI tiene experiencia en la gestión de amenazas y existen herramientas de monitoreo automatizadas para ciertas áreas.	Contar con un proceso formal, proactivo y continuo que utilice mejores prácticas, herramientas automatizadas y roles bien definidos.
Oportunidades de mejora del proceso	Áreas dentro del proceso formal que se pueden optimizar o mejorar.	Falta de documentación, informalidad en la toma de decisiones y dependencia excesiva en el juicio del encargado de TI.	Implementar un sistema formal de gestión de riesgos, con documentación adecuada, automatización y distribución de responsabilidades.

Variable	Concepto	Estado actual	Estado ideal
Limitaciones del proceso	Factores que limitan la efectividad del proceso formal de gestión de riesgos.	La falta de un sistema formal, la dependencia en una sola persona y la carencia de registros limitan la capacidad de gestionar y analizar amenazas de manera eficiente.	Desarrollar un sistema de gestión de riesgos que sea escalable, con roles distribuidos y soportado por documentación y herramientas de monitoreo.
Amenazas que posee el proceso	Riesgos o amenazas que pueden afectar el éxito del proceso formal de gestión de riesgos de TI.	Falta de registro de incidentes, capacidad limitada para escalar la respuesta a amenazas complejas y dependencia de un solo encargado.	Identificación y gestión de todas las amenazas potenciales con planes de mitigación, escalabilidad y monitoreo continuo, al mismo tiempo que se distribuyen las responsabilidades.

4.4.1 Comparativa con la norma técnica del MICITT

La Norma Técnica del MICITT establece un marco detallado para la gestión de riesgos de TI en instituciones públicas de Costa Rica, con el objetivo de garantizar que los riesgos asociados a las tecnologías de información sean identificados, evaluados y gestionados de manera eficiente. En la Municipalidad de Turrialba, actualmente el único encargado del proceso de gestión de riesgos es el responsable del departamento de TI, quien gestiona todas las actividades relacionadas con la identificación y mitigación de riesgos. Esta situación presenta una clara limitación, ya que el manejo de riesgos se realiza de forma centralizada, sin una distribución de responsabilidades ni un respaldo institucional.

La norma del MICITT establece la necesidad de definir roles y responsabilidades claras y específicas, asignando a un equipo multifuncional encargado de la gestión de riesgos de TI. Idealmente, este equipo debería incluir no solo al responsable de TI, sino también a representantes de áreas clave como administración, operaciones y seguridad, con roles diferenciados para cada etapa del proceso

En el estado actual, la gestión de riesgos en la Municipalidad carece de documentación formal. No existen políticas, procedimientos ni registros históricos que respalden las actividades realizadas. Las decisiones se toman de manera informal y no quedan evidencias de las evaluaciones o tratamientos implementados.

En contraste, la norma del MICITT exige que el proceso de gestión de riesgos esté documentado de manera integral. Esto incluye:

- Políticas de gestión de riesgos de TI, que definan los lineamientos generales para la identificación, evaluación y tratamiento de riesgos.
- Procedimientos documentados, que detallen las acciones específicas a realizar en cada etapa del proceso.
- Matriz de riesgos, que permita registrar, clasificar y priorizar los riesgos identificados, así como sus respectivos planes de tratamiento.
- Registros históricos de incidentes y evaluaciones, para facilitar la trazabilidad y la mejora continua del proceso.

El enfoque actual en la Municipalidad de Turrialba es reactivo, ya que las actividades de gestión de riesgos se limitan a responder a incidentes reportados por los usuarios o detectados por las herramientas de monitoreo. No existe un proceso estructurado que permita identificar y mitigar riesgos antes de que se conviertan en incidentes.

La norma técnica del MICITT enfatiza la necesidad de implementar un enfoque proactivo en la gestión de riesgos. Esto implica:

- Identificación temprana de riesgos potenciales, antes de que estos afecten las operaciones de la organización.
- Evaluación continua de los riesgos, considerando tanto las amenazas internas como externas.
- Tratamiento preventivo de riesgos, mediante la implementación de controles y medidas que reduzcan su probabilidad de ocurrencia o impacto.
- Monitoreo constante y revisión periódica, para ajustar las estrategias de gestión de riesgos en función de los cambios en el entorno tecnológico y organizacional.

Actualmente, el proceso de gestión de riesgos en la Municipalidad es informal y depende en gran medida de la experiencia y criterio del encargado de TI. No existe un marco formal que defina las etapas del proceso ni cómo deben ejecutarse.

4.4.2 Comparativa con COBIT 2019

El marco de COBIT 2019 proporciona una estructura detallada para la gobernanza y gestión de riesgos de TI, enfocándose en alinear las actividades de TI con los objetivos estratégicos de la organización. En el estado actual, la gestión de riesgos en la Municipalidad de Turrialba carece de una estructura formal que defina un marco de gobernanza. No se recopilan ni se mantienen datos de manera sistemática sobre los riesgos, activos críticos, amenazas o vulnerabilidades.

Actualmente, la Municipalidad no realiza evaluaciones formales de riesgos, y las decisiones se basan en el criterio del encargado de TI, sin un análisis sistemático de probabilidad e impacto. Según COBIT 2019, el análisis de riesgos debe ser una actividad estructurada y continua, que incluya:

- Evaluación cualitativa y/o cuantitativa de los riesgos en términos de probabilidad y severidad del impacto.
- Identificación de interdependencias entre riesgos, activos y procesos de negocio.
- Uso de herramientas y metodologías estándar para analizar y priorizar riesgos, como mapas de calor o matrices de riesgos.

El estado actual refleja una ausencia de documentación y actualización continua del perfil de riesgo de la Municipalidad. No existe un registro formal que permita monitorear la evolución de los riesgos a lo largo del tiempo. COBIT 2019 establece la necesidad de mantener un perfil de riesgo actualizado, que incluya:

- Inventario dinámico de riesgos identificados, categorizados por nivel de criticidad.
- Actualización periódica del perfil de riesgo en función de cambios en el entorno tecnológico, organizacional o regulatorio.
- Integración del perfil de riesgo con los objetivos estratégicos y operativos de la organización.

Actualmente, los riesgos no son articulados ni comunicados a nivel institucional. Las decisiones relacionadas con los riesgos de TI se toman exclusivamente dentro del departamento de TI, sin la participación de otras áreas clave.

En el estado actual, no existe un portafolio formal de acciones para mitigar, transferir, aceptar o evitar los riesgos identificados. Las respuestas a los riesgos son reactivas y se implementan de forma ad hoc.

La respuesta a los riesgos en la Municipalidad es limitada y se basa en la experiencia del encargado de TI, sin un enfoque estructurado o basado en mejores prácticas. COBIT 2019 establece que la respuesta a los riesgos debe ser:

- Proactiva, anticipando la materialización de los riesgos críticos.
- Basada en políticas y procedimientos documentados, que definan claramente las acciones a tomar en diferentes escenarios de riesgo.
- Alineada con los objetivos de negocio, asegurando que las respuestas a los riesgos contribuyan a la continuidad operativa y la resiliencia de la organización.

4.4.3 Comparativa con la ISO 27005

La norma ISO 27005 es una referencia fundamental para la gestión de riesgos de seguridad de la información, proporcionando un enfoque estructurado que permite identificar, analizar, evaluar, tratar y monitorear los riesgos que afectan la confidencialidad, integridad y disponibilidad de la información.

En la situación actual, la gestión de riesgos de TI es realizada por un único encargado, lo que limita la capacidad de supervisar todas las etapas del proceso de forma efectiva y reduce la posibilidad de asignar roles especializados. La ISO 27005 recomienda una definición clara de roles y responsabilidades para cada etapa del proceso de gestión de riesgos. Esto incluye:

- Propietario del riesgo: Responsable de la identificación, gestión y tratamiento del riesgo en sus respectivas áreas.
- Equipo de gestión de riesgos: Encargado de coordinar el proceso de gestión de riesgos, garantizar su documentación y comunicarlo a las partes interesadas.
- Auditores internos o externos: Encargados de verificar la eficacia del proceso de gestión de riesgos y proporcionar recomendaciones de mejora.

Actualmente, el proceso de gestión de riesgos carece de documentación formal adecuada. No existen políticas ni procedimientos definidos que respalden la gestión de riesgos, y no se mantienen registros históricos de evaluaciones o incidentes. La ISO 27005 enfatiza la importancia de una documentación formal que abarque:

- Política de gestión de riesgos de seguridad de la información, alineada con los objetivos de la organización.
- Procedimientos de identificación, análisis, evaluación, tratamiento y monitoreo de riesgos.
- Registros históricos de evaluaciones de riesgos, incidentes, decisiones de tratamiento y resultados de monitoreo.

En la actualidad, la Municipalidad no realiza una identificación ni análisis estructurado de riesgos. Las actividades son reactivas, enfocadas en resolver problemas una vez que se han materializado. La ISO 27005 establece que el proceso de gestión de riesgos debe ser proactivo y estructurado, abarcando las siguientes etapas:

- Identificación de riesgos: Identificar los activos de información, las amenazas asociadas y las vulnerabilidades explotables.
- Análisis de riesgos: Evaluar la probabilidad de ocurrencia y el impacto de cada riesgo, estableciendo una valoración inicial.
- Evaluación de riesgos: Comparar los riesgos identificados con los criterios establecidos para determinar si son aceptables o requieren tratamiento.
- Tratamiento de riesgos: Implementar medidas para mitigar, transferir, evitar o aceptar los riesgos, documentando cada decisión tomada.

En la situación actual, la gestión de riesgos no abarca todas las etapas del ciclo de vida, como la monitorización y revisión continua. Las actividades suelen finalizar una vez que se aborda

un problema puntual. La ISO 27005 promueve un enfoque de gestión continua, donde cada etapa del ciclo de vida es abordada de manera integral:

- Identificación inicial de riesgos en función de cambios tecnológicos, organizacionales o regulatorios.
- Evaluación periódica de los riesgos existentes y emergentes.
- Monitoreo constante del entorno de amenazas y de la eficacia de las medidas de tratamiento implementadas.
- Revisión y mejora continua del proceso de gestión de riesgos, adaptándolo a las nuevas condiciones del entorno.

En su estado actual, el proceso de gestión de riesgos no está explícitamente alineado con los objetivos estratégicos de la Municipalidad, lo que dificulta justificar la asignación de recursos y priorizar acciones. La ISO 27005 establece que la gestión de riesgos debe estar alineada con los objetivos organizacionales, asegurando que:

- Los riesgos que puedan afectar la continuidad operativa y el cumplimiento normativo sean priorizados.
- Las medidas de mitigación se enfoquen en proteger los activos de información más críticos para la organización.
- La gestión de riesgos sea vista como un proceso estratégico que respalda la misión y visión institucional.

Actualmente, la Municipalidad carece de una política formal de gestión de riesgos que guíe las actividades relacionadas con la seguridad de la información. La ISO 27005 requiere la creación de una política de gestión de riesgos que:

- Establezca los principios, objetivos y alcance del proceso de gestión de riesgos.
- Defina los roles y responsabilidades de todas las partes involucradas.
- Especifique los criterios para la aceptación de riesgos y las condiciones bajo las cuales se tomarán decisiones de mitigación.
- Incluya un compromiso explícito de la alta dirección para apoyar y supervisar el proceso de gestión de riesgos.

4.4.4 Comparativa con la NIST SP 800-30

La NIST SP 800-30 es un estándar clave en la gestión de riesgos, proporcionando un enfoque detallado y sistemático para identificar, evaluar y tratar los riesgos que afectan a la seguridad de la información en una organización.

En la actualidad, el proceso de gestión de riesgos en la Municipalidad de Turrialba está centralizado en una sola persona, lo que limita la capacidad de gestionar adecuadamente todos los aspectos del proceso de manera eficiente. La NIST SP 800-30 establece que se debe conformar un equipo de gestión de riesgos con funciones claramente definidas que aborden todas las etapas del proceso. Estas funciones incluyen:

- Análisis de riesgos: Evaluación de la probabilidad e impacto de los riesgos identificados.
- Monitoreo de riesgos: Supervisión continua de los riesgos y el entorno organizacional para identificar cambios que puedan impactar la seguridad de la información.
- Mitigación de riesgos: Implementación de medidas para reducir o eliminar los riesgos identificados.
- Comunicación de riesgos: Asegurar que las partes interesadas reciban la información adecuada sobre los riesgos y las acciones tomadas.

La Municipalidad no cuenta con documentación formal y detallada que respalde el proceso de gestión de riesgos, lo que dificulta la supervisión y la mejora continua. La NIST SP 800-30 resalta la importancia de documentar todas las actividades de gestión de riesgos, creando y manteniendo una serie de documentos clave:

- Políticas y procedimientos de gestión de riesgos: Guías claras para la identificación, evaluación, tratamiento y monitoreo de riesgos.
- Controles de gestión de riesgos: Medidas específicas implementadas para mitigar los riesgos identificados.
- Registros de tratamiento de riesgos: Evidencia de las decisiones tomadas y las medidas implementadas para tratar los riesgos.

Las actividades de gestión de riesgos se realizan de manera reactiva, enfocándose principalmente en la resolución de incidentes a medida que ocurren. La NIST SP 800-30 promueve un enfoque proactivo y continuo para la gestión de riesgos, que debe abarcar las siguientes actividades:

- Identificación de riesgos: Evaluar de manera regular los activos de información, las amenazas potenciales y las vulnerabilidades.
- Análisis de riesgos: Evaluar la probabilidad de que los riesgos se materialicen y su posible impacto en los objetivos organizacionales.
- Tratamiento de riesgos: Implementar medidas para reducir, mitigar o transferir los riesgos antes de que se materialicen en incidentes.

Este enfoque proactivo es clave para identificar riesgos emergentes antes de que afecten a la organización y garantizar que las acciones correctivas se tomen con suficiente antelación.

El proceso actual de gestión de riesgos en la Municipalidad no está completamente estructurado y carece de actividades específicas para cada etapa del ciclo de vida del riesgo. La NIST SP 800-30 establece un proceso detallado y estructurado que cubre todas las etapas, incluyendo:

- Planificación: Establecer un enfoque claro para la gestión de riesgos, definir los recursos necesarios y establecer los criterios de éxito.

- Identificación de riesgos: Realizar una evaluación detallada de los riesgos asociados a los activos de información de la organización.
- Evaluación de riesgos: Calcular el impacto potencial y la probabilidad de los riesgos, y compararlos con los criterios establecidos para determinar cuáles son aceptables y cuáles no.
- Tratamiento de riesgos: Seleccionar e implementar estrategias de mitigación adecuadas para los riesgos inaceptables.
- Monitoreo y seguimiento: Realizar un monitoreo continuo para evaluar la eficacia de las medidas de mitigación y la aparición de nuevos riesgos.

La gestión de riesgos en la Municipalidad se maneja principalmente por una sola persona, lo que limita la capacidad de aplicar un enfoque multidisciplinario al proceso. La NIST SP 800-30 recomienda la creación de un equipo multidisciplinario que esté compuesto por miembros con diversas especializaciones y experiencia, tales como:

- Expertos en TI: Encargados de identificar riesgos tecnológicos y recomendar medidas de mitigación específicas.
- Auditores internos: Responsables de evaluar la eficacia de las medidas de control y el cumplimiento de políticas.
- Gerentes de área: Responsables de identificar y evaluar los riesgos específicos de sus áreas y colaborar en la implementación de soluciones.

Actualmente, no existe una guía estructurada para la gestión de riesgos ni documentos detallados de evaluación de impacto en la Municipalidad de Turrialba. La NIST SP 800-30 recomienda la creación de una guía de gestión de riesgos que defina claramente los procedimientos y estándares para la identificación, evaluación, tratamiento y monitoreo de riesgos. Además, es fundamental desarrollar documentos de evaluación de impacto que permitan analizar el efecto potencial de cada riesgo en la organización, considerando aspectos como:

- Impacto en la continuidad operativa.
- Impacto financiero.
- Impacto en la reputación y cumplimiento normativo.

5 Propuesta de Solución

En el presente capitulo se busca poner en práctica la propuesta de la solución al problema presentado en el primer capítulo. Además, esta unidad pretende abordar todas las oportunidades de mejora encontradas en el análisis de resultados. De esta forma, el capítulo en cuestión permite ejecutar las fases dos y tres definidas en el procedimiento metodológico de la investigación, con el objetivo de definir un proceso formal de gestión de riesgos de TI que se alinee a las buenas prácticas de la industria y el cumplimiento normativo.

5.1 Diseño de Solución

En este apartado se presenta la ejecución de la fase dos definida en el apartado 3.7.2 Fase 2: Diseño del Marco de Gestión de Riesgos de TI referente al procedimiento metodológico de la investigación, la cual busca crear un marco para la gestión de los riesgos de TI en la municipalidad de Turrialba.

5.1.1 Desarrollo de Políticas de Gestión de Riesgos de TI

Se desarrollan políticas claras que establecen los principios y directrices generales para la gestión de riesgos de TI, siguiendo las prácticas de gestión de COBIT 2019 con un nivel de capacidad de dos y tres, la Norma MICITT y las mejores prácticas internacionales. En el apartado se presenta la creación del documento referente a la política para la gestión de riesgos de TI (Apéndice R Política para la Gestión de Riesgos de Tecnologías de Información). Este documento tiene como objetivo establecer las bases de trabajo del departamento de Tecnologías de Información.

A continuación, se presenta la **Tabla *18***, la cual permite dar descripciones a los apartados de la política que se abordan en el Apéndice R Política para la Gestión de Riesgos de Tecnologías de Información. Además, deja ver la manera en la que estas posibilitan la alineación con las buenas prácticas de la industria relacionadas con la gestión de riesgos de TI.

Tabla 18 *Apartados de la política de gestión de riesgos de TI*

Apartado	Descripción
Aprobación	Primer apartado se indica quien elaboro la política, quien la revisó y la persona que aprobó a nivel interno la política.
Revisión	La política cuenta con un cuadro de revisión donde se lleva un control de las versiones del documento con la fecha y un resumen de la revisión.

Apartado	Descripción
Objetivo	El objetivo de la política de gestión es establecer un marco formal y estructurado para la identificación, evaluación, tratamiento y monitoreo de los riesgos asociados a los sistemas de tecnología de la información de la Municipalidad de Turrialba.
Alcance	La política se aplica a todas las áreas, procesos, activos de información y sistemas tecnológicos gestionados por el Departamento de Tecnologías de Información de la Municipalidad de Turrialba. Cubre a todos los colaboradores, incluyendo la gerencia municipal, directores, jefes de departamento, funcionarios, contratistas y terceros que prestan servicios o tienen relación con el departamento.
Términos y definiciones	Se proporcionan definiciones clave para estandarizar el entendimiento y la aplicación de la política.
Principios	La gestión de riesgos de TI en la municipalidad se basa en los siguientes principios: adaptación al contexto, colaboración, dinamismo, enfoque en el valor y mejora continua.
Proceso de evaluación de riesgos	El proceso de evaluación de riesgos sigue un enfoque sistemático que incluye las siguientes etapas: 1) preparación para la evaluación, donde se establecen los objetivos, el alcance, los supuestos y limitaciones; 2) realización de la identificación de riesgos y la evaluación de la probabilidad e impacto de los riesgos; 3) comunicación de los resultados a las partes interesadas de manera comprensible y oportuna; 4) mantenimiento continuo de la evaluación, que implica actualizarla conforme cambian los riesgos, el entorno o los sistemas involucrados.
Roles y responsabilidades	La política asigna responsabilidades específicas para garantizar una gestión adecuada de los riesgos.

Apartado	Descripción
Prácticas de gestión	La política establece las prácticas de gestión que incluyen recopilación de datos, análisis del riesgo, mantenimiento del perfil de riesgo, articulación del riesgo, articulación del riesgo y respuesta al riesgo. Como se definen las tareas requeridas en la sección 4.2.4 Tareas o actividades que requiere el proceso formal de gestión de riesgos.
Definición de la metodología de evaluación de riesgos	La metodología de evaluación de riesgos se define como un proceso estructurado y continuo que comienza con la identificación de los riesgos a través de la clasificación de activos, la identificación de amenazas y vulnerabilidades, y la consideración del contexto operativo.
Revisión y mejora continua	La política establece que el proceso de gestión de riesgos debe ser revisado de manera periódica, al menos una vez al año, o inmediatamente después de la ocurrencia de un incidente de seguridad significativo.
Cumplimiento y auditoría	La política incluye disposiciones para garantizar el cumplimiento normativo y regulatorio, incluyendo auditorías periódicas tanto internas como externas.
Documentos relacionados	La política define aquellos documentos que se relacionan con este, el cual complementa es el documento de procedimientos para la gestión de riesgos de TI.
Referencias	La política se apoya en varias normativas y guías internacionales, como la ISO 31000, para la gestión de riesgos; la ISO 27005, para la gestión de riesgos de seguridad de la información; el marco ITIL 4, la NIST 800-30, para la evaluación de riesgos, la ISO 9001 para los estándares de calidad y el marco COBIT 2019, el cual facilita la gobernanza y la gestión de TI, siendo base del proceso de gestión de riesgos de TI.

La Tabla 18 resume los aspectos que se desarrollaron para definir la normativa interna de la municipalidad que está relacionada con la gestión de riesgos de TI. Este documento facilita formalizar el proceso que se describe en la siguiente sección.

5.1.1.1 Proceso de evaluación de riesgos

El propósito de esta sección es proporcionar orientación para la realización de evaluaciones de riesgos de los sistemas de información tomando los principios de la Publicación Especial 800-30. Las evaluaciones de riesgos, llevadas a cabo en los tres niveles de la jerarquía de gestión de riesgos, son parte de un proceso general de gestión de riesgos, proporcionando a los líderes/ejecutivos de alto nivel la información necesaria para determinar los cursos de acción apropiados en respuesta a los riesgos identificados (NIST, 2012). En esta sección se proponen los siguientes pasos para la evaluación de los riesgos:

5.1.1.1.1 Paso 1 Prepararse para la evaluación

La preparación implica reconocer el objetivo, como el establecimiento de una línea de base de riesgos o la identificación de vulnerabilidades, amenazas, probabilidad e impacto. También incluye definir el alcance, determinar qué secciones de un sistema u organización participan en la evaluación de riesgos y especificar las decisiones en las que influyen los resultados (NIST, 2012).

5.1.1.1.2 Etapa 2 Realización de la evaluación

Durante la fase de identificación, la atención se centra en reconocer las amenazas, las vulnerabilidades, la probabilidad y el impacto. El enfoque varía en función de la naturaleza del sistema y de los resultados de la fase de preparación. El NIST proporciona un conjunto específico de tareas, que abarcan tareas como la identificación de las fuentes de amenaza, las capacidades del adversario, la intención y los objetivos, así como la evaluación de la relevancia de los eventos de amenaza para el sistema (NIST, 2012).

5.1.1.1.3 Paso 3 Comunicar los resultados

Esta fase se encuentra entre las más críticas, aunque a menudo se pasa por alto, del proceso de gestión de riesgos. La evaluación de riesgos proporciona datos esenciales para orientar las acciones destinadas a mejorar la seguridad del sistema. Sin embargo, la comunicación eficaz es primordial en esta etapa (NIST, 2012).

5.1.1.1.4 Paso 4 Mantener la evaluación

Según NIST SP 800-30, implica supervisar y actualizar continuamente la evaluación para reflejar los cambios en el sistema, el entorno y las amenazas. Este proceso continuo garantiza que la evaluación de riesgos siga siendo pertinente y eficaz a lo largo del tiempo. Incluye revisiones periódicas de los factores de riesgo, la reevaluación de las vulnerabilidades y amenazas, y el ajuste de las estrategias de gestión de riesgos según sea necesario (NIST, 2012).

5.1.1.2 Creación de inventarios

Para la gestión de los riesgos es requerido la elaboración de un inventario exhaustivo de todos los activos de la organización, tanto materiales como inmateriales. Los activos materiales pueden incluir hardware, software, instalaciones y equipos, mientras que los activos inmateriales pueden incluir propiedad intelectual, datos y reputación de marca (Asociación Española de Normalización, 2024). Para la municipalidad se propone la siguiente estructura para este inventario de activos:

Tabla 19 Creación de Inventarios

Categoría	**Descripción**
Nombre del activo	El nombre del activo que se está evaluando.
Confidencialidad	El impacto que tendría una violación de la confidencialidad del activo. Esto podría incluir pérdidas financieras, daños a la reputación o responsabilidad legal, tomando valores bajos, medios y altos.
Integridad	El impacto que tendría una alteración de la integridad del activo. Esto podría incluir corrupción de datos, información inexacta o mal funcionamiento del sistema, tomando valores bajos, medios y altos.
Disponibilidad	El impacto que tendría una alteración de la disponibilidad del activo. Esto podría incluir la interrupción del negocio, pérdidas de productividad o insatisfacción del cliente, tomando valores bajos, medios y altos.

Categorizar los activos en función de su criticidad, valor y relevancia para las operaciones empresariales. Este paso ayuda a priorizar los activos para su posterior análisis y medidas de protección (Asociación Española de Normalización, 2024). La categorización se propone a través de tres dimensiones fundamentales:

1. Confidencialidad:
    a. Impacto bajo: La violación provoca pérdidas financieras mínimas, un daño limitado a la reputación o una responsabilidad legal mínima.
    b. Impacto medio: La violación provoca pérdidas económicas moderadas, daños notables a la reputación o cierta responsabilidad legal.

c. Impacto alto: La brecha causa pérdidas financieras significativas, daño reputacional severo, o responsabilidad legal sustancial.

2. Integridad:

   a. Impacto bajo: La alteración da lugar a una corrupción menor de los datos, inexactitudes limitadas o disfunciones mínimas del sistema.

   b. Impacto medio: La alteración provoca una corrupción moderada de los datos, inexactitudes notables o algunos fallos del sistema.

   c. Impacto alto: La alteración provoca una corrupción sustancial de los datos, inexactitudes críticas o graves disfunciones del sistema.

3. Disponibilidad:

   a. Impacto bajo: La alteración provoca una interrupción menor del negocio, pérdidas limitadas de productividad o una insatisfacción mínima de los clientes.

   b. Impacto medio: La perturbación provoca una interrupción moderada del negocio, pérdidas notables de productividad o cierta insatisfacción de los clientes.

   c. Impacto alto: La perturbación provoca una interrupción significativa de la actividad, pérdidas sustanciales de productividad o una grave insatisfacción de los clientes.

5.1.1.3 Clasificación del riesgo

Para la clasificación de los riesgos, se proponen en la política las siguientes categorías:

- Amenazas humanas: Riesgos derivados de la acción o error humano, ya sea intencional (como ataques internos) o no intencional (como errores operativos o de configuración).
- Amenazas tecnológicas: Riesgos asociados a la infraestructura tecnológica, como fallos de hardware, ciberataques, vulnerabilidades de software, o problemas derivados del uso indebido de la tecnología.
- Riesgos ambientales: Riesgos relacionados con factores naturales, como desastres naturales (terremotos, inundaciones, huracanes) o condiciones climáticas adversas que puedan afectar la operación de la organización.
- Riesgos operativos: Riesgos relacionados con fallos en los procesos internos, la gestión de recursos, o la incapacidad para ejecutar operaciones de manera efectiva.
- Riesgos regulatorios y de cumplimiento: Riesgos derivados del incumplimiento de leyes, regulaciones o normativas aplicables, lo que puede resultar en sanciones legales o daños a la reputación.
- Riesgos sociales y políticos: Riesgos relacionados con cambios en el entorno social y político, como inestabilidad política, cambios legislativos, o problemas de reputación organizacional derivados de factores sociales.

- Riesgos emergentes: Riesgos asociados a nuevas amenazas que pueden surgir debido a avances tecnológicos, cambios en el mercado, o nuevas regulaciones que aún no se han identificado completamente.
- Amenazas a la cadena de suministro: Riesgos derivados de interrupciones en la cadena de suministro, como la falta de proveedores, problemas logísticos, o riesgos asociados con la calidad y la seguridad de los productos y servicios adquiridos.

5.1.1.4 Criterios para realizar evaluaciones de riesgos

La ISO 27005, especifican que los criterios de evaluación de riesgos se determinan en términos de sus consecuencias, probabilidad y nivel de riesgo. Los criterios de consecuencia deben desarrollarse y especificarse en términos del alcance del daño o pérdida, o del perjuicio para una organización o individuo resultante de la pérdida de confidencialidad, integridad y disponibilidad de la información. Para determinar el nivel de consecuencia se propone dentro de la política seguir la siguiente escala cualitativa:

Tabla 20 Escala para determinar el Impacto

Consecuencias	Valor semi cuantitativo	Descripción
5 - Catastrófico	96-100	Consecuencias regulatorias o sectoriales más allá de la organización. Ecosistema(s) sectorial(es) sustancialmente impactado(s), con consecuencias que pueden ser duraderas. Y/o: dificultad para el Estado, e incluso una incapacidad para asegurar una función reguladora o una de sus misiones de vital importancia. Y/o: consecuencias críticas en la seguridad de las personas y la propiedad (crisis sanitaria, contaminación ambiental, destrucción de infraestructuras esenciales, etc.).
4 - Crítico	80-95	Consecuencias desastrosas para la organización. Incapacidad de la organización para asegurar todo o parte de su actividad, con posibles consecuencias graves en la seguridad de las personas y la propiedad. Es poco probable que la organización supere la situación (su supervivencia está amenazada), los sectores de actividad o los sectores del Estado en los que opera probablemente se verán ligeramente afectados, sin consecuencias duraderas.
3 - Serio	21-79	Consecuencias sustanciales para la organización. Alta degradación en el desempeño de la actividad, con posibles consecuencias significativas en la seguridad de las personas y la propiedad. La organización superará la situación con serias dificultades (operación en modo altamente degradado), sin impacto en el sector o en el Estado.

Consecuencias	Valor semi cuantitativo	Descripción
2 - Significativo	5-20	Consecuencias significativas pero limitadas para la organización. Degradación en el desempeño de la actividad sin consecuencias en la seguridad de las personas y la propiedad. La organización superará la situación a pesar de algunas dificultades (operación en modo degradado).
1 - Menor	0-4	Consecuencias insignificantes para la organización. Sin consecuencias en las operaciones o el desempeño de la actividad o en la seguridad de las personas y la propiedad. La organización superará la situación sin muchas dificultades (se consumirán los márgenes).

La probabilidad de un riesgo se determina a partir de:

- La utilización de información proveniente de incidentes anteriores, estadísticas del sector y mejores prácticas de la industria.
- Consulta de informes de inteligencia de amenazas, bases de datos de vulnerabilidades y estudios de casos relevantes.
- Aplicación del conocimiento y la experiencia de los miembros del equipo de gestión de riesgos para complementar los datos objetivos.

La probabilidad de un riesgo no es un valor estático, sino que puede variar en el tiempo debido a cambios en el entorno de la organización, la aparición de nuevas amenazas o la implementación de nuevas medidas de seguridad. Para determinar la probabilidad se propone la siguiente escala cualitativa de probabilidad:

Tabla 21 Escala de Probabilidad

Probabilidad	Valor semi cuantitativo	Descripción
5 - Casi seguro	96%-100%	La fuente de riesgo casi con certeza alcanzará su objetivo utilizando uno de los métodos de ataque considerados. La probabilidad del escenario de riesgo es muy alta.
4 - Muy probable	80%-95%	La fuente de riesgo probablemente alcanzará su objetivo utilizando uno de los métodos de ataque considerados. La probabilidad del escenario de riesgo es alta.
3 - Probable	21%-79%	La fuente de riesgo es capaz de alcanzar su objetivo utilizando uno de los métodos de ataque considerados. La probabilidad del escenario de riesgo es significativa.

Probabilidad	Valor semi cuantitativo	Descripción
2 - Poco probable	5%-20%	La fuente de riesgo tiene relativamente pocas posibilidades de alcanzar su objetivo utilizando uno de los métodos de ataque considerados. La probabilidad es baja.
1 - Improbable	0%-4%	La fuente de riesgo tiene muy pocas posibilidades de alcanzar su objetivo utilizando uno de los métodos de ataque considerados. La probabilidad es muy baja.

El propósito de las escalas para el nivel de riesgo es ayudar a los propietarios del riesgo a decidir sobre la retención o el tratamiento de los riesgos y a priorizarlos para su tratamiento.

5.1.1.5 Determinar el Nivel de Riesgo

El nivel de riesgo asociado con los eventos de riesgos identificados representa una determinación del grado en que la municipalidad está amenazada por tales eventos. Las organizaciones hacen explícita la incertidumbre en las determinaciones de riesgo, incluyendo, por ejemplo, las suposiciones organizacionales y los juicios/decisiones subjetivas. Las organizaciones pueden ordenar la lista de eventos de amenaza de interés según el nivel de riesgo determinado durante la evaluación de riesgos, prestando mayor atención a los eventos de alto riesgo. El nivel de riesgo se mapea en el siguiente mapa de calor:

Tabla 22 Mapa de Calor Nivel de Riesgo

Probabilidad	Consecuencia				
	Catastrófico	**Crítico**	**Serio**	**Significativo**	**Menor**
Casi seguro	Muy alto	Muy alto	Alto	Alto	Medio
Muy probable	Muy alto	Alto	Alto	Medio	Bajo
Probable	Alto	Alto	Medio	Bajo	Bajo
Poco probable	Medio	Medio	Bajo	Bajo	Muy bajo
Improbable	Bajo	Bajo	Bajo	Muy bajo	Muy bajo

El tratamiento de riesgos implica la identificación de la gama de opciones para hacer frente a los riesgos, la evaluación de dichas opciones, la preparación de planes de tratamiento de riesgos y su aplicación. Con el fin de controlar los riesgos identificados en el proyecto, se establen las siguientes medidas para tratarlos adecuadamente:

- Reducción de riesgos
- Transferencia
- Evitar el riesgo
- Aceptación del riesgo

5.1.2 Elaboración de Procedimientos de Gestión de Riesgos de TI

Se elaboraron procedimientos detallados que describan cómo se deben implementar las políticas para la gestión de riesgos definidas. Estos procedimientos especifican los pasos operativos para cada actividad de gestión de riesgos. Además, se detallan los pasos para la identificación, evaluación, priorización, y tratamiento de riesgos. También se incluyen procedimientos para el monitoreo y revisión continua.

A continuación, se presenta la **Tabla *23***, la cual describe los apartados de los procedimientos que se abordan en el Apéndice S Procedimientos para la gestión de Riesgos de TI.

Tabla 23 *Apartados de Procedimientos de gestión de riesgos de TI*

Apartado	Descripción
Aprobación	Primer apartado se indica quien elaboro la política, quien la revisó y la persona que aprobó a nivel interno la política.
Revisión	La política cuenta con un cuadro de revisión donde se lleva un control de las versiones del documento con la fecha y un resumen de la revisión.
Objetivo	El objetivo de los procedimientos de gestión de riesgos de tecnología de la información es presentar de manera clara y coherente las actividades y pasos por seguir para implementar y cumplir con los elementos clave de la política de gestión de riesgos de TI.
Términos y Definiciones	Se proporcionan definiciones clave para estandarizar el entendimiento y la aplicación del procedimiento.
Proceso: valoración de riesgos de TI	Consiste en la identificación de activos críticos, amenazas y vulnerabilidades, clasificación de riesgos, estimación de probabilidad e impacto y priorización de riesgos. Este proceso busca asegurar una evaluación coherente y alineada con las normativas aplicables. También se trabaja como un proceso continuo para darle monitoreo y seguimiento a los riesgos y eventos identificados.

Apartado	Descripción
Proceso: especificación de requisitos para proyectos de mitigación	Define los proyectos y controles necesarios para mitigar los riesgos identificados en la valoración, alineando estos proyectos con las mejores prácticas de la industria y las normativas regulatorias. Además, se contará con métricas para monitorear su implementación y efectividad.
Proceso: inventario de procesos de negocio y dependencias	Implica la creación y mantenimiento de un inventario actualizado de los procesos clave de la municipalidad, detallando sus dependencias con la infraestructura tecnológica. Además, aborda la identificación de responsables, infraestructuras críticas y proveedores esenciales. Esto proporciona una visión integral del entorno operativo, facilitando la evaluación de riesgos asociados a interrupciones, fallos tecnológicos o dependencias externas, y apoyando la priorización de medidas preventivas y correctivas para mitigar impactos en los servicios esenciales.
Proceso: preparación y prueba de planes de respuesta a incidentes	Establece planes detallados para responder a incidentes críticos de TI. Incluye la identificación de escenarios de incidentes, rutas de escalamiento, asignación de roles y pruebas periódicas del plan para garantizar su efectividad ante posibles crisis. Aseguran que las respuestas estén alineadas con los riesgos identificados y que los controles sean efectivos
Proceso: aplicación de los planes de respuesta	Describe los pasos por seguir, según las medidas previamente definidas ante la materialización de un riesgo. Incluye la activación de planes de respuesta, escalamiento del incidente, coordinación entre equipos y comunicación con las partes interesadas para minimizar el impacto y asegurar una rápida recuperación.
Indicadores de Desempeño	El procedimiento define sus indicadores de desempeño estableciendo el nombre del indicador, código, responsable, fórmula para calcular el indicador, frecuencia, fuente de datos, meta de desempeño y el nivel de tolerancia.

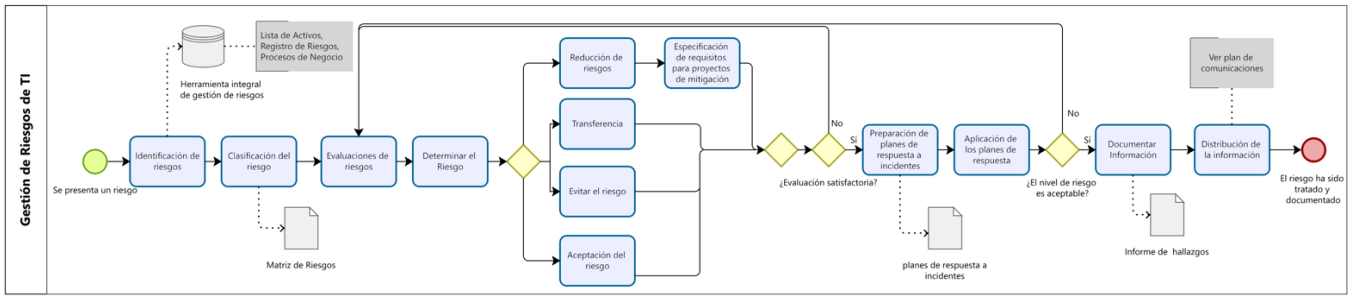
Apartado	Descripción
Plan de comunicaciones	Asegura que todas las partes interesadas estén debidamente informadas sobre el proceso de gestión de riesgos. Incluye una matriz de comunicación que detalla el tipo de información que se compartirá, la frecuencia, el emisor, el receptor y los medios utilizados para la transmisión de la información.
Documentos relacionados	El procedimiento define aquellos documentos que se relacionan con este, el cual complementa es el documento de política para la gestión de riesgos de TI.
Referencias	El procedimiento se apoya en varias normativas y guías internacionales, como la ISO 31000, para la gestión de riesgos; la ISO 27005, para la gestión de riesgos de seguridad de la información; el marco ITIL 4, la NIST 800-30, para la evaluación de riesgos, la ISO 9001 para los estándares de calidad y el marco COBIT 2019, el cual facilita la gobernanza y la gestión de TI, siendo base del proceso de gestión de riesgos de TI.

La Tabla 23 resume los apartados que se desarrollaron para definir los procedimientos internos de la municipalidad en relación con la gestión de riesgos de TI. Este documento facilita formalizar el proceso de gestión de riesgos de TI.

5.1.2.1 Modelado del proceso to-be

El modelado del proceso to-be representa el proceso posterior a la implementación de la propuesta. El modelado se puede ver en la Figura 16 o en el Apéndice Q Modelado to-be y permite visualizar los cambios propuestos de manera gráfica e identificar claramente las nuevas secuencias de actividades.

Figura 16 *Modelado del Proceso to-be*



Este procedimiento detalla las actividades necesarias para la recolección, clasificación, análisis y registro de datos relacionados con los riesgos de TI dentro de la municipalidad. A partir de dicho procedimiento, se asegura la consistencia en la gestión de riesgos y se ajusta a los cambios en el entorno operativo y normativo.

1. Identificación de riesgos:
    a. Identificación de activos críticos: en este proceso se realiza un inventario exhaustivo de los activos tecnológicos, clasificándolos según su importancia para la continuidad del negocio. Los activos deben categorizarse en función de su criticidad, valor y relevancia para las operaciones, en las dimensiones de confidencialidad, integridad y disponibilidad.
    b. Identificación de amenazas y vulnerabilidades: se listan las amenazas potenciales y las vulnerabilidades asociadas a cada activo crítico.
    c. Identificación de eventos de riesgo: se registra cualquier incidente de seguridad, vulnerabilidad detectada, problema operativo o evento que afecte la continuidad del negocio o la seguridad de los sistemas.
    d. Identificación de procesos de negocios: se debe crear y mantener un inventario detallado y actualizado de los procesos de negocio de la municipalidad, que toma como punto de partida la identificación de la dependencia de cada uno con los servicios de TI y la infraestructura tecnológica. El inventario debe incluir el personal clave, las infraestructuras críticas, las aplicaciones y los proveedores y terceros que sean esenciales para el funcionamiento del negocio.
    e. Registro del riesgo: se registran los eventos con el código E00 y se indican el nombre del evento, sus causas, el impacto, las medidas correctivas que se deben adoptar, las recomendaciones para prevenir incidentes y el estado del evento (registrado, en proceso o solucionado).
2. Clasificación de los riesgos: se deben clasificar los riesgos identificados en categorías como amenazas humanas, amenazas tecnológicas, riesgos ambientales, riesgos operativos, riesgos regulatorios y de cumplimiento, riesgos sociales y políticos, riesgos emergentes y amenazas a la cadena de suministro.
3. Evaluación del riesgo:
    a. Determinación de la probabilidad: se utilizan datos históricos, informes de incidentes y el conocimiento del equipo para estimar la probabilidad de que un riesgo ocurra.
    b. Evaluación del impacto: se estima las pérdidas potenciales en términos financieros, operacionales y reputacionales para cada activo en riesgo.
4. Determinar el riesgo: se determina el nivel de riesgo combinando probabilidad e impacto y destacando aquellos riesgos que requieren atención inmediata.

5. Identificación de opciones de tratamiento: para cada riesgo se deben definir las estrategias de tratamiento:
    a. Reducción de riesgos: a través de la implementación de medidas que disminuyen el riesgo general.
    b. Riesgo compartido o transferencia: se transfiere el riesgo a terceros mediante seguros o proveedores de servicios.
    c. Evitar el riesgo: se elimina el riesgo absteniéndose de realizar actividades que expongan a la municipalidad a amenazas potenciales.
    d. Aceptar el riesgo: se opta por aceptar el riesgo si se encuentra dentro de los parámetros de tolerancia de la municipalidad.
6. En caso de que la evaluación del riesgo no sea satisfactoria, el riesgo debe volver a ser evaluado, por lo tanto, ir al paso 3.
7. Preparación y prueba de planes de respuesta a incidentes: se deben preparar, mantener y probar regularmente planes de respuesta ante incidentes críticos que puedan generar un impacto significativo en las operaciones. Los planes deben documentar pasos claros por seguir, rutas de escalamiento dentro de la municipalidad y roles y responsabilidades para minimizar el impacto de los incidentes.
8. Aplicación de los planes de respuesta: cuando ocurra un incidente de riesgo, los planes de respuesta documentados deben aplicarse de manera efectiva. Esto implica seguir los pasos predefinidos en el plan y asegurar que las acciones minimicen el impacto del incidente, además de continuar con los procedimientos de escalamiento apropiados para gestionar la situación.
9. En caso de que el nivel de riesgo tras su tratamiento no sea aceptable, el riesgo debe de volver a ser evaluado, es decir, volver al paso 3.
10. Documentar información: se debe preparar un informe estructurado que resuma los hallazgos clave y las descripciones claras, y que resalte los riesgos críticos.
    a. Generación de informes de seguimiento: se crean informes que incluyan el estado actual del perfil de riesgo, destacando las áreas de mayor preocupación y los avances en las acciones correctivas implementadas.
11. Distribución de la información: se deben proporcionar los informes detallados a los responsables de la toma de decisiones, asegurando una respuesta oportuna y bien informada. Para este paso, ver la matriz de comunicaciones.

5.1.3 Diseño de una Herramienta Integral de Gestión de Riesgos

Se diseña una herramienta integral utilizando Excel con una serie de tablas que incluyen los mecanismos de monitoreo y seguimiento de riesgos, así como un plan de comunicación para asegurar la involucración y el compromiso de todas las partes interesadas. Por otro lado, se incorpora una matriz de riesgos que permite la visualización y el seguimiento continuo de los riesgos identificados.

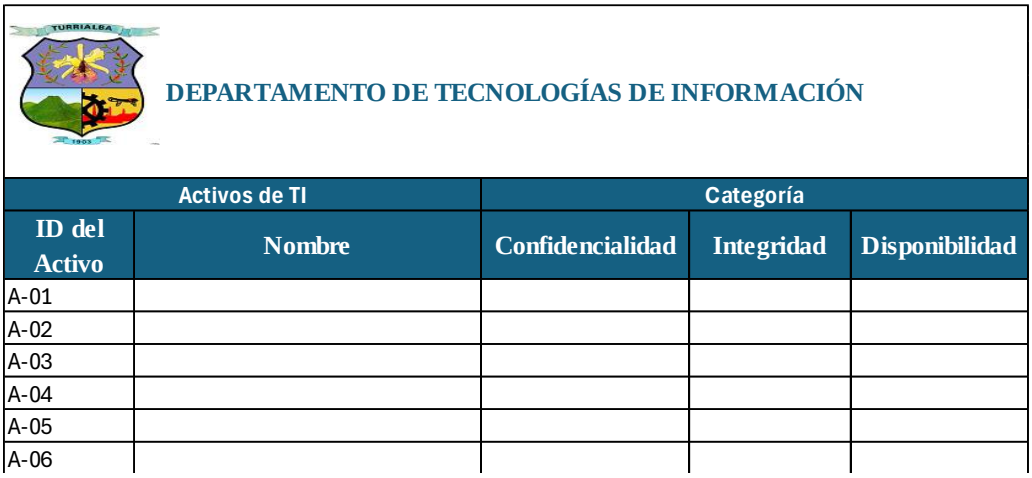
5.1.3.1 Lista de activos

Uno de los pasos fundamentales dentro de la gestión de riesgos es la identificación y clasificación de los activos de tecnología de la información. Los activos de TI son todos aquellos recursos tecnológicos críticos para la operación de la Municipalidad de Turrialba, que incluyen *hardware, software,* redes, datos e infraestructuras. La correcta identificación y categorización de estos activos permite evaluar su criticidad y vulnerabilidad dentro del entorno operativo, asegurando que los controles y medidas de mitigación de riesgos sean aplicados de manera adecuada. La lista de activos no solo incluye la identificación de cada recurso tecnológico, sino que también los clasifica en función de tres dimensiones clave:

1. Confidencialidad:
    a. Impacto bajo: la violación provoca pérdidas financieras mínimas, un daño limitado a la reputación o una responsabilidad legal mínima.
    b. Impacto medio: la violación provoca pérdidas económicas moderadas, daños notables a la reputación o cierta responsabilidad legal.
    c. Impacto alto: la brecha causa pérdidas financieras significativas, daño reputacional severo, o responsabilidad legal sustancial.
2. Integridad:
    a. Impacto bajo: la alteración da lugar a una corrupción menor de los datos, inexactitudes limitadas o disfunciones mínimas del sistema.
    b. Impacto medio: la alteración provoca una corrupción moderada de los datos, inexactitudes notables o algunos fallos del sistema.
    c. Impacto alto: la alteración provoca una corrupción sustancial de los datos, inexactitudes críticas o graves disfunciones del sistema.
3. Disponibilidad:
    a. Impacto bajo: la alteración provoca una interrupción menor del negocio, pérdidas limitadas de productividad o una insatisfacción mínima de los clientes.
    b. Impacto medio: la perturbación provoca una interrupción moderada del negocio, pérdidas notables de productividad o cierta insatisfacción de los clientes.
    c. Impacto alto: la perturbación provoca una interrupción significativa de la actividad, pérdidas sustanciales de productividad o una grave insatisfacción de los clientes.

Estas dimensiones reflejan la importancia de proteger la información y los sistemas, asegurando que los datos se mantengan privados, correctos y accesibles cuando sean requeridos. La clasificación permite priorizar los esfuerzos de mitigación y establecer los controles adecuados para cada activo, según su impacto potencial en la operación de la organización. En la Figura 17 se presenta la plantilla para la lista de activos de TI:

Figura 17 *Plantilla lista de activos*



DEPARTAMENTO DE TECNOLOGÍAS DE INFORMACIÓN

Activos de TI		Categoría		
ID del Activo	Nombre	Confidencialidad	Integridad	Disponibilidad
A-01				
A-02				
A-03				
A-04				
A-05				
A-06				

Las columnas de confidencialidad, integridad y disponibilidad tienen una lista desplegable con las clasificaciones definidas en la política.

5.1.3.2 Registro de Riesgos

El registro de riesgos es una herramienta que permite llevar un control detallado de los riesgos identificados, su clasificación y evaluación y las medidas sugeridas para su tratamiento. Este registro no solo facilita la visualización y el seguimiento continuo de los riesgos, sino que también proporciona una base sólida para la toma de decisiones informadas.

Cada riesgo registrado es evaluado según su probabilidad de ocurrencia y el impacto potencial en los activos críticos de la Municipalidad de Turrialba. Estos factores determinan el nivel de riesgo según lo establece el proceso (Apéndice S Procedimientos para la gestión de Riesgos de TI). El registro incluye información detallada de los riesgos:

- Nombre del riesgo: descripción clara y concisa del riesgo identificado.
- Clasificación: categoría a la que pertenece el riesgo.
    - Amenazas humanas
    - Amenazas tecnológicas
    - Riesgos ambientales
    - Riesgos operativos
    - Riesgos regulatorios y de cumplimiento
    - Riesgos sociales y políticas
    - Riesgos emergentes
    - Amenazas a la cadena de suministro
- Descripción del evento: explicación del posible incidente que podría ocurrir si el riesgo se materializa.
- Activo afectado: identificación del activo de TI que se vería impactado.
- Causas y consecuencias: factores que podrían detonar el riesgo y las consecuencias en términos operativos, financieros o reputacionales.

- Probabilidad e impacto: evaluación del riesgo en términos de su probabilidad de ocurrencia y su impacto potencial.
- Nivel de riesgo: valoración del riesgo combinando probabilidad e impacto para determinar su criticidad.
- Tratamiento sugerido: recomendaciones sobre el modo de mitigar, evitar, transferir o aceptar el riesgo.
    - Reducción de riesgos
    - Transferencia
    - Evitar el riesgo
    - Aceptación del riesgo

En la **Figura *18*** se muestra la plantilla para el registro de los riesgos:

Figura 18 *Plantilla Registro de riesgos*

ID del Riesgo	NOMBRE DEL RIESGO	CLASIFICACIÓN	DESCRIPCIÓN DEL EVENTO	ACTIVO AFECTADO	CAUSAS	CONSECUENCIAS	NIVEL DE RIESGO						TRATAMIENTO SUGERIDO
							PROBABILIDAD		IMPACTO		VALOR	NIVEL DE RIESGO	
							VALOR	NIVEL	VALOR	NIVEL			
R01	Abuso de derechos por parte de los usuarios del sistema	Amenazas Humanas					99,0%	Casi seguro	99	Catastrófico	98,01	Muy Alto	Evitar el riesgo
R02	Acceso no autorizado a aplicaciones por parte de los	Amenazas Humanas					0,0%	Improbable	0	Menor	0	Muy Bajo	
R03	Conformación inadecuada de contraseñas (insegura, débiles)	Amenazas Humanas						Improbable		Menor	0	Muy Bajo	
R04	Uso compartido de contraseñas por parte de los usuarios	Amenazas Humanas						Improbable		Menor	0	Muy Bajo	
R05	Robo o perdida de información por controles inadeacuados	Amenazas Humanas						Improbable		Menor	0	Muy Bajo	
R06	Capacitación inadecuada a los usuarios del sistema en la forma de administrar los recursoa asignados	Amenazas Humanas						Improbable		Menor	0	Muy Bajo	

Los riesgos de la plantilla son los identificados por el MICITT en su portafolio de riesgos (2021).

5.1.3.3 Procesos de Negocio

Para garantizar una adecuada gestión de los riesgos tecnológicos que puedan impactar en la operación de la Municipalidad de Turrialba, es necesario la identificación de los procesos de negocio clave y sus respectivas dependencias tecnológicas. El proceso de identificación de dependencias se enfoca en cuatro áreas principales:

- Dependencias tecnológicas: se refiere a los sistemas, aplicaciones o redes de los que el proceso de negocio depende para su correcto funcionamiento.
- Infraestructura: incluye los componentes físicos, como servidores, centros de datos y redes que soportan los procesos.
- Personal: identificación del personal clave responsable de la operación, supervisión y mantenimiento del proceso.
- Proveedores: se refiere a los terceros que proveen servicios críticos para el desarrollo de los procesos de negocio.
- Dueño del proceso: es la persona o área de la municipalidad que tiene la responsabilidad final sobre el proceso de negocio. Además, es quien supervisa la implementación, el monitoreo y la mejora continua del proceso, asegurando que este funcione conforme a los objetivos establecidos.

El análisis de estas áreas permite visualizar la infraestructura y los sistemas necesarios para cada proceso y evaluar los riesgos potenciales y determinar las medidas para cada proceso. En la Figura 19 se presenta la plantilla para identificar los procesos de negocio de la municipalidad, junto con sus dependencias tecnológicas, infraestructura asociada, personal clave y proveedores relevantes.

Figura 19 *Plantilla Lista de Procesos de Negocio*

DEPARTAMENTO DE TECNOLOGÍAS DE INFORMACIÓN

ID del Proceso	Nombre del Proceso	Dependencias Tecnológicas	Infraestructura	Personal	Proveedor	Dueño del proceso
P01						
P02						
P03						
P04						

5.1.3.4 Matriz de Riesgo

La matriz de riesgos es una herramienta diseñada para la identificación, seguimiento y monitoreo de los eventos una vez que se ha materializado. La matriz incluye detalles sobre:

- Nombre del evento: breve descripción del incidente o situación de riesgo.
- Fecha del evento: fecha en la que el riesgo fue identificado o se materializó.
- Reportado por: nombre del funcionario o sistema que notifica del evento.
- Descripción del evento: resumen detallado del evento de riesgo, sus causas y posibles consecuencias.
- Tipo de riesgo: clasificación del riesgo.
- Activo afectado: el recurso de TI impactado por el riesgo.
- Causa del evento: factores que contribuyeron a la materialización del riesgo.
- Impacto del evento: evaluación de las consecuencias del riesgo, tanto operativas como financieras o reputacionales.
- Nivel de riesgo: combina la probabilidad que tenía el evento de manifestarse, según los riesgos registrados, y el impacto del riesgo, a la vez que determina su criticidad.
- Tratamiento del riesgo: acciones sugeridas para mitigar, evitar, transferir o aceptar el riesgo.
- Responsable: persona o equipo responsable de gestionar el riesgo.
- Acciones realizadas: detalle de las medidas implementadas para gestionar o mitigar el riesgo.
- Estado: estado actual del riesgo (registrado, en proceso de gestión, solucionado).

En la **Figura *20*** se presenta una tabla que detalla la plantilla de la matriz de riesgos.

Figura 20 *Plantilla Matriz de Riesgos*

ID del Evento	Nombre del Evento	Fecha del evento	Reportado por:	Descripción del evento	Tipo de Riesgo	Activo Afectado	Causa del evento	Impacto del evento	NIVEL DE RIESGO						Tratamiento del riesgo	Responsable	Acciones realizadas	ESTADO
									PROBABILIDAD		IMPACTO		VALOR	NIVEL DE RIESGO				
									VALOR	NIVEL	VALOR	NIVEL						
E01										Improbable		Menor	0	Muy Bajo	Evitar el riesgo			
E02										Improbable		Menor	0	Muy Bajo				
E03										Improbable		Menor	0	Muy Bajo				
E04										Improbable		Menor	0	Muy Bajo				
E05										Improbable		Menor	0	Muy Bajo				

5.1.4 Plan de Comunicaciones

Se proporciona el plan de comunicaciones respecto al proceso de gestión de riesgos de TI (el Apéndice S Procedimientos para la gestión de Riesgos de TI), que es esencial para asegurar la ejecución adecuada del mismo.

5.1.4.1 Grupos de Interés

Los grupos de interés dentro del proceso de gestión de riesgos de TI de la Municipalidad de Turrialba incluyen a todas las personas o entidades que tienen un rol activo o que son impactadas por el éxito o el fracaso en la mitigación de riesgos. En la **Tabla *24*** se detallan los principales grupos de interés y sus respectivas responsabilidades:

Tabla 24 *Grupos de Interés*

Grupo	Rol	Interés	Necesidades de información
Alcalde municipal y concejo	Aprobar políticas y decisiones estratégicas relacionadas con la gestión de riesgos de TI.	Asegurar que los riesgos tecnológicos no afecten las operaciones críticas de la municipalidad y que se alineen con los objetivos institucionales.	Resultados de evaluaciones de riesgos, recomendaciones de mitigación, informes de auditoría y cumplimiento normativo.
Encargados de departamento	Supervisar la implementación de los controles y acciones de mitigación dentro de sus respectivos departamentos.	Garantizar que los riesgos relacionados con sus áreas de operación sean gestionados adecuadamente y no afecten la continuidad de sus actividades.	Actualizaciones periódicas sobre los riesgos identificados y los controles implementados.
Departamento de TI	Responsable de la implementación y monitoreo continuo de las medidas de seguridad y control en la infraestructura tecnológica, así como de la gestión operativa de los riesgos tecnológicos.	Asegurar que los riesgos relacionados con la infraestructura tecnológica sean identificados y gestionados de manera eficiente, manteniendo la disponibilidad, integridad y confidencialidad de los sistemas de TI.	Procedimientos detallados de evaluación de riesgos, actualizaciones sobre amenazas emergentes, planes de respuesta a incidentes y cambios normativos que afecten la gestión de los riesgos tecnológicos.
Contratistas y terceros	Contratar proveedores de servicios que interactúan con los sistemas de TI de la municipalidad.	Asegurar que sus actividades cumplan con los estándares de seguridad establecidos por la municipalidad y que no introduzcan nuevos riesgos.	Políticas de seguridad, estándares técnicos y procedimientos de gestión de riesgos.

5.1.4.2 Priorización de la Información

La prioridad de la información que se debe comunicar dentro del proceso de gestión de riesgos de TI se establece en función de su relevancia para la ejecución de tareas críticas y su impacto en el logro de los objetivos institucionales. A continuación, se describen los niveles de prioridad asignados a la información:

- Prioridad alta: la información clasificada con prioridad alta es esencial para la ejecución de tareas críticas y tiene un impacto directo en la continuidad y calidad de los servicios prestados por la municipalidad de Turrialba. Cualquier retraso o falta de comunicación de esta información puede resultar en riesgos significativos o en el fracaso de procesos importantes. La comunicación de este tipo de información debe ser inmediata.
- Prioridad media: la información de prioridad media es importante para el desarrollo de las actividades, pero no es crítica para el éxito inmediato de los procesos. Esta información se comunica de forma oportuna, pero no es necesario hacerlo de inmediato, ya que no compromete de manera significativa las operaciones si se retrasa.
- Prioridad baja: la información clasificada como de prioridad baja es aquella que puede ser útil para los colaboradores y partes interesadas, pero cuya falta de comunicación inmediata no afecta de manera considerable los procesos operativos o la gestión de riesgos. Esta información se puede comunicar cuando los recursos y el tiempo lo permitan, sin un sentido de urgencia.

5.1.4.3 Matriz de Comunicaciones

Para sintetizar los anteriores puntos y visualizar de forma clara el plan de comunicaciones se desarrolla la **Tabla 25** Matriz de comunicaciones del proceso de gestión de riesgos de TI, una matriz que identifica la forma en que se comunican los diferentes aspectos planteados en el proceso. Dentro de la matriz de comunicaciones se incluyen los siguientes elementos:

- Información: nombre del documento o anuncio que se debe comunicar.
- Contenido: puntos por abordar dentro del documento.
- Emisor: persona encargada de comunicar la información.
- Receptor: destinatarios que reciben la información.
- Medio de comunicación: métodos utilizados para enviar la información.
- Frecuencia: período definido por tiempo o cumplimiento de condiciones en el cual se envía la información.

Tabla 25 *Matriz de comunicaciones*

Información	Contenido	Prioridad	Emisor	Receptor	Medio de comunicación	Frecuencia
Informe de evaluación de riesgos críticos	Resultados de la evaluación de riesgos críticos o recomendaciones para mitigación inmediata	Alta	Encargado de Servicios de TI	Alcalde, Concejo o encargados de departamento	Correo electrónico o reuniones ejecutivas	Inmediata tras la identificación de un riesgo crítico
Informe de riesgos de TI	Estado actual del perfil de riesgos, controles implementados o nuevas amenazas identificadas	Media	Encargado de Servicios de TI	Alcalde, concejo o encargados de departamento	Correo electrónico	Trimestral
Actualización de procedimientos de seguridad	Cambios en los procedimientos de respuesta a incidentes o medidas de seguridad adicionales	Alta	Encargado de Servicios de TI	Alcalde, concejo o encargados de departamento	Correo electrónico o reuniones ejecutivas	Semestral o cuando se produzcan cambios significativos
Informe de cumplimiento normativo	Resultados de auditorías o análisis de cumplimiento de las normativas locales e internacionales	Alta	Responsable de Auditoría Interna	Alcalde, concejo o encargados de departamento	Correo electrónico o reuniones ejecutivas	Anual o tras auditorías
Plan de respuesta a incidentes	Pasos detallados para la respuesta a incidentes críticos, roles y responsabilidades	Media	Responsable de seguridad del sistema	Alcalde, concejo o encargados de departamento	Correo electrónico o reuniones ejecutivas	Semestral
Boletín de buenas prácticas de seguridad	Consejos y recomendaciones sobre seguridad de la información o actualización de amenazas	Baja	Departamento de TI	Todos los colaboradores de la municipalidad	Correo electrónico	Mensual
Simulacro de respuesta a incidentes	Ejercicio práctico de respuesta a incidentes, evaluación del desempeño o retroalimentación	Media	Encargado de Servicios de TI	Alcalde, concejo o encargados departamento	Correo electrónico	Semestral

5.2 Verificación de Conformidad

El siguiente apartado equivale a la fase tres del procedimiento metodológico, el cual busca verificar la conformidad del marco propuesto con la norma técnica del MICITT, así mismo se define una estrategia para la implementación del proceso.

5.2.1 Revisión de Conformidad Normativa

Se realiza una revisión para asegurar que el proceso de gestión de riesgos cumple con los requisitos de la Norma Técnica del MICITT. Primero se mostrará el perfil del proceso, utilizando la plantilla del Apéndice P Plantilla Perfil del Proceso y una lista de comprobación (Apéndice K Plantilla Lista de Comprobación del Proceso de Gestión de Riesgos), junto con las actividades del proceso de gestión de riesgos de TI, que abarcan las políticas (Apéndice R Política para la Gestión de Riesgos de Tecnologías de Información) y los procedimientos (Apéndice S Procedimientos para la gestión de Riesgos de TI).

5.2.1.1 Perfil del proceso.

Para asegurar el cumplimiento de los requisitos establecidos en la Norma Técnica del MICITT, es esencial que el proceso de gestión de riesgos de TI esté formalmente definido y estructurado. El perfil del proceso es una herramienta que permite detallar los componentes del proceso, proporcionando claridad sobre los objetivos, responsabilidades, actividades y medidas de control necesarias para una gestión de riesgos eficaz.

Este perfil sigue los requerimientos establecidos por la norma, como se mencionan en la sección 2.2.3 Perfil del Proceso. En la Tabla 26 se presenta el perfil del proceso de gestión de riesgos de TI de la Municipalidad de Turrialba.

Tabla 26 *Perfil del proceso*

Perfil del proceso	
Elemento	**Descripción**
1. Objetivo y metas	**Objetivo del proceso:** identificar, evaluar y reducir continuamente los riesgos relacionados con TI dentro de los niveles de tolerancia establecidos por la gerencia ejecutiva de la empresa.
	Metas específicas: - Gestión de riesgo de negocio - Continuidad y disponibilidad del servicio de negocio - Gestión de riesgo relacionado con TI - Seguridad de la información, infraestructura de procesamiento y aplicaciones y privacidad
2. Propiedad del proceso	**Propietario del proceso:** encargado del Departamento de Tecnologías de Información.

Perfil del proceso	
Elemento	**Descripción**
3. Secuencia de actividades	Se establecen los subprocesos de: - Valoración de riesgos de TI - Especificación de requisitos para proyectos de mitigación - Inventario de procesos de negocio y dependencias - Preparación y prueba de planes de respuesta a incidentes - Aplicación de los planes de respuesta
4. Roles y responsabilidades	Ejecutivo de riesgos (ER): supervisa todo el proceso de gestión de riesgos, garantizando la alineación con las metas y objetivos de la municipalidad. Propietario del riesgo (RO): responsable de un riesgo específico y facultado para tomar decisiones en relación con ese riesgo; pueden ser jefes de departamento, gestores de proyectos o propietarios de sistemas. Analista de riesgos (AR): realiza evaluaciones de riesgos, incluyendo la identificación, el análisis y la evaluación de los riesgos y proporcionando los datos necesarios para la toma de decisiones.
5. Indicadores de Desempeño	• Porcentaje de objetivos y servicios críticos del negocio, cubiertos por la evaluación de riesgos. • Número de interrupciones del servicio al cliente o procesos empresariales que han causado incidentes significativos. • Coste de incidentes para el negocio. • Número de incidentes significativos relacionados con TI que no se identificaron en la evaluación de riesgos. • Número de incidentes de confidencialidad que causan pérdidas financieras, interrupción del negocio o descrédito público. • Número de incidentes de disponibilidad que causan pérdidas financieras, interrupción del negocio o descrédito público. • Número de incidentes de integridad que causan pérdidas financieras, interrupción del negocio o descrédito público.

5.2.1.2 Lista de comprobación.

Como parte de la revisión de conformidad normativa, se utiliza una lista de comprobación que incluye las actividades definidas por COBIT 2019 y que son requeridas por la Norma Técnica del MICITT. Esta lista de comprobación permite verificar que las actividades clave del proceso de gestión de riesgos de TI han sido contempladas en las políticas y procedimientos. Es importante mencionar que las actividades correspondientes a los niveles de capacidad cuatro y cinco no se han implementado en esta fase, dado que la Municipalidad de Turrialba actualmente no está capacitada para ejecutar dichas tareas.

En esta primera etapa, el enfoque se centra en formalizar las actividades de los niveles de capacidad dos y tres, asegurando que estos procesos se ejecuten de manera eficiente y que se establezcan controles y procedimientos sólidos, según los requerimientos del Encargado de TI (Apéndice L Minuta de Reunión 04 – Aplicación de Entrevista). Una vez que se logre este objetivo y se alcance el nivel de madurez adecuado, se desarrollarán las políticas y procedimientos necesarios para implementar las actividades correspondientes a los niveles de capacidad cuatro y cinco, alineando así la gestión de riesgos de TI con los más altos estándares de gobernanza. En la **Tabla 27** se muestran las actividades, divididas por práctica de gestión, y las secciones de las políticas (Apéndice R Política para la Gestión de Riesgos de Tecnologías de Información) y los procedimientos (Apéndice S Procedimientos para la gestión de Riesgos de TI).

Tabla 27 Lista de comprobación del Proceso de Gestión de Riesgos Tecnológicos

Nivel de capacidad	Actividad	Se estableció la actividad	Sección de la política	Sección del procedimiento
01 Recopilar datos				
2	Establecer y mantener un método para la recolección, clasificación y análisis de datos relacionados con el riesgo de TI.	Sí	7.1.1 Establecimiento de un método para la recolección, clasificación y análisis de datos	3.1 Valoración de riesgos de TI
	Registrar datos relevantes y significativos relacionados con los riesgos de TI en el entorno operativo interno y externo de la empresa.	Sí	7.1.2 Registro de eventos de riesgo	3.1 Valoración de riesgos de TI

Nivel de capacidad	Actividad	Se estableció la actividad	Sección de la política	Sección del procedimiento
3	Adoptar o definir una taxonomía de riesgo para las definiciones consistentes de escenarios de riesgo y categorías de impacto y probabilidad.	Sí	7.1.3 Definición y adopción de una taxonomía de riesgos	3.1 Valoración de riesgos de TI
	Registrar datos de eventos de riesgo que han causado o podrían causar impacto en el negocio conforme a las categorías de impacto definidas en la taxonomía de riesgo. Este registro se obtiene mediante la captura de datos relevantes de cuestiones, incidentes, problemas e investigaciones.	Sí	7.1.4 Registro de eventos de riesgo conforme a la taxonomía	3.1 Valoración de riesgos de TI
02 Analizar el riesgo				
3	Definir el alcance adecuado de los esfuerzos en análisis de riesgos, considerando todos los factores de riesgo y/o la criticidad de los activos para el negocio.	Sí	7.2.1 Definición del alcance del análisis de riesgos	3.1 Valoración de riesgos de TI

Nivel de capacidad	Actividad	Se estableció la actividad	Sección de la política	Sección del procedimiento
	Crear y actualizar regularmente los escenarios de riesgo de TI, las exposiciones a pérdidas relacionadas con TI y los escenarios relacionados con el riesgo reputacional, incluidos escenarios compuestos de tipos de amenazas y eventos en cascada y/o coincidentes. Para esto, es necesario desarrollar previsiones para actividades de control específicas y capacidades de detección.	Sí	7.2.2 Evaluación de controles y estimación de la frecuencia de riesgos	3.1 Valoración de riesgos de TI
	Estimar la frecuencia (o probabilidad) y la magnitud de la pérdida o ganancia asociada con escenarios de riesgos de TI. Esta actividad requiere tener en cuenta todos los factores de riesgo aplicables y evaluar controles operativos conocidos.	Sí	7.2.3 Estimación de la frecuencia y magnitud del riesgo	3.1 Valoración de riesgos de TI
	Comparar el riesgo actual (exposición a pérdidas de TI) con el apetito de riesgo y la tolerancia de riesgo aceptable. Para lograr lo anterior, se debe identificar el riesgo inaceptable o elevado.	Sí	7.2.4 Comparación del riesgo actual con el apetito y la tolerancia al riesgo	3.1 Valoración de riesgos de TI

Nivel de capacidad	Actividad	Se estableció la actividad	Sección de la política	Sección del procedimiento
	Proponer respuestas al riesgo para aquellos que excedan el apetito de riesgo y los niveles de tolerancia.	Sí	7.2.5 Propuesta de respuestas al riesgo	3.1 Valoración de riesgos de TI
	Especificar los requisitos de alto nivel para los proyectos o programas que implementarán las respuestas a los riesgos seleccionados. Esta actividad implica la identificación de los requisitos y expectativas para los controles clave adecuados a fin de proporcionar respuestas de mitigación de riesgos.	Sí	7.2.6 Especificación de requisitos para proyectos de mitigación	3.2 Especificación de requisitos para proyectos de mitigación
03 Mantener un perfil de riesgo				
2	Hacer un inventario de los procesos de negocio y documentar su dependencia de los procesos de gestión de servicios de TI y los recursos de infraestructura de TI. Para su concreción, se debe identificar el personal de apoyo, aplicaciones, infraestructura, instalaciones, registros manuales críticos, contratistas, proveedores, y terceros.	Sí	7.3.1 Inventario de procesos de negocio y dependencias	3.3 Inventario de procesos de negocio y dependencias

Nivel de capacidad	Actividad	Se estableció la actividad	Sección de la política	Sección del procedimiento
	Determinar y acordar qué servicios de TI y recursos de infraestructura de TI son esenciales para sostener el funcionamiento de los procesos de negocio. Por esta razón, se deben analizar las dependencias e identificar los eslabones débiles.	Sí	7.3.2 Consolidación del perfil de riesgo	3.3 Inventario de procesos de negocio y dependencias
	Agregar los escenarios de riesgos actuales por categoría, línea de negocio y área funcional.	Sí	7.3.3 Incorporación de escenarios de riesgos actuales	3.3 Inventario de procesos de negocio y dependencias
3	Capturar regularmente toda la información del perfil de riesgo y consolidarla en un perfil de riesgo agregado.	Sí	7.3.4 Consolidación de información en un perfil de riesgo agregado	3.3 Inventario de procesos de negocio y dependencias
	Capturar información sobre el estado del plan de acción de riesgos para su inclusión en el perfil de riesgo de TI de la empresa.	Sí	7.3.5 Inclusión del estado del plan de acción en el perfil de riesgo	3.3 Inventario de procesos de negocio y dependencias
04 Articular el riesgo				

Nivel de capacidad	Actividad	Se estableció la actividad	Sección de la política	Sección del procedimiento
3	Informar sobre los resultados del análisis de riesgo a todas las partes interesadas afectadas en términos y formatos útiles para soportar las decisiones empresariales. Siempre que sea posible, se deben incluir las probabilidades y rangos de pérdidas o ganancias, junto con los niveles de confianza, para permitir que la gerencia haga balance del retorno del riesgo.	Sí	7.4.1 Comunicación de los resultados del análisis de riesgos	3.1 Valoración de riesgos de TI
	Proporcionar a los responsables de la toma de decisiones la comprensión de los escenarios más probables y peores, exposiciones a pérdidas de TI y consideraciones significativas de reputación, legales y regulatorias, o cualquier otra categoría de impacto conforme a la taxonomía de riesgos.	Sí	7.4.2 Provisión de información detallada a los responsables de la toma de decisiones	3.1 Valoración de riesgos de TI
	Informar sobre el perfil de riesgo actual a todas las partes interesadas. Se debe incluir información sobre la eficacia del proceso de gestión de riesgos, eficacia del control, brechas, inconsistencias, redundancias, estado de remediación y sus impactos en el perfil de riesgo.	Sí	7.4.3 Informe del perfil de riesgo	3.1 Valoración de riesgos de TI

Nivel de capacidad	Actividad	Se estableció la actividad	Sección de la política	Sección del procedimiento
	De forma periódica, en áreas con riesgos relativos y capacidades de riesgo similares, identificar oportunidades relacionadas con TI que permitirían la aceptación de un riesgo mayor y un mayor crecimiento y retorno.	Sí	7.4.4 Identificación periódica de oportunidades	3.1 Valoración de riesgos de TI
05 Definir un portafolio con acciones de gestión de riesgos				
2	Mantener un inventario de las actividades de control que se han implantado para mitigar el riesgo y que permiten que se tomen riesgos alineados con el apetito y la tolerancia al riesgo. Clasificar las actividades de control y asignarlas a escenarios de riesgos de TI específicos y escenarios de riesgos de TI agregados.	Sí	7.5.1 Mantenimiento del inventario de actividades de control	3.1 Valoración de riesgos de TI
3	Determinar si cada entidad organizativa monitoriza el riesgo y acepta la responsabilidad de actuar dentro de los niveles de tolerancia individuales y del portafolio.	Sí	7.5.2 Evaluación de la responsabilidad organizacional en la gestión de riesgos	3.1 Valoración de riesgos de TI

Nivel de capacidad	Actividad	Se estableció la actividad	Sección de la política	Sección del procedimiento
	Definir un conjunto de propuestas de proyectos equilibrada diseñada para reducir el riesgo y/o proyectos que permitan oportunidades empresariales estratégicas, con consideración de los costes, beneficios, efecto en el perfil de riesgo actual y en las regulaciones.	Sí	7.5.3 Definición de proyectos estratégicos para la mitigación de riesgos	3.1 Valoración de riesgos de TI
06 Responder al riesgo				
3	Preparar, mantener y probar planes que documenten los pasos específicos que deben darse cuando un evento de riesgo pudiera causar un incidente significativo de desarrollo u operativo con un impacto grave para el negocio. Por esta razón, se debe asegurar que los planes incluyan vías de escalamiento en la empresa.	Sí	7.6.1 Preparación y prueba de planes de respuesta a incidentes	3.4 Preparación y prueba de planes de respuesta a incidentes
	Aplicar el plan de respuesta adecuado para minimizar el impacto cuando ocurren incidentes de riesgo.	Sí	7.6.2 Aplicación de los planes de respuesta	3.5 Aplicación de los planes de respuesta

De las 36 actividades del proceso de gestión de riesgos de TI que se encuentran en el Apéndice K Plantilla Lista de Comprobación del Proceso de Gestión de Riesgos, el proceso propuesto cubre 24 de estas actividades, que corresponden al 100% de las actividades de nivel de capacidad dos y tres, y representa un 66,67% del total de actividades. Estas actividades aseguran el cumplimiento de los requisitos de los niveles dos y tres, necesarios para establecer una base sólida en la gestión de riesgos. Las actividades restantes corresponden a los niveles cuatro y cinco, las cuales no se contemplan en esta fase, dado que requieren una base previa robusta, generada por la implementación de los niveles dos y tres, como el desarrollo de un histórico de riesgos.

5.2.2 Estrategia de Implementación

El siguiente plan de actividades describe las acciones clave necesarias para implementar el proceso de gestión de riesgos de TI en la Municipalidad de Turrialba. Estas actividades se alinean con los principios establecidos en la Norma Técnica del MICITT y se enfocan en identificar, evaluar y mitigar los riesgos relacionados con los activos tecnológicos y los procesos críticos de la organización.

5.2.2.1 Desarrollo de Políticas de Gestión de Riesgos

El primer paso es diseñar y desarrollar las políticas de gestión de riesgos de TI, que servirán como base para todo el proceso. Estas políticas establecen los principios, objetivos y directrices que guiarán la gestión de riesgos en la municipalidad. Las políticas deben alinearse con la Norma Técnica del MICITT y con estándares internacionales, como ISO 31000 y COBIT 2019.

5.2.2.2 Desarrollo de Procedimientos de Gestión de Riesgos

Una vez que las políticas estén establecidas, se desarrollan los procedimientos que describirán, paso a paso, cómo se llevarán a cabo las actividades relacionadas con la gestión de riesgos.

5.2.2.3 Desarrollo de Herramientas de Gestión de Riesgos

Se deben crear las herramientas de gestión de riesgos, que incluyen plantillas y listas de verificación para el registro y seguimiento de riesgos. Estas herramientas facilitan la identificación, clasificación y priorización de riesgos, así como su monitoreo continuo.

5.2.2.4 Aprobación de Políticas y Procedimientos

Las políticas y procedimientos de gestión de riesgos deben ser presentados al Concejo Municipal para su revisión y aprobación formal. Este paso formaliza el proceso de gestión de riesgos a nivel institucional y establece una base sólida para implementar las directrices establecidas en la norma técnica del MICITT. A través de esta aprobación, la municipalidad podrá ejecutar el proceso de gestión de riesgos de TI, alineándose con las mejores prácticas internacionales y garantizando una gestión integral y efectiva de los riesgos tecnológicos.

5.2.2.5 Identificación de Activos Críticos

Esta actividad consiste en realizar un inventario exhaustivo de todos los activos tecnológicos utilizados por la municipalidad. Cada activo debe ser clasificado según su importancia para la continuidad del negocio, considerando las dimensiones de confidencialidad, integridad y disponibilidad.

5.2.2.6 Identificación de Amenazas y Vulnerabilidades

Se debe realizar una lista exhaustiva de las amenazas potenciales (internas y externas) y de las vulnerabilidades asociadas a cada uno de los activos críticos previamente identificados. Esta actividad implica un análisis detallado de las posibles amenazas tecnológicas, operativas, regulatorias, ambientales y sociales.

5.2.2.7 Valoración de los Riesgos

Los riesgos identificados se deben clasificar en categorías como amenazas humanas, amenazas tecnológicas, riesgos ambientales, riesgos operativos, riesgos regulatorios y de cumplimiento, riesgos sociales y políticos, riesgos emergentes y amenazas a la cadena de suministro. Esta clasificación permitirá priorizar los riesgos con base en su naturaleza y probabilidad de ocurrencia. Además, los riesgos deben de ser evaluados según su probabilidad e impacto, describiendo las posibles causas y consecuencias en caso de ser materializados.

5.2.2.8 Identificación de Procesos de Negocio

Esta actividad consiste en identificar y listar todos los procesos de negocio clave de la municipalidad. Cada proceso debe estar asociado con sus dependencias tecnológicas y los servicios de TI que lo soportan, esto incluye identificar la infraestructura crítica y el personal involucrado en la ejecución de los procesos.

5.2.2.9 Identificación de Escenarios de Incidentes Críticos

Se deben identificar y documentar los escenarios de incidentes críticos que podrían ocurrir en los sistemas de TI de la municipalidad. Estos incidentes pueden incluir fallos de *hardware*, ataques cibernéticos, desastres naturales, interrupciones en la cadena de suministro, entre otros.

5.2.2.10 Cronograma de Implementación

El cronograma de implementación que se muestra en la **Tabla *28***, está diseñado para asegurar una ejecución de las actividades necesarias en la implementación del proceso de gestión de riesgos de TI. Las actividades se distribuyen a lo largo de un periodo de cinco meses y se han priorizado aquellas que requieren mayor esfuerzo para su realización. A medida que se avanza en las actividades, el plan será monitoreado y actualizado para asegurar que los plazos establecidos se cumplan y que las metas de cada fase sean alcanzadas.

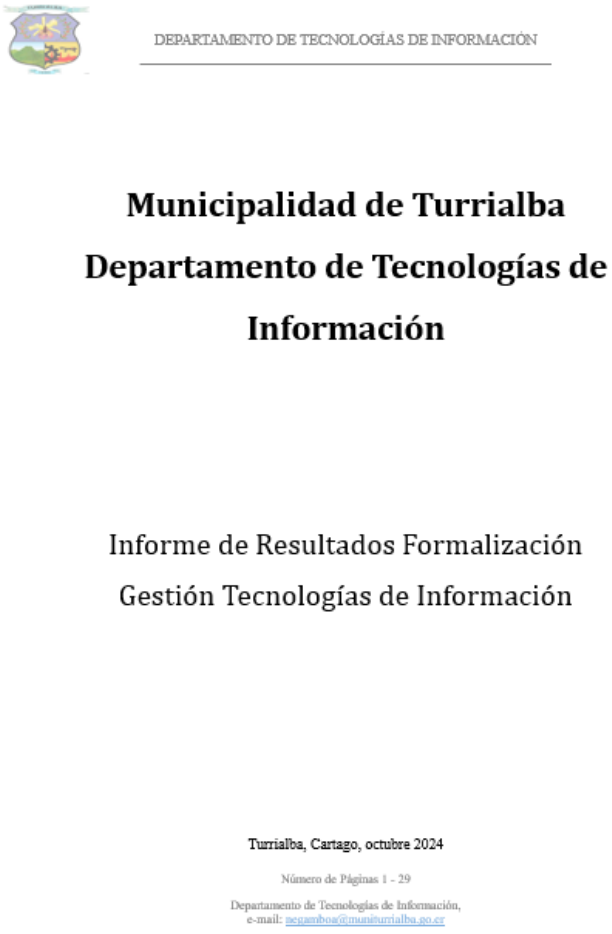
Tabla 28 *Cronograma de Implementación*

Actividad	Periodo Estimado	Estado
Desarrollo de políticas de gestión de riesgos	Septiembre 2024	Completado
Desarrollo de procedimientos de gestión de riesgos	Octubre 2024	Completado
Desarrollo de herramientas de gestión de riesgos	Octubre 2024	Completado
Aprobación de Políticas y Procedimientos	Octubre 2024	En proceso
Identificación de Activos Críticos	Noviembre 2024	En proceso
Identificación de Amenazas y Vulnerabilidades	Noviembre 2024	No iniciado
Clasificación de los Riesgos	Diciembre 2024	No iniciado
Descripción de los Eventos de Riesgo	Diciembre 2024	No iniciado
Identificación de Procesos de Negocio	Enero 2024	No iniciado
Identificación de Escenarios de Incidentes Críticos	Enero 2024	No iniciado

5.2.3 Informe de Resultados:

Se consolidan todos los hallazgos y recomendaciones en un informe final que servirá como guía para la implementación del proceso formal de gestión de riesgos de TI en la Municipalidad de Turrialba. Este informe (**Figura *21***) contiene el análisis de resultados; el desarrollo de las políticas y de los procedimientos; una herramienta integral de gestión de riesgos, y la verificación de la conformidad de este proyecto.

Figura 21 *Informe de resultados*


DEPARTAMENTO DE TECNOLOGÍAS DE INFORMACIÓN

Municipalidad de Turrialba

Departamento de Tecnologías de Información

Informe de Resultados Formalización

Gestión Tecnologías de Información

Turrialba, Cartago, octubre 2024

Número de Páginas 1 - 29

Departamento de Tecnologías de Información,
e-mail: negamboa@muniturrialba.go.cr

5.3 Análisis de la viabilidad de la propuesta.

El análisis de la viabilidad de la propuesta se fundamenta en un análisis costo-beneficio que incluye los costos asociados a la implementación del proceso de gestión de riesgos de TI y a los beneficios financieros obtenidos mediante la reducción de horas dedicadas a la atención de incidentes. Este análisis tiene como objetivo demostrar la viabilidad financiera de la propuesta y su retorno sobre la inversión (ROI), lo que justifica su implementación para la Municipalidad de Turrialba.

5.3.1 Costo por hora del encargado de TI

El encargado de TI es el encargado de la implementación del proceso. Su salario mensual es de ₡765 985,67, según la lista de salario mínimo del Ministerio de Trabajo y Seguridad Social (2024). Su jornada laboral es de 40 horas por semana, lo que equivale a 160 horas al mes. El cálculo del costo por hora es:

$$\textbf{Costo por hora} = \frac{₡765\ 985{,}67}{160\ \text{horas}} = ₡4\ 787{,}41$$

5.3.2 Costo del encargado de TI para la implementación

El encargado dedica 15 horas semanales para la implementación, lo que equivale a 60 horas al mes. El costo mensual asociado es

$$\textbf{Costo mensual} = ₡4\ 787{,}41\ x\ 60\ horas = ₡287\ 244{,}6\ al\ mes$$

5.3.3 Costo de Office 365:

El costo de la licencia de Microsoft 365 Empresa Básico es de $6,00 al mes por usuario. Convertido a colones al tipo de cambio de ₡535,91, este cambio varía según el día tomando el dato del BCCR, el costo mensual por usuario es de ₡3 215.46.

5.3.4 Costo total de implementación:

El proceso de gestión de riesgos de TI se planea implementar durante un periodo de cuatro meses. El costo total del encargado de TI y la licencia de Office 365 para ese periodo es

$$\textbf{Costo total} = \textbf{Costo mensual del encargado} + \textbf{Costo de Office365 x 4 meses}$$
$$= (₡287\ 244{,}6 + ₡3\ 215{,}46)\ x\ 4\ meses = ₡1\ 161\ 840{,}24$$

5.3.5 Ahorro en horas por semana:

Actualmente, el encargado de TI dedica 25 horas semanales a la atención de incidentes. Una vez implementado el proceso, esta carga se reducirá a 15 horas semanales, lo que genera un ahorro de tiempo.

$$\textbf{Ahorro semanal} = 25\ horas - 15\ horas = 10\ horas$$

El valor de este ahorro semanal multiplicado por el costo por hora del encargado de TI es

$$\textbf{Valor Ahorro semanal} = 10\ horas\ x\ ₡4\ 787{,}41 = ₡47\ 874{,}1$$

El valor del ahorro mensual es el ahorro semanal multiplicado por cuatro semanas:

$$\textbf{Valor Ahorro mensual} = ₡47\ 874{,}1\ x\ 4\ semanas = ₡191\ 496{,}4$$

5.3.6 Ahorro total durante la implementación:

El ahorro total estimado durante los cuatro meses de implementación del proyecto es

$$\textbf{Valor Ahorro} = ₡191\ 496{,}4\ x\ 4\ meses = ₡765\ 985{,}6$$

5.3.7 Cálculo del Retorno sobre la Inversión (ROI)

El retorno sobre la inversión (ROI) se calcula de la siguiente manera:

- Costo total de la implementación: ₡1 161 840,24
- Ahorro de la implementación: ₡765 985,6

$$\textbf{ROI} = \frac{(\text{Beneficios} - \text{Costo de implementación})}{\text{Costo de implementación}}\ x\ 100$$

$$\textbf{ROI} = \frac{(₡765\ 985.6 - ₡1\ 161\ 840{,}24)}{₡1\ 161\ 840{,}24}\ x\ 100$$

$$\textbf{ROI} = \frac{-₡395\ 854.64}{₡1\ 161\ 840{,}24}\ x\ 100$$

$$\textbf{ROI} = -0{,}3407\ x\ 100\ \approx -34{,}07\%$$

Esto muestra que, durante los cuatro meses de implementación, el ROI es negativo –34,07% porque los ahorros son menores que el costo de implementación en este periodo.

5.3.8 Cálculo del Período de Recuperación de la Inversión

El período de recuperación de la inversión es una medida financiera que permite calcular el tiempo que se necesita para recuperar el costo total de un proyecto a partir de los ahorros o beneficios generados por su implementación. En este caso, se ha evaluado el período necesario para que la Municipalidad de Turrialba recupere los costos de la implementación del proceso de gestión de riesgos de TI.

El proyecto tiene un costo total de implementación de ₡1 161 840,24 durante un periodo de cuatro meses, que incluye los costos asociados al tiempo dedicado por el encargado de TI y la licencia de Office 365. El costo mensual de la licencia es de ₡3 215,46 por mes; sin embargo, este costo pasado el cuarto mes sigue sumando al costo total debido a que el proceso requiere de esta licencia. El cálculo del periodo de recuperación se muestra en la **Tabla *29***.

Tabla 29 *Cálculo del Período de Recuperación de la Inversión*

Mes	Costo total acumulado	Ahorro total acumulado	Saldo (costo - ahorro)
1	₡ 290 460,06	₡191 496,40	₡ 98 963,66
2	₡ 580 920,12	₡382 992,80	₡197 927,32
3	₡ 871 380,18	₡574 489,20	₡296 890,98
4	₡1 161 840,24	₡765 985,60	₡395 854,64
5	₡1 165 055,70	₡957 482,00	₡207 573,70
6	₡1 168 271,16	₡1 148 978,40	₡ 19 292,76
7	₡1 171 486,62	₡1 340 474,80	**-₡ 168 988,18**

El período de recuperación de la inversión es de aproximadamente seis meses. Esto significa que la municipalidad recuperará los costos iniciales del proyecto en un plazo razonable, después de lo cual, comenzará a generar ahorros derivados de la implementación del proceso de gestión de riesgos de TI.

5.3.9 Cumplimiento Normativo y Beneficios Asociados

Además de los beneficios financieros obtenidos por la reducción de horas dedicadas a la atención de incidentes, la implementación del proceso de gestión de riesgos de TI en la Municipalidad de Turrialba es esencial para cumplir con los requerimientos normativos. La Norma Técnica del MICITT establece directrices claras para la gestión de riesgos tecnológicos en el sector público; además, el cumplimiento de esta norma es obligatorio para evitar sanciones y asegurar la aprobación de los presupuestos municipales. Los beneficios clave asociados al cumplimiento normativo incluyen:

- Identificación proactiva de riesgos: la implementación del proceso formal permitirá a la municipalidad identificar proactivamente los riesgos potenciales que afecten sus sistemas de información, datos y operaciones. Este proceso incluirá análisis de amenazas, vulnerabilidades, evaluaciones de impacto y análisis de probabilidad.
- Evaluación y priorización de riesgos: cada riesgo identificado será evaluado mediante metodologías cuantitativas y cualitativas, lo que permitirá priorizar los riesgos y asignar eficientemente los recursos para su tratamiento.
- Generación de estrategias de tratamiento de riesgos: se desarrollarán estrategias efectivas de tratamiento de los riesgos identificados, que incluyen medidas de control técnico, organizativo y físico, alineadas con las mejores prácticas internacionales.
- Reducción de incidentes de seguridad: La correcta gestión de los riesgos disminuirá la frecuencia y severidad de incidentes de seguridad, dentro de los cuales se encuentran ataques cibernéticos, pérdida de datos e interrupciones en los servicios críticos de la municipalidad.
- Garantía de continuidad operativa: la municipalidad garantizará la continuidad operativa de sus servicios mediante la implementación de planes de recuperación ante desastres y planes de continuidad del negocio, los cuales se verán fortalecidos por el proceso de gestión de riesgos.
- Cumplimiento normativo: la Municipalidad de Turrialba estará en cumplimiento del cuarto proceso de la Norma Técnica del MICITT para la gestión de riesgos de TI. Esta acción permitirá evitar sanciones por parte de entidades reguladoras y aprobar el presupuesto por parte de la Contraloría General de la República, todo lo anterior al demostrar el cumplimiento de los requisitos de seguridad de la información; al fortalecer la reputación de la municipalidad, y al mostrar a los ciudadanos y otras entidades su compromiso con la protección de datos y la seguridad de la información.
- Protección de la información sensible: las medidas de gestión de riesgos protegerán la confidencialidad, integridad y disponibilidad de la información sensible, asegurando que los datos críticos de la municipalidad estén adecuadamente resguardados.

6 Conclusiones

El siguiente capítulo brinda la oportunidad de identificar las enseñanzas adquiridas durante el desarrollo del proyecto final de graduación. A continuación, se detallan aquellos hallazgos y conclusiones que se evidenciaron a lo largo de la ejecución de este proyecto y que, a su vez, están asociados con cada uno de los objetivos específicos definidos en la sección 1.4.

6.1 Objetivo General

Proponer un proceso formal de gestión de riesgos de tecnologías de información en la Municipalidad de Turrialba para la identificación, evaluación y tratamiento de riesgos tecnológicos y cumplimiento normativo a partir de la Norma Técnica del MICITT y las buenas prácticas de la industria en el segundo semestre del año 2024. Con base en este objetivo se concluye lo siguiente:

- En el desarrollo del proceso formal de gestión de riesgos de TI detallado en el Capítulo 5, se alcanzó un diseño que cumple con los lineamientos de la Norma Técnica del MICITT, que también se alinea con las mejores prácticas internacionales de marcos como ISO 31000, ISO 27005, COBIT 2019 e ITIL 4. Este marco proporciona una estructura sólida y adaptable que fomenta una respuesta organizada y efectiva ante los riesgos tecnológicos, permitiendo una mejora en la madurez del proceso y en la seguridad organizacional.
- A través del Análisis de Viabilidad presentado en la sección 5.3, se identificó un período inicial de retorno negativo sobre la inversión del –34,07% en los primeros cuatro meses. Sin embargo, el análisis proyecta una recuperación completa de la inversión en aproximadamente seis meses, lo que indica viabilidad económica en el mediano plazo. Más allá de los beneficios financieros, la implementación del proceso de gestión de riesgos de TI responde a una necesidad imperativa de cumplimiento normativo según los requerimientos de la Norma Técnica del MICITT. Su adopción refuerza la postura de la organización en términos de seguridad y operatividad, impulsando mejoras en la resiliencia institucional y asegurando el cumplimiento regulatorio a largo plazo, lo cual es fundamental para la sostenibilidad del proceso y la mitigación de riesgos tecnológicos de manera estructurada.

6.2 Objetivo Específico 1

Analizar la situación actual del proceso de gestión de amenazas de TI que afectarían a la Municipalidad de Turrialba en la identificación de oportunidades de mejora del proceso existente contra las buenas prácticas de la industria. A partir de este objetivo se concluye lo siguiente:

- Mediante la revisión documental detallada en la sección 4.1.1, se determinó que la Municipalidad de Turrialba carece de documentación formal sobre el proceso de gestión de amenazas de TI.
- La existencia de una sola persona en el departamento de TI representa un riesgo adicional para la continuidad operativa del área, dado que la dependencia en una única persona en el proceso de gestión de TI aumenta la vulnerabilidad frente a ausencias por vacaciones, enfermedad u otros imprevistos, como se evidencia en la sección 4.2.

- A través del análisis de datos recopilados de la sección 4.2, se identificó que el proceso actual es reactivo y no sigue un enfoque estructurado ni estandarizado, lo que incrementa la exposición a riesgos.
- El proceso actual es de nivel uno según el Modelo de Madurez de la Capacidad. Este modelo muestra que el proceso tiene algunas actividades básicas, pero es incompleto y poco organizado y carece de actividades clave como la evaluación formal de riesgos y la implementación de controles preventivos como lo evidencia la sección 4.3.

6.3 Objetivo Específico 2

Diseñar un marco de gestión de riesgos de TI basado en la norma técnica del MICITT y las mejores prácticas de la industria para la estandarización de las actividades del proceso. Con base en este objetivo se concluye lo siguiente:

- La propuesta de políticas y procedimientos para la gestión de riesgos de TI se diseñó alineada con la norma técnica del MICITT y las buenas prácticas internacionales, adaptándose específicamente a las necesidades operativas y contextuales de la Municipalidad de Turrialba, como se describe en la sección 5.1.
- El marco de gestión de riesgos se clasifica en nivel tres según el Modelo de Madurez de la Capacidad, que hace referencia a un proceso estructurado y organizado con recursos y actividades bien definidos. Ambos aspectos fortalecen su aplicabilidad y valor dentro de la institución, como lo evidencia la sección 0
- Se desarrolló una herramienta en Excel para facilitar la implementación y seguimiento del proceso de gestión de riesgos, considerando la limitación de personal y promoviendo una gestión de riesgos ágil, práctica y accesible, como se muestra en la sección 5.1.3.
- El Plan de Comunicaciones asegura la participación de las partes interesadas y una adecuada difusión del marco de gestión de riesgos de TI, promoviendo una cultura de conciencia y colaboración en torno a la gestión de riesgos en la municipalidad, como se muestra en la en la sección 5.1.4.

6.4 Objetivo Específico 3

Verificar la conformidad del proceso de gestión de riesgos de TI con los requisitos establecidos en la norma técnica del MICITT para el cumplimiento regulatorio y la protección de los activos de información. A partir de este objetivo se concluye lo siguiente:

- Mediante la utilización de la Lista de Comprobación del Proceso de Gestión de Riesgos Tecnológicos, se verificó que el marco propuesto cumple con el 100% de las actividades de nivel de capacidad dos y tres requeridas por la municipalidad, que representan el 66,7% de las actividades establecidos por la Norma Técnica del MICITT, como se muestra en la sección 5.2.1.
- El Perfil del Proceso elaborado confirma que se han definido claramente el objetivo, las metas, los roles y responsabilidades y las actividades secuenciales del proceso de gestión de riesgos de TI, en concordancia con la norma técnica del MICITT, como se muestra en la sección 0.

7 Recomendaciones

A partir de los hallazgos y conclusiones obtenidos durante el desarrollo de este proyecto, se presentan las recomendaciones clave para fortalecer el proceso de gestión de riesgos de TI en la Municipalidad de Turrialba.

7.1 Objetivo General

Proponer un proceso formal de gestión de riesgos de tecnologías de información en la Municipalidad de Turrialba para la identificación, evaluación y tratamiento de riesgos tecnológicos y cumplimiento normativo a partir de la Norma Técnica del MICITT y las buenas prácticas de la industria en el segundo semestre del año 2024. Con base en este objetivo se recomienda lo siguiente:

- Durante la fase de maduración del proceso, contar con consultores externos en gestión de riesgos asegurará el cumplimiento inicial y el alineamiento con las normativas. Esto puede incluir asesoría en el diseño de procedimientos específicos y revisión de la efectividad de los controles implementados.
- Adaptar el proceso ante cambios en la infraestructura tecnológica y nuevas amenazas. Se sugiere una revisión anual del proceso para asegurar que los controles y procedimientos se mantengan actualizados ante el cambio de contextos y normativas.
- Establecer un programa de auditorías periódicas internas y externas para evaluar el cumplimiento y la efectividad del proceso de gestión de riesgos. Los resultados deben servir como base para ajustes continuos que mantengan la eficacia y el cumplimiento de las normativas.
- A medida que el equipo de TI se consolide y se fortalezca el cumplimiento del tercer nivel de la Norma Técnica del MICITT, iniciar la planificación para implementar actividades de niveles cuatro y cinco. Esto fortalecerá la postura de seguridad y la madurez en la gestión de riesgos de la municipalidad.
- Construir los procesos del negocio usando BPM de forma gradual para que terceros puedan comprender y ejecutar los procesos en caso de ausencia del personal actual. Esto también facilitará la integración de futuros miembros del equipo de TI y la detección de riesgos en los procesos.
- Implementar un sistema de gestión documental que permita gestionar, actualizar y consultar toda la documentación del proceso de gestión de riesgos. Se puede considerar un sistema en la nube seguro y accesible para las partes autorizadas.
- Se recomienda implementar todas las propuestas desarrolladas en el marco de este proyecto para establecer un proceso formal de gestión de riesgos de TI en la Municipalidad de Turrialba. La implementación integral de este proyecto garantizará una gestión de riesgos de TI alineada con la Norma Técnica del MICITT y las mejores prácticas de la industria, permitiendo una protección efectiva de los activos de información y un cumplimiento normativo sostenible.

7.2 Objetivo específico 1

Analizar la situación actual del proceso de gestión de amenazas de TI que afectarían a la Municipalidad de Turrialba para la identificación de oportunidades de mejora del proceso existente contra las buenas prácticas de la industria. A partir de este objetivo se recomienda lo siguiente:

- Considerar la incorporación de personal especializado en áreas clave como la gestión de riesgos tecnológicos y la seguridad de la información para reducir la dependencia de una sola persona. Para este fin, se podría comenzar con la contratación de roles temporales o de medio tiempo hasta que se logre un equipo permanente y multifuncional.
- Mientras se consolida el equipo interno, se sugiere contratar servicios externos para gestionar tareas como auditorías de seguridad y evaluaciones de vulnerabilidades. Esta iniciativa brindará una visión objetiva y permitirá a la municipalidad priorizar áreas de mejora en la gestión de riesgos. Además, este apoyo externo aliviará la carga operativa del actual encargado de TI.
- Invertir en plataformas de monitoreo en tiempo real, alertas de seguridad y sistemas de gestión de incidentes automatizados. Esto facilitará el trabajo del equipo de TI y reducirá el enfoque en respuestas reactivas, permitiendo una gestión más proactiva de riesgos. El proceso puede iniciarse evaluando opciones de *software* compatibles con la infraestructura actual de la municipalidad.

7.3 Objetivo Específico 2

Diseñar un marco de gestión de riesgos de TI basado en la norma técnica del MICITT y las mejores prácticas de la industria para la estandarización de las actividades del proceso. Con base en este objetivo se recomienda lo siguiente:

- Realizar revisiones periódicas del marco para asegurar su alineación con la evolución de normativas como ISO 27005 e ISO 31000 y adaptarse a cambios en el contexto de riesgos y objetivos de la organización. Considerando la implementación de la ISO 9001, que permite estandarizar los elementos necesarios para la generación de políticas y procedimientos. También, permite facilitar la gestión del proceso calidad de los procesos tecnológicos mencionado en la norma técnica del MICITT.
- Esto podría incluir una revisión semestral de la documentación y la actualización de prácticas conforme a las tendencias emergentes.
- Adaptar el marco ante cambios significativos en la estructura de TI, procesos internos y objetivos estratégicos de la municipalidad. La revisión anual del marco o su actualización tras cambios importantes garantizará que se mantenga relevante y efectivo.
- Coordinar con departamentos como administración y finanzas para apoyar la gestión documental y el control de riesgos. Este enfoque permitirá al equipo de TI enfocarse en actividades técnicas, mientras otros departamentos asumen tareas administrativas relacionadas.
- Implementar un plan de capacitación para el equipo de TI y personal clave de otros departamentos. Este plan debe incluir sesiones anuales de actualización sobre gestión de

riesgos y prácticas de seguridad de la información adaptadas a los roles específicos de cada área.

7.4 Objetivo Específico 3

Verificar la conformidad del proceso de gestión de riesgos de TI con los requisitos establecidos en la norma técnica del MICITT para el cumplimiento regulatorio y la protección de los activos de información. A partir de este objetivo se recomienda lo siguiente:

- Establecer un calendario anual de auditorías internas para verificar la ejecución y eficacia de las actividades de gestión de riesgos. Estas auditorías deben ser detalladas y considerar indicadores de conformidad para identificar áreas de mejora tempranamente.
- Una vez consolidadas las actividades de nivel tres, planificar la incorporación gradual de actividades de nivel cuatro y cinco del modelo de madurez. Esta planificación debe basarse en los resultados de auditorías y en la disponibilidad de recursos, asegurando que los objetivos de cada nuevo nivel se cumplan antes de avanzar al siguiente.
- Programar auditorías anuales por parte de consultores externos para obtener una evaluación imparcial y recibir recomendaciones sobre mejoras. Esto también brindará una validación independiente y externa del cumplimiento de la Norma Técnica del MICITT.

8 Referencias

Alfaro Campos, J. C. (2017). *Metodología para la gestión de riesgos de TI basada en COBIT 5.*

Asociación Española de Normalización. (2018). *UNE-ISO 31000 Gestión del riesgo Directrices.* www.iso.org/patents.

Asociación Española de Normalización. (2024). Seguridad de la información, ciberseguridad y protección de la privacidad. Guía para la gestión de los riesgos de seguridad de la información (ISO/IEC 27005:2022) (Ratificada por la Asociación Española de Normalización en septiembre de 2024.). www.une.org

Asociación Española de Normalización. (2015). *UNE-EN ISO 9001 Sistemas de gestión de la calidad Requisitos*.

Axelos. (2019). *ITIL ® Foundation ITIL 4 Edition 2*. https://www.axelos.com

Bizagi. (2024). *Bizagi, one platform; every process. Guía de uso estudio.* Https://Help.Bizagi.Com/Bpm-Suite/Es/Index.Html?Glossary.Htm.

Dumas, M., La Rosa, M., Mendling, J. y Reijers, H. (s.f.). *Fundamentals of Business Process Management.*

Gamboa Calderón, N. (2022). *Políticas de Seguridad en Materia de Tecnologías de Información y Comunicación TICS.*

Hernández Sampieri, R., Fernández Collado, C., y Baptista Lucio, P. (2014). *Metodología de la Investigación.*

Instituto Nacional de Estadística y Censos. (2022). Censo costarricense de 2022. https://inec.cr/estadisticas-fuentes/censos/censo-2022

ISACA. (2018). *Marco de Referencia COBIT® 2019: Objetivos de gobierno y gestión.* http://linkd.in/ISACAOfficial

Mata Solís, L. (26 de enero de 2021). *Investigación Los sujetos de estudio.* https://investigaliacr.com/investigacion/los-sujetos-de-estudio/

MICITT. (2021). *Portafolio Riesgos.*

Microsoft. (2024). *Buscar el plan de Microsoft 365 más adecuado para tu empresa.*

Ministerio de Trabajo y Seguridad Social. (2024). *Lista de salarios mínimos 2024.* https://www.mtss.go.cr/temas-laborales/salarios/Documentos-Salarios/lista_salarios_2024.pdf

Municipalidad de Turrialba. (2021). *Municipalidad de Turrialba.* https://www.muniturrialba.go.cr/index.php/en/

National Institute of Standards and Technology. (2012). *NIST 800-30: Guide for Conducting Risk Assessments.* https://doi.org/10.6028/NIST.SP.800-30r1

Soberón, U. E. M., & Acosta, Z. (2008). *FUENTES DE INFORMACIÓN PARA LA RECOLECCIÓN DE INFORMACIÓN CUANTITATIVA Y CUALITATIVA 1 TEXTO No 2.*

Solís García, S., Montillano Vivas, M., Chinchilla Sáenz, S., Tenorio Chacón, O., Badilla Picado, I. y Lemaitre Picado, R. (2021). *Normas técnicas para la gestión y el control de las Tecnologías de Información.*

9 Apéndices

9.1 Apéndice A Plantilla de Minuta

MINUTA DE REUNIÓN

Propuesta De Un Proceso Formal De Gestión De Riesgos De Tecnologías De Información Para La Municipalidad De Turrialba

Reunión No.	N°xx	Fecha:	Indicar la fecha exacta de la reunión
Lugar:	Indicar dónde fue la reunión	Hora Inicio/Finalización:	xx:00 am. / yy:00 am
Objetivo de la reunión:			
Participantes:	Presentes:		
	Ausentes:		

Temas Tratados			
No.	Asunto	Comentarios	Acuerdos
1	Debe ser detallado, explícito	Debe ser detallado, explícito	Debe ser detallado, explícito
2	Debe ser detallado, explícito	Debe ser detallado, explícito	Debe ser detallado, explícito
3	Debe ser detallado, explícito	Debe ser detallado, explícito	Debe ser detallado, explícito

Próxima reunión		
Temas a tratar	Fecha	Convocados
En la próxima reunión	indicar	Nombre de quiénes asistirán a esta próxima reunión.

Fuente: Elaboración propia (2024).

9.2 Apéndice B Plantilla Gestión de Cambios

Hoja de Control de Cambios			
Datos Generales del Cambio			
N° Cambio			
Solicitante		**Fecha de solicitud del cambio**	
Responsable de la implementación		**Fecha de realización del cambio**	
Estado	☐Aprobado ☐ En Revisión ☐Rechazado		
Detalles del Cambio			
Categoría	Introducción / Alcance / Marco Teórico / Metodología /___		
Descripción detallada			
Justificación			
Implicaciones de realizar el cambio			
Impacto	Especificar si el cambio genera impacto en otras áreas del proyecto, tales como recursos, cronogramas, otros proyectos, entre otros.		
Comentarios/ Observaciones			

Revisado por:	**Elaborado por:**
Nombre tutor	Pablo Alonso Chaves Rivera
Firma	Firma
(Prof. tutor)	(Estudiante)
Revisado por:	**Aprobado por:**
Nombre representante empresa	Nombre Coordinadora TFG
Firma	Firma
(Empresa)	(Coordinadora de TFG)

Fuente: Elaboración propia (2024)

9.3 Apéndice C Minuta 01 | Reunión inicial con la organización

MINUTA DE REUNIÓN

Proyecto: Propuesta De Un Proceso Formal De Gestión De Riesgos De Tecnologías De Información Para La Municipalidad De Turrialba

Reunión No.	N°01	Fecha:	08/05/2024
Lugar:	Municipalidad de Turrialba	Hora Inicio/Finalización:	10:00 am. / 11:00 am
Objetivo de la reunión:	Discutir y analizar las problemáticas actuales que enfrenta la Municipalidad de Turrialba en el área de tecnologías de la información (TI) con el fin de obtener una comprensión detallada de los desafíos de la municipalidad.		
Participantes:	Presentes: Pablo Chaves y Encargado de TI (Nelson Gamboa)		
	Ausentes:		

Temas Tratados

No.	Asunto	Comentarios	Acuerdos
1	Problemáticas de la municipalidad.	Se hablo de los problemas de cumplimiento de la norma técnica, sobre la falta de un proceso de gestión de riesgos y sobre la implementación de una mesa de servicios para la municipalidad.	
2	Prioridad de los problemas.	El encargado del área indica que para la municipalidad ahora es prioridad la gestión de riesgos por la vulnerabilidad de está al no tener un proceso de gestión de riesgo de TI, y por cumplimiento de la norma técnica del MICITT	Se acuerda que el estudiante Pablo Chaves trabajará con la problemática de la vulnerabilidad de la municipalidad y el encargado del área le enviará los documentos relacionados con la gestión de riesgos y la norma técnica del MICITT para ser estudiada por el estudiante y formular el anteproyecto. Los involucrados se comunicarán por correo electrónico en estas primeras etapas del anteproyecto.

Próxima reunión

Temas a tratar	Fecha	Convocados

NELSON EDUARDO GAMBOA CALDERON (FIRMA)

Uso Confidencial Pág. 1/1

Fuente: Elaboración propia (2024)

9.4 Apéndice D Minuta reunión 02 | Reunión con el profesor Tutor

MINUTA DE REUNIÓN

Proyecto: Propuesta De Un Proceso Formal De Gestión De Riesgos De Tecnologías De Información Para La Municipalidad De Turrialba

Reunión No.	N°02	**Fecha:**	3/08/2024
Lugar:	En remoto-Teams	**Hora Inicio/Finalización:**	2:00 pm. / 3:00 pm
Objetivo de la reunión:	Primera reunión con el profesor tutor, conocer al estudiante y al proyecto.		
Participantes:	Presentes: Pablo Alonso Chaves Rivera, Luis Pablo Soto Chaves (profesor tutor)		
	Ausentes: NA		

Temas Tratados

No.	Asunto	Comentarios	Acuerdos
1	Conocer la empresa	El estudiante explica la situación con la empresa y la disponibilidad para la primera reunión.	El estudiante realizará la consulta para la disponibilidad de la contraparte de la empresa para la primera reunión
2	Cronograma	Se modifican y se acuerdan las fechas de entrega del cronograma	El estudiante y el profesor tutor acuerdan realizar las tareas según las fechas acordadas. El estudiante realizará los recordatorios en el calendario institucional.
3	Conocer el proyecto	El estudiante explica la situación problemática y lo realizado en el anteproyecto.	El estudiante realizará los cambios comentados sobre el capitulo I y revisará el objetivo específico 2 y 3.
4	Entregables	Se comenta como se realizarán los entregables, el medio y el formato.	El estudiante realizará un directorio en una carpeta compartida en OneDrive para realizar los entregables

Próxima reunión

Temas a tratar	Fecha	Convocados
Primera reunión con la empresa.	07/08/2024	Pablo Alonso Chaves Rivera. Luis Pablo Soto Chaves (profesor tutor). Encargado de TI (Nelson Gamboa)

9.5 Apéndice E Minuta reunión 03 | Reunión con la organización

MINUTA DE REUNIÓN

Proyecto: Propuesta De Un Proceso Formal De Gestión De Riesgos De Tecnologías De Información Para La Municipalidad De Turrialba

Reunión No.	N°03	Fecha:	07/08/2024
Lugar:	Remoto-mediante Teams	Hora Inicio/Finalización:	10:00 am. / 11:00 am
Objetivo de la reunión:	Conocer a la contraparte de la organización y explicar el proceso de TFG.		
Participantes:	Presentes: Pablo Alonso Chaves Rivera, Luis Pablo Soto Chaves (profesor tutor), Encargado de TI (Nelson Gamboa)		
	Ausentes: NA		

Temas Tratados

No.	Asunto	Comentarios	Acuerdos
1	El proceso de TFG	Se comento el reglamento del TFG.	Las partes quedan enteradas y comprometidos con sus responsabilidades.
2	Confidencialidad.	Se explica la opción de confidencialidad del TFG.	No se requiere acuerdo de confidencialidad.

Próxima reunión

Temas a tratar	Fecha	Convocados
Avance del Proyecto.	11/09/2024	Pablo Alonso Chaves Rivera, Luis Pablo Soto Chaves (profesor tutor), Encargado de TI (Nelson Gamboa)

NELSON EDUARDO GAMBOA CALDERON (FIRMA)

Digitally signed by NELSON EDUARDO GAMBOA CALDERON (FIRMA)
Date: 2024.10.14 11:07:21 -06'00'

Uso Confidencial Pág. 1/1

9.6 Apéndice F Bitácora Revisión Documental

Bitácora de Revisión Documental			
Id	**Fecha**	**Nombre del Documento**	**Hallazgo**
RD-01			
…			

Fuente: Elaboración propia (2024).

9.7 Apéndice G Entrevista Situación Actual

Objetivo: Obtener información detallada sobre la gestión actual de amenazas de TI, identificar las percepciones de los responsables sobre los riesgos y las prácticas actuales, y recoger sugerencias de mejoras.

Preguntas:

1. **¿Quiénes son los principales responsables de la gestión de amenazas de TI en la Municipalidad y cuáles son sus roles específicos?**
    - **R/**:
2. **¿Existe documentación formal que describa el proceso actual de gestión de amenazas de TI? ¿Está actualizada y accesible para el personal relevante?**
    - **R/**
3. **¿Qué actividades o tareas específicas se realizan actualmente para gestionar las amenazas de TI? ¿Son manuales o automatizadas?**
    - **R/**:
4. **Cuando se identifica una amenaza de TI, ¿qué pasos sigue el equipo para gestionarla?**
    - **R/**:
5. **¿Cómo describiría el estado de las políticas y procedimientos actuales para manejar las amenazas de TI?**
    - **R/**:
6. **¿Cómo calificaría la efectividad de las capacitaciones sobre gestión de riesgos de TI proporcionadas al personal? ¿Qué áreas podrían mejorarse?**
    - **R/**:
7. **¿Qué tipo de documentación respalda el proceso actual de gestión de riesgos de TI?**
    - **R/**:

8. **Desde su experiencia, ¿qué mejoras cree que se podrían implementar en el proceso de gestión de riesgos de TI en la Municipalidad?**
    - **R/**:
9. **¿La Municipalidad de Turrialba utiliza servicios de outsourcing para la gestión de TI? Si es así, ¿qué tipo de servicios se externalizan y cómo se gestionan los riesgos asociados?**
    - **R/**:
10. **¿Existen mecanismos de control para garantizar que los proveedores externos cumplan con las políticas de seguridad y gestión de riesgos?**
    - **R/**:
11. **¿Se ha definido un apetito de riesgo para las operaciones de TI en la Municipalidad? ¿Cómo se determina y comunica?**
    - **R/**:
12. **¿Qué actividades o tareas se requerirán en el nuevo marco formal de gestión de riesgos de TI?**
    - **R/**:

9.8 Apéndice H Entrevista Miembro Comisión de Control Interno

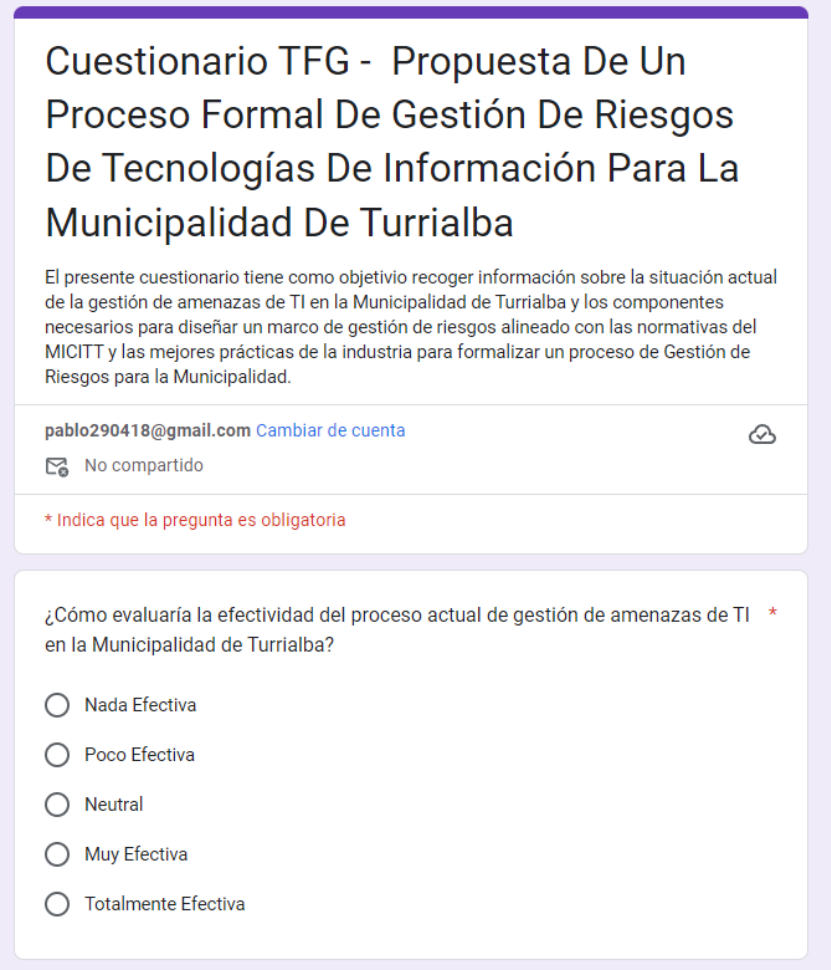
Objetivo: El objetivo de esta entrevista es obtener una visión clara de cómo se gestionan los riesgos generales a nivel municipal, incluyendo las políticas, procedimientos y prácticas utilizadas para identificar, evaluar y mitigar amenazas en diversas áreas de la municipalidad.

Preguntas:

1. **¿Quiénes son los responsables principales del proceso de gestión de riesgos generales en la Municipalidad?**
    a. **R/**:
2. **¿Cuál es el estado de la documentación relacionada con el proceso de gestión de riesgos generales? ¿Es fácilmente accesible?**
    a. **R/**:
3. **¿Qué actividades o tareas específicas se realizan para identificar y gestionar los riesgos generales en la Municipalidad?**
    a. **R/**:
4. **¿Cómo describiría la efectividad de las estrategias actuales de mitigación de riesgos? ¿Qué medidas considera más efectivas?**
    a. **R/**:

5. **¿Existen áreas donde cree que el proceso de gestión de riesgos generales puede ser optimizado o mejorado?**
    a. **R/**:
6. **¿Qué limitaciones enfrenta la Municipalidad en la implementación de un proceso efectivo de gestión de riesgos?**
    a. **R/**:
7. **¿Cuáles son las principales amenazas que enfrenta el proceso de gestión de riesgos de TI en la Municipalidad?**
    a. **R/**:
8. ¿Existe un apetito de riesgo claramente definido para la gestión de riesgos en la Municipalidad de Turrialba?
    a. **R/**:

9.9 Apéndice I Cuestionario Situación Actual



Cuestionario TFG - Propuesta De Un Proceso Formal De Gestión De Riesgos De Tecnologías De Información Para La Municipalidad De Turrialba

El presente cuestionario tiene como objetivio recoger información sobre la situación actual de la gestión de amenazas de TI en la Municipalidad de Turrialba y los componentes necesarios para diseñar un marco de gestión de riesgos alineado con las normativas del MICITT y las mejores prácticas de la industria para formalizar un proceso de Gestión de Riesgos para la Municipalidad.

pablo290418@gmail.com Cambiar de cuenta

No compartido

* Indica que la pregunta es obligatoria

¿Cómo evaluaría la efectividad del proceso actual de gestión de amenazas de TI en la Municipalidad de Turrialba? *

- Nada Efectiva
- Poco Efectiva
- Neutral
- Muy Efectiva
- Totalmente Efectiva

¿Cuáles de las siguientes prácticas de gestión actualmente no están cubiertas por el proceso? *

- [ ] Recopilar datos
- [ ] Analizar el riesgo
- [ ] Mantener un perfil de riesgo.
- [ ] Articular el riesgo.
- [ ] Definir un portafolio con acciones de gestión de riesgos.
- [ ] Responder al riesgo.

¿Con qué marcos internacionales de gestión de riesgos de TI está familiarizado? * Puede marcar multiples opciones.

- [ ] COBIT 2019
- [ ] ITIL 4
- [ ] ISO 31000
- [ ] NIST 800-30
- [ ] ISO 27005
- [ ] Otro: _____

¿Cuánto considera que su conocimiento actual de estas prácticas podría influir en la implementación efectiva del marco de gestión de riesgos de TI en la Municipalidad?

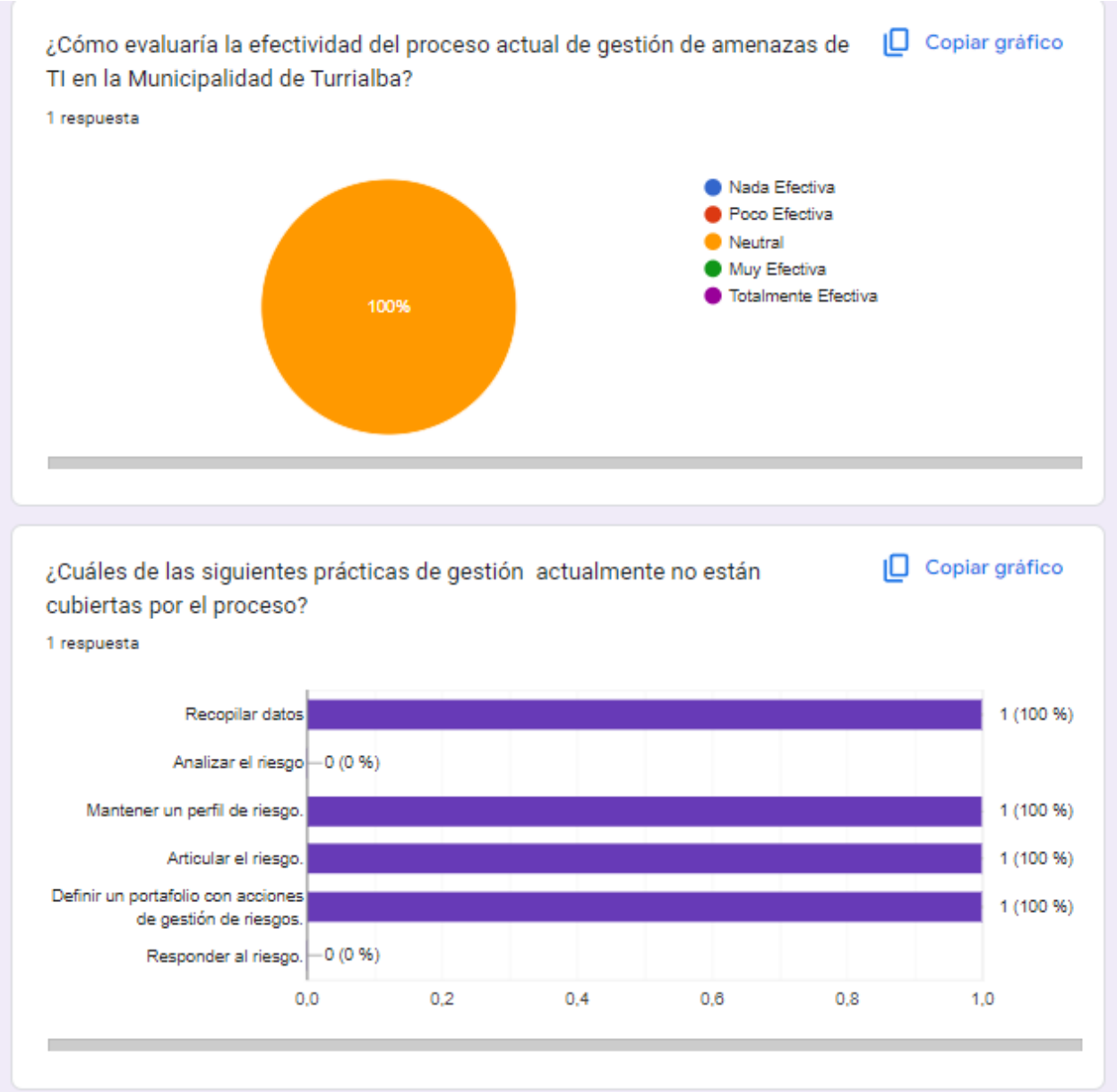
- ○ Muy poco
- ○ Poco
- ○ Moderado
- ○ Alto
- ○ Muy Alto

¿Qué desafíos anticipa en la implementación de un nuevo marco de gestión de riesgos de TI basado en las normativas del MICITT y las prácticas internacionales conocidas?

Tu respuesta

Fuente: Elaboración propia (2024).

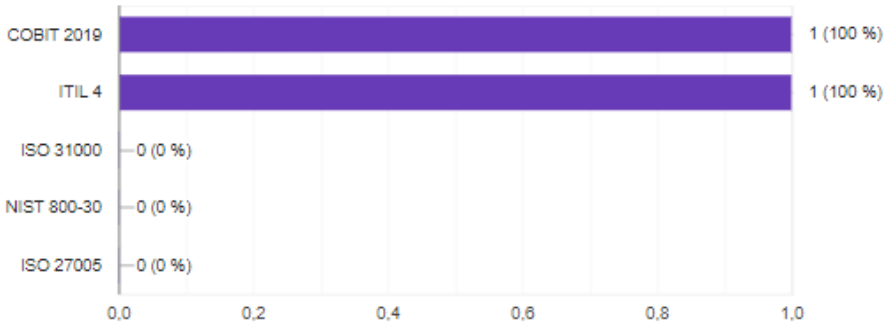
9.10 Apéndice J Resultados Cuestionario Situación Actual



¿Con qué marcos internacionales de gestión de riesgos de TI está familiarizado? Puede marcar multiples opciones.

Copiar gráfico

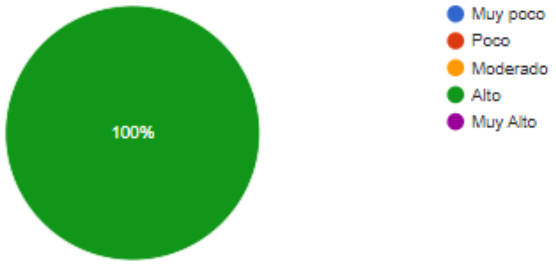
1 respuesta



¿Cuánto considera que su conocimiento actual de estas prácticas podría influir en la implementación efectiva del marco de gestión de riesgos de TI en la Municipalidad?

Copiar gráfico

1 respuesta



¿Qué desafíos anticipa en la implementación de un nuevo marco de gestión de riesgos de TI basado en las normativas del MICITT y las prácticas internacionales conocidas?

1 respuesta

Tiempo que le pueda dedicar así como recursos financieros necesarios para implementar algunas mejores prácticas.

¡Gracias por su participación!

9.11 Apéndice K Plantilla Lista de Comprobación del Proceso de Gestión de Riesgos

Lista de Chequeo del Proceso de Gestión de Riesgos Tecnologicos Municipalidad de Turrialba				
Objetivo de Gestión:		APO12 - Gestionar el Riesgo		
Nivel de capacid	Actividades por Práctica de gestión			
01 Recopilar datos		Se estableció la actividad	Sección de la Política	Sección del Procedimiento
2	Establecer y mantener un método para la recogida, clasificación y análisis de datos relacionados con el riesgo de I&T.			
	Registrar datos relevantes y significativos relacionados con los riesgos de I&T en el entorno operativo interno y externo de la			
3.	Adoptar o definir una taxonomía de riesgo para las definiciones consistentes de escenarios de riesgo y categorías de impacto y probabilidad.			
	Registrar datos de eventos de riesgo que han causado o podrían causar impacto en el negocio conforme a las categorías de impacto definidas en la taxonomía de riesgo. Capturar datos relevantes de cuestiones, incidentes, problemas e investigaciones.			
4	Estudiar y analizar los datos históricos de riesgo de I&T y de pérdidas experimentadas a partir de datos y tendencias externos disponibles, homólogos de la industria a través de logs de eventos de la industria, bases de datos, y acuerdos de la industria, para la publicación común de eventos.			
	Para clases de eventos similares, organizar los datos recopilados y resaltar los factores causantes. Determinar los factores causantes comunes en múltiples eventos.			
	Determinar las condiciones específicas que existieron o estuvieron ausentes cuando tuvieron lugar los eventos de riesgo y la forma en que las condiciones afectaron a la frecuencia del evento y la magnitud de la pérdida.			
	Realizar un análisis periódico de eventos y factores de riesgo para identificar riesgos nuevos o emergentes y para mejorar el entendimiento de los factores de riesgo internos y externos			

	02 Analizar el riesgo	Se estableció la actividad	Sección de la Política	Sección del Procedimiento
3	Definir el alcance adecuado de los esfuerzos en análisis de riesgos, considerando todos los factores de riesgo y/o la criticidad de los activos para el negocio.			
	Crear y actualizar regularmente los escenarios de riesgo de I&T; las exposiciones a pérdidas relacionadas con I&T; y los escenarios relacionados con el riesgo reputacional, incluidos escenarios compuestos de tipos de amenazas y eventos en cascada y/o coincidentes. Desarrollar previsiones para actividades de control específicas y capacidades de detección.			
	Estimar la frecuencia (o probabilidad) y la magnitud de la pérdida o ganancia asociada con escenarios de riesgos de I&T. Tener en cuenta todos los factores de riesgo aplicables y evaluar controles operativos conocidos.			
	Comparar el riesgo actual (exposición a pérdidas de I&T) con el apetito al riesgo y la tolerancia de riesgo aceptable. Identificar el riesgo inaceptable o elevado.			
	Proponer respuestas al riesgo para riesgos que excedan el apetito al riesgo y los niveles de tolerancia.			
	Especificar los requisitos de alto nivel para los proyectos o programas que implementarán las respuestas a los riesgos seleccionadas. Identificar los requisitos y expectativas para los controles clave adecuados a fin de proporcionar respuestas de			
4	Validar el análisis de riesgo y los resultados del análisis de impacto del negocio (BIA) antes de usarlos en la toma de decisiones. Confirmar que el análisis se corresponde con los requisitos empresariales y comprobar que los sesgos de las estimaciones se calibraron y analizaron de forma adecuada.			
5	Analizar el coste/beneficio de las posibles opciones de respuesta al riesgo, como evitar, reducir/mitigar, transferir/compartir y aceptar y explotar/ aprovechar. Confirmar la respuesta óptima al riesgo.			

03 Mantener un perfil de riesgo.		Se estableció la actividad	Sección de la Política	Sección del Procedimiento
2	Hacer un inventario de los procesos de negocio y documentar su dependencia con los procesos de gestión de servicios de I&T y los recursos de infraestructura de TI. Identificar el personal de apoyo, aplicaciones, infraestructura, instalaciones, registros manuales criticos, contratistas, proveedores, y terceros.			
	Determinar y acordar qué servicios de I&T y recursos de infraestructura de TI son esenciales para sostener el funcionamiento de los procesos de negocio. Analizar las dependencias e identificar los eslabones débiles.			
	Agregar los escenarios de riesgos actuales por categoria, línea de negocio y área funcional.			
3	Capturar regularmente toda la información del perfil de riesgo y consolidarla en un perfil de riesgo agregado.			
	Capturar información sobre el estado del plan de acción de riesgos para su inclusión en el perfil de riesgo de I&T de la empresa.			
4	Con base en todos los datos del perfil de riesgo, definir un conjunto de indicadores de riesgo que permitan una identificación y monitorización rápida del riesgo actual y las tendencias de			
	Capturar información sobre eventos de riesgo de I&T que se han materializado para su inclusión en el perfil de riesgo de TI de la empresa.			

04 Articular el riesgo.		Se estableció la actividad	Sección de la Política	Sección del Procedimiento
3	Informar sobre los resultados del análisis de riesgo a todas las partes interesadas afectadas en términos y formatos útiles para soportar las decisiones empresariales. Siempre que sea posible, incluir las probabilidades y rangos de pérdidas o ganancias, junto con los niveles de confianza, para permitir que la gerencia haga balance del retorno del riesgo.			
	Proporcionar a los responsables de la toma de decisiones la comprensión de los escenarios más probables y peores, exposiciones a pérdidas de I&T y consideraciones significativas de reputación, legales y regulatorias, o cualquier otra categoria de impacto conforme a la taxonomia de riesgos.			
	Informar sobre el perfil de riesgo actual a todas las partes interesadas. Incluir información sobre la eficacia del proceso de gestión de riesgos, eficacia del control, brechas, inconsistencias, redundancias, estado de remediación y sus impactos en el perfil			
	De forma periódica, en áreas con riesgos relativos y capacidades de riesgo similares, identificar portunidades relacionadas con I&T que permitirían la aceptación de un riesgo mayor y un mayor crecimiento y retorno.			
4	Revisar los resultados de las evaluaciones objetivas de terceros y revisiones de auditoria interna y de aseguramiento de la calidad. Incluirlos en el perfil de riesgo. Revisar las brechas identificadas y las exposiciones de pérdidas relacionadas con I&T para determinar la necesidad de un análisis de riesgos adicional.			

05 Definir un portafolio con acciones de gestión de riesgos.		Se estableció la actividad	Sección de la Política	Sección del Procedimiento
2	Mantener un inventario de las actividades de control que se han implantado para mitigar el riesgo y que permiten que se tomen riesgos alineados con el apetito y la tolerancia al riesgo. Clasificar las actividades de control y asignarlas a escenarios de riesgos de I&T específicos y escenarios de riesgos de I&T agregados.			
3	Determinar si cada entidad organizativa monitoriza el riesgo y acepta la responsabilidad de actuar dentro de los niveles de tolerancia individuales y del portafolio.			
	Definir un conjunto de propuestas de proyectos equilibrada diseñada para reducir el riesgo y/o proyectos que permitan oportunidades empresariales estratégicas, con consideración de los costes, beneficios, efecto en el perfil de riesgo actual y en las			
06 Responder al riesgo.		**Se estableció la actividad**	**Sección de la Política**	**Sección del Procedimiento**
3	Preparar, mantener y probar planes que documenten los pasos específicos que deben darse cuando un evento de riesgo pudiera causar un incidente significativo de desarrollo u operativo con un impacto grave para el negocio. Asegurar que los planes incluyan vías de escalamiento en la empresa.			
	Aplicar el plan de respuesta adecuado para minimizar el impacto cuando ocurren incidentes de riesgo.			
4	Clasificar los incidentes y comparar las exposiciones a pérdidas relacionadas con I&T con los umbrales de tolerancia al riesgo. Comunicar los impactos de negocio a los responsables de la toma de decisiones como parte del reporte y actualización del perfil de			
	Examinar eventos adversos/pérdidas y oportunidades del pasado no consideradas y determinar las causas raíz.			
5	Comunicar la causa raíz, requisitos adicionales de respuestas al riesgo y mejoras del proceso a los responsables de la toma de decisiones correspondientes. Asegurar que la causa, requisitos de respuesta y mejora del proceso se incluyan en los procesos de			

Fuente: Elaboración propia (2024).

9.12 Apéndice L Minuta de Reunión 04 – Aplicación de Entrevista

MINUTA DE REUNIÓN

Proyecto: Propuesta De Un Proceso Formal De Gestión De Riesgos De Tecnologías De Información Para La Municipalidad De Turrialba

Reunión No.	N°04	Fecha:	17/09/2024
Lugar:	Municipalidad de Turrialba	Hora Inicio/Finalización:	10:00 am / 11:00 am
Objetivo de la reunión:	Aplicación de las Entrevistas Apéndice G Entrevista Situación Actual y Apéndice H Entrevista Miembro Comisión de Control Interno		
Participantes:	Presentes: Pablo Alonso Chaves Rivera, Encargado de TI (Nelson Gamboa) y Miembro de la Comisión de Control Interno		
	Ausentes:		

Temas Tratados

No.	Asunto	Comentarios	Acuerdos
1	Aplicación de la encuesta Apéndice H Entrevista Miembro Comisión de Control Interno	Se grabo la entrevista con la autorización del miembro de la comisión de control interno.	El miembro de la Comisión de Control Interno aprueba la entrevista.
2	Aplicación de la encuesta Apéndice G Entrevista Situación Actual	Se grabo la entrevista con la autorización del encargado de TI.	El encargado de TI aprueba la entrevista.
3	Determinar el nivel de Capacidad del proceso de gestión de riesgos de TI.	El estudiante explica al encargado de TI que son los niveles de capacidad del APO12 Gestionar el Riesgo de COBIT 2019 y cuales son las actividades de cada nivel, consultando al encargado el nivel deseado para el proceso formal de gestión de riegos de TI.	El encargado de TI requiere que el proceso contemple las actividades de nivel tres e inferiores.

Próxima reunión

Temas a tratar	Fecha	Convocados

NELSON EDUARDO GAMBOA CALDERON (FIRMA) digitally signed by NELSON EDUARDO GAMBOA CALDERON (FIRMA)

Uso Confidencial Pág. 1/1

9.13 Apéndice M Resultados Entrevista Situación Actual

Apéndice M Resultados Entrevista Situación Actual

Preguntas:

1. ¿Quiénes son los principales responsables de la gestión de amenazas de TI en la Municipalidad y cuáles son sus roles específicos?
    - R/: Actualmente, el responsable principal de la gestión de amenazas de TI en la Municipalidad es una sola persona que asume todos los roles y responsabilidades. No hay un equipo dedicado, lo que limita la capacidad de distribución de tareas.
2. ¿Existe documentación formal que describa el proceso actual de gestión de amenazas de TI? ¿Está actualizada y accesible para el personal relevante?
    - R/: No existe una documentación formal que describa el proceso de gestión de amenazas de TI. Todo se gestiona de manera reactiva y no hay un sistema formalizado de documentación accesible.
3. ¿Qué actividades o tareas específicas se realizan actualmente para gestionar las amenazas de TI? ¿Son manuales o automatizadas?
    - R/: La mayoría de las actividades para gestionar amenazas de TI son manuales, como la identificación de riesgos y la asignación de prioridades. Aunque existen herramientas de monitoreo automatizado para ciberataques, muchas tareas aún dependen de la intervención manual.
4. Cuando se identifica una amenaza de TI, ¿qué pasos sigue el equipo para gestionarla?
    - R/: El primer paso es identificar la amenaza, evaluar su gravedad y tomar las medidas necesarias. Dependiendo del tipo de amenaza, las acciones pueden ser internas (como ajustes de configuración o reemplazo de hardware) o externas (como contactar a proveedores de servicios).
5. ¿Cómo describiría el estado de las políticas y procedimientos actuales para manejar las amenazas de TI?
    - R/: No existen políticas ni procedimientos formales establecidos para la gestión de amenazas de TI. La gestión de estas amenazas se realiza de manera reactiva y no sigue un protocolo definido.
6. ¿Cómo calificaría la efectividad de las capacitaciones sobre gestión de riesgos de TI proporcionadas al personal? ¿Qué áreas podrían mejorarse?
    - R/: No se han proporcionado capacitaciones formales sobre la gestión de riesgos de TI. Sin embargo, se realizan esfuerzos informales para concientizar al personal a través de cápsulas informativas sobre ciberseguridad.
7. ¿Qué tipo de documentación respalda el proceso actual de gestión de riesgos de TI?
    - R/: No existe documentación formal para respaldar el proceso de gestión de riesgos de TI. Aunque se generan alertas y se llevan a cabo acciones correctivas, no se documentan de manera formal.
8. Desde su experiencia, ¿qué mejoras cree que se podrían implementar en el proceso de gestión de riesgos de TI en la Municipalidad?
    - R/: Se podrían implementar mejoras como la formalización de políticas y procedimientos, la creación de un sistema de registro de amenazas, y la implementación de capacitaciones regulares para el personal. Además, sería beneficioso contar con más personal especializado en TI.
9. ¿La Municipalidad de Turrialba utiliza servicios de outsourcing para la gestión de TI? Si es así, ¿qué tipo de servicios se externalizan y cómo se gestionan los riesgos asociados?
    - R/: Sí, se externalizan algunos servicios, como la provisión de Internet y la gestión de la base de datos de cobros. Los proveedores son responsables del mantenimiento de estos sistemas, pero la Municipalidad no cuenta con un sistema formal para gestionar los riesgos asociados a la externalización.

10. ¿Existen mecanismos de control para garantizar que los proveedores externos cumplan con las políticas de seguridad y gestión de riesgos?
    - R/: No existen mecanismos formales para asegurar que los proveedores cumplan con políticas de seguridad y gestión de riesgos. La comunicación con los proveedores se limita a resolver incidentes cuando ocurren.
11. ¿Se ha definido un apetito de riesgo para las operaciones de TI en la Municipalidad? ¿Cómo se determina y comunica?
    - R/: No se ha definido ni comunicado un apetito de riesgo formal para las operaciones de TI en la Municipalidad. Las decisiones se toman caso por caso, sin un marco claro para la gestión del riesgo.
12. ¿Qué actividades o tareas se requerirán en el nuevo marco formal de gestión de riesgos de TI?
    - R/: Se requerirá la implementación de tareas como la documentación formal del proceso, la identificación regular de riesgos, la evaluación y clasificación de amenazas, la implementación de medidas preventivas y correctivas, y el monitoreo constante de los sistemas.

NELSON EDUARDO GAMBOA CALDERON (FIRMA)

Encargado de TI

9.14 Apéndice N Resultados Entrevista Miembro de la Comisión de Control Interno

Apéndice N Resultados Entrevista Miembro de la Comisión de Control Interno

1. ¿Quiénes son los responsables principales del proceso de gestión de riesgos generales en la Municipalidad?
    a. R/: El responsable principal del proceso de gestión de riesgos generales en la Municipalidad es el máximo jerarca, es decir, el alcalde. El alcalde puede delegar esta responsabilidad en la Comisión de Control Interno, cuya función es asesorar, no gestionar directamente los riesgos. Sin embargo, el alcalde sigue siendo el responsable final. La Comisión dejó de ser convocada regularmente en el último año y medio.
2. ¿Cuál es el estado de la documentación relacionada con el proceso de gestión de riesgos generales? ¿Es fácilmente accesible?
    a. R/: No existe una documentación formal y actualizada sobre la gestión de riesgos generales. Aunque se realizó una autoevaluación institucional hace un año, no se ha documentado de manera consistente.
3. ¿Qué actividades o tareas específicas se realizan para identificar y gestionar los riesgos generales en la Municipalidad?
    a. R/: No se realizan actividades planificadas para identificar los riesgos. Estos se abordan según aparecen, de manera reactiva, sin un proceso estructurado.
4. ¿Cómo describiría la efectividad de las estrategias actuales de mitigación de riesgos? ¿Qué medidas considera más efectivas?
    a. R/: No existen estrategias formales para la mitigación de riesgos en la Municipalidad. Los riesgos se abordan conforme van surgiendo.
5. ¿Existen áreas donde cree que el proceso de gestión de riesgos generales puede ser optimizado o mejorado?
    a. R/: Sí, hay varias áreas que pueden mejorarse. La principal es la falta de personal dedicado a la gestión de riesgos, así como la carencia de asignación presupuestaria y de recursos financieros.
6. ¿Qué limitaciones enfrenta la Municipalidad en la implementación de un proceso efectivo de gestión de riesgos?
    a. R/: Las principales limitaciones son la falta de personal capacitado y la sobrecarga de los pocos empleados que manejan estas tareas, junto con la falta de recursos financieros y presupuesto asignado para la gestión de riesgos.
7. ¿Cuáles son las principales amenazas que enfrenta el proceso de gestión de riesgos de TI en la Municipalidad?
    a. R/: Las principales amenazas incluyen interrupciones en el fluido eléctrico y riesgos naturales, ya que el cantón es propenso a catástrofes naturales como inundaciones o deslizamientos de tierra, además del volcán activo en la zona.
8. ¿Existe un apetito de riesgo claramente definido para la gestión de riesgos en la Municipalidad de Turrialba?
    a. R/: No, no existe un apetito de riesgo formalmente documentado. La información relacionada con el apetito de riesgo está en las mentes de los responsables, pero no se ha formalizado ni comunicado claramente. El responsable de determinar el apetito de riesgo de la municipalidad sería el alto jerarca, es decir el alcalde que lleva en funciones solo tres meses.

NELSON EDUARDO GAMBOA CALDERON (FIRMA)

Encargado de TI

9.15 Apéndice O Transcripción de Entrevistas.

Apéndice O Transcripción de la entrevista:

Estudiante: Entonces, te comento que la primera pregunta es: dentro de la municipalidad, ¿quiénes son responsables del proceso de gestión de riesgos?

Encargado de TI: Primero, según la ley, el responsable es el máximo jerarca, es decir, el alcalde. El alcalde puede delegar esta responsabilidad en una comisión llamada **Comisión de Control Interno**, que se formó hace cerca de ocho años. El alcalde anterior estuvo en el cargo durante ocho años y mantuvo la comisión en funcionamiento. Sin embargo, nosotros, como comisión—y hablo en nombre de la comisión—no somos los responsables directos, sino que simplemente asesoramos al alcalde. El control interno incluye la gestión de riesgos institucionales, donde hacemos recomendaciones. Lamentablemente, en los últimos año y medio, la comisión ha dejado de funcionar porque el alcalde es quien convoca a las reuniones y, debido a otras prioridades, no se han llevado a cabo.

Estudiante: Entiendo.

Encargado de TI: Cuando llegó la nueva alcaldía en mayo y estamos en septiembre, todavía no se han pronunciado sobre nuestras recomendaciones, así que no sabemos cómo procederán.

Estudiante: Ok, ¿cómo está actualmente la documentación relacionada con la gestión de riesgos en la municipalidad?

Encargado de TI: No existe una comunicación formal relacionada con la gestión de riesgos. Se hizo una autoevaluación institucional hace un año, donde se les pasó un formulario a los jefes de departamento para que opinaran sobre aspectos de control interno, incluyendo riesgos. Sin embargo, no hay documentación formal, solo recomendaciones que quedaron en rojo, indicando que estamos en una situación grave.

Estudiante: ¿Han realizado una auditoría interna solo para la autoevaluación?

Encargado de TI: Sí, solo para la autoevaluación. En la gestión de riesgos, solo se atienden los riesgos a medida que aparecen, sin una identificación proactiva.

Estudiante: Eso me lleva a la siguiente pregunta: ¿Actualmente, ¿cómo está la documentación relacionada con la gestión de riesgos en la municipalidad?

Encargado de TI: No existe una comunicación formal. La autoevaluación fue la única acción realizada, pero no se ha documentado adecuadamente.

Estudiante: ¿Existen estrategias para la gestión de riesgos?

Encargado de TI: No, no hay estrategias definidas.

Estudiante: ¿Cuáles son las limitaciones que enfrenta la municipalidad para implementar un proceso de gestión de riesgos?

Encargado de TI: Las principales limitaciones son el personal y los recursos financieros. No hay personal dedicado exclusivamente a la planificación; solo tenemos una persona que está sobrecargada. Además, no existe asignación presupuestaria para contratar personal adicional o contratar servicios externos.

Estudiante: Entiendo. Mencionaste que las amenazas se van atendiendo a medida que surgen. ¿Cuáles son las amenazas o riesgos más comunes a nivel institucional?

Encargado de TI: Principalmente riesgos naturales, ya que el cantón es muy propenso a catástrofes naturales como erupciones volcánicas, ríos y montañas. Además, hay problemas con el suministro eléctrico y otras emergencias que consumen nuestros recursos.

Estudiante: Entonces, ¿no hay un apetito de riesgo definido dentro de la organización?

Encargado de TI: Correcto, no hay documentación al respecto. Todo está en nuestra cabeza y la del alcalde. Actualmente, el apetito de riesgo recae casi completamente sobre el alcalde.

Estudiante: Entiendo. Ahora, pasando a tu rol como encargado del departamento de TI, ¿cuáles son los responsables de la gestión de amenazas de TI y cuáles son tus roles?

Encargado de TI: Actualmente, soy la única persona en TI, así que asumo todas las responsabilidades.

Estudiante: Ya me comentaste que no existe documentación a nivel municipal ni a nivel del departamento. Cuando se presenta una amenaza, ¿cuáles son los procesos o tareas que realizas para mitigarlas?

Encargado de TI: Primero identifico la amenaza, le asigno prioridad y tomo las acciones necesarias. Dependiendo del caso, puede requerir cambiar o reconfigurar equipos físicos, o contactar a proveedores si la falla es externa. Luego, actúo en consecuencia, ya sea de manera interna o externa.

Estudiante: ¿Quién te comunica una amenaza cuando la identificas?

Encargado de TI: Los usuarios me lo comunican directamente, generalmente por correo electrónico o por teléfono en casos urgentes. A veces, me abordan en persona si el edificio es pequeño.

Estudiante: Perfecto. ¿Qué tipos de amenazas sueles enfrentar a nivel institucional?

Encargado de TI: Principalmente amenazas naturales como erupciones volcánicas y problemas con el suministro eléctrico. También enfrentamos riesgos relacionados con la infraestructura, como árboles que caen en caminos, etc.

Estudiante: ¿Existe algún sistema para monitorear y registrar estas amenazas?

Encargado de TI: Sí, utilizo dashboard en la nube para monitorear constantemente. Tengo mecanismos de respaldo y utilizo plataformas con inteligencia artificial que me envían alertas ante anomalías. Sin embargo, no tengo tiempo para documentar estos reportes formalmente.

Estudiante: ¿Utilizas algún software específico para el monitoreo?

Encargado de TI: Por motivos de seguridad, no puedo precisar los programas, pero utilizo desde plataformas en la nube hasta equipos físicos como firewalls y configuraciones en routers y puntos de acceso. También manejo antivirus y servidores DNS para administrar el tráfico web.

Estudiante: ¿Los reportes de las alertas están registrados de alguna forma?

Encargado de TI: Recibo las alertas por correo electrónico y actúo de acuerdo con lo que sea necesario. En algunos casos, informo al usuario y al jefe sobre la situación y las acciones tomadas.

Estudiante: ¿Existe algún seguimiento formal de estas acciones?

Encargado de TI: No formalmente. Aunque informo a los usuarios y a los jefes, no hay un registro formal de todas las acciones y seguimientos realizados.

Estudiante: ¿Han recibido alguna capacitación sobre riesgos?

Encargado de TI: Nunca hemos recibido una capacitación formal. Sin embargo, envío cápsulas informativas regularmente sobre ciberseguridad a los funcionarios.

Estudiante: ¿Qué tipo de correo institucional utilizan?

Encargado de TI: Usamos un hosting propio, no de Microsoft ni de Google. Configuro los equipos para acceder al correo a través de nuestra página web y utilizo filtros antispam e inteligencia artificial para gestionar las amenazas.

Estudiante: ¿Documentan los análisis y registros de amenazas en algún formato, como Excel?

Encargado de TI: No, no tenemos documentación formal debido a la falta de tiempo. Las comunicaciones son principalmente por correo electrónico sin un registro estructurado.

Estudiante: Mencionaste el uso de servicios de outsourcing para la gestión de TI. ¿Qué servicios externalizan?

Encargado de TI: Principalmente el servicio de internet y la base de datos de cobros. El sistema integrado es propiedad de una empresa que maneja el código fuente y el mantenimiento del sistema.

Estudiante: Finalmente, sobre las actividades de gestión de riesgos, ¿conoces el concepto de nivel de capacidad y cómo se relaciona con las actividades de gestión de riesgos?

Encargado de TI: La verdad, no estoy familiarizado con el concepto.

Estudiante: Te explico rápidamente: el nivel de capacidad se refiere a qué tan madura es la empresa en términos de gestión de riesgos y qué actividades pueden realizarse según esa madurez. Por ejemplo, en nivel 2, se establece un método para la recopilación y análisis de datos de riesgos. En nivel 3, se define una taxonomía de riesgos para categorizar escenarios. Actualmente, estamos en proceso de alcanzar el nivel 3 y aspiramos a nivel 5 en los próximos tres años, aunque por ahora solo puedo enfocarme en el nivel 3 debido a que soy la única persona en el departamento.

Encargado de TI: Sí, eso es correcto. Mientras siga siendo solo yo en el departamento, es difícil avanzar más allá del nivel 3, pero estamos aspirando a mejorar progresivamente.

Estudiante: Perfecto. Gracias por la información. Esto servirá como base para la auditoría y para planificar futuras mejoras en la gestión de riesgos de la municipalidad.

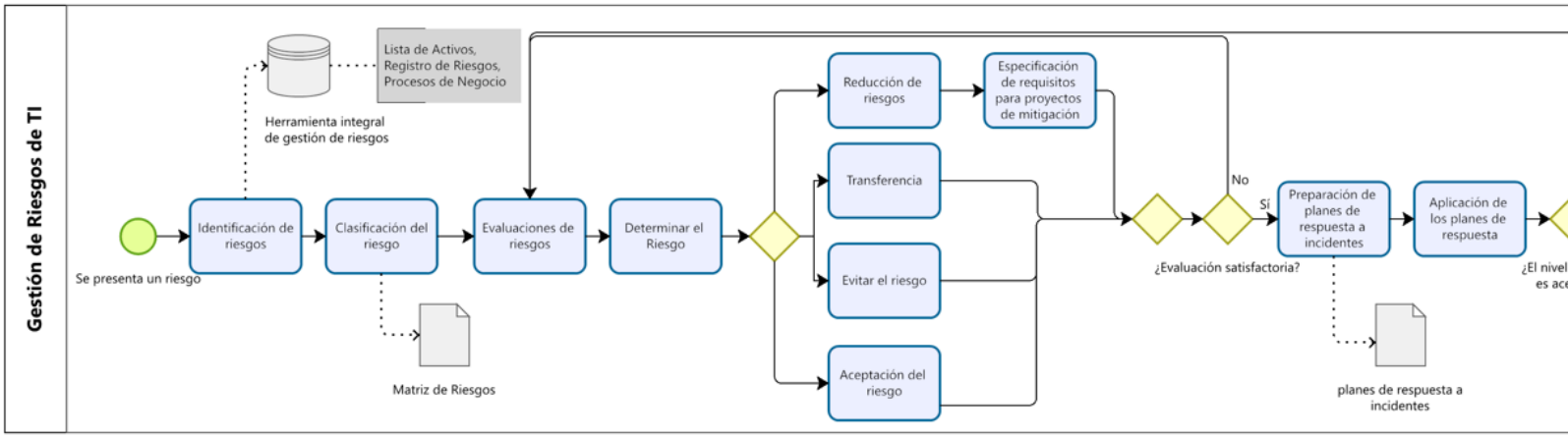
Encargado de TI

9.16 Apéndice P Plantilla Perfil del Proceso

Perfil del Proceso	
Elemento	**Descripción**
1. Objetivo y Metas	**Objetivo del Proceso:** (Describir claramente el objetivo del proceso) **Metas Específicas:** (Detallar las metas específicas que deben ser ejecutables, orientadas a resultados, medibles y realistas).
2. Propiedad del Proceso	**Propietario del Proceso:** (Establecer el responsable del diseño del proceso, la interacción con otros procesos, la rendición de cuentas de los resultados, la medición del desempeño y la identificación de mejoras).

3. Secuencia de Actividades	**Secuencia Lógica de Actividades:** (Establecer una secuencia de actividades clara, lógica y escalable que asegure la flexibilidad y los resultados esperados. Debe considerar excepciones y emergencias).
4. Roles y Responsabilidades	**Roles Asignados:** (Identificar los roles exactos asignados para la ejecución de actividades clave). **Responsabilidades:** (Detallar las responsabilidades para la ejecución y documentación de las actividades, así como la rendición de cuentas de los entregables finales).
5. Lineamientos y Planes	**Planes de Gestión, Trabajo y Acción:** (Describir los planes formales para las actividades y tareas en un período específico, orientados a lograr resultados). **Políticas y Directrices:** (Incluir las políticas que proporcionan la información sobre normas y mecanismos que deben cumplirse). **Normas:** (Especificar las normas que definen los propósitos generales dentro del marco regulatorio). **Procedimientos:** (Indicar los procedimientos detallados para las actividades operativas y administrativas). **Estándares Técnicos:** (Definir los estándares técnicos necesarios). **Instructivos, Listas de Comprobación y Formularios:** (Detallar los documentos anexos que guían las actividades y proporcionan evidencia de las actividades realizadas).
6. Indicadores de Desempeño	**Indicadores de Desempeño:** (Definir los indicadores que miden el nivel de logro de las metas). **Método de Recolección de Datos:** (Especificar cómo se recopilan los datos asociados a los indicadores). **Acciones para Desviaciones:** (Describir las acciones correctivas a tomar en caso de que los indicadores revelen desviaciones en los resultados esperados).

9.17 Apéndice Q Modelado to-be



9.18 Apéndice R Política para la Gestión de Riesgos de Tecnologías de Información

DEPARTAMENTO DE TECNOLOGÍAS DE INFORMACIÓN

Municipalidad de Turrialba Departamento de Tecnologías de Información

Política para la Gestión de Riesgos de Tecnologías de Información

Turrialba, Cartago, octubre 2024

Número de Páginas 1 - 31

Departamento de Tecnologías de Información,
e-mail: negamboa@muniturrialba.go.cr

DEPARTAMENTO DE TECNOLOGÍAS DE INFORMACIÓN

ELABORADO POR:	SUPERVISADO POR:	REVISADO POR:	APROBADO POR:
Sr. Pablo Alonso Chaves Rivera	Ing. Nelson Eduardo Gamboa Calderón	M.S.c. Carlos Eduardo Hidalgo Flores,	M.S.c. Carlos Eduardo Hidalgo Flores
	Departamento de Tecnologías de Información	Alcalde Municipal	Alcalde Municipal

REVISION	FECHA	RESUMEN DE LA REVISION

ELABORADO POR:

FECHA dd/mm/aaaa

APROBADO POR:

FECHA dd/mm/aaaa

Número de Páginas 2 - 30

Departamento de Tecnologías de Información,
e-mail: negamboa@muniturrialba.go.cr

1 Objetivo

Presentar en forma clara y coherente los elementos que conforman la política de gestión de riesgos de tecnología de información que deben conocer y cumplir: Gerencia Municipal (Alcalde y Concejo Municipal,) Directores, Jefes de Departamento y colaboradores en general, funcionarios contratistas y terceros que presten sus servicios o tengan algún tipo de relación con el Departamento de Tecnologías de Información de la Municipalidad de Turrialba.

2 Alcance

Las Políticas de gestión de riesgos de tecnología de información son aplicables para todos los aspectos administrativos y de control que deben ser cumplidos por: Gerencia Municipal (Alcalde y Concejo Municipal), Directores, Jefes de Departamento y colaboradores en general, funcionarios contratistas y terceros que presten sus servicios o tengan algún tipo de relación con el Departamento de Tecnologías de Información de la Municipalidad de Turrialba, para el adecuado cumplimiento de sus funciones y para conseguir un adecuado nivel de protección de las características de calidad y seguridad de la información, aportando con su participación en la toma de medidas preventivas y correctivas, siendo un punto clave para el logro del objetivo y la finalidad de dicho instrumento. Los usuarios tienen la obligación de dar cumplimiento a las presentes políticas emitidas y aprobadas por la Alcaldía.

3 Términos y Definiciones

Aceptación del riesgo: Decisión informada de asumir un determinado riesgo.

Amenaza: Cualquier circunstancia o evento con el potencial de impactar negativamente las operaciones organizacionales mediante acceso no autorizado, destrucción, divulgación o modificación de la información y/o denegación de servicio.

Análisis de riesgos: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

Apetito de riesgo: Cantidad y tipo de riesgo que una organización está dispuesta a perseguir o retener.

Ataque: Cualquier tipo de actividad maliciosa que intente recolectar, interrumpir, negar, degradar o destruir los recursos del sistema de información o la propia información.

Autenticación: Verificar la identidad de un usuario, proceso o dispositivo, a menudo como requisito previo para permitir

Departamento de Tecnologías de Información,
e-mail: negamboa@muniturrialba.go.cr

el acceso a los recursos en un sistema de información.

Autenticidad: La propiedad de ser genuino y poder ser verificado y confiable; confianza en la validez de una transmisión, un mensaje o el origen de un mensaje.

Autorización: La decisión de gestión oficial otorgada por un funcionario organizacional superior para autorizar la operación de un sistema de información y aceptar explícitamente el riesgo para las operaciones organizacionales (incluyendo misión, funciones, imagen o reputación), activos organizacionales, individuos, otras organizaciones y la Nación.

Comunicación y consulta de riesgos: Conjunto de procesos continuos e iterativos que una organización lleva a cabo para proporcionar, compartir u obtener información, y para entablar un diálogo con las partes interesadas en relación con la gestión de riesgos.

Confidencialidad: Preservar las restricciones autorizadas sobre el acceso y la divulgación de información, incluyendo medios para proteger la privacidad personal e información propietaria.

Consecuencia: Resultado de un acontecimiento que afecta a los objetivos.

Contexto externo: Entorno externo en el que la organización pretende alcanzar sus objetivos. El contexto externo puede incluir el entorno social, cultural, político, jurídico, normativo, financiero, tecnológico, económico, geológico, ya sea internacional, nacional, regional o local, los principales impulsores y tendencias que afectan a los objetivos de la organización, las relaciones, percepciones, valores, necesidades y expectativas de las partes interesadas externas, las relaciones y compromisos contractuales y la complejidad de las redes y dependencias.

Contexto interno: Entorno interno en el que la organización trata de alcanzar sus objetivos.

Criterios de riesgo: Términos de referencia con los que se evalúa la importancia de un riesgo.

Criticidad: Una medida del grado en que una organización depende de la información o del sistema de información para el éxito de una misión o función comercial.

Disponibilidad: Asegurar el acceso oportuno y confiable a la información y su uso.

Enfoque de Evaluación: El enfoque utilizado para evaluar el riesgo y sus factores de contribución, incluyendo cuantitativa, cualitativa o semi-cuantitativamente.

Entorno de Operación: El entorno físico, técnico y organizacional en el que opera un sistema de información, que incluye, pero no se limita a varios factores que influyen en la seguridad y el riesgo del sistema.

Escenario de riesgo: Secuencia o combinación de acontecimientos que conducen de la causa inicial a la consecuencia no deseada.

Departamento de Tecnologías de Información,
e-mail: negamboa@muniturrialba.go.cr

Evaluación de Amenaza: Proceso de evaluación formal del grado de amenaza a un sistema de información o empresa y descripción de la naturaleza de la amenaza.

Evaluación de Vulnerabilidad: Examen sistemático de un sistema de información o producto para determinar la adecuación de las medidas de seguridad, identificar deficiencias de seguridad y predecir la efectividad de las medidas propuestas.

Evaluación del riesgo: Proceso de comparación de los resultados del análisis del riesgo con los criterios de riesgo para determinar si el riesgo y/o su importancia son aceptables o tolerables.

Evento: Ocurrencia o cambio de un conjunto particular de circunstancias.

Fuente de riesgo: Elemento que por sí solo o en combinación tiene el potencial de dar lugar a un riesgo.

Identificación de riesgos: Proceso de búsqueda, reconocimiento y descripción de riesgos.

Incidente de seguridad de la información: Suceso único o serie de sucesos de seguridad de la información no deseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones de la empresa y amenazar la seguridad de la información.

Información: Cualquier comunicación o representación de conocimientos tales como hechos, datos u opiniones en cualquier medio o forma, incluyendo textual, numérico, gráfico, cartográfico, narrativo o audiovisual.

Integridad: Protección contra la modificación o destrucción indebida de la información e incluye asegurar la no repudio y autenticidad de la información.

Nivel de riesgo: Importancia de un riesgo, expresada en términos de la combinación de consecuencias y su probabilidad.

Propietario del riesgo: Persona o entidad con responsabilidad y autoridad para gestionar un riesgo.

Retención del riesgo: Aceptación temporal del beneficio potencial de ganancia, o de la carga de pérdida, de un riesgo concreto.

Riesgo compartido: Forma de tratamiento del riesgo que implica la distribución acordada del riesgo con otras partes.

Riesgo de Seguridad de la Información: El riesgo para las operaciones organizacionales, activos, individuos, otras organizaciones y la Nación debido a la posibilidad de acceso, uso, divulgación, interrupción, modificación o destrucción no autorizados de información y/o sistemas de información.

Riesgo residual: Riesgo que permanece tras el tratamiento del riesgo.

Riesgo: Efecto de la incertidumbre sobre los objetivos.

Seguridad de la Información: La protección de la información y los sistemas de información contra el acceso, uso, divulgación, interrupción, modificación o destrucción no autorizados para proporcionar confidencialidad, integridad y

Departamento de Tecnologías de Información,
e-mail: negamboa@muniturrialba.go.cr

disponibilidad.

Sistema de Información: Un conjunto discreto de recursos de información organizados para la recolección, procesamiento, mantenimiento, uso, intercambio, difusión o disposición de información.

Tecnología de la Información: Cualquier equipo o sistema interconectado o subsistema de equipos utilizado en la adquisición automática, almacenamiento, manipulación, gestión, movimiento, control, visualización, transmisión o recepción de datos o información.

Tratamiento del riesgo: Proceso para modificar el riesgo.

Vulnerabilidad: Debilidad en un sistema de información, procedimientos de seguridad del sistema, controles internos o implementación que podría ser explotada por una fuente de amenaza.

4 Principios

Adaptada: El marco de referencia y el proceso de la gestión del riesgo se adaptan y son proporcionales a los contextos externo e interno de la organización relacionados con sus objetivos.

Adaptar al Contexto: Adaptar las prácticas de gestión de riesgos a las necesidades específicas de la Municipalidad y a los cambios en el entorno legal y tecnológico.

Colaborar y Promover Visión Integral: Impulsar la colaboración entre los departamentos involucrados en la gestión de riesgos y mantener una visión holística de los riesgos en toda la organización.

Dinámica: Los riesgos pueden aparecer, cambiar o desaparecer con los cambios de los contextos externo e interno de la organización. La gestión del riesgo anticipa, detecta, reconoce y responde a esos cambios y eventos de una manera apropiada y oportuna.

Enfocarse en el Valor: Asegurar que la gestión de riesgos esté alineada con la entrega de valor al ciudadano y los objetivos de servicio público de la Municipalidad.

Estructurada y exhaustiva: Un enfoque estructurado y exhaustivo hacia la gestión del riesgo contribuye a resultados coherentes y comparables.

Factores humanos y culturales: El comportamiento humano y la cultura influyen considerablemente en todos los aspectos de la gestión del riesgo en todos los niveles y etapas.

Inclusiva: La participación apropiada y oportuna de las partes interesadas permite que se consideren su conocimiento, puntos de vista y percepciones. Esto resulta en una mayor toma de conciencia y una gestión del riesgo informada.

Departamento de Tecnologías de Información,
e-mail: negamboa@muniturrialba.go.cr

Integrada: La gestión del riesgo es parte integral de todas las actividades de la organización.

Mejor información disponible: Las entradas a la gestión del riesgo se basan en información histórica y actualizada, así como en expectativas. La gestión del riesgo tiene en cuenta explícitamente cualquier limitación e incertidumbre asociada con tal información y expectativas. La información debería ser oportuna, clara y disponible para las partes interesadas pertinentes.

Mejora continua: La gestión del riesgo mejora continuamente mediante aprendizaje y experiencia.

Optimización y Automatización: Identificar áreas donde los procesos de gestión de riesgos pueden ser optimizados, reduciendo tareas manuales y mejorando la eficiencia con tecnología y automatización.

5 Proceso de evaluación de riesgos

El propósito de la Publicación Especial 800-30 es proporcionar orientación para la realización de evaluaciones de riesgos de los sistemas de información federales y organizaciones. Las evaluaciones de riesgos, llevadas a cabo en los tres niveles de la jerarquía de gestión de riesgos, son parte de un proceso general de gestión de riesgos, proporcionando a los líderes/ejecutivos de alto nivel la información necesaria para determinar los cursos de acción apropiados en respuesta a los riesgos identificados.

5.1 Paso 1 Prepararse para la evaluación

La preparación implica reconocer el objetivo, como el establecimiento de una línea de base de riesgos o la identificación de vulnerabilidades, amenazas, probabilidad e impacto. También incluye definir el alcance, determinar qué secciones de un sistema u organización participan en la evaluación de riesgos y especificar las decisiones en las que influyen los resultados.

Esta etapa implica además el establecimiento de supuestos y limitaciones, incluidas las necesidades de recursos y las condiciones predisponentes que configuran la evaluación de riesgos. Durante esta fase se establecen el enfoque de la evaluación y las tolerancias de riesgo, y se identifican las fuentes de información relacionadas con las amenazas, las vulnerabilidades y el impacto.

5.2 Etapa 2 Realización de la evaluación

Durante la fase de identificación, la atención se centra en reconocer las amenazas, las vulnerabilidades, la probabilidad y el impacto. El enfoque varía en función de la naturaleza del sistema y de los resultados de la fase de preparación. El NIST proporciona un conjunto específico de tareas, que abarcan tareas como la identificación de las fuentes de amenaza, las capacidades del adversario, la intención y los objetivos, así como la evaluación de la relevancia de los eventos de

Departamento de Tecnologías de Información,
e-mail: negamboa@muniturrialba.go.cr

amenaza para el sistema.

Las tareas generalizables a través de varias perspectivas del sistema incluyen la identificación de vulnerabilidades, las condiciones predisponentes, la evaluación de la probabilidad de explotación de la amenaza y la evaluación de los impactos y los activos afectados. Cabe destacar que en el enfoque del NIST, la identificación de amenazas precede a la identificación de vulnerabilidades, dando por sentado que todas las amenazas pueden asociarse a vulnerabilidades.

5.3 Paso 3 Comunicar los resultados

Esta fase se encuentra entre las más críticas, aunque a menudo se pasa por alto, del proceso de gestión de riesgos. La evaluación de riesgos proporciona datos esenciales para orientar las acciones destinadas a mejorar la seguridad del sistema. Sin embargo, la comunicación eficaz es primordial en esta etapa.

Las distintas partes interesadas, como los consejos de administración, los equipos operativos y el personal general de la organización, necesitan información presentada de distintas maneras. Los consejos de administración necesitan una visión general de alto nivel, los equipos operativos buscan información detallada y el personal en general necesita material educativo y orientativo. La comunicación de los resultados y las pruebas de la evaluación de riesgos debe adaptarse a cada parte interesada, garantizando la accesibilidad y la participación en la planificación y ejecución de la gestión de riesgos.

5.4 Paso 4 Mantener la evaluación

Según NIST SP 800-30, implica supervisar y actualizar continuamente la evaluación para reflejar los cambios en el sistema, el entorno y las amenazas. Este proceso continuo garantiza que la evaluación de riesgos siga siendo pertinente y eficaz a lo largo del tiempo. Incluye revisiones periódicas de los factores de riesgo, la reevaluación de las vulnerabilidades y amenazas, y el ajuste de las estrategias de gestión de riesgos según sea necesario.

Además, abarca la documentación de cambios y actualizaciones, manteniendo informadas a las partes interesadas y manteniendo una postura proactiva a la hora de abordar los riesgos emergentes. Este paso hace hincapié en la naturaleza dinámica e iterativa de la gestión de riesgos, destacando la importancia de la adaptabilidad y la capacidad de respuesta al cambiante panorama de la ciberseguridad.

Departamento de Tecnologías de Información,
e-mail: negamboa@muniturrialba.go.cr

6 Roles y Responsabilidades

La Municipalidad tiene un responsable de la gestión de riesgos, estas responsabilidades recaen en el Encargado de los Servicios de Tecnología de Información. Algunas responsabilidades son:

Rol	Descripción
Ejecutivo de Riesgos (ER)	Supervisa todo el proceso de gestión de riesgos, garantizando la alineación con las metas y objetivos de la municipalidad.
Propietario del riesgo (RO)	Responsable de un riesgo específico y facultado para tomar decisiones en relación con ese riesgo; pueden ser jefes de departamento, gestores de proyectos o propietarios de sistemas.
Analista de riesgos (AR)	Realiza evaluaciones de riesgos, incluyendo la identificación, el análisis y la evaluación de los riesgos, proporcionando los datos necesarios para la toma de decisiones.

7 Prácticas de gestión

7.1 Recopilación de Datos

7.1.1 Establecimiento de un método para la recolección, clasificación y análisis de datos

- **Descripción**: Se deberá establecer y mantener un método formal y estandarizado para la recolección, clasificación y análisis de datos relacionados con los riesgos de TI, así como con el entorno operativo tanto interno como externo. Los datos recopilados deberán ser precisos, actualizados y relevantes para la evaluación efectiva de los riesgos de la organización.
- **Frecuencia de Revisión**: Trimestral, con actualización del procedimiento según se identifiquen nuevas necesidades.

Departamento de Tecnologías de Información,
e-mail: negamboa@muniturrialba.go.cr

7.1.2 *Registro de eventos de riesgo*

- **Descripción**: Todos los eventos de riesgo que puedan generar o hayan generado un impacto en la organización deberán ser registrados de forma consistente y conforme a una taxonomía de riesgos previamente definida. Los incidentes, problemas y eventos de riesgo deben documentarse detalladamente, incluyendo causas y efectos, así como las acciones correctivas adoptadas.
- **Frecuencia de Registro**: Continuo, con revisión y consolidación mensual de la información.

7.1.3 *Definición y adopción de una taxonomía de riesgos*

- **Descripción**: La organización deberá adoptar o definir una taxonomía de riesgos que permita la clasificación consistente de los escenarios de riesgo, así como de las categorías de impacto y probabilidad. Esta taxonomía deberá estar alineada con las mejores prácticas internacionales y deberá ser actualizada regularmente para reflejar cambios en el entorno de riesgos.
- **Frecuencia de Revisión**: Anual, con actualizaciones según cambios en el perfil de riesgo o las regulaciones.

7.1.4 *Registro de eventos de riesgo conforme a la taxonomía*

- **Descripción**: Todos los eventos de riesgo que hayan causado o puedan causar un impacto en el negocio deberán registrarse conforme a las categorías de impacto definidas en la taxonomía de riesgo adoptada por la organización. Este registro deberá incluir información detallada sobre cuestiones, incidentes, problemas e investigaciones relacionadas con el riesgo, asegurando que los datos relevantes sean capturados y analizados para prevenir futuros incidentes.
- **Frecuencia de Registro**: Continuo, con revisiones trimestrales para consolidar la información y extraer conclusiones sobre patrones o tendencias emergentes.

7.2 Análisis del Riesgo

7.2.1 *Definición del alcance del análisis de riesgos*

- **Descripción**: Se deberá definir claramente el alcance del análisis de riesgos, teniendo en cuenta todos los factores de riesgo pertinentes y la criticidad de los activos para el negocio. Los escenarios de riesgo, las exposiciones a pérdidas y los posibles impactos reputacionales deberán ser actualizados de manera continua, asegurando un enfoque integral en la gestión de riesgos.
- **Frecuencia de Revisión**: Semestral, con actualización en función de los cambios en el entorno de TI y de negocio.

7.2.2 *Evaluación de controles y estimación de la frecuencia de riesgos*

- **Descripción**: Se deberá estimar la frecuencia y magnitud de las pérdidas o ganancias asociadas a los riesgos de

Departamento de Tecnologías de Información,
e-mail: negamboa@munituriralba.go.cr

TI, evaluando los controles operativos existentes y proponiendo respuestas a los riesgos que superen los niveles aceptables de apetito y tolerancia al riesgo de la organización.

- **Frecuencia de Evaluación**: Trimestral, con ajustes y revisiones en función de los cambios en los controles y la exposición a nuevos riesgos.

7.2.3 *Estimación de la frecuencia y magnitud del riesgo*

- **Descripción**: La organización deberá estimar la frecuencia o probabilidad de ocurrencia y la magnitud de las pérdidas o ganancias asociadas con cada escenario de riesgo de I&T. Para realizar estas estimaciones, se tomarán en cuenta todos los factores de riesgo aplicables, incluyendo la criticidad de los activos de TI y los controles operativos conocidos. Esta evaluación permitirá priorizar las acciones necesarias para mitigar o gestionar los riesgos.
- **Frecuencia de Revisión**: Anual, o cuando haya cambios significativos en el entorno de riesgo.

7.2.4 *Comparación del riesgo actual con el apetito y la tolerancia al riesgo*

- **Descripción**: La organización deberá comparar el nivel actual de exposición a pérdidas relacionadas con I&T con los límites de apetito y tolerancia al riesgo previamente establecidos. Esta comparación permitirá identificar aquellos riesgos que superan los umbrales aceptables, considerados inaceptables o elevados. Dichos riesgos deberán ser gestionados de manera prioritaria para evitar impactos adversos en las operaciones y la reputación de la organización.
- **Frecuencia de Revisión**: Semestral.

7.2.5 *Propuesta de respuestas al riesgo*

- **Descripción**: Para aquellos riesgos que excedan los niveles de apetito y tolerancia al riesgo, la organización deberá proponer respuestas adecuadas que incluyan medidas de mitigación, transferencia, aceptación o evitación del riesgo. Estas respuestas deberán ser proporcionales al impacto y probabilidad del riesgo y deberán ser revisadas y aprobadas por las partes interesadas.
- **Frecuencia de Revisión**: Continuo, con revisiones trimestrales.

7.2.6 *Especificación de requisitos para proyectos de mitigación*

- **Descripción**: Los proyectos o programas que implementen las respuestas a los riesgos seleccionadas deberán tener especificados requisitos de alto nivel, incluyendo los controles clave necesarios para mitigar los riesgos identificados. Estos controles deberán ser alineados con las mejores prácticas de la industria y deberán cumplir con las normativas y estándares regulatorios aplicables.
- **Frecuencia de Revisión**: Conforme a los ciclos de vida de los proyectos.

Departamento de Tecnologías de Información,
e-mail: negamboa@muniturrialba.go.cr

7.3 Mantenimiento del Perfil de Riesgo

7.3.1 Inventario de procesos de negocio y dependencias

- **Descripción**: Se deberá crear y mantener un inventario detallado y actualizado de los procesos de negocio de la organización, identificando su dependencia con los servicios de TI y los recursos de infraestructura tecnológica. Dicho inventario deberá incluir personal clave, infraestructuras críticas, aplicaciones, proveedores y terceros.
- **Frecuencia de Actualización**: Anual, con revisiones adicionales tras cualquier cambio significativo en los procesos de negocio o la infraestructura de TI.

7.3.2 Consolidación del perfil de riesgo

- **Descripción**: Se deberá consolidar de manera regular toda la información relacionada con los riesgos en un perfil de riesgo integrado, que incluya el estado de los planes de acción y la evolución de los riesgos identificados. Este perfil deberá ser utilizado como referencia para la toma de decisiones estratégicas.
- **Frecuencia de Consolidación**: Mensual, o con mayor frecuencia en caso de incidentes o eventos significativos.

7.3.3 Incorporación de escenarios de riesgos actuales

- **Descripción**: La organización deberá clasificar y agregar los escenarios de riesgos actuales en función de categorías de riesgo, líneas de negocio y áreas funcionales. Esta categorización permitirá una mejor visualización y comprensión del impacto de los riesgos sobre las distintas partes de la organización, facilitando la toma de decisiones y la priorización de las acciones correctivas.
- **Frecuencia de Revisión**: Trimestral o según sea necesario ante la aparición de nuevos riesgos.

7.3.4 Consolidación de información en un perfil de riesgo agregado

- **Descripción**: Se deberá capturar regularmente toda la información relevante del perfil de riesgo, incluyendo datos sobre incidentes, amenazas y vulnerabilidades, y consolidarla en un perfil de riesgo agregado. Este perfil proporcionará una visión global del entorno de riesgos de TI y permitirá gestionar de manera centralizada la exposición a los riesgos en toda la organización.
- **Frecuencia de Revisión**: Mensual.

7.3.5 Inclusión del estado del plan de acción en el perfil de riesgo

- **Descripción**: La organización deberá capturar información actualizada sobre el estado del plan de acción para la mitigación de riesgos y reflejarla en el perfil de riesgo de I&T. Esto incluye la documentación de las medidas implementadas, los plazos de ejecución, y los responsables de cada acción, así como los avances y pendientes en la mitigación de riesgos.
- **Frecuencia de Revisión**: Continuo, con actualizaciones trimestrales.

Departamento de Tecnologías de Información,
e-mail: negamboa@muniturrialba.go.cr

7.4 Articulación del Riesgo

7.4.1 *Comunicación de los resultados del análisis de riesgos*

- **Descripción**: Se deberá informar de manera estructurada y oportuna a todas las partes interesadas sobre los resultados del análisis de riesgos, utilizando términos claros y formatos que faciliten la toma de decisiones estratégicas. Los informes deberán incluir las probabilidades de ocurrencia, rangos de impacto y niveles de confianza en las evaluaciones realizadas.
- **Frecuencia de Comunicación**: Trimestral, o inmediatamente tras la identificación de riesgos críticos.

7.4.2 *Provisión de información detallada a los responsables de la toma de decisiones*

- **Descripción**: Se deberá proporcionar a los responsables de la toma de decisiones un análisis completo de los escenarios de riesgo más probables y de los peores casos posibles. Esto incluirá las exposiciones a pérdidas relacionadas con las tecnologías de la información y las comunicaciones (I&T), así como consideraciones significativas en cuanto a la reputación, implicaciones legales, regulatorias y otras categorías de impacto, según lo definido en la taxonomía de riesgos. Esta información debe estar diseñada para apoyar decisiones estratégicas informadas y gestionar adecuadamente los riesgos inherentes.
- **Frecuencia de Revisión**: Trimestral, con actualizaciones adicionales según la evolución de los riesgos.

7.4.3 *Informe del perfil de riesgo*

- **Descripción**: Se deberá proporcionar información actualizada sobre el perfil de riesgo a todas las partes interesadas relevantes, incluyendo la efectividad de los controles, brechas identificadas, inconsistencias, y el estado de los esfuerzos de remediación. Este informe debe permitir la evaluación continua de la eficacia del proceso de gestión de riesgos.
- **Frecuencia de Informes**: Mensual o con mayor frecuencia si se identifican riesgos críticos o brechas importantes.

7.4.4 *Identificación periódica de oportunidades*

- **Descripción**: De manera periódica, la organización deberá identificar áreas con riesgos relativos y capacidades de riesgo similares para evaluar oportunidades que permitan aceptar un mayor nivel de riesgo en aquellas áreas que presenten un balance positivo entre riesgo y retorno. Estas oportunidades deberán ser vinculadas con la estrategia empresarial para fomentar un mayor crecimiento y retorno, siempre alineadas con los límites de tolerancia al riesgo establecidos.
- **Frecuencia de Revisión**: Anualmente, con revisiones adicionales durante ciclos de evaluación estratégica.

Departamento de Tecnologías de Información,
e-mail: negamboa@muniturrialba.go.cr

7.5 Definición de un Portafolio de Acciones de Gestión de Riesgos

7.5.1 Mantenimiento del inventario de actividades de control

- **Descripción**: Se deberá mantener un inventario exhaustivo y actualizado de todas las actividades de control implementadas para mitigar los riesgos de TI. Dichas actividades deben estar alineadas con el apetito y la tolerancia al riesgo definidos por la organización, y ser asignadas a escenarios específicos de riesgos de TI.
- **Frecuencia de Actualización**: Trimestral, con revisión adicional tras cualquier cambio en las condiciones operativas o tecnológicas.

7.5.2 Evaluación de la responsabilidad organizacional en la gestión de riesgos

- **Descripción**: Cada entidad organizativa dentro de la organización deberá monitorear de manera continua los riesgos relacionados con las tecnologías de la información y aceptar la responsabilidad de actuar dentro de los niveles de tolerancia al riesgo individual y del portafolio general de riesgos de la empresa. Esta supervisión debe estar alineada con los objetivos estratégicos y garantizar que las acciones correctivas o preventivas se implementen según sea necesario.
- **Frecuencia de Revisión**: Continuamente, con informes mensuales presentados a la alta dirección.

7.5.3 Definición de proyectos estratégicos para la mitigación de riesgos

- **Descripción**: Se deberá definir un conjunto equilibrado de proyectos o iniciativas estratégicas orientadas a la mitigación de riesgos de TI, teniendo en cuenta los costos, beneficios y su impacto en el perfil de riesgo de la organización. Estos proyectos deberán ser priorizados según su contribución a la reducción de riesgos o al aprovechamiento de oportunidades empresariales.
- **Frecuencia de Revisión**: Anual, con actualizaciones en función de la evolución del perfil de riesgo y los cambios regulatorios.

7.6 Respuesta al Riesgo

7.6.1 Preparación y prueba de planes de respuesta a incidentes

- **Descripción**: Se deberán preparar, mantener y probar regularmente planes de respuesta ante incidentes críticos que puedan generar un impacto significativo en la organización. Estos planes deberán documentar los pasos específicos a seguir, incluyendo rutas de escalamiento dentro de la organización para minimizar el impacto de dichos incidentes.
- **Frecuencia de Pruebas**: Semestral, con revisión y ajustes según los resultados de las pruebas o tras la ocurrencia de un incidente significativo.

Departamento de Tecnologías de Información,
e-mail: negamboa@muniturrialba.go.cr

7.6.2 *Aplicación de los planes de respuesta*

- **Descripción**: Se deberán aplicar de manera efectiva los planes de respuesta documentados cuando ocurra un incidente de riesgo, asegurando que las acciones minimicen el impacto y que se sigan los procedimientos de escalamiento apropiados.
- **Frecuencia de Aplicación**: Activación inmediata durante la ocurrencia de incidentes.

8 Definición de la metodología de evaluación de riesgos

El primer paso crucial de esta metodología es la fase de preparación, en la que se definen el propósito y el alcance de la evaluación de riesgos, incluida la identificación de los elementos que se incluirán en la evaluación y las decisiones que informará. A continuación, la fase de identificación de riesgos consiste en reconocer y clasificar las amenazas potenciales, las vulnerabilidades y sus riesgos asociados. Este paso es crucial para determinar el riesgo de referencia y establecer una base para el análisis posterior.

Las siguientes etapas implican un análisis cualitativo y cuantitativo de los riesgos identificados. En el análisis cualitativo se describen la magnitud de las consecuencias potenciales, la probabilidad de que se produzcan y el nivel de riesgo global. El análisis cuantitativo, por su parte, consiste en asignar valores numéricos a estos elementos para proporcionar una evaluación más precisa.

A lo largo de este proceso, la metodología de evaluación de riesgos garantiza la consideración de diversos elementos, como la tolerancia al riesgo, las hipótesis, las limitaciones y la definición de medidas de control. La metodología también hace hincapié en la comunicación eficaz de los resultados a las distintas partes interesadas, adaptando la información a sus funciones y responsabilidades dentro de la organización. En última instancia, una metodología de evaluación de riesgos bien definida constituye la piedra angular de un sólido programa de gestión de riesgos, permitiendo a las organizaciones tomar decisiones informadas y asignar recursos de forma eficaz para mitigar y gestionar los riesgos.

8.1 Identificación de riesgos

8.1.1 *Establecer el contexto*

La municipalidad de Turrialba describe la relación entre la organización y su entorno, al tiempo que destaca las oportunidades, amenazas y áreas en las que la organización puede mejorar. El contexto de la municipalidad como función de la organización incluye todos los elementos financieros, operativos, competitivos, políticos, sociales, de clientes, culturales y legales. Identifique a las partes interesadas internas y externas, tenga en cuenta sus objetivos y perspectivas y establezca canales de comunicación con ellas.

Departamento de Tecnologías de Información,
e-mail: negamboa@muniturrialba.go.cr

8.1.2 Identificación de activos

La identificación de activos es un componente crucial de la gestión de riesgos, ya que garantiza que todos los recursos valiosos de una organización se identifiquen y categoricen adecuadamente. Para la municipalidad, un enfoque exhaustivo de identificación de activos implica varios pasos clave para garantizar un conocimiento exhaustivo de los activos en riesgo.

8.1.2.1 Creación de inventarios:

Elabore un inventario exhaustivo de todos los activos de la organización, tanto materiales como inmateriales. Los activos materiales pueden incluir hardware, software, instalaciones y equipos, mientras que los activos inmateriales pueden incluir propiedad intelectual, datos y reputación de marca.

Categoría	Descripción
Nombre del activo	El nombre del activo que se está evaluando.
Confidencialidad	El impacto que tendría una violación de la confidencialidad del activo. Esto podría incluir pérdidas financieras, daños a la reputación o responsabilidad legal, tomando valores bajos, medios y altos.
Integridad	El impacto que tendría una alteración de la integridad del activo. Esto podría incluir corrupción de datos, información inexacta o mal funcionamiento del sistema, tomando valores bajos, medios y altos.
Disponibilidad	El impacto que tendría una alteración de la disponibilidad del activo. Esto podría incluir la interrupción del negocio, pérdidas de productividad o insatisfacción del cliente, tomando valores bajos, medios y altos.

8.1.2.2 Categorización:

Categorizar los activos en función de su criticidad, valor y relevancia para las operaciones empresariales. Este paso ayuda a priorizar los activos para su posterior análisis y medidas de protección. La categorización se realiza a través de tres dimensiones fundamentales:

1. Confidencialidad:
    a. Impacto bajo: La violación provoca pérdidas financieras mínimas, un daño limitado a la reputación o una responsabilidad legal mínima.
    b. Impacto medio: La violación provoca pérdidas económicas moderadas, daños notables a la reputación o cierta responsabilidad legal.

Departamento de Tecnologías de Información,
e-mail: negamboa@muniturrialba.go.cr

c. Impacto alto: La brecha causa pérdidas financieras significativas, daño reputacional severo, o responsabilidad legal sustancial.

2. Integridad:

   a. Impacto bajo: La alteración da lugar a una corrupción menor de los datos, inexactitudes limitadas o disfunciones mínimas del sistema.

   b. Impacto medio: La alteración provoca una corrupción moderada de los datos, inexactitudes notables o algunos fallos del sistema.

   c. Impacto alto: La alteración provoca una corrupción sustancial de los datos, inexactitudes críticas o graves disfunciones del sistema.

3. Disponibilidad:

   a. Impacto bajo: La alteración provoca una interrupción menor del negocio, pérdidas limitadas de productividad o una insatisfacción mínima de los clientes.

   b. Impacto medio: La perturbación provoca una interrupción moderada del negocio, pérdidas notables de productividad o cierta insatisfacción de los clientes.

   c. Impacto alto: La perturbación provoca una interrupción significativa de la actividad, pérdidas sustanciales de productividad o una grave insatisfacción de los clientes.

8.2 Clasificación del riesgo

8.2.1 Amenazas Humanas:

Amenazas Internas:

- Divulgación no autorizada de información sensible por parte de un empleado descontento.
- Sabotaje intencionado de sistemas críticos por un interno con acceso privilegiado.
- Manejo negligente de datos confidenciales que lleva a filtraciones accidentales.
- Modificación no autorizada de configuraciones del sistema por parte de un interno.
- Ataques de ingeniería social que explotan la confianza de los empleados para acceder sin autorización.
- Robo de propiedad intelectual por parte de un empleado que planea unirse a un competidor.

Departamento de Tecnologías de Información,
e-mail: negamboa@muniturrialba.go.cr

Actores de Amenaza Externos:

- Cibercriminales que intentan infiltrarse en la red de la organización para robar datos.
- Actores de estados-nación que participan en ciber espionaje para obtener ventajas políticas o económicas.
- Grupos activistas que lanzan ataques de denegación de servicio distribuido (DDoS).
- Competidores que realizan espionaje industrial para obtener una ventaja competitiva.
- Crimen organizado que apunta a activos financieros a través de ataques cibernéticos.
- Individuos externos que buscan acceso no autorizado para explotar vulnerabilidades.

8.2.2 Amenazas Tecnológicas:

Malware:

- Propagación de ransomware que tiene como objetivo cifrar archivos críticos para extorsión.
- Caballos de Troya que infiltrarse en sistemas para proporcionar acceso no autorizado.
- Distribución de spyware para vigilancia no autorizada y recolección de datos.
- Adware que afecta la experiencia del usuario al mostrar anuncios no deseados.
- Gusanos que explotan vulnerabilidades de red para replicarse automáticamente.
- Registradores de teclas sigilosos que capturan información sensible ingresada por los usuarios.

Phishing e Ingeniería Social:

- Correos electrónicos de phishing que engañan a los empleados para que revelen credenciales de inicio de sesión.
- Ataques de suplantación de identidad dirigidos a ejecutivos para autorizar transacciones fraudulentas.
- Pretexting para manipular a los empleados para que proporcionen información confidencial.
- Ataques de cebo utilizando ofertas atractivas para atraer a individuos a realizar acciones maliciosas.
- Cuestionarios o encuestas que recopilan información para ataques de ingeniería social.
- Campañas de spear-phishing personalizadas para individuos específicos dentro de la organización.

Acceso No Autorizado:

- Ataques de fuerza bruta que intentan obtener acceso no autorizado a cuentas de usuario.
- Explotación de vulnerabilidades de software sin parches para acceder al sistema.

Departamento de Tecnologías de Información,
e-mail: negamboa@muniturrialba.go.cr

- Ataques de credential stuffing que aprovechan credenciales de inicio de sesión comprometidas.
- Amenazas internas que abusan de sus privilegios de acceso para realizar acciones no autorizadas.
- Ataques de acceso remoto que apuntan a mecanismos de autenticación débiles.
- Robo físico de dispositivos que conduce a acceso no autorizado a datos almacenados.

8.2.3 Riesgos Ambientales:

Desastres Naturales:

- Terremotos que causan daños físicos a la infraestructura y a los centros de datos.
- Inundaciones que provocan daños por agua y destrucción de equipos electrónicos.
- Incendios que amenazan la continuidad de las operaciones y la pérdida de datos.
- Tormentas que causan cortes de energía e interrupciones en la infraestructura de TI.
- Deslizamientos de tierra que afectan la accesibilidad y seguridad de las instalaciones.
- Tornados que representan riesgos para los activos físicos y la estabilidad operativa.

Desastres Causados por el Hombre:

- Sabotaje o vandalismo dirigidos a componentes críticos de infraestructura.
- Derrames o filtraciones accidentales de materiales peligrosos que impactan el medio ambiente.
- Fallos en la red eléctrica debido a acciones intencionales o no intencionales.
- Accidentes industriales que causan interrupciones y riesgos para la seguridad.
- Ataques ciberfísicos que afectan la funcionalidad de la tecnología operativa.
- Ataques físicos a instalaciones, como bombardeos o intrusiones armadas.

8.2.4 Riesgos Operativos:

Fallos Tecnológicos:

- Fallos de hardware que interrumpen la disponibilidad de sistemas críticos.
- Errores o fallos de software que causan malfuncionamientos en aplicaciones operativas.
- Cortes de red que afectan la comunicación y la transferencia de datos.
- Cortes de energía que conducen al apagado de la infraestructura de TI.
- Corrupción de datos debido a fallos en dispositivos de almacenamiento.

Departamento de Tecnologías de Información,
e-mail: negamboa@muniturrialba.go.cr

- Fallo de sistemas de respaldo durante periodos críticos.

Filtraciones de Datos:

- Acceso no autorizado a bases de datos de clientes que resulta en la exposición de información personal.
- Filtraciones internas de información confidencial a entidades externas.
- Ciberataques que conducen al robo de documentos comerciales sensibles.
- Filtraciones de terceros que exponen datos compartidos y credenciales.
- Ataques de phishing que llevan a la comprometida de credenciales de inicio de sesión de empleados.
- Cifrado de datos inadecuado que resulta en el acceso no autorizado a registros confidenciales.

8.2.5 Riesgos Regulatorios y de Cumplimiento:

Violaciones Legales y Regulatorias:

- Incumplimiento de regulaciones de protección de datos que conlleva consecuencias legales.
- Violaciones de estándares de cumplimiento específicos de la industria que impactan las operaciones.
- Falta de adherencia a regulaciones de ciberseguridad que resultan en sanciones.
- Infracción de regulaciones de privacidad que afecta la confianza del cliente.
- Incumplimiento de requisitos de informes financieros que lleva a acciones legales.
- Falta de implementación de controles necesarios exigidos por organismos reguladores.

8.2.6 Riesgos Sociales y Políticas:

Activismo:

- Ciberataques llevados a cabo por grupos activistas por razones ideológicas.
- Protestas o interrupciones organizadas por activistas que impactan las operaciones comerciales.
- Boicots iniciados por grupos sociales o políticos que afectan la reputación de la marca.
- Campañas en línea dirigidas a organizaciones por supuestas violaciones éticas.
- Movimientos en redes sociales liderados por activistas que influyen en la percepción pública.
- Crisis de relaciones públicas derivadas de conflictos con grupos activistas.

Departamento de Tecnologías de Información,
e-mail: negamboa@muniturrialba.go.cr

Ciber espionaje:

- Ciber espionaje patrocinado por naciones dirigido a tecnologías propietarias.
- Ciberataques para obtener información sobre las estrategias de competidores.
- Infiltración de sistemas de infraestructura crítica para obtener ventaja estratégica.
- Hacking patrocinado por el estado que impacta las relaciones diplomáticas.
- Robo de propiedad intelectual para fines económicos o militares.
- Vigilancia encubierta de actividades organizacionales por entidades extranjeras.

8.2.7 Riesgos Emergentes:

Avances Tecnológicos:

- Riesgos asociados con la adopción de tecnologías emergentes como la inteligencia artificial.
- Desafíos de ciberseguridad planteados por la integración de dispositivos IoT.
- Vulnerabilidades en aplicaciones de software recién desarrolladas.
- Amenazas derivadas del uso de tecnología blockchain.
- Riesgos asociados con los avances en computación cuántica.
- Implicaciones de seguridad de los desarrollos en biotecnología.

Eventos Globales:

- Pandemias que interrumpen la continuidad de la fuerza laboral y las cadenas de suministro.
- Cambios geopolíticos que afectan las operaciones comerciales internacionales.
- Recesiones económicas que impactan la estabilidad financiera.
- Eventos relacionados con el cambio climático que afectan las operaciones regionales.
- Cambios regulatorios influenciados por eventos globales.
- Amenazas cibernéticas influenciadas por las relaciones internacionales.

Departamento de Tecnologías de Información,
e-mail: negamboa@muniturrialba.go.cr

8.2.8 Amenazas a la Cadena de Suministro:

Riesgos de Terceros:

- Vulnerabilidades de seguridad en software de terceros que impactan la seguridad general del sistema.

8.3 Criterios para realizar evaluaciones de riesgos

La ISO 27005, especifican que los criterios de evaluación de riesgos se determinan en términos de sus consecuencias, probabilidad y nivel de riesgo. Los criterios de consecuencia deben desarrollarse y especificarse en términos del alcance del daño o pérdida, o del perjuicio para una organización o individuo resultante de la pérdida de confidencialidad, integridad y disponibilidad de la información. Para determinar el nivel de consecuencia se sigue la siguiente escala cualitativa:

Consecuencias	Valor semi cuantitativo	Descripción
5 - Catastrófico	96-100	Consecuencias regulatorias o sectoriales más allá de la organización. Ecosistema(s) sectorial(es) sustancialmente impactado(s), con consecuencias que pueden ser duraderas. Y/o: dificultad para el Estado, e incluso una incapacidad para asegurar una función reguladora o una de sus misiones de vital importancia. Y/o: consecuencias críticas en la seguridad de las personas y la propiedad (crisis sanitaria, contaminación ambiental, destrucción de infraestructuras esenciales, etc.).
4 - Crítico	80-95	Consecuencias desastrosas para la organización. Incapacidad de la organización para asegurar todo o parte de su actividad, con posibles consecuencias graves en la seguridad de las personas y la propiedad. Es poco probable que la organización supere la situación (su supervivencia está amenazada), los sectores de actividad o los sectores del Estado en los que opera probablemente se verán ligeramente afectados, sin consecuencias duraderas.
3 - Serio	21-79	Consecuencias sustanciales para la organización. Alta degradación en el desempeño de la actividad, con posibles consecuencias significativas en la seguridad de las personas y la propiedad. La organización superará la situación con serias dificultades (operación en modo altamente degradado), sin impacto en el sector o en el Estado.

Departamento de Tecnologías de Información,
e-mail: negamboa@muniturrialba.go.cr

Consecuencias	Valor semi cuantitativo	Descripción
2 - Significativo	5-20	Consecuencias significativas pero limitadas para la organización. Degradación en el desempeño de la actividad sin consecuencias en la seguridad de las personas y la propiedad. La organización superará la situación a pesar de algunas dificultades (operación en modo degradado).
1 - Menor	0-4	Consecuencias insignificantes para la organización. Sin consecuencias en las operaciones o el desempeño de la actividad o en la seguridad de las personas y la propiedad. La organización superará la situación sin muchas dificultades (se consumirán los márgenes).

La probabilidad de un riesgo se determina a partir de:

- La utilización de información proveniente de incidentes anteriores, estadísticas del sector y mejores prácticas de la industria.
- Consulta de informes de inteligencia de amenazas, bases de datos de vulnerabilidades y estudios de casos relevantes.
- Aplicación del conocimiento y la experiencia de los miembros del equipo de gestión de riesgos para complementar los datos objetivos.

La probabilidad de un riesgo no es un valor estático, sino que puede variar en el tiempo debido a cambios en el entorno de la organización, la aparición de nuevas amenazas o la implementación de nuevas medidas de seguridad. Para determinar la probabilidad se sigue la siguiente escala cualitativa de probabilidad:

Probabilidad	Valor semi cuantitativo	Descripción
5 - Casi seguro	96%-100%	La fuente de riesgo casi con certeza alcanzará su objetivo utilizando uno de los métodos de ataque considerados. La probabilidad del escenario de riesgo es muy alta.
4 - Muy probable	80%-95%	La fuente de riesgo probablemente alcanzará su objetivo utilizando uno de los métodos de ataque considerados. La probabilidad del escenario de riesgo es alta.
3 - Probable	21%-79%	La fuente de riesgo es capaz de alcanzar su objetivo utilizando uno de los métodos de ataque considerados. La probabilidad del escenario de riesgo es significativa.

Departamento de Tecnologías de Información,
e-mail: negamboa@muniturrialba.go.cr

Probabilidad	Valor semi cuantitativo	Descripción
2 - Poco probable	5%-20%	La fuente de riesgo tiene relativamente pocas posibilidades de alcanzar su objetivo utilizando uno de los métodos de ataque considerados. La probabilidad es baja.
1 - Improbable	0%-4%	La fuente de riesgo tiene muy pocas posibilidades de alcanzar su objetivo utilizando uno de los métodos de ataque considerados. La probabilidad es muy baja.

El propósito de las escalas para el nivel de riesgo es ayudar a los propietarios del riesgo a decidir sobre la retención o el tratamiento de los riesgos y a priorizarlos para su tratamiento. La municipalidad debe elaborar una clasificación de los riesgos teniendo en cuenta lo siguiente:

- Los criterios de consecuencia y probabilidad;
- Las consecuencias que los eventos de seguridad de la información pueden tener a nivel estratégico, táctico y operativo (esto puede definirse como el peor de los casos o, en otros términos, siempre que se utilice la misma base de forma coherente);
- Requisitos legales y reglamentarios, y obligaciones contractuales;
- Los riesgos que aparecen más allá de los límites del ámbito de la organización, incluidos los efectos imprevistos sobre terceros.

8.4 Determinar el Riesgo

La municipalidad evalúa los riesgos de eventos de amenazas como una combinación de probabilidad e impacto. El nivel de riesgo asociado con los eventos de amenaza identificados representa una determinación del grado en que la municipalidad está amenazada por tales eventos. Las organizaciones hacen explícita la incertidumbre en las determinaciones de riesgo, incluyendo, por ejemplo, las suposiciones organizacionales y los juicios/decisiones subjetivas. Las organizaciones pueden ordenar la lista de eventos de amenaza de interés según el nivel de riesgo determinado durante la evaluación de riesgos, prestando mayor atención a los eventos de alto riesgo.

Departamento de Tecnologías de Información,
e-mail: negamboa@munituralba.go.cr

El nivel de riesgo se mapea en el siguiente mapa de calor:

Probabilidad	Consecuencia				
	Catastrófico	Crítico	Serio	Significativo	Menor
Casi seguro	Muy alto	Muy alto	Alto	Alto	Medio
Muy probable	Muy alto	Alto	Alto	Medio	Bajo
Probable	Alto	Alto	Medio	Bajo	Bajo
Poco probable	Medio	Medio	Bajo	Bajo	Muy bajo
Improbable	Bajo	Bajo	Bajo	Muy bajo	Muy bajo

8.5 Tratamiento de riesgos

El tratamiento de riesgos implica la identificación de la gama de opciones para hacer frente a los riesgos, la evaluación de dichas opciones, la preparación de planes de tratamiento de riesgos y su aplicación. Con el fin de controlar los riesgos identificados en el proyecto, se han establecido las siguientes medidas para tratarlos adecuadamente.

8.5.1 Reducción de riesgos

- Aplicación de medidas para disminuir el riesgo global para los activos.
- Selección de contramedidas, como controles técnicos o cambios en el entorno, para reducir la probabilidad o gravedad de las pérdidas potenciales.
- Evaluación de la solidez del control, teniendo en cuenta si los controles son preventivos o detectivos.

8.5.2 Riesgo compartido / Transferencia

- Compartir el riesgo con terceros a través de seguros o proveedores de servicios.
- El seguro sirve como mecanismo compensatorio tras el suceso, reduciendo la carga de la pérdida.
- La transferencia implica trasladar la responsabilidad del riesgo y los costes a los proveedores de servicios, como los proveedores de almacenamiento seguro.

8.5.3 Evitar el riesgo

- Eliminar el riesgo absteniéndose de realizar actividades que expongan a la organización a amenazas potenciales o interrumpiéndolas.
    - Por ejemplo, interrumpir un proceso de negocio para evitar la exposición al riesgo.

Departamento de Tecnologías de Información,
e-mail: pezamboa@muniturrialba.go.cr

8.5.4 Aceptación del riesgo

- Elección de aceptar un riesgo específico dentro de los parámetros de tolerancia de la organización.
- Aceptar, asumir el coste cuando el riesgo se materializa.
- Esta estrategia es viable cuando el coste a largo plazo de asegurarse contra el riesgo supera las pérdidas potenciales totales.

8.6 Riesgo compartido Transferencia

La distribución y la transferencia de riesgos son componentes esenciales de la estrategia de gestión de riesgos de la municipalidad. Estos enfoques implican distribuir o trasladar la carga del riesgo a entidades externas, garantizando que la organización esté mejor preparada para hacer frente a posibles acontecimientos adversos.

8.6.1 Participación de proveedores de servicios:

La organización se compromete con proveedores de servicios externos para compartir o transferir determinados riesgos.

Por ejemplo, la municipalidad puede recurrir a proveedores de servicios seguros para los cobros tributarios, trasladando la responsabilidad y los costes asociados al proveedor de servicios.

8.6.2 Gestión de riesgos rentable:

Al compartir o transferir riesgos, la municipalidad garantiza un enfoque rentable de la gestión de riesgos. Esto permite a la organización centrarse en sus competencias básicas mientras confía en la experiencia y los recursos externos para la mitigación de riesgos especializados.

8.6.3 Mitigación del impacto financiero:

Las estrategias de distribución y transferencia de riesgos tienen como objetivo mitigar el impacto financiero de posibles incidentes en la municipalidad. Este enfoque proactivo contribuye a la resistencia general de la organización frente a retos imprevistos.

9 Revisión y Mejora Continua

La política debe revisarse anualmente o después de cualquier incidente significativo de TI.

Realizar auditorías periódicas para evaluar la efectividad de las prácticas y ajustarlas conforme sea necesario.

Departamento de Tecnologías de Información,
e-mail: negamboa@muniturrialba.go.cr

10 Cumplimiento y Auditoría

La organización deberá establecer y mantener un programa integral de auditorías internas y externas con el propósito de garantizar el cumplimiento de esta política de gestión de riesgos de TI, así como de las normativas y regulaciones nacionales aplicables, tales como la Norma Técnica para la Gestión de TI emitida por el MICITT. Este programa de auditoría deberá incluir:

Auditorías Internas: Evaluaciones periódicas realizadas por personal interno capacitado o por equipos independientes dentro de la organización, con el objetivo de verificar la adherencia a los procedimientos establecidos en la política y la correcta implementación de las medidas de control. Las auditorías internas deben realizarse al menos una vez al año y cuando haya cambios significativos en el entorno de riesgo.

Auditorías Externas: Evaluaciones realizadas por auditores independientes externos para asegurar la objetividad y transparencia en la verificación del cumplimiento de las normativas nacionales, así como de los estándares internacionales aplicables. Estas auditorías deberán realizarse conforme a las exigencias de los reguladores y siempre que se considere necesario para asegurar la mejora continua de los procesos de gestión de riesgos.

Los resultados de estas auditorías deberán ser documentados y presentados a la alta dirección y a las partes interesadas relevantes, asegurando la implementación de las acciones correctivas necesarias para mantener la conformidad con los requisitos establecidos y mejorar continuamente la eficacia del programa de gestión de riesgos de TI.

11 Documentos relacionados

Esta política se complementa con los siguientes documentos:

- Procedimiento de Gestión de Riesgos de TI: El objetivo de los procedimientos de gestión de riesgos de tecnología de la información es presentar de manera clara y coherente las actividades y pasos a seguir para implementar y cumplir con los elementos clave de la política de gestión de riesgos de TI.

Departamento de Tecnologías de Información,
e-mail: negamboa@muniturrialba.go.cr

12 Referencias

Asociación Española de Normalización. (2018). *UNE-ISO 31000 Gestión del riesgo Directrices*. www.iso.org/patents.

Asociación Española de Normalización. (2024). *Seguridad de la información, ciberseguridad y protección de la privacidad. Guía para la gestión de los riesgos de seguridad de la información (ISO/IEC 27005:2022) (Ratificada por la Asociación Española de Normalización en septiembre de 2024.)*. www.une.org

Axelos. (2019). *ITIL ® Foundation ITIL 4 Edition 2*. https://www.axelos.com

Gamboa Calderón, N. E. (2022). *Políticas de Seguridad en Materia de Tecnologías de Información y Comunicación TICS*.

ISACA. (2018). *Marco de Referencia COBIT® 2019: Objetivos de gobierno y gestión*. http://linkd.in/ISACAOfficial

National Institute of Standards and Technology. (2012). *NIST 800-30: Guide for Conducting Risk Assessments*. https://doi.org/10.6028/NIST.SP.800-30r1

Solís García, S., Montillano Vivas, M., Chinchilla Sáenz, S., Tenorio Chacón, O., Badilla Picado, I., & Lemaitre Picado, R. (2021). *Normas técnicas para la gestión y el control de las Tecnologías de Información*.

Departamento de Tecnologías de Información,
e-mail: negamboa@muniturrialba.go.cr

9.19 Apéndice S Procedimientos para la gestión de Riesgos de TI

DEPARTAMENTO DE TECNOLOGÍAS DE INFORMACIÓN

Municipalidad de Turrialba
Departamento de Tecnologías de Información

Procedimientos para la Gestión Tecnologías de Información

Turrialba, Cartago, octubre 2024

Número de Páginas 1 - 24

Departamento de Tecnologías de Información,
e-mail: nezamboa@muniturrialba.go.cr

DEPARTAMENTO DE TECNOLOGÍAS DE INFORMACIÓN

ELABORADO POR:	SUPERVISADO POR:	REVISADO POR:	APROBADO POR:
Sr. Pablo Alonso Chaves Rivera	Ing. Nelson Eduardo Gamboa Calderón	M.S.c. Carlos Eduardo Hidalgo Flores,	M.S.c. Carlos Eduardo Hidalgo Flores
	Departamento de Tecnologías de Información	Alcalde Municipal	Alcalde Municipal

REVISIÓN	FECHA	RESUMEN DE LA REVISIÓN

ELABORADO POR:

FECHA dd/mm/aaaa

APROBADO POR:

FECHA dd/mm/aaaa

Número de Páginas 2 - 24

Departamento de Tecnologías de Información,
e-mail: negamboa@muniturrialba.go.cr

DEPARTAMENTO DE TECNOLOGÍAS DE INFORMACIÓN

1 Objetivo

El objetivo de los procedimientos de gestión de riesgos de tecnología de la información es presentar de manera clara y coherente las actividades y pasos a seguir para implementar y cumplir con los elementos clave de la política de gestión de riesgos de TI. Estos procedimientos están diseñados para ser conocidos y aplicados por la Gerencia Municipal (Alcalde y Concejo Municipal), Directores, Jefes de Departamento, colaboradores en general, funcionarios contratistas y terceros que presten servicios o tengan alguna relación con el Departamento de Tecnologías de Información de la Municipalidad de Turrialba. El propósito es asegurar que todas las partes involucradas contribuyan de manera efectiva a la mitigación de riesgos y la seguridad de la información.

2 Alcance

Los procedimientos de gestión de riesgos de tecnología de información son aplicables a todas las actividades administrativas, operativas y de control que deben ser cumplidas por la Gerencia Municipal (Alcalde y Concejo Municipal), Directores, Jefes de Departamento, colaboradores en general, funcionarios contratistas y terceros que presten servicios o tengan algún tipo de relación con el Departamento de Tecnologías de Información de la Municipalidad de Turrialba. Estos procedimientos tienen como objetivo garantizar un adecuado nivel de protección de la calidad y seguridad de la información en toda la municipalidad. Los usuarios están obligados a cumplir con estos procedimientos, contribuyendo activamente en la identificación de riesgos, la toma de medidas preventivas y correctivas, y el mantenimiento de la seguridad integral de los activos de TI.

Departamento de Tecnologías de Información,
e-mail: negamboa@muniturrialba.go.cr

3 Términos y Definiciones

Aceptación del riesgo: Decisión informada de asumir un determinado riesgo.

Amenaza: Cualquier circunstancia o evento con el potencial de impactar negativamente las operaciones organizacionales mediante acceso no autorizado, destrucción, divulgación o modificación de la información y/o denegación de servicio.

Análisis de riesgos: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

Apetito de riesgo: Cantidad y tipo de riesgo que una organización está dispuesta a perseguir o retener.

Ataque: Cualquier tipo de actividad maliciosa que intente recolectar, interrumpir, negar, degradar o destruir los recursos del sistema de información o la propia información.

Autenticación: Verificar la identidad de un usuario, proceso o dispositivo, a menudo como requisito previo para permitir el acceso a los recursos en un sistema de información.

Autenticidad: La propiedad de ser genuino y poder ser verificado y confiable; confianza en la validez de una transmisión, un mensaje o el origen de un mensaje.

Autorización: La decisión de gestión oficial otorgada por un funcionario organizacional superior para autorizar la operación de un sistema de información y aceptar explícitamente el riesgo para las operaciones organizacionales (incluyendo misión, funciones, imagen o reputación), activos organizacionales, individuos, otras organizaciones y la Nación.

Comunicación y consulta de riesgos: Conjunto de procesos continuos e iterativos que una organización lleva a cabo para proporcionar, compartir u obtener información, y para entablar un diálogo con las partes interesadas en relación con la gestión de riesgos.

Confidencialidad: Preservar las restricciones autorizadas sobre el acceso y la divulgación de información, incluyendo medios para proteger la privacidad personal e información propietaria.

Consecuencia: Resultado de un acontecimiento que afecta a los objetivos.

Contexto externo: Entorno externo en el que la organización pretende alcanzar sus objetivos. El contexto externo puede incluir el entorno social, cultural, político, jurídico, normativo, financiero, tecnológico, económico, geológico, ya sea internacional, nacional, regional o local, los principales impulsores y tendencias que afectan a los objetivos de la organización, las relaciones, percepciones, valores, necesidades y expectativas de las partes interesadas externas, las relaciones y compromisos contractuales y la complejidad de las redes y dependencias.

Contexto interno: Entorno interno en el que la organización trata de alcanzar sus objetivos.

Departamento de Tecnologías de Información,
e-mail: negamboa@muniturrialba.go.cr

Criterios de riesgo: Términos de referencia con los que se evalúa la importancia de un riesgo.

Criticidad: Una medida del grado en que una organización depende de la información o del sistema de información para el éxito de una misión o función comercial.

Disponibilidad: Asegurar el acceso oportuno y confiable a la información y su uso.

Enfoque de Evaluación: El enfoque utilizado para evaluar el riesgo y sus factores de contribución, incluyendo cuantitativa, cualitativa o semi-cuantitativamente.

Entorno de Operación: El entorno físico, técnico y organizacional en el que opera un sistema de información, que incluye, pero no se limita a varios factores que influyen en la seguridad y el riesgo del sistema.

Escenario de riesgo: Secuencia o combinación de acontecimientos que conducen de la causa inicial a la consecuencia no deseada.

Evaluación de Amenaza: Proceso de evaluación formal del grado de amenaza a un sistema de información o empresa y descripción de la naturaleza de la amenaza.

Evaluación de Vulnerabilidad: Examen sistemático de un sistema de información o producto para determinar la adecuación de las medidas de seguridad, identificar deficiencias de seguridad y predecir la efectividad de las medidas propuestas.

Evaluación del riesgo: Proceso de comparación de los resultados del análisis del riesgo con los criterios de riesgo para determinar si el riesgo y/o su importancia son aceptables o tolerables.

Evento: Ocurrencia o cambio de un conjunto particular de circunstancias.

Fuente de riesgo: Elemento que por sí solo o en combinación tiene el potencial de dar lugar a un riesgo.

Identificación de riesgos: Proceso de búsqueda, reconocimiento y descripción de riesgos.

Incidente de seguridad de la información: Suceso único o serie de sucesos de seguridad de la información no deseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones de la empresa y amenazar la seguridad de la información.

Información: Cualquier comunicación o representación de conocimientos tales como hechos, datos u opiniones en cualquier medio o forma, incluyendo textual, numérico, gráfico, cartográfico, narrativo o audiovisual.

Integridad: Protección contra la modificación o destrucción indebida de la información e incluye asegurar la no repudio y autenticidad de la información.

Nivel de riesgo: Importancia de un riesgo, expresada en términos de la combinación de consecuencias y su probabilidad.

Propietario del riesgo: Persona o entidad con responsabilidad y autoridad para gestionar un riesgo.

Departamento de Tecnologías de Información,
e-mail: negamboa@muniturrialba.go.cr

Retención del riesgo: Aceptación temporal del beneficio potencial de ganancia, o de la carga de pérdida, de un riesgo concreto.

Riesgo compartido: Forma de tratamiento del riesgo que implica la distribución acordada del riesgo con otras partes.

Riesgo de Seguridad de la Información: El riesgo para las operaciones organizacionales, activos, individuos, otras organizaciones y la Nación debido a la posibilidad de acceso, uso, divulgación, interrupción, modificación o destrucción no autorizados de información y/o sistemas de información.

Riesgo residual: Riesgo que permanece tras el tratamiento del riesgo.

Riesgo: Efecto de la incertidumbre sobre los objetivos.

Seguridad de la Información: La protección de la información y los sistemas de información contra el acceso, uso, divulgación, interrupción, modificación o destrucción no autorizados para proporcionar confidencialidad, integridad y disponibilidad.

Sistema de Información: Un conjunto discreto de recursos de información organizados para la recolección, procesamiento, mantenimiento, uso, intercambio, difusión o disposición de información.

Tecnología de la Información: Cualquier equipo o sistema interconectado o subsistema de equipos utilizado en la adquisición automática, almacenamiento, manipulación, gestión, movimiento, control, visualización, transmisión o recepción de datos o información.

Tratamiento del riesgo: Proceso para modificar el riesgo.

Vulnerabilidad: Debilidad en un sistema de información, procedimientos de seguridad del sistema, controles internos o implementación que podría ser explotada por una fuente de amenaza.

Departamento de Tecnologías de Información,
e-mail: negamboa@muniturrialba.go.cr

4 Proceso

Perfil del Proceso	
Elemento	**Descripción**
1. Objetivo y Metas	**Objetivo del Proceso:** Identificar, evaluar y reducir continuamente los riesgos relacionados con I&T dentro de los niveles de tolerancia establecidos por la gerencia ejecutiva de la empresa.
	Metas Específicas: - Gestión de riesgo de negocio - Continuidad y disponibilidad del servicio de negocio. - Gestión de riesgo relacionado con TI - Seguridad de la información, infraestructura de procesamiento y aplicaciones, y privacidad
2. Propiedad del Proceso	**Propietario del Proceso:** Encargado del Departamento de Tecnologías de Información.
3. Secuencia de Actividades	Se establecen los subprocesos de: - Valoración de riesgos de TI. - Especificación de requisitos para proyectos de mitigación - Inventario de procesos de negocio y dependencias - Preparación y prueba de planes de respuesta a incidentes - Aplicación de los planes de respuesta
4. Roles y Responsabilidades	Ejecutivo de Riesgos (ER): Supervisa todo el proceso de gestión de riesgos, garantizando la alineación con las metas y objetivos de la municipalidad. Propietario del riesgo (RO): Responsable de un riesgo específico y facultado para tomar decisiones en relación con ese riesgo; pueden ser jefes de departamento, gestores de proyectos o propietarios de sistemas. Analista de riesgos (AR): Realiza evaluaciones de riesgos, incluyendo la identificación, el análisis y la evaluación de los riesgos, proporcionando los datos necesarios para la toma de decisiones.

Departamento de Tecnologías de Información,
e-mail: negamboa@muniturrialba.go.cr

DEPARTAMENTO DE TECNOLOGÍAS DE INFORMACIÓN

Perfil del Proceso	
5. Indicadores de Desempeño	• Porcentaje de objetivos y servicios críticos del negocio, cubiertos por la evaluación de riesgos • Número de interrupciones del servicio al cliente o procesos empresariales que han causado incidentes significativos • Coste de incidentes para el negocio • Número de incidentes significativos relacionados con TI que no se identificaron en la evaluación de riesgos • Número de incidentes de confidencialidad que causan pérdidas financieras, interrupción del negocio o descrédito público • Número de incidentes de disponibilidad que causan pérdidas financieras, interrupción del negocio o descrédito público • Número de incidentes de integridad que causan pérdidas financieras, interrupción del negocio o descrédito público

4.1 Valoración de riesgos de TI.

Este procedimiento detalla las actividades necesarias para la recolección, clasificación, análisis y registro de datos relacionados con los riesgos de TI dentro de la municipalidad. Se asegura la consistencia en la gestión de riesgos y se ajusta a los cambios en el entorno operativo y normativo.

,

1. Identificación Riesgos:

   a. Identificación de activos críticos: Realizar un inventario exhaustivo de los activos tecnológicos, clasificándolos según su importancia para la continuidad del negocio. Los activos deben categorizarse en función de su criticidad, valor y relevancia para las operaciones, en las dimensiones de Confidencialidad, Integridad y Disponibilidad.

   b. Identificación de amenazas y vulnerabilidades: Listar las amenazas potenciales y las vulnerabilidades asociadas a cada activo crítico.

   c. Identificación de eventos de riesgo: Registrar cualquier incidente de seguridad, vulnerabilidad detectada, problema operativo o evento que afecte la continuidad del negocio o la seguridad de los sistemas.

   d. Identificación de procesos de Negocios: Se debe crear y mantener un inventario detallado y actualizado de los procesos de negocio de la municipalidad, identificando la dependencia de cada uno con los servicios de TI y la infraestructura tecnológica. El inventario debe incluir personal clave, infraestructuras críticas, aplicaciones, proveedores y terceros que sean esenciales para el funcionamiento del negocio.

Departamento de Tecnologías de Información,
e-mail: negamboa@muniturrialba.go.cr

e. Registro del riesgo: Registrar los eventos con el código E00, indicando el nombre del evento, sus causas, el impacto, las medidas correctivas a adoptar, las recomendaciones para prevenir incidentes y el estado del evento (registrado, en proceso o solucionado).

2. Clasificación de los riesgos: Clasificar los riesgos identificados en categorías como Amenazas Humanas, Amenazas Tecnológicas, Riesgos Ambientales, Riesgos Operativos, Riesgos Regulatorios y de Cumplimiento, Riesgos Sociales y Políticos, Riesgos Emergentes y Amenazas a la Cadena de Suministro.

3. Evaluación del riesgo:

   a. Determinación de la probabilidad: Utilizar datos históricos, informes de incidentes y el conocimiento del equipo para estimar la probabilidad de que un riesgo ocurra.

Probabilidad	Valor semi cuantitativo	Descripción
5 - Casi seguro	96%-100%	La fuente de riesgo casi con certeza alcanzará su objetivo utilizando uno de los métodos de ataque considerados. La probabilidad del escenario de riesgo es muy alta.
4 - Muy probable	80%-95%	La fuente de riesgo probablemente alcanzará su objetivo utilizando uno de los métodos de ataque considerados. La probabilidad del escenario de riesgo es alta.
3 – Probable	21%-79%	La fuente de riesgo es capaz de alcanzar su objetivo utilizando uno de los métodos de ataque considerados. La probabilidad del escenario de riesgo es significativa.
2 - Poco probable	5%-20%	La fuente de riesgo tiene relativamente pocas posibilidades de alcanzar su objetivo utilizando uno de los métodos de ataque considerados. La probabilidad es baja.
1 - Improbable	0%-4%	La fuente de riesgo tiene muy pocas posibilidades de alcanzar su objetivo utilizando uno de los métodos de ataque considerados. La probabilidad es muy baja.

   b. Evaluación del impacto: Estimar las pérdidas potenciales en términos financieros, operacionales y reputacionales para cada activo en riesgo

Departamento de Tecnologías de Información,
e-mail: negamboa@muniturrialba.go.cr

DEPARTAMENTO DE TECNOLOGÍAS DE INFORMACIÓN

Consecuencias	Valor semi cuantitativo	Descripción
5 - Catastrófico	96-100	Consecuencias regulatorias o sectoriales más allá de la municipalidad. Ecosistema(s) sectorial(es) sustancialmente impactado(s), con consecuencias que pueden ser duraderas. Y/o: dificultad para el Estado, e incluso una incapacidad para asegurar una función reguladora o una de sus misiones de vital importancia. Y/o: consecuencias críticas en la seguridad de las personas y la propiedad (crisis sanitaria, contaminación ambiental, destrucción de infraestructuras esenciales, etc.).
4 – Crítico	80-95	Consecuencias desastrosas para la municipalidad. Incapacidad de la municipalidad para asegurar todo o parte de su actividad, con posibles consecuencias graves en la seguridad de las personas y la propiedad. Es poco probable que la municipalidad supere la situación (su supervivencia está amenazada), los sectores de actividad o los sectores del Estado en los que opera probablemente se verán ligeramente afectados, sin consecuencias duraderas.
3 – Serio	21-79	Consecuencias sustanciales para la municipalidad. Alta degradación en el desempeño de la actividad, con posibles consecuencias significativas en la seguridad de las personas y la propiedad. La municipalidad superará la situación con serias dificultades (operación en modo altamente degradado), sin impacto en el sector o en el Estado.
2 - Significativo	5-20	Consecuencias significativas pero limitadas para la municipalidad. Degradación en el desempeño de la actividad sin consecuencias en la seguridad de las personas y la propiedad. La municipalidad superará la situación a pesar de algunas dificultades (operación en modo degradado).
1 – Menor	0-4	Consecuencias insignificantes para la municipalidad. Sin consecuencias en las operaciones o el desempeño de la actividad o en la seguridad de las personas y la propiedad. La municipalidad superará la situación sin muchas dificultades (se consumirán los márgenes).

4. Determinar el riesgo: Determinar el nivel de riesgo combinando probabilidad e impacto, destacando aquellos riesgos que requieren atención inmediata.

Departamento de Tecnologías de Información,
e-mail: negamboa@muniturrialba.go.cr

DEPARTAMENTO DE TECNOLOGÍAS DE INFORMACIÓN

Probabilidad	Consecuencia				
	Catastrófico	Crítico	Serio	Significativo	Menor
Casi seguro	Muy alto	Muy alto	Alto	Alto	Medio
Muy probable	Muy alto	Alto	Alto	Medio	Bajo
Probable	Alto	Alto	Medio	Bajo	Bajo
Poco probable	Medio	Medio	Bajo	Bajo	Muy bajo
Improbable	Bajo	Bajo	Bajo	Muy bajo	Muy bajo

5. Identificación de opciones de tratamiento: Para cada riesgo, definir las estrategias de tratamiento:
   a. Reducción de riesgos: Implementar medidas para disminuir el riesgo general.
   b. Riesgo compartido o transferencia: Transferir el riesgo a terceros mediante seguros o proveedores de servicios.
   c. Evitar el riesgo: Eliminar el riesgo absteniéndose de realizar actividades que expongan a la municipalidad a amenazas potenciales.
   d. Aceptar el riesgo: Decidir aceptar el riesgo si se encuentra dentro de los parámetros de tolerancia de la municipalidad.
6. En caso de que la evaluación del riesgo no sea satisfactoria, el riesgo debe de volver a ser evaluado, ir al paso 3.
7. Preparación y prueba de planes de respuesta a incidentes: se debe preparar, mantener y probar regularmente planes de respuesta ante incidentes críticos que puedan generar un impacto significativo en las operaciones. Los planes deben documentar pasos claros a seguir, rutas de escalamiento dentro de la municipalidad, y roles y responsabilidades para minimizar el impacto de los incidentes.
8. Aplicación de los planes de respuesta: Cuando ocurra un incidente de riesgo, los planes de respuesta documentados deben aplicarse de manera efectiva. Esto implica seguir los pasos predefinidos en el plan y asegurar que las acciones minimicen el impacto del incidente, y que se sigan los procedimientos de escalamiento apropiados para gestionar la situación.
9. En caso de que el nivel de riesgo tras su tratamiento no sea aceptable, el riesgo debe de volver a ser evaluado, ir al paso 3.
10. Documentar información: Preparar un informe estructurado que resuma los hallazgos clave, descripciones claras, y resalte los riesgos críticos.

Departamento de Tecnologías de Información,
e-mail: negamboa@munituralba.go.cr

a. Generación de informes de seguimiento: Crear informes que incluyan el estado actual del perfil de riesgo, destacando las áreas de mayor preocupación y los avances en las acciones correctivas implementadas.

11. Distribución de la información: Proporcionar los informes detallados a los responsables de la toma de decisiones, asegurando una respuesta oportuna y bien informada, ver Matriz de Comunicaciones.

Frecuencia de Revisión: Continuo, con actualizaciones trimestrales.

4.2 Especificación de requisitos para proyectos de mitigación

Los proyectos o programas destinados a mitigar los riesgos deben tener requisitos claramente especificados, incluyendo los controles clave necesarios para reducir el riesgo a niveles aceptables. Estos controles deben alinearse con las mejores prácticas de la industria y las normativas aplicables. Pasos para la Especificación de Requisitos:

1. Identificación de proyectos de mitigación: Definir los proyectos que implementarán las acciones correctivas propuestas.
2. Especificación de controles clave: Identificar los controles específicos que cada proyecto debe implementar para reducir el riesgo.
3. Cumplimiento normativo: Asegurar que los controles cumplen con los estándares regulatorios y las mejores prácticas de la industria.
4. Monitoreo y seguimiento: Establecer métricas para monitorear la implementación de los proyectos y su efectividad en la mitigación del riesgo.

Frecuencia de Revisión: Conforme a los ciclos de vida de los proyectos.

4.3 Inventario de procesos de negocio y dependencias

Se debe crear y mantener un inventario detallado y actualizado de los procesos de negocio de la municipalidad, identificando la dependencia de cada uno con los servicios de TI y la infraestructura tecnológica. El inventario debe incluir personal clave, infraestructuras críticas, aplicaciones, proveedores y terceros que sean esenciales para el funcionamiento del negocio. Pasos para Crear y Mantener el Inventario:

1. Identificación de procesos de negocio: Listar todos los procesos clave de la municipalidad, detallando su dependencia con la infraestructura tecnológica y los servicios de TI.
2. Determinación de dependencias tecnológicas: Para cada proceso de negocio, identificar las aplicaciones,

Departamento de Tecnologías de Información,
e-mail: negamboa@muniturrialba.go.cr

sistemas, hardware, y redes que soportan el proceso.

3. Registro de infraestructuras críticas: Documentar las infraestructuras tecnológicas críticas, incluyendo centros de datos, servidores, y redes esenciales.
4. Identificación de personal y terceros: Listar los responsables clave de cada proceso y las dependencias con proveedores y servicios externos.
5. Revisión y validación: Revisar el inventario con las áreas funcionales para asegurar la precisión de la información.

Frecuencia de Actualización: Anual, con revisiones adicionales tras cualquier cambio significativo en los procesos de negocio o la infraestructura de TI.

4.4 Preparación y prueba de planes de respuesta a incidentes

La municipalidad debe preparar, mantener y probar regularmente planes de respuesta ante incidentes críticos que puedan generar un impacto significativo en las operaciones. Los planes deben documentar pasos claros a seguir, rutas de escalamiento dentro de la municipalidad, y roles y responsabilidades para minimizar el impacto de los incidentes. Pasos para la Preparación del Plan:

1. Identificación de escenarios de incidentes críticos: Definir los tipos de incidentes que podrían tener un impacto significativo en la municipalidad (por ejemplo, ciberataques, fallos críticos de infraestructura, filtraciones de datos).
2. Documentación de los pasos de respuesta: Desarrollar un plan de respuesta detallado para cada tipo de incidente crítico, especificando las acciones inmediatas a tomar, las personas o equipos responsables y las herramientas necesarias para gestionar el incidente.
3. Establecimiento de rutas de escalamiento: Definir claramente las rutas de escalamiento en caso de que el incidente supere la capacidad de respuesta de los equipos de primera línea. Especificar los niveles jerárquicos y contactos para la escalación interna.
4. Definición de roles y responsabilidades: Asignar roles específicos a los miembros del equipo de respuesta a incidentes, incluyendo responsables de comunicación, manejo técnico y toma de decisiones estratégicas.
5. Pruebas de los planes de respuesta: Implementar simulaciones semestrales para probar la efectividad de los planes de respuesta. Utilizar escenarios realistas para asegurar que los planes puedan manejar incidentes reales.
6. Evaluación de los resultados de la prueba: Revisar los resultados de cada prueba, identificar áreas de mejora y realizar los ajustes necesarios en los planes de respuesta.

Departamento de Tecnologías de Información,
e-mail: negamboa@muniturrialba.go.cr

7. Revisión de planes tras incidentes: Actualizar los planes de respuesta inmediatamente después de cualquier incidente significativo para reflejar las lecciones aprendidas y ajustar procedimientos ineficientes.

Frecuencia de Pruebas: Semestral, con revisión y ajustes según los resultados de las pruebas o tras la ocurrencia de un incidente significativo.

4.5 Aplicación de los planes de respuesta

Cuando ocurra un incidente de riesgo, los planes de respuesta documentados deben aplicarse de manera efectiva. Esto implica seguir los pasos predefinidos en el plan y asegurar que las acciones minimicen el impacto del incidente, y que se sigan los procedimientos de escalamiento apropiados para gestionar la situación. Pasos para la Aplicación de los Planes de Respuesta:

1. Detección del incidente: Implementar sistemas y herramientas de monitoreo para detectar incidentes críticos de forma temprana.
2. Activación inmediata del plan: Al confirmar un incidente, activar el plan de respuesta correspondiente. Asegurarse de que todos los miembros del equipo de respuesta reciban notificaciones inmediatas.
3. Implementación de acciones inmediatas: Ejecutar las primeras acciones documentadas en el plan de respuesta, tales como contener el incidente, mitigar el impacto y asegurar la protección de los activos críticos.
4. Escalamiento del incidente: Si la incidente escala más allá de la capacidad del equipo inicial de respuesta, activar las rutas de escalamiento predefinidas y notificar a los niveles jerárquicos superiores.
5. Coordinación de equipos: Asegurar que todos los equipos involucrados (TI, comunicaciones, legal, seguridad, etc.) trabajen de manera coordinada para mitigar el impacto del incidente.
6. Comunicación con partes interesadas: Implementar las acciones de comunicación según el plan, notificando a las partes interesadas internas y externas según lo requiera el incidente.
7. Registro y documentación: Durante y después del incidente, documentar todas las acciones tomadas, las decisiones clave y los resultados de las acciones de mitigación para su análisis posterior.
8. Evaluación post-incidente: Una vez finalizada la gestión del incidente, realizar una revisión detallada del proceso de respuesta para identificar lecciones aprendidas y ajustar el plan si es necesario.

Frecuencia de Aplicación: Activación inmediata durante la ocurrencia de incidentes.

Departamento de Tecnologías de Información,
e-mail: negamboa@munituriralba.go.cr

5 Indicadores de Desempeño

5.1 Porcentaje de objetivos y servicios críticos del negocio cubiertos por la evaluación de riesgos

Elemento	Descripción
Nombre	Cobertura de Evaluación de Riesgos en Objetivos Críticos
Código	GR-TI-001
Responsable	Encargado de Servicios de TI
Fórmula	Número de procesos críticos evaluados/Total de procesos críticos identificados x 100%
Frecuencia	Trimestral
Fuente de Datos	Informes de Evaluación de Riesgos
Meta	95%
Niveles de Tolerancia	90% - 100% (Aceptable) 80% - 89% (Advertencia) < 80% (Crítico)

5.2 Número de interrupciones del servicio al cliente o procesos empresariales que han causado incidentes significativos

Elemento	Descripción
Nombre	Incidentes Significativos de Interrupción de Servicio
Código	GR-TI-002
Responsable	Encargado de Servicios de TI
Fórmula	Conteo de incidentes significativos que han interrumpido el servicio al cliente
Frecuencia	Mensual
Fuente de Datos	Reportes de Incidentes, Bitácoras de Servicio
Meta	≤ 2 interrupciones por trimestre
Niveles de Tolerancia	0 - 2 (Aceptable) 3 - 4 (Advertencia) > 4 (Crítico)

Departamento de Tecnologías de Información,
e-mail: negamboa@muniturrialba.go.cr

5.3 Coste de incidentes para el negocio

Elemento	Descripción
Nombre	Impacto Financiero de Incidentes
Código	GR-TI-003
Responsable	Responsable de Auditoría Interna
Fórmula	Suma del coste total de los incidentes significativos (∑Coste de cada incidente significativo)
Frecuencia	Trimestral
Fuente de Datos	Reportes Financieros, Evaluación de Impacto de Incidentes
Meta	≤ ₡1,000,000 por trimestre
Niveles de Tolerancia	0 - ₡1,000,000 (Aceptable) ₡1,000,001 - ₡1,500,000 (Advertencia) > ₡1,500,000 (Crítico)

5.4 Número de incidentes significativos relacionados con TI que no se identificaron en la evaluación de riesgos

Elemento	Descripción
Nombre	Incidentes No Identificados en Evaluación de Riesgos
Código	GR-TI-004
Responsable	Encargado de Servicios de TI
Fórmula	Conteo de incidentes significativos no identificados previamente en la evaluación de riesgos
Frecuencia	Mensual
Fuente de Datos	Reportes de Incidentes, Evaluación de Riesgos
Meta	≤ 1 incidente por trimestre
Niveles de Tolerancia	0 - 1 (Aceptable) 2 - 3 (Advertencia) > 3 (Crítico)

Departamento de Tecnologías de Información,
e-mail: negamboa@muniturrialba.go.cr

5.5 Número de incidentes de confidencialidad que causan pérdidas financieras, interrupción del negocio o descrédito público

Elemento	Descripción
Nombre	Incidentes de Confidencialidad Críticos
Código	GR-TI-005
Responsable	Responsable de Seguridad del Sistema
Fórmula	Conteo de incidentes de confidencialidad con impacto significativo
Frecuencia	Mensual
Fuente de Datos	Reportes de Seguridad, Bitácoras de Incidentes
Meta	0 incidentes por trimestre
Niveles de Tolerancia	0 (Aceptable) 1 (Advertencia) > 1 (Crítico)

5.6 Número de incidentes de disponibilidad que causan pérdidas financieras, interrupción del negocio o descrédito público

Elemento	Descripción
Nombre	Incidentes de Disponibilidad Críticos
Código	GR-TI-006
Responsable	Encargado de Servicios de TI
Fórmula	Conteo de incidentes de disponibilidad con impacto significativo
Frecuencia	Mensual
Fuente de Datos	Reportes de Seguridad, Bitácoras de Incidentes
Meta	0 incidentes por trimestre
Niveles de Tolerancia	0 (Aceptable) 1 (Advertencia) > 1 (Crítico)

5.7 Número de incidentes de integridad que causan pérdidas financieras, interrupción del negocio o descrédito público

Elemento	Descripción
Nombre	Incidentes de Integridad Críticos
Código	GR-TI-007
Responsable	Encargado de Servicios de TI
Fórmula	Conteo de incidentes de integridad con impacto significativo
Frecuencia	Mensual
Fuente de Datos	Reportes de Seguridad, Bitácoras de Incidentes
Meta	0 incidentes por trimestre
Niveles de Tolerancia	0 (Aceptable) 1 (Advertencia) > 1 (Crítico)

Departamento de Tecnologías de Información,
e-mail: negamboa@muniturrialba.go.cr

6 Plan de Comunicaciones

Se proporciona el plan de comunicaciones respecto al proceso de gestión de riesgos de TI, que es esencial para asegurar la ejecución adecuada del mismo.

6.1 Grupos de Interés

Los grupos de interés dentro del proceso de gestión de riesgos de TI de la Municipalidad de Turrialba incluyen a todas las personas o entidades que tienen un rol activo o que son impactadas por el éxito o el fracaso en la mitigación de riesgos. A continuación, se detallan los principales grupos de interés y sus respectivas responsabilidades:

1. **Alcalde Municipal y Concejo**
   - **Rol**: Aprobación de políticas y decisiones estratégicas relacionadas con la gestión de riesgos de TI.
   - **Interés**: Asegurar que los riesgos tecnológicos no afecten las operaciones críticas de la municipalidad y que se alineen con los objetivos institucionales.
   - **Necesidades de información**: Resultados de evaluaciones de riesgos, recomendaciones de mitigación, informes de auditoría y cumplimiento normativo.
2. **Directores y Jefes de Departamento**
   - **Rol**: Supervisar la implementación de los controles y acciones de mitigación dentro de sus respectivos departamentos.
   - **Interés**: Garantizar que los riesgos relacionados con sus áreas de operación sean gestionados adecuadamente y no afecten la continuidad de sus actividades.
   - **Necesidades de información**: Actualizaciones periódicas sobre riesgos identificados, controles implementados.
3. **Departamento de TI**
   - **Rol**: Responsable de la implementación y monitoreo continuo de las medidas de seguridad y control en la infraestructura tecnológica, así como de la gestión operativa de los riesgos tecnológicos.
   - **Interés**: Asegurar que los riesgos relacionados con la infraestructura tecnológica sean identificados y gestionados de manera eficiente, manteniendo la disponibilidad, integridad y confidencialidad de los sistemas de TI.
   - **Necesidades de información**: Procedimientos detallados de evaluación de riesgos, actualizaciones sobre amenazas emergentes, planes de respuesta a incidentes, y cambios normativos que afecten la

Departamento de Tecnologías de Información,
e-mail: negamboa@muniturrialba.go.cr

gestión de los riesgos tecnológicos.

4. **Contratistas y Terceros**
    - **Rol**: Proveedores de servicios que interactúan con los sistemas de TI de la municipalidad.
    - **Interés**: Asegurar que sus actividades cumplan con los estándares de seguridad establecidos por la municipalidad y no introduzcan nuevos riesgos.
    - **Necesidades de información**: Políticas de seguridad, estándares técnicos y procedimientos de gestión de riesgos.

6.2 Priorización de la Información

La prioridad de la información a comunicar dentro del proceso de gestión de riesgos de TI se establece en función de su relevancia para la ejecución de tareas críticas y su impacto en el logro de los objetivos institucionales. A continuación, se describen los niveles de prioridad asignados a la información:

6.2.1 Prioridad Alta

La información clasificada con prioridad alta es esencial para la ejecución de tareas críticas y tiene un impacto directo en la continuidad y calidad de los servicios prestados por la Municipalidad de Turrialba. Cualquier retraso o falta de comunicación de esta información puede resultar en riesgos significativos o en el fracaso de procesos importantes. La comunicación de este tipo de información debe ser **inmediata**.

- **Ejemplos**:
    - Resultados críticos de las evaluaciones de riesgos que requieren acciones correctivas inmediatas.
    - Identificación de amenazas o incidentes de seguridad que puedan afectar los sistemas operativos clave.
    - Informes de auditoría que evidencien fallos graves en los controles implementados.

6.2.2 Prioridad Media

La información de prioridad media es importante para el desarrollo de las actividades, pero no es crítica para el éxito inmediato de los procesos. Esta información se comunica de forma **oportuna**, pero no es necesario hacerlo de inmediato, ya que no compromete de manera significativa las operaciones si se retrasa.

- **Ejemplos**:
    - Actualizaciones sobre la implementación de controles de mitigación de riesgos.
    - Informes trimestrales sobre el estado del perfil de riesgos.

Departamento de Tecnologías de Información,
e-mail: negamboa@munituralba.go.cr

- Recomendaciones para mejorar procesos o controles de seguridad que no requieren intervención inmediata.

6.2.3 Prioridad Baja

La información clasificada como de prioridad baja es aquella que puede ser útil para los colaboradores y partes interesadas, pero cuya falta de comunicación inmediata no afecta de manera considerable los procesos operativos o la gestión de riesgos. Esta información se puede comunicar **cuando los recursos y el tiempo lo permitan**, sin un sentido de urgencia.

- **Ejemplo**s:
  - Boletines informativos sobre buenas prácticas de seguridad que no están relacionadas con riesgos inmediatos.
  - Informes generales sobre tendencias de riesgos a largo plazo.
  - Actualizaciones menores sobre mejoras técnicas en sistemas que no están en producción.

6.3 Matriz de Comunicaciones

Para sintetizar los anteriores puntos y visualizar de forma clara el plan de comunicaciones se desarrolla la Matriz de comunicaciones del proceso de gestión de riesgos de TI, una matriz de comunicaciones que identifica la forma en qué se comunicaran los diferentes aspectos a planteados en el proceso. Dentro de la matriz de comunicaciones, se incluyen los siguientes elementos:

1. Información: Nombre del documento o anuncio a comunicar.
2. Contenido: Puntos a abordar dentro del documento.
3. Emisor: Persona encargada de comunicar la información.
4. Receptor: Destinatarios que reciben la información.
5. Medio de comunicación: Métodos utilizados para enviar la información.
6. Frecuencia: Período definido por tiempo o cumplimiento de condiciones en el cual se envía la información.

Departamento de Tecnologías de Información,
e-mail: negamboa@muniturrialba.go.cr

DEPARTAMENTO DE TECNOLOGÍAS DE INFORMACIÓN

Información	Contenido	Emisor	Receptor	Medio de comunicación	Frecuencia
Informe de Evaluación de Riesgos Críticos	Resultados de la evaluación de riesgos críticos; recomendaciones para mitigación inmediata	Encargado de Servicios de TI	Alcalde, Concejo, Directores de Departamento	Correo electrónico, reuniones ejecutivas	Inmediata tras la identificación de un riesgo crítico
Informe de Riesgos de TI	Estado actual del perfil de riesgos, controles implementados, nuevas amenazas identificadas	Encargado de Servicios de TI	Alcalde, Concejo, Directores	Correo electrónico	Trimestral
Actualización de Procedimientos de Seguridad	Cambios en los procedimientos de respuesta a incidentes, medidas de seguridad adicionales	Encargado de Servicios de TI	Alcalde, Concejo, Directores	Correo electrónico, reuniones ejecutivas	Semestral o cuando se produzcan cambios significativos
Informe de Cumplimiento Normativo	Resultados de auditorías, análisis de cumplimiento de las normativas locales e internacionales	Responsable de Auditoría Interna	Alcalde, Concejo, Directores de Departamento	Correo electrónico, reuniones ejecutivas	Anual o tras auditorías
Plan de Respuesta a Incidentes	Pasos detallados para la respuesta a incidentes críticos, roles y responsabilidades	Responsable de Seguridad del Sistema	Alcalde, Concejo, Directores de Departamento	Correo electrónico, reuniones ejecutivas	Semestral
Boletín de Buenas Prácticas de Seguridad	Consejos y recomendaciones sobre seguridad de la información, actualización de amenazas	Departamento de TI	Todos los colaboradores de la Municipalidad	Correo electrónico	Mensual
Simulacro de Respuesta a Incidentes	Ejercicio práctico de respuesta a incidentes, evaluación del desempeño, retroalimentación	Encargado de Servicios de TI	Alcalde, Concejo, Directores de Departamento	Correo electrónico	Semestral

Número de Páginas 22 - 24

Departamento de Tecnologías de Información,
e-mail: negonicos@municurrualba.go.cr

7 Revisión y Mejora Continua

Los procedimientos de gestión de riesgos de tecnología de la información deben revisarse anualmente o tras la ocurrencia de cualquier incidente significativo que pueda impactar los sistemas de TI. Esta revisión tiene como objetivo asegurar que los procedimientos sigan siendo eficaces y pertinentes, adaptándose a los cambios en el entorno de riesgos y las tecnologías. Además, se deben realizar auditorías periódicas para evaluar la efectividad de las prácticas implementadas y ajustar los procedimientos conforme sea necesario, garantizando la mejora continua de los procesos de gestión de riesgos.

8 Cumplimiento y Auditoría

Los procedimientos deben cumplir con los requisitos establecidos para auditorías internas y externas, con el fin de asegurar el alineamiento con las normativas aplicables, como la Norma Técnica para la gestión de TI del MICITT y otras regulaciones nacionales relevantes. Las auditorías se realizarán para verificar que los procedimientos se están aplicando correctamente y que los controles implementados son efectivos para mitigar los riesgos identificados. Cualquier incumplimiento identificado durante las auditorías deberá ser corregido de manera oportuna, y los informes de auditoría serán utilizados para mejorar los procedimientos y garantizar el cumplimiento continuo.

9 Documentos relacionados

Este procedimiento se complementa con los siguientes documentos:

- Política para la Gestión de Riesgos de Tecnologías de Información: son aplicables para todos los aspectos administrativos y de control que deben ser cumplidos por: Gerencia Municipal (Alcalde y Concejo Municipal), Directores, Jefes de Departamento y colaboradores en general, funcionarios contratistas y terceros que presten sus servicios o tengan algún tipo de relación con el Departamento de Tecnologías de Información de la Municipalidad de Turrialba, para el adecuado cumplimiento de sus funciones y para conseguir un adecuado nivel de protección de las características de calidad y seguridad de la información, aportando con su participación en la toma de medidas preventivas y correctivas, siendo un punto clave para el logro del objetivo y la finalidad de dicho instrumento. Los usuarios tienen la obligación de dar cumplimiento a las presentes políticas emitidas y aprobadas por la Alcaldía.

10 Referencias

Asociación Española de Normalización. (2018). *UNE-ISO 31000 Gestión del riesgo Directrices*. www.iso.org/patents.

Departamento de Tecnologías de Información,
e-mail: negamboa@muniturrialba.go.cr

DEPARTAMENTO DE TECNOLOGÍAS DE INFORMACIÓN

Asociación Española de Normalización. (2024). *Seguridad de la información, ciberseguridad y protección de la privacidad. Guía para la gestión de los riesgos de seguridad de la información (ISO/IEC 27005:2022) (Ratificada por la Asociación Española de Normalización en septiembre de 2024.)*. www.une.org

Asociación Española de Normalización. (2015). *UNE-EN ISO 9001 Sistemas de gestión de la calidad Requisitos*.

Axelos. (2019). *ITIL ® Foundation ITIL 4 Edition 2*. https://www.axelos.com

Gamboa Calderón, N. E. (2022). *Políticas de Seguridad en Materia de Tecnologías de Información y Comunicación TICS*.

ISACA. (2018). *Marco de Referencia COBIT® 2019: Objetivos de gobierno y gestión*. http://linkd.in/ISACAOfficial

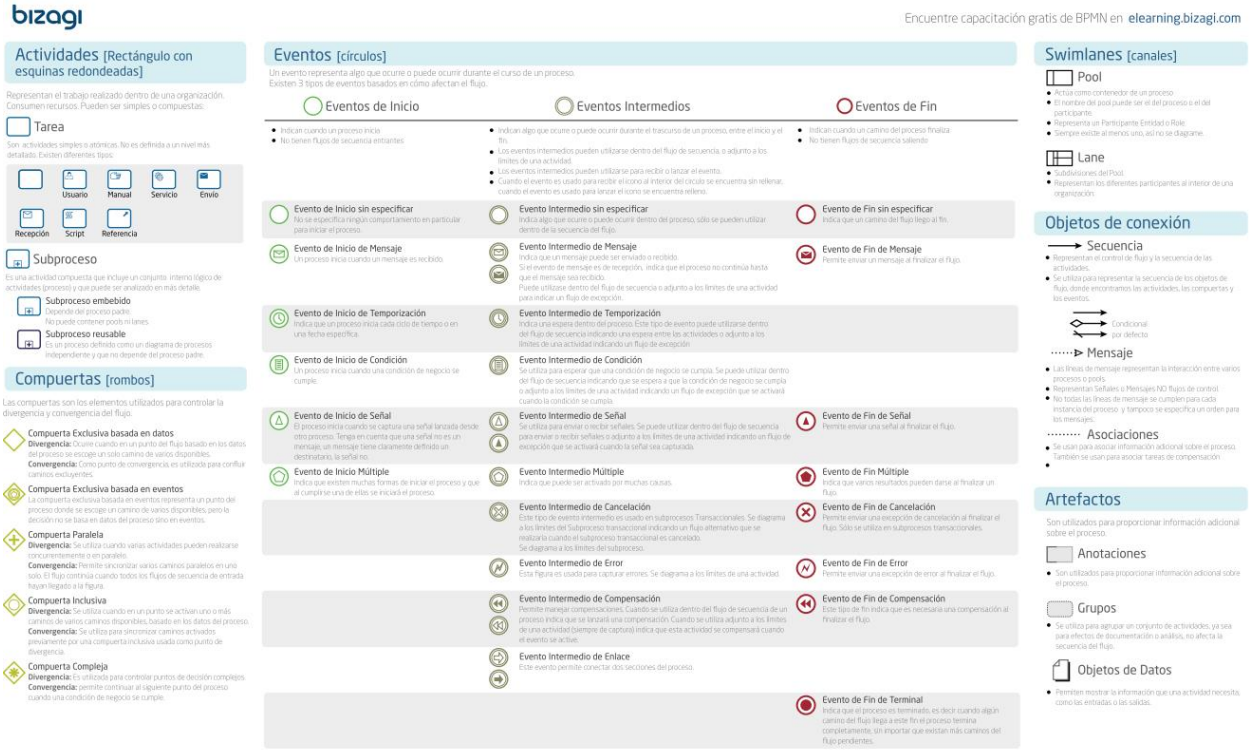
National Institute of Standards and Technology. (2012). *NIST 800-30: Guide for Conducting Risk Assessments*. https://doi.org/10.6028/NIST.SP.800-30r1

Solís García, S., Montillano Vivas, M., Chinchilla Sáenz, S., Tenorio Chacón, O., Badilla Picado, I., & Lemaitre Picado, R. (2021). *Normas técnicas para la gestión y el control de las Tecnologías de Información*.

Departamento de Tecnologías de Información,
e-mail: negamboa@muniturrialba.go.cr

10 **Anexos**

10.1 Anexo I BPMN Guía de Referencia



Nota. Adaptado de Bizagi (2023) *BPMN Guía de Referencia* (bizagi.com).

10.2 Anexo II Actividades EDM03 — Asegurar la optimización del riesgo.

Dominio: Evaluar, Dirigir y Monitorizar **Objetivo de gobierno: EDM03 — Asegurar la optimización del riesgo**	**Área prioritaria: Modelo Core de COBIT**
Descripción	
Asegurar que el apetito y la tolerancia al riesgo de la empresa se entiendan, articulen y comuniquen, y que se identifique y gestione el riesgo para el valor de negocio relacionado con el uso de I&T.	
Propósito	
Asegurarse de que el riesgo de negocio relacionado con la I&T no exceda el apetito y tolerancia al riesgo de la empresa, que se identifique y gestione el impacto del riesgo de I&T para el valor de negocio y que se minimicen los posibles fallos de cumplimiento.	
El objetivo de gobierno respalda la realización de un conjunto de metas empresariales y de alineamiento primarias:	

Metas empresariales	**Metas de alineamiento**
• EG02 Gestión de riesgo de negocio • EG06 Continuidad y disponibilidad del servicio del negocio	• AG02 Gestión de riesgo relacionado con I&T • AG07 Seguridad de la información, infraestructura de procesamiento y aplicaciones, y privacidad
Métricas modelo para metas empresariales	**Métricas modelo para metas de alineamiento**
EG02 a. Porcentaje de objetivos y servicios empresariales críticos cubiertos por la evaluación de riesgos b. Número de incidentes significativos que no se identificaron en la evaluación de riesgos frente al total de incidentes c. Frecuencia de actualización del perfil de riesgo	AG02 a. Frecuencia de actualización del perfil de riesgo b. Porcentaje de las evaluaciones de riesgo empresarial, incluido el riesgo relacionado con I&T c. Número de incidentes significativos relacionados con I&T que no se identificaron en la evaluación de riesgos
EG06 a. Número de interrupciones del servicio al cliente o procesos empresariales que han causado incidentes significativos b. Coste empresarial de los incidentes c. Número de horas de procesamiento perdidas en el negocio debido a interrupciones inesperadas del servicio d. Porcentaje de quejas en función de los objetivos de disponibilidad del servicio acordados	AG07 a. Número de incidentes de confidencialidad que causan pérdidas financieras, interrupción del negocio o descrédito público b. Número de incidentes de disponibilidad que causan pérdidas financieras, interrupción del negocio o descrédito público c. Número de incidentes de integridad que causan pérdidas financieras, interrupción del negocio o descrédito público

A. Componente: Proceso	
Práctica de gobierno	**Métricas modelo**
EDM03.01 Evaluar la gestión de riesgos. Examinar y evaluar continuamente el efecto del riesgo sobre el uso actual y futuro de las I&T en la empresa. Considerar si el apetito al riesgo de la empresa es apropiada, y que se identifique y gestione el riesgo para el valor de la empresa relacionado con el uso de I&T.	a. Nivel de impacto empresarial inesperado b. Porcentaje de riesgo de I&T que excede la tolerancia al riesgo de la empresa c. Frecuencia de actualización de la evaluación del factor de riesgo

Actividades	**Nivel de capacidad**
1. Conocer la organización y su contexto en relación al riesgo de I&T.	2
2. Determinar el apetito al riesgo de la organización, es decir, el nivel de riesgo relacionado con I&T que la empresa está dispuesta a tomar en la búsqueda de sus objetivos empresariales.	
3. Determinar los niveles de tolerancia al riesgo frente al apetito al riesgo, es decir, las desviaciones aceptables temporalmente del apetito al riesgo.	
4. Determinar el grado de alineamiento de la estrategia de riesgos en I&T de la empresa con la estrategia de riesgos de la empresa en su conjunto y garantizar que el apetito al riesgo se sitúe por debajo de la capacidad de riesgo de la organización.	
5. Evaluar los factores de riesgo de I&T de forma proactiva antes de tomar decisiones estratégicas a nivel de empresa y garantizar que las consideraciones del riesgo formen parte del proceso de decisión estratégico de la empresa.	3
6. Evaluar las actividades de gestión de riesgos para asegurar que se alineen con la capacidad de la empresa para las pérdidas relacionadas con I&T y la tolerancia correspondiente por parte de la dirección.	
7. Atraer y conservar las habilidades y el personal necesarios para la gestión de riesgos de las I&T	

Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	**Referencia específica**
COSO Enterprise Risk Management, junio de 2017	Strategy and Objective-Setting—Principles 6 and 7; 9. Review and Revision—Principle 16

A. Componente: Proceso *(cont.)*	
Práctica de gobierno	**Métricas modelo**
EDM03.02 Dirigir la gestión de riesgos. Dirigir el establecimiento de prácticas de gestión de riesgos para ofrecer una seguridad razonable de que las prácticas de gestión de riesgos de I&T son apropiadas y que el riesgo de I&T actual no sobrepasa al apetito al riesgo del consejo de administración.	a. Nivel de alineamiento entre el riesgo de I&T y el riesgo empresarial b. Porcentaje de proyectos de la empresa que consideran el riesgo de I&T.

Actividades	Nivel de capacidad
1. Dirigir la traducción e integración de la estrategia de riesgo de I&T en las prácticas de gestión de riesgos y las actividades operativas.	2
2. Dirigir el desarrollo de planes de comunicación de riesgos (que se extiendan a todos los niveles de la empresa).	
3. Dirigir la implementación de los mecanismos adecuados para responder de forma rápida al cambio de riesgos e informar inmediatamente a los cargos de dirección correspondientes, siguiendo los principios de escalamiento (qué comunicar, cuándo, dónde y cómo).	
4. Ordenar que el riesgo, oportunidades, problemas o preocupaciones puedan identificarse y comunicarse por cualquier persona a la parte correspondiente en cualquier momento. El riesgo debe gestionarse conforme a las políticas y procedimientos publicados y comunicados a los responsables de la toma de decisiones.	
5. Identificar las metas y métricas claves de los procesos de gobierno y gestión de riesgos que deben monitorizarse, y aprobar las estrategias, métodos, técnicas y procesos para capturar y comunicar la información de las mediciones.	3

Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
CMMI Cybermaturity Platform, 2018	RS.AS Apply Risk Management Strategy; BC.RO Determine Strategic Risk Objectives
ISF, The Standard of Good Practice for Information Security 2016	IR1.1 Information Risk Assessment–Management Approach
King IV Report on Corporate Governance for South Africa, 2016	Part 5.4: Governance functional areas–Principle 11
National Institute of Standards and Technology Special Publication 800-37, Revisión 2 (Borrador), mayo de 2018	3.5 Assessment (Task 2)

Práctica de gobierno	Métricas modelo
EDM03.03 Monitorizar la gestión de riesgos. Monitorizar r las metas y las métricas clave de los procesos de gestión de riesgos. Establecer cómo las desviaciones o los problemas se identificarán, se les dará seguimiento y se comunicarán para su solución.	a. Número de áreas potenciales de riesgo de I&T identificadas y gestionadas b. Porcentaje de riesgo crítico que ha sido mitigado efectivamente c. Porcentaje de planes de acción de riesgo de I&T ejecutados a tiempo

Actividades	Nivel de capacidad
1. Comunicar cualquier problema de gestión de riesgos al consejo de administración o comité ejecutivo.	2
2. Supervise hasta qué punto se gestiona el perfil de riesgo dentro de los umbrales de tolerancia y apetito de riesgo de la empresa.	3
3. Monitorizarr las metas y métricas de los procesos de gobierno y gestión de riesgos contra los objetivos, analizar la causa de las posibles desviaciones, y poner en marcha las acciones remediales s para solucionar las causas subyacentes.	4
4. Facilitar la revisión por parte de las partes interesadas clave del progreso de la empresa con respecto a las metas identificadas.	

Documentación relacionada (Estándares, Marcos, Requisitos de cumplimiento)	Referencia específica
COSO Enterprise Risk Management, junio de 2017	9. Review and Revision–Principle 17
National Institute of Standards and Technology Special Publication 800-37, Revisión 2 (Borrador), mayo de 2018	3.1 Preparation (Task 7); 3.5 Assessment (Task 1); 3.6 Authorization (Task 1)
The Open Group IT4IT Reference Architecture, Versión 2.0	6. Requirement to Deploy (R2D) Value Stream; 7. Request to Fulfill (R2F) Value Stream

10.3 Anexo III Actividades APO12-Gestionar el riesgo.

Práctica de gestión	Métricas modelo
APO12.01 Recopilar datos. Identificar y recopilar datos relevantes para habilitar una efectiva identificación, análisis y reporte de los riesgos relacionados con I&T.	a. Número de eventos de pérdida con características clave capturados en repositorios b. Porcentaje de auditorías, eventos y tendencias capturados en repositorios c. Porcentaje de sistemas críticos con problemas conocidos

Actividades	Nivel de capacidad
1. Establecer y mantener un método para la recogida, clasificación y análisis de datos relacionados con el riesgo de I&T.	2
2. Registrar datos relevantes y significativos relacionados con los riesgos de I&T en el entorno operativo interno y externo de la empresa.	
3. Adoptar o definir una taxonomía de riesgo para las definiciones consistentes de escenarios de riesgo y categorías de impacto y probabilidad.	3
4. Registrar datos de eventos de riesgo que han causado o podrían causar impacto en el negocio conforme a las categorías de impacto definidas en la taxonomía de riesgo. Capturar datos relevantes de cuestiones, incidentes, problemas e investigaciones.	
5. Estudiar y analizar los datos históricos de riesgo de I&T y de pérdidas experimentadas a partir de datos y tendencias externos disponibles, homólogos de la industria a través de logs de eventos de la industria, bases de datos, y acuerdos de la industria, para la publicación común de eventos.	4
6. Para clases de eventos similares, organizar los datos recopilados y resaltar los factores causantes. Determinar los factores causantes comunes en múltiples eventos.	
7. Determinar las condiciones específicas que existieron o estuvieron ausentes cuando tuvieron lugar los eventos de riesgo y la forma en que las condiciones afectaron a la frecuencia del evento y la magnitud de la pérdida.	
8. Realizar un análisis periódico de eventos y factores de riesgo para identificar riesgos nuevos o emergentes y para mejorar el entendimiento de los factores de riesgo internos y externos asociados.	

Práctica de gestión	Métricas modelo
APO12.02 Analizar el riesgo. Desarrollar una visión fundamentada del riesgo de I&T vigente, que soporte las decisiones de riesgo.	a. Número de escenarios de riesgo de I&T identificados b. Tiempo transcurrido desde la última actualización de los escenarios de riesgos de I&T

Actividades	Nivel de capacidad
1. Definir el alcance adecuado de los esfuerzos en análisis de riesgos, considerando todos los factores de riesgo y/o la criticidad de los activos para el negocio.	3
2. Crear y actualizar regularmente los escenarios de riesgo de I&T; las exposiciones a pérdidas relacionadas con I&T; y los escenarios relacionados con el riesgo reputacional, incluidos escenarios compuestos de tipos de amenazas y eventos en cascada y/o coincidentes. Desarrollar previsiones para actividades de control específicas y capacidades de detección.	
3. Estimar la frecuencia (o probabilidad) y la magnitud de la pérdida o ganancia asociada con escenarios de riesgos de I&T. Tener en cuenta todos los factores de riesgo aplicables y evaluar controles operativos conocidos.	
4. Comparar el riesgo actual (exposición a pérdidas de I&T) con el apetito al riesgo y la tolerancia de riesgo aceptable. Identificar el riesgo inaceptable o elevado.	
5. Proponer respuestas al riesgo para riesgos que excedan el apetito al riesgo y los niveles de tolerancia.	
6. Especificar los requisitos de alto nivel para los proyectos o programas que implementarán las respuestas a los riesgos seleccionadas. Identificar los requisitos y expectativas para los controles clave adecuados a fin de proporcionar respuestas de mitigación de riesgos.	
7. Validar el análisis de riesgo y los resultados del análisis de impacto del negocio (BIA) antes de usarlos en la toma de decisiones. Confirmar que el análisis se corresponde con los requisitos empresariales y comprobar que los sesgos de las estimaciones se calibraron y analizaron de forma adecuada.	4
8. Analizar el coste/beneficio de las posibles opciones de respuesta al riesgo, como evitar, reducir/mitigar, transferir/compartir y aceptar y explotar/aprovechar. Confirmar la respuesta óptima al riesgo.	5

Práctica de gestión	Métricas modelo
APO12.03 Mantener un perfil de riesgo. Mantener un inventario de los riesgos conocidos y los atributos de riesgo, incluidos la frecuencia esperada, impacto potencial y respuestas. Documentar los recursos, capacidades y actividades de control actuales relacionados con elementos de riesgo.	a. Completitud de atributos y valores en el perfil de riesgo b. Porcentaje de procesos clave de negocio incluidos en el perfil de riesgo

Actividades	Nivel de capacidad
1. Hacer un inventario de los procesos de negocio y documentar su dependencia con los procesos de gestión de servicios de I&T y los recursos de infraestructura de TI. Identificar el personal de apoyo, aplicaciones, infraestructura, instalaciones, registros manuales críticos, contratistas, proveedores, y terceros.	2
2. Determinar y acordar qué servicios de I&T y recursos de infraestructura de TI son esenciales para sostener el funcionamiento de los procesos de negocio. Analizar las dependencias e identificar los eslabones débiles.	
3. Agregar los escenarios de riesgos actuales por categoría, línea de negocio y área funcional.	
4. Capturar regularmente toda la información del perfil de riesgo y consolidarla en un perfil de riesgo agregado.	3
5. Capturar información sobre el estado del plan de acción de riesgos para su inclusión en el perfil de riesgo de I&T de la empresa.	
6. Con base en todos los datos del perfil de riesgo, definir un conjunto de indicadores de riesgo que permitan una identificación y monitorización rápida del riesgo actual y las tendencias de riesgo.	4
7. Capturar información sobre eventos de riesgo de I&T que se han materializado para su inclusión en el perfil de riesgo de TI de la empresa.	

Práctica de gestión	Métricas modelo
APO12.04 Articular el riesgo. Comunicar de manera oportuna información sobre el estado actual de las exposiciones y oportunidades relacionadas con I&T a todas las partes interesadas requeridas para obtener una respuesta apropiada.	a. Nivel de satisfacción de las partes interesadas con los informes de riesgos proporcionados b. Completitud de los informes del perfil de riesgos (incluida información alineada con los requisitos de las partes interesadas) c. Uso de informes de riesgos en la toma de decisiones de gestión

Actividades	Nivel de capacidad
1. Informar sobre los resultados del análisis de riesgo a todas las partes interesadas afectadas en términos y formatos útiles para soportar las decisiones empresariales. Siempre que sea posible, incluir las probabilidades y rangos de pérdidas o ganancias, junto con los niveles de confianza, para permitir que la gerencia haga balance del retorno del riesgo.	3
2. Proporcionar a los responsables de la toma de decisiones la comprensión de los escenarios más probables y peores, exposiciones a pérdidas de I&T y consideraciones significativas de reputación, legales y regulatorias, o cualquier otra categoría de impacto conforme a la taxonomía de riesgos.	
3. Informar sobre el perfil de riesgo actual a todas las partes interesadas. Incluir información sobre la eficacia del proceso de gestión de riesgos, eficacia del control, brechas, inconsistencias, redundancias, estado de remediación y sus impactos en el perfil de riesgo.	
4. De forma periódica, en áreas con riesgos relativos y capacidades de riesgo similares, identificar oportunidades relacionadas con I&T que permitirían la aceptación de un riesgo mayor y un mayor crecimiento y retorno.	
5. Revisar los resultados de las evaluaciones objetivas de terceros y revisiones de auditoría interna y de aseguramiento de la calidad. Incluirlos en el perfil de riesgo. Revisar las brechas identificadas y las exposiciones de pérdidas relacionadas con I&T para determinar la necesidad de un análisis de riesgos adicional.	4

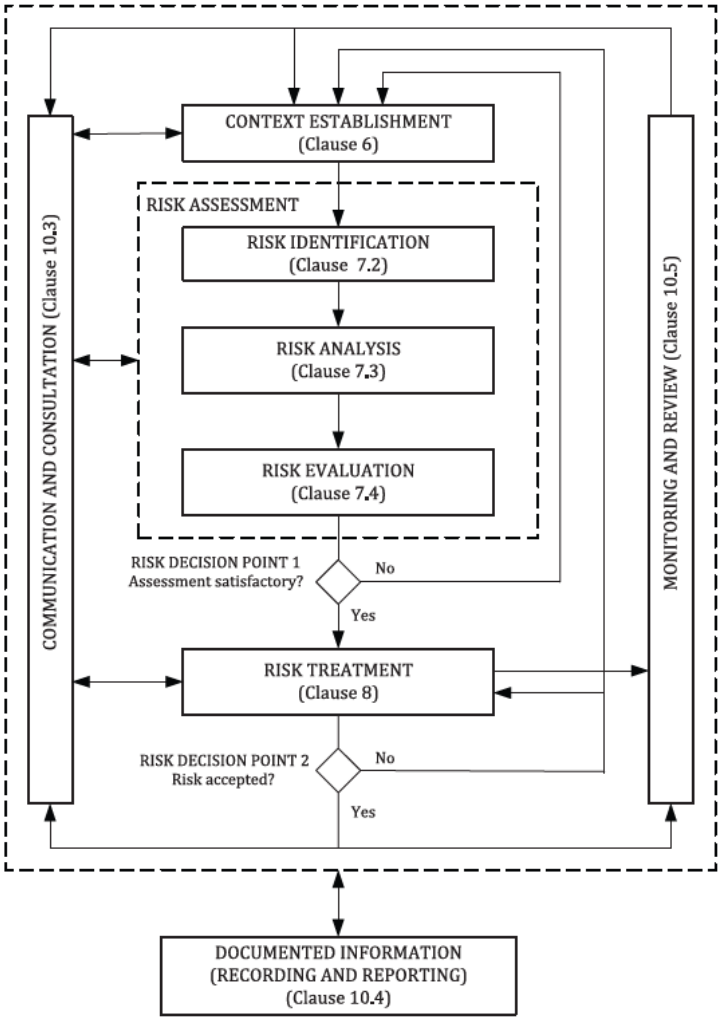
Práctica de gestión	Métricas modelo
APO12.05 Definir un portafolio con acciones de gestión de riesgos. Gestionar las oportunidades para reducir el riesgo a un nivel aceptable como un portafolio.	a. Número de incidentes significativos no identificados e incluidos en el portafolio de gestión de riesgos b. Porcentaje de propuestas de proyectos de gestión de riesgos rechazadas por falta de consideración de otros riesgos relacionados

Actividades	Nivel de capacidad
1. Mantener un inventario de las actividades de control que se han implantado para mitigar el riesgo y que permiten que se tomen riesgos alineados con el apetito y la tolerancia al riesgo. Clasificar las actividades de control y asignarlas a escenarios de riesgos de I&T específicos y escenarios de riesgos de I&T agregados.	2
2. Determinar si cada entidad organizativa monitoriza el riesgo y acepta la responsabilidad de actuar dentro de los niveles de tolerancia individuales y del portafolio.	3
3. Definir un conjunto de propuestas de proyectos equilibrada diseñada para reducir el riesgo y/o proyectos que permitan oportunidades empresariales estratégicas, con consideración de los costes, beneficios, efecto en el perfil de riesgo actual y en las regulaciones.	

Práctica de gestión	Métricas modelo	
APO12.06 Responder al riesgo. Responder de manera oportuna a eventos de riesgo materializados con medidas eficaces para limitar la magnitud de las pérdidas.	a. Número de medidas que no reducen el riesgo residual b. Porcentaje de planes de acción de riesgo de I&T ejecutados según se diseñaron	
Actividades		**Nivel de capacidad**
1. Preparar, mantener y probar planes que documenten los pasos específicos que deben darse cuando un evento de riesgo pudiera causar un incidente significativo de desarrollo u operativo con un impacto grave para el negocio. Asegurar que los planes incluyan vías de escalamiento en la empresa.		3
2. Aplicar el plan de respuesta adecuado para minimizar el impacto cuando ocurren incidentes de riesgo.		
3. Clasificar los incidentes y comparar las exposiciones a pérdidas relacionadas con I&T con los umbrales de tolerancia al riesgo. Comunicar los impactos de negocio a los responsables de la toma de decisiones como parte del reporte y actualización del perfil de riesgo.		4
4. Examinar eventos adversos/pérdidas y oportunidades del pasado no consideradas y determinar las causas raíz.		
5. Comunicar la causa raíz, requisitos adicionales de respuestas al riesgo y mejoras del proceso a los responsables de la toma de decisiones correspondientes. Asegurar que la causa, requisitos de respuesta y mejora del proceso se incluyan en los procesos de gobierno del riesgo.		5

Nota. Adaptado de ISACA, 2018.

10.4 Anexo IV Proceso de gestión de riesgos ISO 27005



Nota. Adaptado de Asociación Española de Normalización, 2024.

11 Glosario

TFG	Trabajo Final de Graduación
TI	Tecnologías de Información
TIC	Tecnologías de Información y Comunicación
COBIT	*Control Objectives for Information and Related Technologies* (Objetivos de Control para Información y Tecnologías Relacionadas)
ITIL	*Information Technology Infrastructure Library* (Biblioteca de Infraestructura de Tecnologías de Información)
ISO	*International Organization for Standardization* (Organización Internacional de Normalización)
NIST	*National Institute of Standards and Technology* (Instituto Nacional de Estándares y Tecnología)
MICITT	Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones
BPM	*Business Process Management* (Gestión de Procesos de Negocio)
BPMN	*Business Process Model and Notation* (Modelo y Notación de Procesos de Negocio)
SVS	*Service Value System* (Sistema de Valor del Servicio)
SGSI	Sistema De Gestión De Seguridad De La Información