UNIVERSIDAD TÉCNICA DE AMBATO

CENTRO DE POSGRADOS

PROGRAMA DE MAESTRÍA EN TECNOLOGÍAS DE LA INFORMACIÓN MENCIÓN SEGURIDAD DE REDES Y COMUNICACIONES
COHORTE 2021

Tema: GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN A TRAVÉS DE NORMAS INTERNACIONALES EN LA EMPRESA PÚBLICA MANCOMUNIDAD DE TRÁNSITO DE TUNGURAHUA

Trabajo de titulación, previo a la obtención del Título de Cuarto Nivel de Magíster en Tecnologías de la Información Mención Seguridad de Redes y Comunicaciones

Modalidad del Trabajo de Titulación: Proyecto de Titulación con Componente de Investigación Aplicada

Autor: Ingeniero Lenin Alexis Aguirre Sánchez

Director: Ingeniero Ángel Gabriel Jaramillo Alcázar, Magister

Ambato – Ecuador

2023

A la Unidad Académica de Titulación del Centro de Posgrados

El Tribunal receptor del Trabajo de Titulación, presidido por la Ingeniera Adriana Priscila Paredes Bermeo, Magister, Delegada por el Ingeniero Héctor Fernando Gómez Alvarado, PhD. Director del Centro de Posgrados e integrado por los señores: *Ingeniero, Walter Fernando Gaibor Naranjo, Magister; Ingeniero, Iván Patricio Ortíz Garcés, Magister*, designados por la Unidad Académica de Titulación del Centro de Posgrados de la Universidad Técnica de Ambato, para receptar el Trabajo de Titulación con el tema: *"Gestión de riesgos de seguridad de la información a través de normas internacionales en la empresa pública Mancomunidad de Tránsito de Tungurahua"* elaborado y presentado por el señor Ingeniero, Lenín Alexis Aguirre Sánchez, para optar por el Titulo de cuarto nivel de Magíster en Tecnologías de la Información Mención Seguridad de Redes y Comunicaciones; una vez escuchada la defensa oral del Trabajo de Titulación, el Tribunal aprueba y remite el trabajo para uso y custodia en las bibliotecas de la UTA.

Ing. Adriana Priscila Paredes Bermeo, Mgtr.

Presidente y Miembro del Tribunal

Ing. Walter Fernando Gaibor Naranjo Mgtr.

Miembro del Tribunal

Ing. Iván Patricio Ortíz Garcés Mgtr.

Miembro del Tribunal

AUTORÍA DEL TRABAJO DE TITULACIÓN

La responsabilidad de las opiniones, comentarios y críticas emitidas en el Trabajo de Titulación presentado con el tema: Gestión de riesgos de seguridad de la información a través de normas internacionales en la empresa pública Mancomunidad de Tránsito de Tungurahua, le corresponde exclusivamente a: Ing. Lenín Alexis Aguirre Sánchez, Autor bajo la Dirección de Ing. Ángel Gabriel Jaramillo Alcázar Mgtr., Director del Trabajo de Titulación, y el patrimonio intelectual a la Universidad Técnica de Ambato.

Ingeniero Lenín Alexis Aguirre Sánchez
c.c.: 1719982256
AUTOR

Ingeniero Ángel Gabriel Jaramillo Alcázar Magister
c.c.: 1715891964
DIRECTOR

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato, para que el Trabajo de Titulación, sirva como un documento disponible para su lectura, consulta y procesos de investigación, según las normas de la Institución.

Cedo los Derechos de mi trabajo, con fines de difusión pública, además apruebo la reproducción de este, dentro de las regulaciones de la Universidad.

Ingeniero Lenín Alexis Aguirre Sánchez
c.c.:1719982256

ÍNDICE GENERAL DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

AGRADECIMIENTO

Quiero expresar un agradecimiento especial a dos pilares fundamentales en mi vida: mis padres, Marcia y Víctor. Su ejemplo de trabajo duro y dedicación ha sido una inspiración constante que ha fomentado mi ambición de progresar en todas las facetas de mi vida.

Agradezco también a mi hermano, Fabián, quien ha sido un compañero incondicional en este emocionante viaje de aprendizaje, compartiendo alegrías y desafíos a lo largo del camino.

No puedo pasar por alto mencionar mi profundo agradecimiento a la Universidad Técnica de Ambato por su compromiso con la excelencia académica. Agradezco a los docentes por su apoyo inquebrantable y orientación durante mi tiempo en la institución, su dedicación ha sido clave en mi formación.

Por último, quiero extender mi gratitud a todos los amigos que tuve el privilegio de conocer durante esta apasionante etapa de mi vida. Su compañía y amistad han enriquecido mi experiencia en la universidad y han dejado una huella imborrable en mi corazón.

Lenín Aguirre

DEDICATORIA

Con profundo cariño, dedico estas palabras a todas las personas que me han apoyado incondicionalmente en cada momento, pero sobre todo a mis queridos padres y hermano, cuyo amor y aliento han sido mi fortaleza.

A la entrañable memoria de mis abuelos, seres maravillosos que han dejado una huella imborrable en mi vida, transmitiéndome valiosas experiencias, invaluables valores y sabios consejos que guían mi camino.

Adicionalmente, quiero expresar mi más sincero agradecimiento a mi esposa Gisella, quien ha sido un pilar fundamental durante este tiempo de estudios, brindándome un amor incondicional y una comprensión que me ha impulsado a alcanzar mis metas.

Lenín Aguirre

UNIVERSIDAD TÉCNICA DE AMBATO
CENTRO DE POSGRADOS
PROGRAMA DE MAESTRÍA EN TECNOLOGÍAS DE LA INFORMACIÓN
COHORTE 2021

TEMA:

GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN A TRAVÉS DE NORMAS INTERNACIONALES EN LA EMPRESA PÚBLICA MANCOMUNIDAD DE TRÁNSITO DE TUNGURAHUA

MODALIDAD DE TITULACIÓN: *Proyecto de Titulación con Componente de Investigación Aplicada*
AUTOR: *Ingeniero Lenín Alexis Aguirre Sánchez*
DIRECTOR: *Ingeniero Ángel Gabriel Jaramillo Alcázar Magister*
FECHA: *Diecisiete de octubre de dos mil veintitrés*

RESUMEN EJECUTIVO

En la nueva era digital la seguridad de la información cumple un papel muy importante al proteger el activo más valioso para cualquier empresa, es decir, su información. Hoy en día la globalización ha facilitado a las empresas extender sus negocios y abrir nuevos mercados, pero al mismo tiempo han abierto las puertas para que la privacidad de la información y datos se vea vulnerada con la probabilidad de que caiga en manos equivocadas (Romero et al., 2018). También se tiene que resaltar que las amenazas programadas coexisten con otras amenazas latentes como fallas eléctricas o errores humanos e incluso desastres naturales, en consecuencia, la empresa pública Mancomunidad de Tránsito de Tungurahua necesita controlar y salvaguardar todos los datos de sus usuarios, asegurando que los mismos no se pierdan o salgan del sistema, debido a que son indispensables para la circulación del transporte terrestre y pueden ser objetivos de falsificaciones.

La investigación busca construir un conjunto de medidas y procedimientos, tanto técnicos como humanos, los cuales permitirán diseñar un plan completo de gestión de riesgos para operar de manera adecuada la seguridad de la información de la empresa a través de normas internacionales.

La metodología implementada en el presente estudio se adhiere a un enfoque cuantitativo y se basa en una investigación de naturaleza aplicada, de campo y explicativa.

Al desarrollar la correcta identificación de riesgos y posteriormente su análisis, se logra reconocer, monitorizar y planificar el riesgo dentro de la Empresa Pública Mancomunidad de Tránsito de Tungurahua. Así pues, se diseña una estrategia donde se define cómo prevenir, controlar, mitigar y superar los riesgos, respaldando los conceptos generales especificados en normas internacionales y ofreciendo directrices para la gestión de los riesgos para la seguridad de la información.

DESCRIPTORES: *AMENAZAS, GESTIÓN, INFORMACIÓN, ISO/IEC 27000, MAGERIT, RIESGO, SEGURIDAD.*

CAPÍTULO I
EL PROBLEMA DE INVESTIGACIÓN

1.1 Introducción

En un mundo sin fronteras potenciado por la aparición del internet y las telecomunicaciones, donde juntos se han establecido como el pilar fundamental para el desarrollo de todas las actividades humanas es inevitable verse expuesto a las amenazas informáticas que ponen en un gran riesgo a la información. Además, se deben considerar otras amenazas de caso fortuito o fuerza mayor como los desastres naturales, falta de suministro de energía eléctrica, robo, fallas de hardware o software y errores humanos que de igual manera ponen en peligro los datos de cualquier organismo (Valencia y Orozco, 2017).

La seguridad de la información no se soluciona únicamente a través de hardware o software, eventualmente las amenazas superarán a la tecnología. Las empresas alrededor del mundo han empezado a equilibrar sus prioridades e inversiones debido a que tecnología se deprecia y se vuelve obsoleta, mientras que la gente aprende y se adapta, por ende, el mejor mecanismo de defensa es un programa de actividades que ponga en práctica estrategias y metodologías que permitan reducir el riesgo, poniendo énfasis en crear una cultura donde la seguridad de la información es responsabilidad de todos.

El Ecuador dispone de algunos organismos que emiten políticas y planes generales de seguridad de la información, definen buenas prácticas, procesos y procedimientos; y, realizan el seguimiento y evaluación de implementaciones que aseguran una permanente protección y salvaguarda de la información. Los principales órganos rectores del desarrollo de las TICs en nuestro país son el ARCOTEL, Agencia de Regulación y Control de las Telecomunicaciones del Ecuador; EcuCERT, Centro de Respuesta a Incidentes Informáticos; MINTEL, Ministerio de Telecomunicaciones y la Sociedad de la Información; y el INEN, Instituto Ecuatoriano de Normalización, que es el organismo el cual definió la norma técnica ecuatoriana NTE INEN-ISO/IEC 27001, siendo un acoplamiento de la Norma Internacional ISO/IEC 27001:2013, Information technology — Security techniques — Information security management

systems — Requirements. Los procesos instituidos en este estándar son generales y se aplican a cualquier tipo de organización, independientemente de su tamaño o naturaleza (Terán, 2018).

En el contexto del caso de estudio planteado, el objetivo es la creación de un plan de gestión de riesgos utilizando metodologías y normas internacionales, las cuales ofrecen métodos que permiten analizar y evaluar las vulnerabilidades, amenazas y riesgos.

El desarrollo de la investigación es presentado en cinco capítulos, como se explica a continuación:

El CAPÍTULO I, EL PROBLEMA DE INVESTIGACIÓN, establece el tema, describe la formulación del problema, estado actual, la estrategia empleada, principales limitaciones, justificación y objetivos.

El CAPÍTULO II, ANTECEDENTES INVESTIGATIVOS, presenta los antecedentes de investigación tomando en cuenta estudios anteriores donde están plasmados los conocimientos empleados.

El CAPÍTULO III, MARCO METODOLÓGICO, detalla la ubicación de la investigación, los recursos utilizados, el tipo de investigación, la hipótesis, su población, la recolección y procesamiento de la información.

El CAPÍTULO IV, RESULTADOS Y DISCUSIÓN, evidencia el análisis de los resultados alcanzados junto con su respectiva explicación y discusión.

El CAPÍTULO V, CONCLUSIONES, RECOMENDACIONES, BIBLIOGRAFÍA Y ANEXOS, desarrolla las conclusiones obtenidas en el desenvolvimiento de la investigación y las sugerencias relacionadas con su culminación, además, se muestra la bibliografía y los respectivos anexos.

El CAPÍTULO VI, PROPUESTA, documenta el desarrollo de la gestión de riesgos de la de la seguridad de la información propuesto para la Empresa Pública Mancomunidad de Tránsito de Tungurahua.

Durante el proceso de investigación, se presentaron limitaciones con la recopilación de datos, ya que el enfoque se basó en encuestas de tipo cuantitativo. Aunque las encuestas son una valiosa herramienta para obtener información estadística y cuantificable, es importante reconocer que pueden estar sujetas a sesgos y errores de interpretación por parte de los encuestados. A pesar de estas limitaciones, se procuró minimizar los posibles sesgos mediante un diseño cuidadoso de las preguntas y una selección representativa de la muestra.

1.2 Justificación

La Empresa Pública Mancomunidad de Tránsito de Tungurahua gestiona, planifica, regula y controla el tránsito, trasporte terrestre y la seguridad vial en los cantones de Baños de Agua Santa, Cevallos, Mocha, Santiago de Quero, San Pedro de Pelileo, Santiago de Píllaro, San Cristóbal de Patate, y Tisaleo, además brinda servicios de matriculación y revisión vehicular.

Para garantizar un ambiente ordenado y seguro en la movilidad motorizada, la empresa emplea equipos informáticos que contienen la información privada de miles de usuarios que manejan un transporte móvil y los mismos son indispensables para la seguridad vial de todas las personas en los cantones descritos.

Por tanto, se propone la creación de un plan de gestión de riesgos con el objetivo de asegurar tanto la protección de la información como la seguridad del transporte terrestre y la circulación vial en la zona territorial de los Gobiernos Autónomos Descentralizados (GAD) Municipales de la Provincia de Tungurahua.

El proyecto cuenta con el apoyo económico y técnico de la empresa, además tanto el acceso físico a las instalaciones como el acceso a los procesos e información privada están garantizados.

En esta perspectiva, la gestión de riesgos involucra una evaluación de los posibles eventos y sus potenciales consecuencias, previo a tomar decisiones sobre las acciones a emprender y el momento oportuno para llevarlas a cabo, todo con el propósito de reducir el riesgo a un nivel considerado aceptable. No existen mecanismos que permitan eliminarlos completamente, por lo que es necesario gestionarlos de una manera adecuada y establecer controles para mitigarlos.

Los resultados de la investigación serán descritos en un plan documentado donde consten las políticas, procedimientos y estrategias necesarias para asegurar la protección de la información de la empresa EPMTT.

1.3 Objetivos

1.3.1 General

Diseñar un plan de gestión de riesgos con sus respectivos procedimientos y políticas basadas en normas internacionales, mediante el análisis y evaluación de vulnerabilidades, amenazas y riesgos de la empresa.

1.3.2 Específicos

a. Identificar el estado de los activos que manejan la información crítica en la empresa.
b. Analizar potenciales vulnerabilidades y amenazas que puedan causar pérdida de la información.
c. Realizar recomendaciones a la empresa con el fin de reducir el riesgo hasta un nivel aceptable.

CAPÍTULO II
ANTECEDENTES INVESTIGATIVOS

2.1 Estado del arte

La seguridad de la información se basa en la premisa de que los datos son un tesoro de inmenso valor, es decir, son los recursos más importantes de una empresa, debido a que son responsables de conectar todas las áreas del negocio, unificar procesos y conducir la productividad. Si se manejan de manera incorrecta, pueden tener consecuencias nefastas para gobiernos, empresas e incluso personas. Su adecuada gestión evita las pérdidas económicas, la vulnerabilidad ante la competencia, el robo de información y mejora la confianza con los clientes, la seguridad personal, la competencia empresarial y la toma de decisiones.

En 2020, a partir de la COVID-19 los incidentes con la seguridad de la información se intensificaron, los atacantes se aprovecharon de la incertidumbre provocados por la inestabilidad socioeconómica y el despliegue de nuevas redes y sistemas por parte de las empresas para implementar el teletrabajo. Con este aumento de vulnerabilidades, empresas ecuatorianas tanto privadas y públicas como: Banco del Pichincha, CNT y ANT; vieron comprometida su información. Por tal motivo, la Empresa Pública Mancomunidad de Tránsito de Tungurahua al ser un objetivo de ciberataques, se ve en la obligación de asegurar sus datos y uno de los primeros pasos es gestionar los riesgos de la seguridad de la información.

Ramos et al. (2017), en su reporte sobre política de seguridad de la información en la Institución Universitaria Colegio Mayor del Cauca y en la Cooperativa Codelcauca, describen la implementación de los estándares de la norma NTC ISO/IEC 27002:2013, teniendo en cuenta los criterios para la gestión de activos, control de acceso, seguridad física y ambiental. En su informe determinan que luego de la intervención del estudio los indicadores de conocimiento relacionados con la seguridad se han desarrollado hasta un nivel aceptable.

Tejena (2018), en su proyecto de investigación, estudia cinco metodologías de análisis de riesgos (OCTAVE, MEHARI, MAGERIT, CRAMM, EBIOS y NIST SP 800-30) con

el objetivo de identificar cuál es el sistema que proporciona una mejor oportunidad de toma de decisiones dentro de una organización. Concluyendo que MAGERIT resulta ser la opción más efectiva y completa que protege la información.

Crespo (2018), en su estudio sobre metodologías para la gestión de riesgos aplicada a MPYMEs en el Ecuador, analiza comparativamente varias metodologías como: Magerit, CRAMM, OCTAVE-S, Microsft Risk Guide, COBIT 5 y COSO III. Finaliza su investigación proponiendo una metodología propia que asimila las mejores cualidades y características para trabajar la gestión de riesgos.

Serrano et al. (2019), en su documento presenta un análisis de riesgos de TIC en el Hospital Básico de Catacocha del Ecuador, que, al ser una institución ligada al Estado, manejan información altamente sensible y confidencial. En su informe se concreta un Plan de Gestión que permite mitigar los riesgos identificados.

Finalmente, en su proyecto de investigación , Ferruzola y sus colaboradores (2019), examinan la metodología Magerit. El artículo expone cómo manejar la metodología y cómo utilizarla en el proceso de gobernabilidad de TI. El estudio concluye con la elaboración del plan de contingencia para equipos y sistemas informáticos.

2.2 Fundamentos y principios de seguridad

La seguridad informática y la seguridad de la información parecen ser lo mismo, pero cuentan con estrategias diferentes para abordar sus dificultades; No obstante, ambos están intrínsecamente relacionadas y es necesario diferenciarlos y explorar detalladamente otros fundamentos asociados a estos temas.

2.2.1 Seguridad informática

La seguridad informática o también conocida como seguridad de tecnologías de la información y comunicación se define como las soluciones y medidas técnicas que se encargan de la parte operativa de la seguridad. Tiene como objetivos preservar las redes e infraestructura de TI, asegurar los recursos informáticos y proteger la información en formato digital que éstos almacenan, es decir, la seguridad informática tiene un

enfoque técnico que protege el hardware y el software empleados por una organización (Valencia & Orozco, 2017).

2.2.2 Seguridad de la información

La seguridad de la información constituye la estrategia central de la seguridad, y va mucho más allá de la seguridad informática, ya que no es exclusivamente un tema técnico. Requiere abordar todas las áreas de seguridad con el propósito de salvaguardar los activos de información, independientemente de su forma o estado. Esto implica la utilización de metodologías, normativas, políticas, estructuras organizativas, planificación, gestión, técnicas, herramientas y tecnología. Además, es fundamental considerar a los individuos, los procesos y las funciones del negocio en un contexto de responsabilidad compartida. Además, se encarga de garantizar la confidencialidad, integridad y disponibilidad de la información analizando y evaluando el impacto de la totalidad de las vulnerabilidades, amenazas y riesgos a la que está expuesta la información con la finalidad de mitigarlos y reducirlos hasta un nivel aceptable (Figueroa et al., 2018).

2.2.3 Confidencialidad

Asegura que personas, entidades, sistemas o procesos no autorizados puedan acceder a la información, evitando que ésta sea divulgada, comunicada, robada o saboteada (Monges & Jimenez, 2020).

2.2.4 Integridad

Certifica que la totalidad del contenido de la información es confiable y exacta, es decir, que permanece inalterado y cualquier modificación no autorizada es evitada (Monges & Jimenez, 2020).

2.2.5 Disponibilidad

Garantiza el acceso confiable y oportuno a la información y que los recursos relacionados estén utilizables en cualquier momento que sean requeridos (Siñani, 2021).

2.2.6 Vulnerabilidad

Las vulnerabilidades son una debilidad en la tecnología o en los procesos relacionados con la información, y como tal, se consideran características propias de los sistemas de información o de la infraestructura que la contiene (Rea et al., 2018).

2.2.7 Amenaza

Es cualquier situación o evento potencial que está asociado a la explotación de una vulnerabilidad y que podría afectar la capacidad de una organización o individuo para realizar actividades que afectan directamente a la información o a los sistemas que la manejan (Rea et al., 2018).

2.2.8 Ataque

Es un acto delictivo y malicioso que se realiza con el objetivo de obtener acceso a información privada para posteriormente robarla, eliminarla o inhabilitarla.

2.2.9 Riesgo

El riesgo de información ocurre cuando dos factores convergen: amenazas y vulnerabilidades. En otros términos, el riesgo es la combinación de probabilidades de que un evento explote una debilidad causando pérdidas o daños en un activo de información (Ortiz & Vizñay, 2019).

2.2.10 Política de seguridad

Una política de seguridad es una declaración escrita que definen los compromisos y protocolos que establecen cómo una organización debe proteger sus activos de información. Sin una política, las prácticas de seguridad se desarrollarán sin objetivos y responsabilidades claramente definidos. Las políticas de seguridad de la información necesitan tener un enfoque múltiple que se valgan de personas, procesos y tecnología al mismo tiempo (Yupanqui y Oré, 2017).

2.2.11 Gestión del riesgo

Se define como los procesos y actividades coordinadas de una organización para dirigir y controlar el riesgo con el objetivo de garantizar la protección de su información (Néstor & Morales, 2019). La gestión tiene como propósito identificar, analizar, valorar y evaluar los riesgos con el fin de cuantificar y calificar sus impactos o medir las probabilidades de pérdidas y efectos secundarios que se desprenden de las vulnerabilidades y amenazas; para finalmente tratar, aceptar, mitigar, transferir y evadir el riesgo.

2.3 Marcos de referencia, estándares, metodologías y mejores prácticas de seguridad

Existen varios marcos, estándares y métodos reconocidos a nivel internacional que tratan el tema de gestión de riesgos de la seguridad de la información, algunos de los más tratados son los marcos de trabajo de la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC), así como el Instituto Nacional de Estándares y Tecnología de EE. UU. (NIST), entre otros.

La Tabla 2.1 presenta un resumen comparativo entre estas normas.

Tabla 2.1 Resumen comparativo entre normas internacionales

Norma	Título	Características	Observación
ISO/IEC 27000 SERIES	Conjunto de estándares de seguridad de la información	La serie ISO 27000 proporciona una guía general de mejores prácticas para el sistema de gestión de seguridad de la información. El marco alienta a las organizaciones primero a evaluar sus riesgos de TI y luego implementar los controles apropiados de acuerdo con sus necesidades. Incorpora retroalimentación continua y actividades de mejora para abordar el panorama actual de amenazas o tener en cuenta los incidentes de seguridad.	El estándar no se fundamenta en una metodología específica de gestión de riesgos, sino en un proceso constante de secuencias organizadas de acciones. La serie ISO 27000 está diseñada para ser utilizada por cualquier organización, sim importar su giro de negocio o tamaño (Aminzade, 2018).
ISO/IEC 27001	Tecnologías de la información - Técnicas de seguridad - Sistemas de gestión de la seguridad de la información - Requisitos	La norma ISO/IEC 27001 describe los conceptos y principios de la tecnología de información y comunicación. Además, proporciona un marco de métodos y procesos para identificar y especificar todos los aspectos para mejorar la preparación de las TIC de una empresa para asegurar la continuidad de negocio (Barafort et al., 2019).	La norma ISO 27001 ayuda a establecer y facilita los requerimientos de un SGSI.
ISO/IEC 27005	Gestión de riesgos de seguridad de la información	La norma ISO/IEC 27005 es el estándar internacional que brinda las pautas y orientación sobre la gestión de riesgos de seguridad de la información en las empresas, apoyando específicamente los requisitos de un Sistema de Gestión de Seguridad de la Información conforme a los establecido en la norma ISO/IEC 27001 (Barafort et al., 2019).	Presenta un enfoque específico para la gestión del riesgo centrado en la tecnología de la información proporcionando una guía clara y detallada.

ISO 31000	Gestión del riesgo	La norma ISO 31000 es una herramienta que establece un conjunto de reglas para implementar un sistema de gestión de riesgos en una empresa.	La norma ISO 31000 puede servir como una referencia o punto de comparación para otras normativas relacionadas con la gestión de riesgos (Barafort et al., 2019).
NIST SP 800-30	Guía para realizar evaluaciones de riesgos	Es un estándar formulado por NIST, se especializa en la evaluación de riesgos en los sistemas de TI y busca proporciona una guía para la seguridad de las infraestructuras desde una perspectiva técnica (Tejena, 2018).	Proporciona una base sólida para el desarrollo de la gestión del riesgo en la empresa, así como información relevante acerca de los controles de seguridad que puedan ser aplicados en función de la rentabilidad del negocio.
COBIT	COBIT 5 (Objetivos de control para la información y tecnologías relacionadas) y COBIT 2019 (Objetivos de gobierno y gestión)	Para las organizaciones particularmente preocupadas por el tiempo de actividad operativa, otra opción fuerte es COBIT 5 y COBIT 2019. El marco empresarial COBIT, creado por la Asociación de Auditoría y Control de Sistemas de Información (ISACA), está destinado a la gobernanza y la gestión de la tecnología de la información empresarial de extremo a extremo en todo el negocio.	El marco se compone de cinco subconjuntos, cada uno de los cuales cubre un dominio: auditoría y aseguramiento, gestión de riesgos, seguridad de la información, cumplimiento normativo y gobierno, y TI empresarial (Aminzade, 2018).
ITIL	Biblioteca de Infraestructura de Tecnología de la Información	Se ha creado este marco de referencia con la finalidad de abarcar la totalidad de la infraestructura de tecnología de la información, incluyendo su desarrollo, operaciones y su administración con el objetivo de elevar la calidad del servicio (Cedeño, 2018).	Es una guía sobre buenas prácticas de los procesos para la gestión de servicios de tecnología de la información.
MODELO COSO	Comité de Organizaciones Patrocinadoras de la Comisión de Normas	El modelo COSO tiene como propósito principal proporcionar a las entidades un modelo común que sirva como guía en aspectos clave de la gestión ejecutiva y de	Actualizado con el modelo COSO ERM 2017, lo que ha permitido una ampliación de la cobertura de los riesgos a

		gobierno, la ética empresarial, el control interno, la gestión del riesgo empresarial, la prevención del fraude y la presentación de informes financieros.	los que se enfrentan las organizaciones, mejorando así el alcance del marco integrado.
OCTAVE	Evaluación operativa crítica, de amenazas, de activos y de vulnerabilidad	Es un método que analiza e identifica los activos que necesitan ser protegidos dentro de la empresa y posteriormente determina porque son un riesgo y desarrolla soluciones con prácticas y tecnología.	Su estructura está diseñada para minimizar la exposición de las organizaciones a las amenazas y para predecir los resultados probables de los ataques y abordar los que tienen éxito (Pacheco et al., 2020).
MEHARI	Método armonizado de análisis de riesgos	Es un método que utiliza un modelo de evaluación de riesgos y módulos de componentes y procesos, esta técnica detecta vulnerabilidades utilizando auditoría y estudia situaciones de riesgo (García & Moreta, 2018).	Mehari proporciona un marco de trabajo para la gestión continua de la seguridad de la información, ayudando a las organizaciones a mantener un enfoque proactivo en la identificación y tratamiento de riesgos.
CRAMM	Análisis de Riesgos y método de gestión	Es una metodología orientada a garantizar la confidencialidad, integridad y disponibilidad de los sistemas y activos de las empresas (López, 2018).	La metodología comprende tres etapas principales: En la primera etapa se definen los objetivos generales de seguridad. En la segunda etapa, se lleva a cabo el análisis de riesgos. Finalmente, en la tercera etapa se identifican y seleccionan las medidas de seguridad.
MAGERIT	Metodología de análisis y gestión de riesgos de los sistemas de información	Es un método sistemático que se basa en analizar el impacto que puede tener la empresa en la violación de la seguridad, identificando amenazas y vulnerabilidades; posteriormente se plantea medidas preventivas y correctivas que sean más convenientes (Caballero & Kuna, 2018).	Compuesta por 3 libros. Método, describe las tareas necesarias para llevar a cabo proyectos de análisis y gestión de riesgos, proporcionando una guía práctica y consejos.

	Catálogo de elementos, contiene una categorización de activos, criterios para valoración de activos, un catálogo de amenazas y medidas. Guía de Técnicas, proporciona diversas técnicas para el análisis de riesgos, tales como algoritmos de análisis, árboles de ataque, análisis coste-beneficio, diagramas de flujo, tablas de procesos, entre otras herramientas como el software PILAR.

Fuente: Elaboración propia

2.3.1 Alineación de los procesos de gestión de riesgos entre las principales normas internacionales

Una vez realizada la comparación entre las normas internacionales, se obtuvo una visión general de sus objetivos y beneficios. No obstante, con el fin de explorar en mayor profundidad el tema y examinar las semejanzas en los procedimientos de gestión de riesgos entre las normativas más vinculadas, se ha contemplado realizar la armonización en el contexto de este proyecto. Para este fin, se tomaron en cuenta los estándares internacionales ISO/IEC 27001, ISO/IEC 27005, ISO 31000, y los modelos de referencia COSO ERM, CRAMM y MAGERIT, identificando así los procesos comunes existentes. Estos estándares, ampliamente utilizados por las empresas, se centran en el estudio de la gestión de riesgos, lo que permite establecer una mejor relación y comprensión de su interconexión.

Tabla 2.2 Alineación de las normas ISO/IEC 27005, ISO/IEC 27005, ISO 31000, COSO ERM, CRAMM y MAGERIT en sus procesos

PROCESO	ISO/IEC 27001	ISO/IEC 27005	ISO 31000	COSO ERM	CRAMM	MAGERIT
1.	**Recogida y preparación de la información**	**Establecimiento del contexto**	**Establecer el contexto:** • Estratégico • Organizacional • Gestión • Criterio • Estructura	**Medio ambiente interno** **Establecimiento de objetivos**	**Definición del alcance**	**Establecimiento del contexto:** • Contexto de la organización • Alcance y límites
2.	**Análisis y evaluación de riesgos:** • Identificación, clasificación y valoración de los grupos de activos • Identificación y clasificación de amenazas • Identificación y estimación de vulnerabilidades • Identificación y valoración de impactos • Evaluación, análisis y sus consecuencias	**Evaluación del riesgo:** • Identificación del riesgo • Estimación del riesgo	**Identificar Riesgos** **Analizar Riesgos:** • Determinar los controles existentes • Determinar la probabilidad • Determinar las consecuencias • Calcular nivel del riesgo **Evaluar Riesgos** • Comparar contra criterios • Establecer prioridades de riesgo	**Identificación de eventos** **Evaluación de riesgos**	**Análisis del riesgo:** • Identificación de bienes • Evaluación de los activos físicos y software • Determinación del valor de los datos • Identificación de amenazas • Identificación de vulnerabilidades • Cálculo de riesgos	**Valoración del riesgo:** • Identificación de activos • Valoración de criticidad • Identificación de amenazas • Identificación de vulnerabilidades • Valoración del impacto • Evaluación del riesgo • Salvaguardas y controles existentes

	Implementación de controles: • Políticas de seguridad de la información • Controles operacionales	**Implementar el plan de tratamiento del riesgo**	**Tratar los riesgos** **Identificar, evaluar y seleccionar opciones:** • Supresión • Transferencia • Mitigación • Explotación	**Respuesta a los riesgos** **Actividades de control**	**Gestión del riesgo:** • Contramedidas • Ejecución • Auditoría	**Tratamiento del riesgo:** • Evitación • Mitigación • Compartición • Financiación
3.	**Definición del plan de tratamiento de los riesgos o esquema de mejora:** • Eliminar el riesgo • Mitigarlo • Trasladarlo		**Preparar planes de tratamiento** **Implementar planes**			**Documentación de resultados** **Auditorías:** • Internas • Externas
4.		**Aceptación del riesgo**	**Aceptación del riesgo**			**Aceptación del riesgo**
5.		**Monitoreo y revisión del riesgo**	**Monitoreo y revisión**	**Supervisión**		**Seguimiento y revisión**
6.		**Comunicación del riesgo**	**Comunicación y consulta**	**Información y comunicación**		**Comunicación y consulta**

Fuente: Elaboración propia

Una vez analizada la relación que existe entre los estándares internacionales de gestión de riesgos, como se muestra en la Tabla 2.2, se puede deducir que los estándares y modelos evaluados son en realidad complementarios entre sí e idealmente deben ser trabajados en conjunto, ya que la mayoría de sus procesos se acoplan de forma integral.

Es fundamental la aplicación de la metodología MAGERIT, ya que se vincula con los estándares ISO/IEC 27001, ISO/IEC 27005 e ISO 31000 pero estos no ofrecen una metodología específica y los métodos de COSO ERM y CRAMM no abarcan la totalidad de los procedimientos requeridos para administrar los riesgos. MAGERIT se destaca por cumplir con todos los procesos establecidos y por contar con pasos metódicos concretos y delimitados; sin embargo, para una gestión de riesgos más completa, es necesario complementarla con los estándares ISO/IEC 27001, ISO/IEC 27005 e ISO 31000, ya que proporcionan un soporte particular para este propósito. Al combinar estas metodologías, se logra una visión más holística y efectiva para abordar los desafíos de seguridad de la información y gestionar los riesgos de manera más completa y eficiente.

2.3.2 Metodología MAGERIT

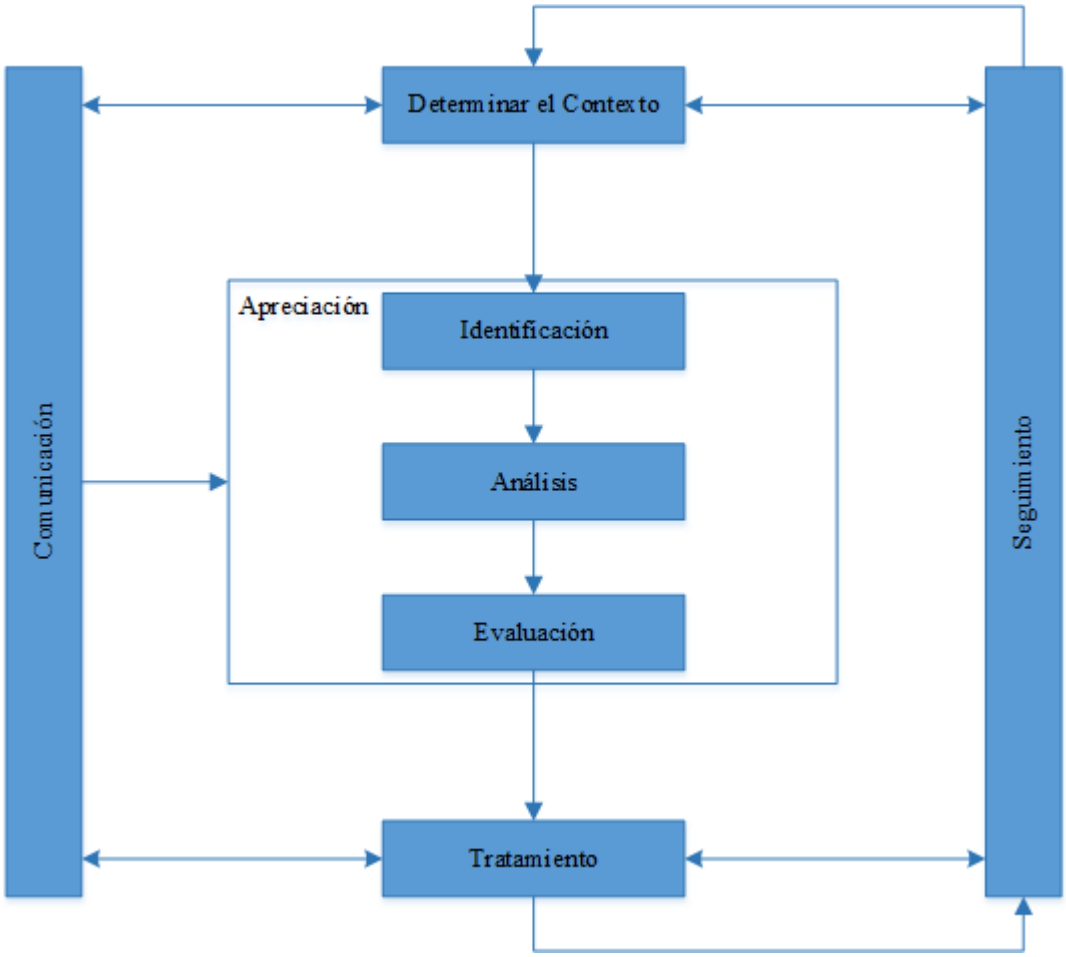
MAGERIT sigue un enfoque sistemático que evita la improvisación y no depende de la subjetividad del analista. Entre sus metas se encuentran sensibilizar a los líderes de las empresas acerca de los peligros y la importancia de gestionarlos, ofreciendo un enfoque sistemático para evaluar los riesgos relacionados con la utilización de tecnologías de la información y comunicación. Ayuda a planificar la gestión para mantener los riesgos bajo control y preparar a la organización para evaluaciones, auditorías, certificaciones o acreditaciones. Además, MAGERIT busca establecer una uniformidad en los informes que documentan los hallazgos y las conclusiones de las actividades de análisis y gestión de riesgos.

2.3.2.1 Proceso de gestión del riesgo de la seguridad de la información con MAGERIT

El proceso de gestión de riesgos utiliza un enfoque iterativo para todas sus actividades, lo que permite aumentar la profundidad y el nivel de detalle en la evaluación de cada

paso, alcanzando una adecuada armonía entre la reducción del tiempo y los recursos requeridos para identificar los controles, y asegurando que la evaluación de riesgos sea eficaz. La Figura 2.1 detalla los pasos de las actividades en el proceso de gestión de riesgos según las directrices establecidas en MAGERIT.

Figura 2.1 Proceso de gestión del riesgo

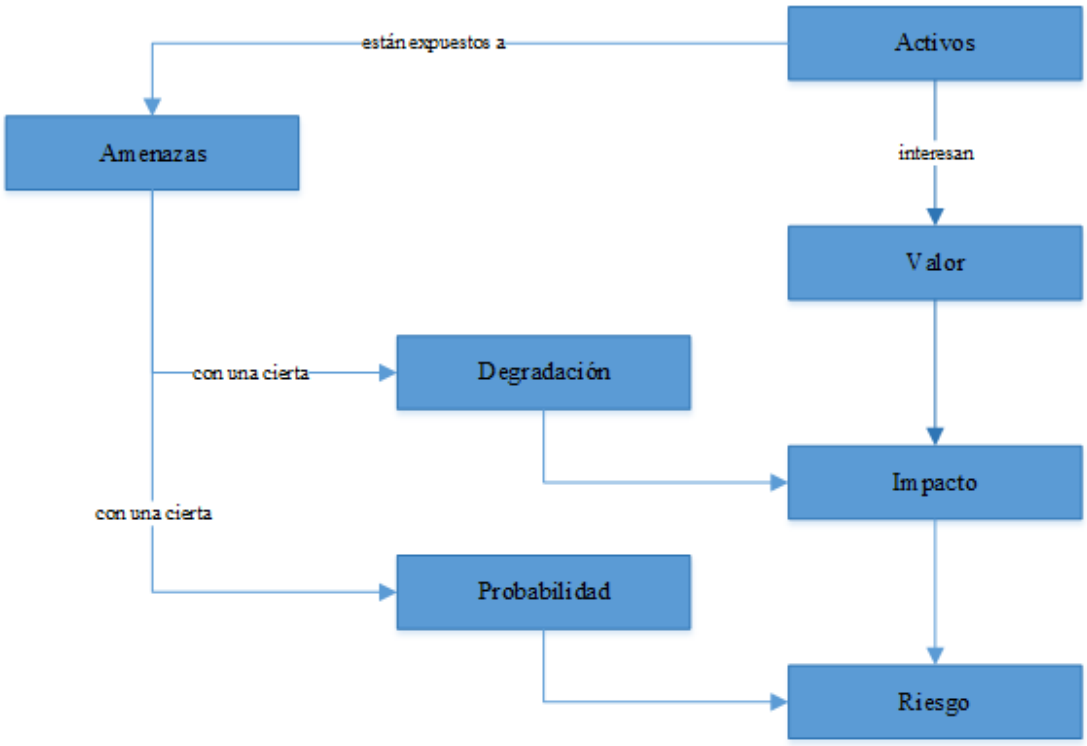


Fuente: Adaptado de MAGERIT v3

2.3.2.2 Análisis y evaluación del riesgo

La Figura 2.2 muestra una representación visual del proceso de análisis de riesgos, detallando las diferentes etapas que lo conforman. Este enfoque sigue una metodología sistemática que facilita la identificación del riesgo a través de una serie de pasos predefinidos conocidos como etapas de evaluación de riesgos.

Figura 2.2 Elementos del análisis y evaluación de riesgos



Fuente: Adaptado de MAGERIT v3

2.3.2.3 Amenazas

En la Tabla 2.3, se describen los tipos de amenazas que existen y que pueden vulnerar los activos de una empresa.

Tabla 2.3 Amenazas

Tipo de amenaza	Amenaza
De origen natural (accidentes naturales)	Terremoto
	Erupción
	Corrimiento de tierras
Del entorno (de origen industrial)	Fuego
	Daños por agua
	Contaminación mecánica (vibraciones, polvo, suciedad)
	Explosiones
	Accidentes de tráfico
	Avería de origen físico o lógico

	Fallos eléctricos (Corte del suministro eléctrico)
	Condiciones inadecuadas de temperatura o humedad (excesivo calor, excesivo frío, exceso de humedad)
	Fallo de servicios de comunicaciones
Errores y fallos no intencionados	Errores de los usuarios
	Errores del administrador
	Errores de monitorización
	Errores de configuración
	Difusión de software dañino (virus, gusanos, spyware, troyanos, ransomware, adware)
	Revelación de información
	Alteración accidental de la información
	Errores de mantenimiento / actualización de programas (software)
	Errores de mantenimiento / actualización de equipos (hardware)
	Caída del sistema por agotamiento de recursos
	Indisponibilidad del personal
Ataques intencionados	Manipulación de la configuración
	Suplantación de la identidad del usuario
	Abuso de privilegios de acceso
	Acceso no autorizado
	Difusión de software dañino (virus, gusanos, spyware, troyanos, ransomware, adware)
	Análisis de tráfico
	Spamming
	Phishing
	Botnets
	Ataques de red (DOS/DDOS)
	Ingeniería social
	Robo
Defectos de las aplicaciones	Vulnerabilidades de los programas (software)

Fuente: Adaptado de MAGERIT v3

2.3.2.4 Tratamiento del riesgo

La gestión de riesgos implica tomar decisiones en relación con los diversos riesgos presentes, en línea con la estrategia de la organización. Es necesario elegir medidas de

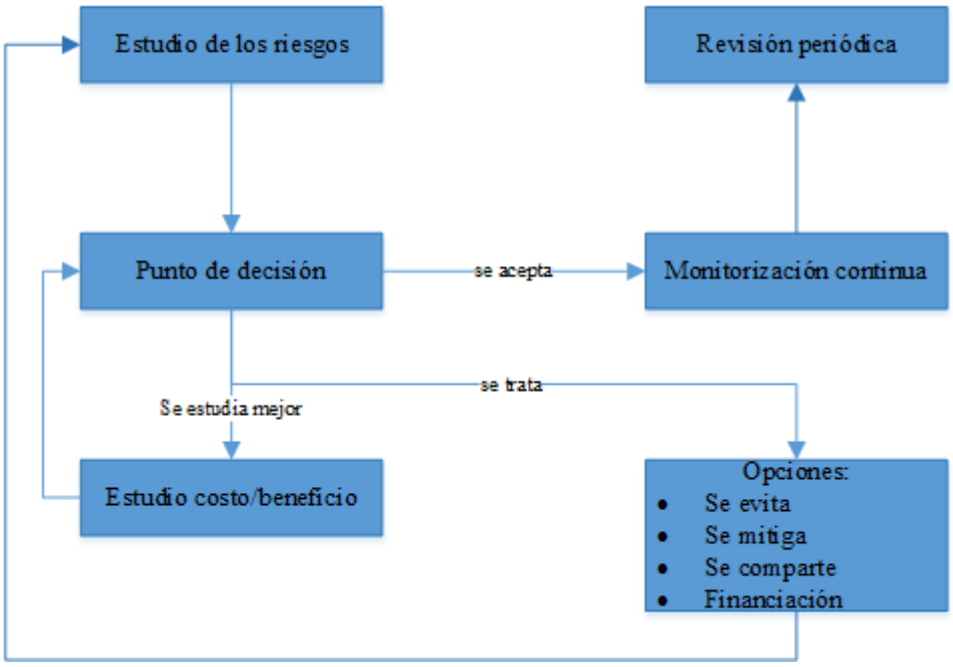
control para disminuir, aceptar, prevenir o transferir los riesgos, y establecer un plan para el manejo de estos.

Existen algunas opciones disponibles para el tratamiento del riesgo:

- Aceptación del riesgo
- Evitación del riesgo
- Mitigación del riesgo
- Compartición del riesgo
- Financiación

La Figura 2.3 ilustra la actividad del tratamiento del riesgo dentro de los procesos de la gestión del riesgo:

Figura 2.3 Decisiones de tratamiento de los riesgos



Fuente: Adaptado de MAGERIT v3

En el Capítulo VI, se amplía la explicación de cada proceso identificado, teniendo en cuenta la realidad específica de la EPMTT.

CAPÍTULO III
MARCO METODOLÓGICO

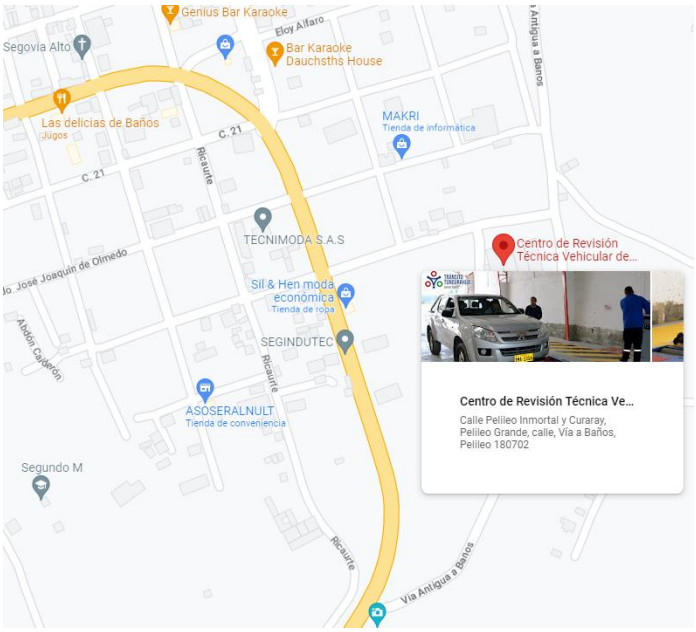
3.1 Ubicación

A continuación, se muestra la información general de empresa en donde se realizó la presente investigación.

- Nombre: Empresa Pública Mancomunidad de Tránsito de Tungurahua;
- Provincia: Tungurahua;
- Cantón: San Pedro de Pelileo;
- Dirección: Pelileo Inmortal y Curarary.

Su función principal implica la administración, planificación, regulación y control eficaces y eficientes del tráfico, el transporte por carretera y la seguridad vial en el área territorial de los Gobiernos Autónomos Descentralizados (GAD) Municipales de la Provincia de Tungurahua, que incluye los Cantones de Baños de Agua Santa, Cevallos, Mocha, Santiago de Quero, San Pedro de Pelileo, Santiago de Píllaro, San Cristóbal de Patate y Tisaleo.

Figura 3.1 Ubicación de la Empresa Pública Mancomunidad de Tránsito de Tungurahua.



3.2 Equipos y materiales

En la Tabla 3.1 se describe los equipos y materiales utilizados para el despliegue de la presente investigación.

Tabla 3.1 Equipos y materiales utilizados

Descripción	Unidad	Cantidad	Costo unitario (USD)	Costo total (USD)
Computador portátil	unidad	1	2.000,00	2.000,00
Software computacional Microsoft 365	unidad	1	59,99	59,99
Internet	horas	1000	0,05	50
Transporte	días	30	2,00	60,00
Presentación de la propuesta	unidad	1	100,00	100,00
			Costo total	**2.269,99**

Fuente: Elaboración propia

3.3 Tipo de investigación

La investigación implica el proceso de adquirir nuevos conocimientos con la aplicación de diversas técnicas y métodos que faciliten conocer el problema y así ampliar el desarrollo de su conocimiento en cualquier área de estudio permitiendo comprobar o descartar hipótesis (Fernández, 2020).

3.3.1 Investigación aplicada

Por el propósito de la investigación, porque se encamina en encontrar estrategias para lograr sus objetivos y ponerlos en práctica.

3.3.2 Investigación de campo

De acuerdo con los medios por los cuales se obtiene la información, es una investigación de campo, debido a que se apoya en encuestas (cuestionarios), observaciones (escalas de estimación, listas de chequeo) y entrevistas.

3.3.3 Investigación explicativa

Según su alcance, es de tipo explicativa, en vista de que la investigación busca expresar las causas o motivos que relacionan las variables, permitiendo así una comprensión más del fenómeno en cuestión.

3.3.4 Enfoque cuantitativo

Por la naturaleza de los datos, la investigación tiene un enfoque cuantitativo, debido a que se mide la realidad objetiva del fenómeno sirviéndose de variables numéricas y de análisis de datos, pero a su vez, también se centra en las acciones humanas. Además, se busca probar una hipótesis y las técnicas de recolección de datos son estandarizadas.

3.4 Hipótesis - pregunta científica – idea a defender

Las hipótesis son un supuesto, es decir son explicaciones tentativas del fenómeno investigado con las cuales se responde el planteamiento del problema y hacen referencia a los objetivos (Espinosa, 2018).

3.4.1 Hipótesis de investigación

Hi: "La implementación de una gestión de riesgos de seguridad de la información, acompañada de políticas adecuadas, procedimientos y controles en los procesos, contribuirá a prevenir, resguardar y proteger de manera efectiva la información de la Empresa Pública Mancomunidad de Tránsito de Tungurahua".

3.4.2 Hipótesis nula

Ho: "No existe una relación significativa entre la implementación de una gestión de riesgos de seguridad de la información, políticas adecuadas, procedimientos y controles en los procesos, y la prevención, resguardo y protección de la información de la Empresa Pública Mancomunidad de Tránsito de Tungurahua".

3.5 Población o muestra

Toda investigación debe ser vista como una búsqueda de datos apropiados que puedan resolver un determinado problema de conocimiento, adquiridos a través del conjunto de unidades que componen el universo en el que se desarrolla la investigación (Robles, 2019).

3.5.1 Población

La población considerada para la presente investigación está conformada por el personal de la empresa de todos los departamentos que tienen acceso a la información, en total 50 personas.

3.5.2 Muestra

Tomando en cuenta la población accesible, se ha decido realizar un muestreo probabilístico estratificado proporcional.

Tabla 3.2 Muestreo probabilístico estratificado proporcional

Tamaño de la población objetivo	50
Tamaño de la muestra que se desea obtener	10
Número de estratos a considerar	1

Estrato	Identificación	Nº sujetos en el estrato	Proporción	Muestra del estrato
1	Personal	50	1/5	10

Fuente: Elaboración propia

3.6 Recolección de información

La información recolectada es la materia prima que se utiliza para explorar los fenómenos del problema de investigación.

3.6.1 Técnicas e instrumentos

Se realizaron encuestas para recolectar la información del personal de la empresa por medio de cuestionarios destinados a obtener respuestas sobre el problema de investigación. Se realizaron tres cuestionarios, destinados al grupo directivo, administrativo y técnico; y cada uno contaba con una escala de Likert de 5 puntos.

Se empleó la observación para obtener datos de los activos de información con ayuda de escalas de estimación y listas de chequeo.

Se utilizó la entrevista para recabar información sobre los servicios de TI y procesos de negocio.

3.6.2 Confiabilidad

Se llevó a cabo la verificación de la confiabilidad de las herramientas de recopilación de información a través de encuentros con profesionales del campo de Tecnologías de la Información y una evaluación preliminar por parte del supervisor de este proyecto de titulación.

3.7 Procesamiento de la información y análisis estadístico:

Se empleó la estadística descriptiva para el procesamiento y análisis de la información, presentando los datos relacionados con un conjunto de datos derivados de una muestra mediante tablas y gráficos. Asimismo, se utilizó el procedimiento Prueba T de Student para muestras emparejadas, el cual compara las medias de dos variables de un solo grupo, mediante el programa Microsoft Excel. Este procedimiento calcula las diferencias entre los valores de las dos variables de cada caso y contrasta si la media difiere de cero.

3.8 Variables respuesta o resultados alcanzados

En este estudio, se definen como las variables de interés: la gestión de riesgos y la seguridad de la información.

3.8.1 Definición de la variable independiente gestión de riesgos

La gestión del riesgo se divide en dos tareas análisis y tratamiento de riesgos; el análisis permite determinar cómo es, cuánto vale y cómo de protegido se encuentra el sistema, mientras que las acciones de tratamiento ayudan a desarrollar un plan de seguridad que permita alcanzar los objetivos (Guerrero et al., 2020).

3.8.2 Definición de la variable dependiente seguridad de la información

La seguridad de la información es cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema, cuyos efectos puedan conllevar daños en la información, comprometiendo su confidencialidad, integridad y disponibilidad.

Tabla 3.3 Variables de respuesta

Variable	Definición	Dimensión	Indicador	Técnica Instrumento
Gestión de riesgos de seguridad de la información	La gestión de riesgos de una organización se define como los procesos coordinados que se aplican para supervisar y gestionar el riesgo, con la finalidad de proteger su información.	Valoración del riesgo Tratamiento del riesgo	Política de seguridad de la información para la Empresa Pública Mancomunidad de Tránsito de Tungurahua Capacitación y concienciación	Entrevista Cuestionario

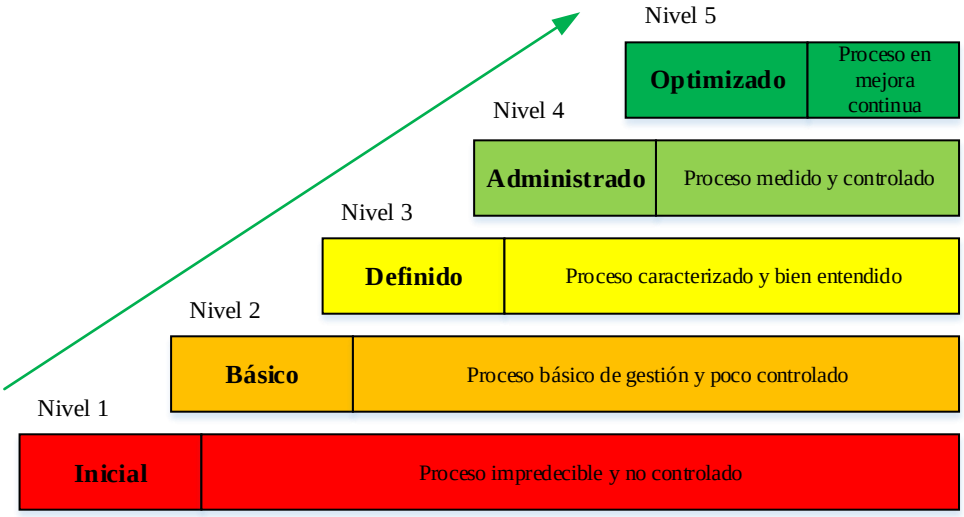
Fuente: Elaboración propia

CAPÍTULO IV
RESULTADOS Y DISCUSIÓN

4.1 Modelo de madurez de gestión de riesgos

El modelo de madurez de gestión de riesgos es un marco conceptual utilizado para evaluar el nivel de preparación de una organización en términos de su capacidad para gestionar riesgos de manera efectiva (Zenklussen, 2017). Este modelo se estructura en diversos niveles, los cuales están detallados a continuación:

Figura 4.1 Niveles de madurez en un sistema de gestión de riesgos



Fuente: Adaptado de Zenklussen

En resumen, el modelo de madurez de gestión de riesgos es una herramienta útil para evaluar el nivel de madurez de una organización en términos de su capacidad para gestionar riesgos y para identificar áreas de mejora y oportunidades de crecimiento.

4.2 Resultados pre-propuesta

En un entorno empresarial en constante evolución y cada vez más exigente, la gestión de riesgos ha tomado mayor importancia debido que permite a las empresas anticiparse a eventos que podrían afectar negativamente su valor y poner en peligro su información, el activo más valioso; por lo tanto, la gestión de riesgos se convierte en

una práctica vital en el proceso de toma de decisiones. En este contexto, se ha llevado a cabo una evaluación y comparación del nivel de madurez actual de la gestión de riesgos en la EPMTT, con el fin de identificar las principales dificultades que la empresa ha experimentado, los desafíos que se presentan en relación con esta práctica y los beneficios que ha obtendrá al implementarla continuamente.

4.2.1 Estudio inicial del nivel de madurez de la gestión de riesgos

La evaluación del nivel de madurez en la gestión de riesgos consiste en analizar la información proporcionada por la EPMTT acerca de su enfoque inicial en la gestión de riesgos, incluyendo los aspectos esenciales y las tendencias que influyen en su estrategia. En este estudio se examinaron las prácticas iniciales implementadas por la empresa en relación con seis componentes claves de la gestión de riesgos: establecimiento del contexto, valoración del riesgo, tratamiento del riesgo, aceptación del riesgo, seguimiento y revisión del riesgo y comunicación y consulta.

En la Tabla 4.1 se presenta el resumen de valores, con los cuales se puede estimar el nivel de madurez inicial de la gestión de riesgos de la EPMTT.

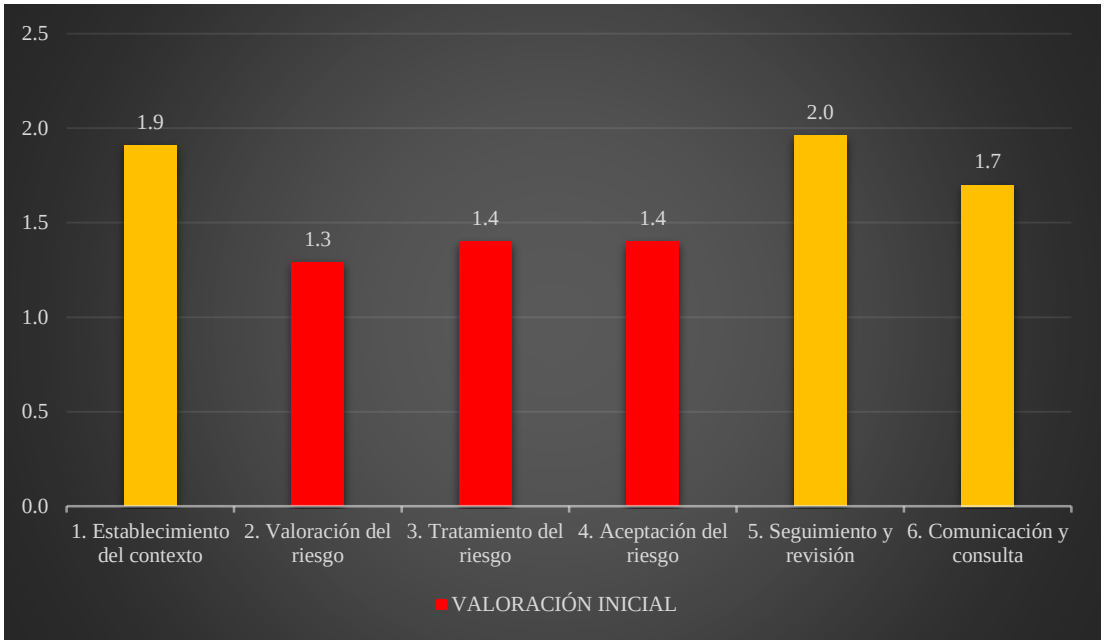
Tabla 4.1 Resumen de valoración inicial

COMPONENTE	VALORACIÓN INICIAL
1. Establecimiento del contexto	1.9
2. Valoración del riesgo	1.3
3. Tratamiento del riesgo	1.4
4. Aceptación del riesgo	1.4
5. Seguimiento y revisión	2.0
6. Comunicación y consulta	1.7
VALORACIÓN INICAL GLOBAL	**1.6**

Fuente: Elaboración propia

La Figura 4.2 muestra los valores iniciales obtenidos de acuerdo con la opinión del personal de la EPMTT

Figura 4.2 Promedio inicial de la evaluación de madurez



Fuente: Elaboración propia

Conforme la valoración global inicial expuesta en la Tabla 4.1, la EPMTT presenta un nivel "Básico" con un valor de 1.6 en la gestión de riesgos de seguridad de la información, esto indica que la empresa cumple con ciertos criterios iniciales de un sistema de gestión de riesgos y tiene en cuenta criterios básicos para abordar incidentes de seguridad; sin embargo, su aplicación es inconsistente debido a la falta de formalización. Así también, se observa que la gestión de riesgos está descentralizada y dispersa, y no se ha proporcionado una capacitación adecuada para mejorar su gestión.

4.3 Resultados post-propuesta

4.3.1 Estudio final del nivel de madurez de la gestión de riesgos

En la Tabla 4.2 se presenta el resumen de valores, con los cuales se puede estimar el nivel de madurez final de la gestión de riesgos de la EPMTT.

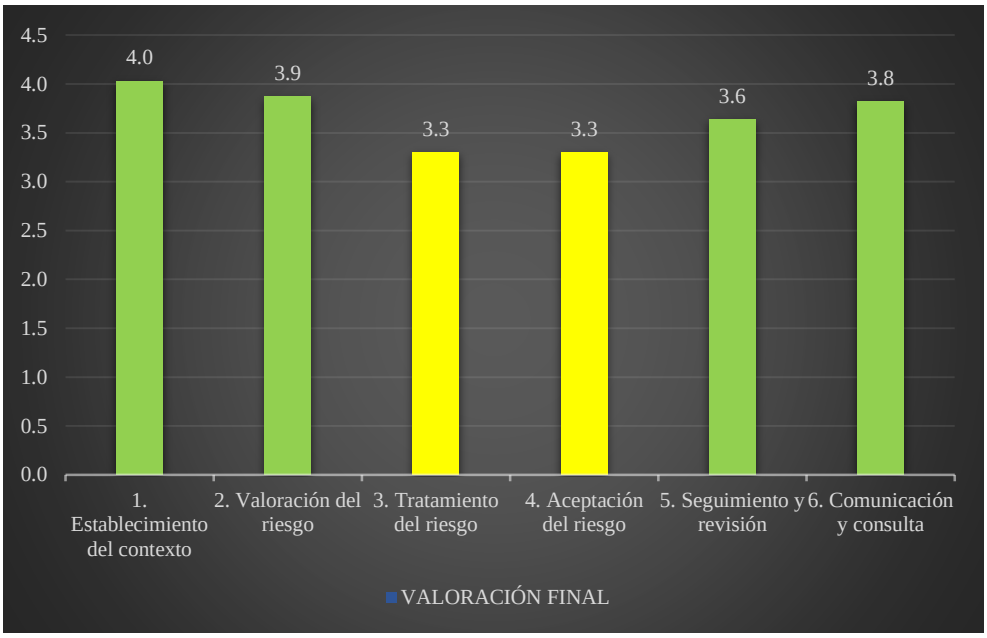
Tabla 4.2 Resumen de valoración final

COMPONENTE	VALORACIÓN FINAL
1. Establecimiento del contexto	4.0
2. Valoración del riesgo	3.9
3. Tratamiento del riesgo	3.3
4. Aceptación del riesgo	3.3
5. Seguimiento y revisión	3.6
6. Comunicación y consulta	3.8
VALORACIÓN FINAL GLOBAL	**3.7**

Fuente: Elaboración propia

En la Figura 4.3 se exponen los valores definitivos obtenidos de acuerdo con la evaluación del personal de la EPMTT.

Figura 4.3 Promedio final de la evaluación de madurez.



Fuente: Elaboración propia

De acuerdo con la evaluación global resumida en la Tabla 4.2, la EPMTT ha alcanzado un nivel de "Administrado," con una calificación de 3.7 en la gestión de riesgos de seguridad de la información. Esto refleja que al implementar el enfoque recomendado para la gestión de riesgos, la empresa ha establecido un sistema completo que cumple con estándares internacionales. Además, este sistema ha sido implementado de manera consistente y completa, y se realiza una revisión periódica de los procesos para

mejorarlos, respaldado por evidencia documental que demuestra su eficiencia y eficacia.

4.4 Discusión

La Tabla 4.3 y la Figura 4.4 presentan un resumen de los valores iniciales y finales del nivel de madurez de la EPMTT. Con estos valores se pude comparar y apreciar la mejora percibida por las personas de la empresa después de llevar a cabo el estudio de gestión de riesgos de seguridad de la información.

Tabla 4.3 Comparación de valores iniciales y finales

COMPONENTE	VALORACIÓN INICIAL	VALORACIÓN FINAL	ÓPTIMO
1. Establecimiento del contexto	1.9	4.0	5
2. Valoración del riesgo	1.3	3.9	5
3. Tratamiento del riesgo	1.4	3.3	5
4. Aceptación del riesgo	1.4	3.3	5
5. Seguimiento y revisión	2.0	3.6	5
6. Comunicación y consulta	1.7	3.8	5
VALORACIÓN FINAL GLOBAL	**1.6**	**3.7**	**5**

Fuente: Elaboración propia

Figura 4.4 Comparativa de niveles de madurez de la gestión del riesgo

Fuente: Elaboración propia

Para corroborar el análisis estadístico, se empleó la funcionalidad de análisis de datos proporcionada por Microsoft Excel para evaluar los resultados obtenidos mediante la aplicación de la prueba T de Student en muestras emparejadas, estableciendo un nivel de confianza del 95% y un margen de error del 5% (0.05).

La Tabla 4.4, corresponde a una prueba de hipótesis de cola izquierda con un valor crítico de t_c= -2.015, donde se encuentra el valor de rechazo.

Tabla 4.4 Prueba t para comparación de medias en muestras emparejadas

	VALORACIÓN INCIAL	VALORACIÓN FINAL
Media	1.616666667	3.65
Varianza	0.085666667	0.091
Observaciones	6	6
Coeficiente de correlación de Pearson	0.373755257	
Diferencia hipotética de las medias	0	
Grados de libertad	5	
Estadístico t	**-14.97186116**	
P(T<=t) una cola	**0.000012032**	
Valor crítico de t (una cola)	**-2.015048373**	
P(T<=t) dos colas	2.40651E-05	
Valor crítico de t (dos colas)	2.570581836	

Fuente: Análisis de datos mediante Microsoft Excel

Como se observa que t = -14.971< t_c= -2.015 y que el valor de p= 0; por lo tanto, se concluye que la hipótesis nula **"Ho"** es rechazada y se comprueba la hipótesis de investigación **"Hi"**, demostrando que la implementación de una gestión de riesgos de seguridad de la información, acompañada de políticas adecuadas, procedimientos y controles en los procesos, contribuye a prevenir, resguardar y proteger de manera efectiva la información de la Empresa Pública Mancomunidad de Tránsito de Tungurahua.

CAPÍTULO V
CONCLUSIONES, RECOMENDACIONES, BIBLIOGRAFÍA Y ANEXOS

5.1 Conclusiones

La Empresa Pública Mancomunidad de Tránsito de Tungurahua, maneja información dedicada a la planificación, regulación y control en el sector del tránsito, transporte y seguridad vial en los ocho cantones mancomunados de la provincia de Tungurahua; En este contexto el diseño de un plan de gestión de riesgos de seguridad de la información basado en normas internacionales garantizó la integridad, confidencialidad y disponibilidad de la información crítica de la empresa.

La identificación del estado de los activos que gestionan información crítica, junto con el análisis de amenazas y riesgos, constituyen etapas fundamentales en el proceso de evaluación de riesgos. Estas fases han posibilitado a la empresa una comprensión más profunda de sus amenazas, permitiéndole así gestionar y abordar de manera más efectiva los riesgos identificados.

El plan de gestión de riesgos propuesto, incluye recomendaciones, la formulación de procedimientos y políticas sustentados en normativas internacionales que se forjan a través de un exhaustivo análisis y evaluación de riesgos permitiendo la prevención, el resguardo y la protección de la información de la empresa.

Al profundizar en la evaluación del nivel de madurez de la empresa, a través de la encuesta inicial, se evidenció una brecha significativa entre su estado inicial (Básico) y el nivel "Óptimo", que es el punto donde una organización logra una adecuada gestión de los riesgos.

Una vez socializado el diseño de la gestión de riesgos y con la aplicación de la encuesta final, se verificó que el nivel madurez de la empresa, llegó a un nivel Administrado; es decir, la empresa ahora es capaz de manejar un sistema completo de gestión de riesgos que se adhiere a estándares internacionales con la capacidad de analizar y evaluar minuciosamente amenazas y riesgos respaldada por evidencia documentada que confirma su eficacia y eficiencia.

Los servidores públicos de la empresa no se encuentran debidamente capacitados respecto de la importancia de una adecuada gestión de riesgos, la cual demostró ser una práctica relativamente ajena para la EPMTT, lo que resalta la necesidad de una mayor socialización, formalización y educación en estos temas para mejorar su capacidad de anticipación y respuesta frente a los riesgos.

5.2 Recomendaciones

Se recomienda implementar el diseño propuesto de la gestión de riesgos, a efectos de mejorar la seguridad de la información de la EPMTT

Capacitar a los servidores públicos de la EPMTT, sobre gestión de riesgos a fin de que adquieran mayores conocimientos y conciencia de que la probabilidad de una amenaza se puede volver realidad.

Una vez implementada la gestión de riesgos, se deberá volver a evaluar los riesgos al menos una vez al año, debido a que es un proceso iterativo que requiere una verificación constante con un proceso de seguimiento y revisión con el fin de obtener una mejora continua.

Es recomendable realizar una comparación con otras normas con el fin de mejorar el esquema planteado, ya que estas normas tienen un enfoque común y los requisitos establecidos son genéricos y aplicables a todas las organizaciones, cualquiera que sea su tipo, tamaño o naturaleza.

5.3 Bibliografía

Aminzade, M. (2018). Confidentiality, integrity and availability – finding a balanced IT framework. *Network Security*, *2018*(5), 9–11. https://doi.org/10.1016/S1353-4858(18)30043-6

Barafort, B., Mesquida, A. L., & Mas, A. (2019). ISO 31000-based integrated risk management process assessment model for IT organizations. *Journal of Software: Evolution and Process*, *31*(1). https://doi.org/10.1002/smr.1984

Caballero, S., & Kuna, H. D. (2018). *Análisis y Gestión de Riesgo en Proyectos Software Un nuevo modelo integrando la metodología SEI y Magerit2*.

Cedeño, R. (2018). *La seguridad de la información: Aspecto crucial que toda empresa del siglo XXI debe gestionar* (Vol. 18). http://cienciaytecnologia.uteg.edu.ec

Crespo, E. (2018). *Una metodología para la gestión de riesgos aplicada a las MPYMEs*.

Espinosa, E. E. (2018). La hipótesis en la investigación. *Mendive*, *16*(1), 122–139.

Fernández, V. H. (2020). Tipos de justificación en la investigación científica. *Espíritu Emprendedor TES*, *4*(3), 65–76. https://doi.org/10.33970/eetes.v4.n3.2020.207

Ferruzola, E., Duchimaza, J., Ramos, J., & Alejandro, M. (2019). Plan de contingencia para los equipos y sistemas informáticos utilizando la metodología MAGERIT. *Revista Científica y Tecnológica UPSE*, *6*(1), 34–41. https://doi.org/10.26423/rctu.v6i1.429

Figueroa, J. A., Rodríguez, R. F., Bone, C. C., & Saltos, J. A. (2018). La seguridad informática y la seguridad de la información. *Polo Del Conocimiento*, *2*(12), 145. https://doi.org/10.23857/pc.v2i12.420

García, F. Y., & Moreta, L. M. (2018). *Modelo de Madurez para el Análisis de Riesgos de los Activos de Información basado en las Metodologías MAGERIT, OCTAVE y MEHARI; con enfoque a Empresas Navieras*.

Guerrero, M., Medina, A., & NOgueira, D. (2020). Procedimiento de gestión de riesgos como apoyo a la toma de decisiones. *Ingeniería Industrial*, *41*(1), 1–14. http://www.rii.cujae.edu.cu

López, M. (2018). *Análisis de riesgos en un sistema de gestión de seguridad de la información (SGSI) con metodologías complementarias*.

Monges, M., & Jimenez, V. (2020). *Seguridad de la informacion en plataformas de e-learning en tiempos de pandemia COVID-19*.

Néstor, M., & Morales, Z. (2019). *Modelo de gestión de riesgos de seguridad de la información: Una revisión del estado del arte*. *2*(1), 43–60. https://doi.org/10.15381/rpcs.v2i2.17103

Ortiz, J. E., & Vizñay, J. K. (2019). Análisis de riesgo y vulnerabilidades de la red de datos, en un ISP, utilizando el estándar ISO/IEC 2007:2008. Caso de estudio: Empresa Sistelcel. *Polo Del Conocimiento*, *4*(7), 174. https://doi.org/10.23857/pc.v4i7.1029

Pacheco, A. E., Suarez, L., & González, J. (2020). *Aplicar la Metodología OCTAVE de Identificación de Amenazas y Vulnerabilidades en una Entidad Bancaria*.

Ramos, Y., Urrutia, O., Ordoñez, D., & Bravo, A. (2017). *Adoptar una política de seguridad de la información basados en un dominio del estándar NTC ISO/IEC 27002:2013 para la Cooperativa Codelcauca*.

Rea, M., Calvo, J. A., & Feliu, T. (2018). *Prototipo para Gestionar la Ciberseguridad en Pequeñas Empresas*.

Robles, B. F. (2019). Población y muestra. *Pueblo Continente*, *30*(1), 245–246. https://doi.org/10.22497/PuebloCont.301.30121

Romero, M. I., Grace, C., Figueroa, L., Denisse, M., Vera, S., José, N., Álava, E., Galo, C., Parrales, R., Christian, A., Álava, J., Ángel, M., Murillo Quimiz, L., Adriana, M., & Merino, C. (2018). *INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA Y EL ANÁLISIS DE VULNERABILIDADES*.

Serrano, J. E., Salazar, V. H., Ruiz, X. N., & Narváez, C. (2019). Gestión de Riesgos de TIC en hospitales públicos. *Revista Iberica de Sistemas e Tecnologias de Informacao*, *20*, 280–291.

Siñani, D. A. (2021). Gestión de servicios TI en la Documentación Clínica basado en Estándares de Seguridad de la Información. *INF-FCPN-PGI Revista PGI*, 58–60.

Tejena, M. A. (2018). Análisis de riesgos en seguridad de la información. *Polo Del Conocimiento*, *3*(4), 230. https://doi.org/10.23857/pc.v3i4.809

Terán Valenzuela, K. M. (2018). *Guía para la implantación del SGSI con base en la NTE ISO/IEC 27000 para el servicio de agendamiento de citas del Contact Center del Ministerio de Salud Pública del Ecuador*. Universidad de las Fuerzas Armadas.

Valencia Duque, F. J., & Orozco Alzate, M. (2017). Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado

en la familia de normas ISO/IEC 27000. *RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação*, *22*, 73–88. https://doi.org/10.17013/risti.22.73-88

Valencia, F. J., & Orozco, M. (2017). Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000. *RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao*, *22*, 73–88. https://doi.org/10.17013/risti.22.73-88

Yupanqui, J. R. A., & Oré, S. B. (2017). Políticas de Seguridad de la Información: Revisión sistemática de las teorías que explican su cumplimiento. *RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao*, *2017*(25), 112–134. https://doi.org/10.17013/risti.25.112-134

Zenklussen, M. (2017). *Modelo de gestión de riesgo-Enterprise Risk Management (ERM)- Análisis en empresa local de Rafaela: Elsener Pinturas S.A.*

5.4 Anexos

5.4.1 Identificación total de activos de información

Tabla 5.1 Identificación total de activos de información

Identificación de Activos		
No.	**Tipos de activo**	**Activos de información**
A1	Activos esenciales Información que se maneja y Servicios que prestan	Datos del conductor
A2		Datos vehiculares
A3		Servicio 1: Sistema de recaudación
A4		Servicio 2: Sistema de matriculación
A5		Servicio 3: Sistema de revisión técnica vehicular
A6	Datos / Información	Ficheros
A7		Copias de respaldo
A8		Datos de configuración
A9	Encriptación	Credenciales/contraseñas
A10		Autenticación
A11		Control de acceso
A12		Claves de cifrado
A13		Claves compartidas
A14	Servicios prestados por el sistema	Acceso remoto a cuenta local (telnet)
A15		Acceso remoto por medio de un canal seguro (SSH)
A16		Internet
A17		Conexión Wireless
A18		Telefonía
A19		Página web
A20		Correo electrónico
A21		Almacenamiento y transferencia de archivos
A22	Software Aplicaciones informáticas	Navegador web
A23		Aplicaciones (SIGAME, Recaudación, AXIS, Eurosystem, Sistema Calificador)
A24		Servidor de ficheros (FTP)
A25		Sistema de gestión de bases de datos
A26		Ofimática (Office)
A27		Antivirus
A28		Sistemas operativos (Windows, Linux)
A29		Hypervisores
A30		Informática personal

A31	Hardware Equipamiento informático	Informática móvil
A32		Equipamiento de respaldo
A33		Impresoras
A34		Escáneres
A35		Módems
A36		Routers
A37		Switchs cap 2
A38		Switchs cap 3
A39		Firewall
A40		Servidores
A41		Puntos de acceso inalámbrico
A42		Central telefónica
A43		Teléfonos IP
A44		Biométricos
A45		Videovigilancia
A46	Redes de comunicaciones	Red telefónica (PSTN)
A47		Red inalámbrica
A48		Redes WAN
A49		Redes LAN
A50		Internet
A51		CCTV
A52	Soportes de información	Almacenamiento en red (NAS)
A53		Material impreso
A54	Equipamiento auxiliar	Sistemas de alimentación ininterrumpida (UPS)
A55		Generador eléctrico
A56		Cableado UTP
A57		Cableado eléctrico
A58		Fibra óptica
A59		Mobiliario (racks, armarios, archivadores)
A60		Cajas fuertes
A61	Instalaciones	Edificio
A62		Data center
A63		Vehículo terrestre: coche, camión, etc.
A64		Contenedores
A65		Canalización
A66	Personal	Usuarios
A67		Operadores (área administrativa y técnica)
A68		Administrador de sistemas
A69		Administrador de comunicaciones

A70	Administrador de seguridad informática
A71	Guardianía y Vigilancia
A72	Subcontratistas
A73	Proveedores

Fuente: Elaboración propia

5.4.2 Cuestionario para el personal de la EPMTT

CUESTIONARIO PARA EL PERSONAL DE LA EPMTT

Nombre del encuestado: _____

Cargo: _____

Instrucciones

Estimado(a) colaborador de la Empresa Pública Mancomunidad de Tránsito de Tungurahua, el presente instrumento tiene la finalidad de recoger información sobre la gestión de riesgos de seguridad de la información. Le pedimos que sea sincero en sus respuestas. Es importante destacar que esta encuesta es completamente anónima, por lo que sus datos personales no se reflejarán en el trabajo final.

Información

Estimado colaborador, marque con una **X** sólo una de las opciones:

Inicial	Básico	Definido	Gestionado	Optimizado
1	2	3	4	5

GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN			
1. CONTEXTO DE LA ORGANIZACIÓN		1.9	4.0
Nº	Pregunta	Valoración inicial	Valoración final
1.1	¿Considera usted, que la empresa tiene una definición clara de su misión, visión, valores, objetivos?	4.1	4.3
1.2	¿Considera usted, que la empresa tiene determinado los límites y alcances de un proceso formal de gestión de riesgos de la seguridad de la información?	1.2	3.3
1.3	¿Considera usted, que la empresa cuenta con políticas de gestión de riesgos?	1.1	4.9

1.4	¿Considera usted, que la política de gestión de riesgos está alineada con los objetivos de la empresa?	1.1	3.6
1.5	¿Conoce usted, los objetivos de sus actividades?	3.6	2.7
1.6	¿Considera usted, que la empresa tiene una comprensión clara de las amenazas a las que está expuesta?	1.1	4.8
1.7	¿Considera usted, que la empresa tiene definidas técnicas de gestión de riesgos como: marcos de referencia, estándares, metodologías o normas internacionales?	1.2	4.2
1.8	¿Cree usted, que se han asignado adecuadamente roles y responsabilidades de las políticas, normas y procedimientos?	1.1	3.8
1.9	¿Considera usted, que la gestión de riesgos puede generar valor para la empresa?	3.4	3.7
1.10	¿Considera usted, que recibe una orientación o capacitación sobre gestión del riesgo de la seguridad de la información?	1.2	5
2. VALORACIÓN DEL RIESGO		**1.3**	**3.9**
Nº	**Pregunta**	**Valoración inicial**	**Valoración final**
2.1	¿En la empresa existe un equipo o departamento dedicado a la gestión de riesgos?	1.0	2.9
2.2	¿Considera usted, que se valoran y evalúan los riesgos en la empresa?	1.4	4.6
2.3	¿Considera usted, que se identifican los activos de información en la empresa?	2.1	4.4
2.4	¿Considera usted, que en la empresa se identifican las amenazas que afectan a los activos de información?	1.2	4.3
2.5	¿Considera usted, se han tomado en cuenta las amenazas de origen natural (terremotos, erupciones) o industrial (fuego, agua, corte de suministro eléctrico) para la gestión de riesgos?	1.2	4.5
2.6	¿Considera usted, que la empresa determina las probabilidades de que una amenaza se convierta en un desastre?	1.0	3.6
2.7	¿Considera usted, que la empresa utiliza herramientas o técnicas avanzadas de análisis de riesgos?	1.0	3.2
2.8	¿En su opinión, se evalúan los eventos que generan riesgos?	1.5	3
2.9	¿Considera usted, que la empresa evalúa el impacto de los riesgos identificados?	1.0	4.6
2.10	¿Considera usted, que la empresa realiza controles y cuenta con salvaguardas para gestionar los riesgos?	1.5	3.6
3. TRATAMIENTO DEL RIESGO		**1.4**	**3.3**

Nº	Pregunta	Valoración inicial	Valoración final
3.1	¿Considera usted, que la empresa maneja un plan estructurado para el tratamiento de riesgos?	1.0	3.7
3.2	¿Considera usted, que la empresa selecciona adecuadamente medidas de control para evitar, mitigar, compartir o financiar los riesgos?	1.6	2.9
3.3	¿Cree usted, que la empresa tiene en cuenta el costo vs beneficio al tratar los riesgos?	1.8	2.4
3.4	¿Considera usted, que la empresa efectúa procedimientos organizados en caso de situaciones de riesgo?	1.3	2.7
3.5	¿Cree usted, que la empresa implementa nuevas estrategias o técnicas de gestión de riesgos?	1.1	4.5
3.6	¿Considera usted, que los procedimientos y mecanismos tecnológicos existentes en la empresa permiten reducir el riesgo actual?	1.6	3.6
4. ACEPTACIÓN DEL RIESGO		**1.4**	**3.3**
Nº	**Pregunta**	**Valoración inicial**	**Valoración final**
4.1	¿Considera usted, que la empresa selecciona adecuadamente controles para aceptar los riesgos?	1.4	3.1
4.2	¿Considera usted, que la empresa evalúa las responsabilidades de aceptar los riesgos?	1.8	2.9
4.3	¿Considera usted, que se lleva un registro detallado de los riesgos que se aceptan?	1.2	3.6
4.4	¿Cree usted, que la empresa decide no implementar un control de seguridad cuando los costos superan el valor del activo de información?	1.2	3.6
5. COMUNICACIÓN Y CONSULTA DEL RIESGO		**2.0**	**3.6**
Nº	**Pregunta**	**Valoración inicial**	**Valoración final**
5.1	¿Considera usted, que existe una comunicación efectiva entre los distintos niveles de la empresa?	2.1	3.6
5.2	¿Considera usted, que existe una comunicación efectiva con clientes, proveedores y otras partes externas?	2.3	2.9
5.3	¿Considera usted, que la empresa suministra la información necesaria para que los servidores puedan cumplir con sus responsabilidades?	2.8	3.7
5.4	¿Considera usted, que la empresa fomenta una cultura y formación de gestión de riesgos en la empresa?	1.2	4.4

5.5	¿Cree usted, que la gestión de riesgos es un tema de discusión común en la empresa?	1.4	3.6
6. SEGUIMINETO Y REVISIÓN DEL RIESGO		**1.7**	**3.8**
Nº	**Pregunta**	**Valoración inicial**	**Valoración final**
6.1	¿La empresa cuenta con un auditor o algún tipo de departamento de auditoría interna?	3.9	4.2
6.2	¿Considera usted, que la empresa realiza monitoreos continuos de los incidentes de la seguridad de la información?	1.3	3.7
6.3	¿Considera usted, que la empresa efectúa alguna evaluación para verificar si la gestión de riesgos se ajusta a los lineamientos establecidos por la dirección?	1	3.5
6.4	¿Cree usted, que el personal está siendo supervisado de manera oportuna frente a posibles amenazas que puedan afectar a los activos de información?	1.3	3.4
6.5	¿Existe un proceso para revisar y actualizar regularmente la gestión de riesgos?	1	4.3

CAPÍTULO VI
PROPUESTA

6.1 Datos Informativos

Título:	Gestión de riesgos de seguridad de la información a través de normas internacionales en la Empresa Pública Mancomunidad de Tránsito de Tungurahua.
Institución:	Empresa Pública Mancomunidad de Tránsito de Tungurahua.
Beneficiarios:	Gerencia General Unidad de Tecnología Usuarios internos y externos
Ubicación:	Pelileo – Tungurahua
Responsable:	Ing. Lenín Alexis Aguirre Sánchez
Director:	Ing. Ángel Gabriel Jaramillo Alcázar, Mg.

6.2 Antecedentes de la propuesta

En un mundo globalizado es indispensable la comunicación y el uso de tecnologías nuevas, pero esto también genera una apertura para que la seguridad de la información se vea comprometida ante múltiples amenazas y vulnerabilidades. La revolución digital ha generado que las organizaciones en todo el mundo presten mayor atención al activo más importante de una empresa, es decir la información. Como defensa ante las amenazas latentes es necesario manejar sistemas y estrategias que permitan proteger la información en todos sus niveles y garanticen la continuidad del negocio.

Para la Empresa Pública Mancomunidad de Tránsito de Tungurahua (EPMTT) es fundamental mantenerse como una empresa líder, que regula y controla el tránsito, trasporte terrestre y la seguridad vial e impulsa el desarrollo de ocho cantones de la provincia de Tungurahua del Ecuador, generando bienestar con altos estándares de calidad y eficiencia, actuando responsablemente con la comunidad en un ambiente sano, ordenado y seguro para la movilidad motorizada. Los activos de información de la empresa son esenciales para el cumplimiento de su misión y visión; por lo tanto, la

administración de la seguridad de información que es un proceso integral, transversal y que genera valor, es imprescindible para mantener la resiliencia de la EPMTT.

6.3 Justificación

La seguridad de la información es responsabilidad de la máxima autoridad, el nivel directivo y de todos los servidores del EPMTT, como un mecanismo estratégico para fortalecer la gestión de sus procesos, personas, infraestructura y tecnología y deben aplicar las medidas de protección que sean necesarias para resguardar la información y datos de miles de usuarios con el objetivo de minimizar el riesgo de difusión, acceso y uso no autorizado: sin embargo, las acciones empleadas dentro de la empresa hasta el momento, no garantizan el cumplimiento de la confidencialidad, integridad y disponibilidad de la información. La EPMTT no dispone de procesos formalizados en el ámbito de las Tecnologías de la Información y Comunicación, ni de una estructura donde se establezcan roles, responsabilidades que garanticen la seguridad de la información.

El alcance de la propuesta comprende la estructuración de la gestión de seguridad de la información, con el fin de mejorar todos los sistemas que involucran a la información y lograr una efectiva seguridad.

6.4 Objetivos

6.4.1 General

Diseñar un plan de gestión de riesgos con sus respectivos procedimientos y políticas basadas en normas internacionales, mediante el análisis y evaluación de vulnerabilidades, amenazas y riesgos de la empresa.

6.4.2 Específicos

a. Identificar el estado de los activos que manejan la información crítica en la empresa.

b. Analizar potenciales vulnerabilidades y amenazas que puedan causar pérdida de la información.
c. Realizar recomendaciones a la empresa con el fin de reducir el riesgo hasta un nivel aceptable.

6.5 Análisis de factibilidad

Para la presente propuesta se consideraron los siguientes tipos de factibilidad:

6.5.1 Factibilidad operativa

El presente proyecto es respaldado por la Gerencia General de la EPMTT y desarrollado en la Unidad Tecnológica, este recurso humano es esencial para efectuar las actividades en los diferentes procesos de la gestión de la seguridad de la información

6.5.2 Factibilidad técnica

La EPMTT cuenta con la infraestructura y software para responder de manera favorable durante la ejecución del proyecto; además, la Unidad Tecnológica cuenta con los conocimientos técnicos necesarios para obtener todos los datos relevantes.

6.5.3 Factibilidad económica

El proyecto es económicamente viable para la EPMTT, debido a que la elaboración de este no constituye un gasto monetario para la empresa, los recursos utilizados corren a cargo del investigador; sin embargo, si en el futuro se desea desarrollar un Sistema de Gestión de Seguridad de la Información (SGSI) a partir del estudio de la gestión de riesgos, se debe contar con una planificación presupuestaria que cubra todos los puntos del tratamiento de riesgos.

6.5.4 Factibilidad tiempo

La realización del proyecto se estima de seis a doce meses, con el fin de alcanzar las metas establecidas.

6.6 Fundamentación

Para la formulación del proceso de la gestión de riesgos de la seguridad de la información se tomaron en cuenta los elementos claves del direccionamiento estratégico de la empresa, tales como son su misión, visión, metas y valores. En este contexto, se identifican, analizan y evalúan riesgos establecidos en estándares internacionales en todos los procesos de la cadena de valor para orientar las decisiones de la EPMTT que puedan afectar el cumplimiento de los objetivos estratégicos.

6.7 Metodología, Modelo operativo

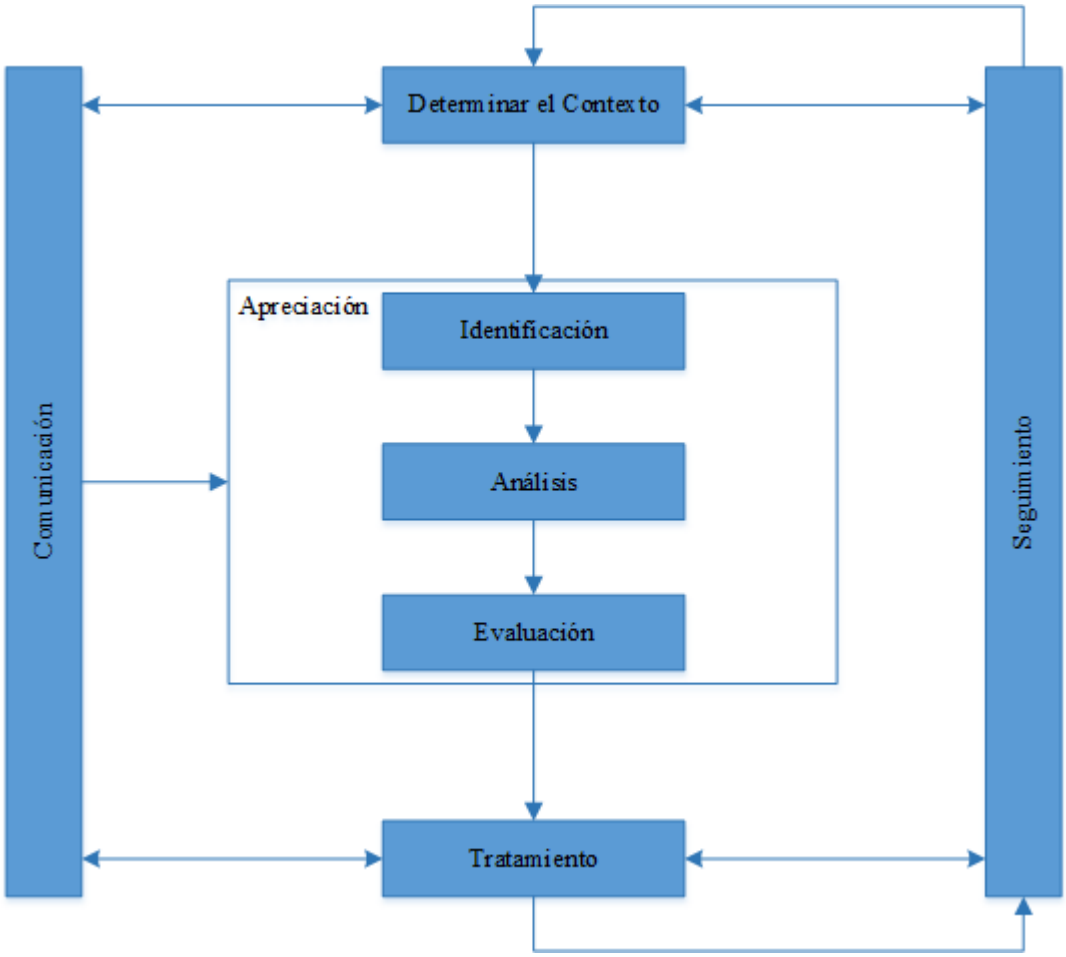
La metodología empleada en el presente proyecto se fundamenta en MAGERIT V3 (Metodología de análisis y gestión de riesgos de los sistema de información), además se utilizaron los criterios establecidos en la ISO/IEC 27001 (Tecnologías de la información - Técnicas de seguridad - Sistemas de gestión de la seguridad de la información – Requisitos), ISO/IEC 27005 (Gestión de riesgos de seguridad de la información) y de la ISO 31000 (Gestión del riesgo).

6.8 Proceso para la gestión del riesgo de la seguridad de la información

El proceso de gestión de riesgos utiliza un enfoque iterativo para todas sus actividades, lo que permite aumentar la profundidad y el nivel de detalle en la evaluación de cada paso, logrando un buen equilibrio entre minimizar el tiempo y el esfuerzo necesario para identificar los controles y garantizar que la evaluación de los riesgos sea efectiva.

En la Figura 6.1 se establecen los pasos de las actividades del proceso de gestión del riesgo.

Figura 6.1 Proceso de gestión del riesgo



Fuente: Adaptado de MAGERIT v3

6.8.1 Establecimiento del contexto

6.8.1.1 Situación actual

La Empresa Pública Mancomunada de Tránsito de Tungurahua es creada en marzo del 2015, iniciando las operaciones en el mismo año, contando con la certificación para la ejecución de la competencia de matriculación y revisión técnica vehicular expedida por la Agencia Nacional de Tránsito. La EPMTT gestiona, planifica, regula y controla el tránsito, trasporte terrestre y la seguridad vial en los Cantones de Baños de Agua Santa, Cevallos, Mocha, Santiago de Quero, San Pedro de Pelileo, Santiago de Píllaro, San Cristóbal de Patate y Tisaleo.

Actualmente, la empresa cuenta con un área administrativa y otra técnica:

Tabla 6.1 Área Administrativa

Área Administrativa	
Gerencia	• Gerente general • Secretaría • Asistente de comunicación • Jurídico
Dirección financiera	• Director financiero • Contador • Tesorería • Recaudador • Asistente de recaudador • Bodeguero
Dirección administrativa	• Director administrativo • Analista talento humano • Analista de compras públicas • Unidad Tecnológica • Analista seguridad y salud del trabajo • Auxiliar de servicios

Fuente: Elaboración propia

Tabla 6.2 Área Técnica

Área Técnica	
Dirección de matriculación	• Director de matriculación • Analista jurídico • Técnico en títulos habilitantes • Atención al cliente • Analista documental y digitador • Técnico en Asistencia tecnológica de matriculación
Dirección del CRTV (Centro de revisión técnica vehicular)	• Director CRTV • Supervisor CRTV • Revisor técnico vehicular • Asistente RTV • Analista TIC CRTV
Dirección de planificación	• Director de planificación • Analista de seguridad vial • Señalizador vial • Técnico de tránsito y transporte

Fuente: Elaboración propia

La EPMTT brinda los siguientes servicios a la población de la provincia de Tungurahua:

- Servicio 1: Sistema de recaudación
- Servicio 2: Sistema de matriculación
- Servicio 3: Sistema de revisión técnica vehicular

6.8.1.2 Alcance y límites de la gestión de riesgos

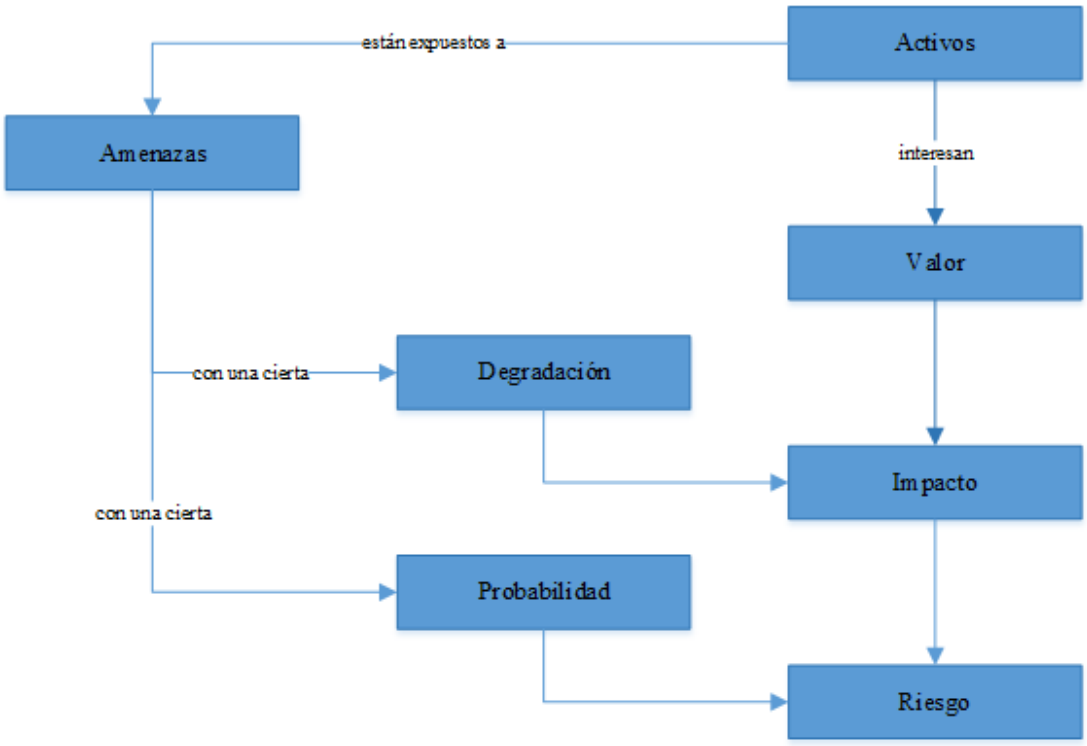
La gestión de riesgos de la seguridad de la información es aplicable a todos los procesos de la EPMTT, así como para todos los servidores y terceras partes que acceden a la información, sea en formato físico o digital y en todas las etapas de su ciclo de vida.

En el proyecto se establecen los lineamientos básicos y el marco general para el proceso de gestión del riesgo, inicia con la estructuración de la gestión de riesgos; comprende el análisis y evaluación de los riesgos, así como el tratamiento de los riesgos de la EPMTT y revisión de las acciones emprendidas para aceptar, eliminar, mitigar, compartir y financiar los riesgos; y, finaliza con la elaboración de las políticas de seguridad de la información y las directrices de capacitación y concientización.

6.8.2 Valoración del Riesgo

La Figura 6.2 es una representación visual del proceso de análisis de riesgos en el que se detallan las diferentes etapas que lo componen. Este método sigue una metodología sistemática que permite identificar el riesgo mediante una serie de pasos predefinidos conocidos como etapas de evaluación de riesgos.

Figura 6.2 Elementos del análisis de riesgos



Fuente: Adaptado de MAGERIT v3

6.8.2.1 Identificación de activos

En la empresa se identificaron 11 diferentes tipos de activos, dentro de los cuales consta 73 activos. En la tabla 6.3 se describen los principales activos de cada tipo, con los cuales se realizó el análisis correspondiente. Los 62 activos restantes están descritos en los Anexos y pueden ser analizados de la misma manera debido a que la mayoría cuentan con las mismas amenazas y vulnerabilidades. Si en el futuro se plantea realizar un SGSI con la base de gestión de riesgos propuesta, se debe utilizar la población completa (total activos) pero debido al tiempo que lleva un SGSI no es posible describirlo completamente en el presente documento, ya que es un proceso iterativo y de continuas mejoras.

Tabla 6.3 Identificación de activos

Identificación de Activos		
No.	**Tipos de activo**	**Nombre del activo**
A1	**Activos esenciales** Información que se maneja y Servicios que prestan	Servicio SRTV: Sistema de revisión técnica vehicular
A2	**Datos/Información**	Copias de respaldo
A3	**Encriptación**	Credenciales/contraseñas
A4	**Servicios** Prestados por el sistema	Internet
A5	**Software** Aplicaciones informáticas	Aplicaciones (SIGAME, Recaudación, AXIS, Eurosystem, Sistema Calificador)
A6	**Hardware** Equipamiento informático	Firewall
A7	**Redes de comunicaciones**	Redes LAN
A8	**Soportes de información**	Almacenamiento en red (NAS)
A9	**Equipamiento auxiliar**	Sistemas de alimentación ininterrumpida (UPS)
A10	**Instalaciones**	Data center
A11	**Personal**	Administrador de sistemas

Fuente: Elaboración propia

6.8.2.2 Valoración de criticidad

En base a las tres propiedades (disponibilidad, integridad, confidencialidad) se evalúa el nivel de criticidad y se describen los criterios de valoración. En las Tablas 6.4, 6.5, 6.6 y 6.7 están definidos los criterios de valoración utilizados.

Tabla 6.4 Criterio de valoración para la criticidad

Criterio de Valoración - CRITICIDAD			
	Nivel	**Peso**	**Definición**
MA	Muy alto	5	Cuando el máximo es 5.
A	Alto	4	Cuando el máximo es 4.
M	Medio	3	Cuando el máximo es 3.
B	Bajo	2	Cuando el máximo es 2.
MB	Despreciable	1	Cuando el máximo es 1.

Fuente: Adaptado de MAGERIT v3

Tabla 6.5 Criterio de valoración de criticidad para la Disponibilidad

Criterio de Valoración – DISPONIBILIDAD (D)			
Nivel		**Peso (P)**	**Definición**
MA	Muy alto	5	La interrupción del acceso a los sistemas de información durante una hora impide la realización de las actividades de la organización.
A	Alto	4	La interrupción del acceso a los sistemas de información durante un día tiene un efecto grave para la organización.
M	Medio	3	La interrupción del acceso a los sistemas de información durante una semana tiene un efecto considerable para la organización.
B	Bajo	2	La interrupción del acceso a los sistemas de información durante un mes tiene un efecto mínimo para la organización.
MB	Despreciable	1	La interrupción del acceso a los sistemas de información no afecta las actividades normales de la organización.

Fuente: Elaboración propia

Tabla 6.6 Criterio de valoración de criticidad para la Integridad

Criterio de Valoración – INTEGRIDAD (I)			
Nivel		**Peso (P)**	**Definición**
MA	Muy alta	5	La destrucción o modificación de los sistemas de información no pueden ser restauradas, impidiendo la realización de las actividades.
A	Alta	4	Los sistemas de información son difíciles de restaurar y podrían causar un daño serio a la organización.
M	Media	3	Los sistemas de información pueden ser restaurados, pero perjudican la eficacia de las actividades.
B	Baja	2	Los sistemas de información pueden ser restaurados fácilmente sin afectar el rendimiento de las actividades.
MB	Despreciable	1	La destrucción o modificación de los sistemas de información no afecta las actividades normales de la organización.

Fuente: Elaboración propia

Tabla 6.7 Criterio de valoración de criticidad para la Confidencialidad

Criterio de Valoración – CONFIDENCIALIDAD (C)			
Nivel		**Peso (P)**	**Definición**
MA	Muy alta	5	La divulgación no autorizada de la información secreta y sensible tiene un efecto crítico para la seguridad de la organización.
A	Alta	4	La divulgación no autorizada de la información utilizada por áreas exclusivas tiene un efecto importante para la organización.
M	Media	3	La divulgación no autorizada de la información interna tiene un efecto limitado para la organización.
B	Baja	2	La divulgación no autorizada de la información interna probablemente disminuya la eficacia de las actividades de la organización.
MB	Despreciable	1	La divulgación de la información pública no tiene ningún efecto para la organización.

Fuente: Elaboración propia

En la Tabla 6.8, se detalla cada activo estudiado con su respectiva valoración de criticidad. La valoración de la criticidad está dada por el peso o valor promedio de los valores de las tres dimensiones D.I.C.

Tabla 6.8 Valoración de criticidad de activos

Valoración de activos							
Activo	**D**	**P**	**I**	**P**	**C**	**P**	**Criticidad**
A1	MA	5	M	3	MA	3	3.67
A2	A	4	MA	5	B	2	3.67
A3	B	2	M	3	MA	5	3.33
A4	MA	5	B	2	B	2	3.00
A5	MA	5	A	4	A	4	4.33
A6	MA	5	A	4	MA	5	4.67
A7	MA	5	M	3	A	4	4.00
A8	M	3	MA	5	MA	5	4.33
A9	MA	5	B	2	D	1	2.67
A10	MA	5	MA	5	A	4	4.67
A11	M	3	D	1	A	4	2.67

Fuente: Elaboración propia

6.8.2.3 Identificación de Amenazas

En la tabla 6.9, se describen las amenazas relacionadas con cada uno de los activos críticos de la empresa.

Tabla 6.9 Identificación de amenazas

Identificación de Amenazas	
Activo	**Descripción**
Servicio SRTV: Sistema de revisión técnica vehicular	Errores de los usuarios
	Errores del administrador
	Errores de configuración
	Alteración accidental de la información
	Revelación de información
	Suplantación de la identidad del usuario
	Abuso de privilegios de acceso
	Acceso no autorizado
Copias de respaldo	Errores de los usuarios
	Errores del administrador
	Errores de configuración
	Alteración accidental de la información
	Revelación de información
	Suplantación de la identidad del usuario
	Abuso de privilegios de acceso
	Acceso no autorizado
Credenciales/contraseñas	Errores de los usuarios
	Errores del administrador
	Alteración accidental de la información
	Revelación de información
	Suplantación de la identidad del usuario
	Abuso de privilegios de acceso
	Acceso no autorizado
Internet	Errores de los usuarios
	Errores del administrador
	Alteración accidental de la información
	Revelación de información
	Caída del sistema por agotamiento de recursos
	Suplantación de la identidad del usuario
	Abuso de privilegios de acceso

	Acceso no autorizado
	Ataques de red (DOS/DDOS)
Aplicaciones (SIGAME, Recaudación, AXIS, Eurosystem, Sistema Calificador)	Avería de origen físico o lógico
	Errores de los usuarios
	Errores del administrador
	Difusión de software dañino
	Alteración accidental de la información
	Revelación de información
	Errores de mantenimiento / actualización de programas (software)
	Suplantación de la identidad del usuario
	Abuso de privilegios de acceso
	Acceso no autorizado
	Vulnerabilidades de los programas (software)
Firewall	Terremoto
	Erupción
	Corrimiento de tierras
	Fuego
	Daños por agua
	Contaminación mecánica (vibraciones, polvo, suciedad)
	Avería de origen físico o lógico
	Corte del suministro eléctrico
	Condiciones inadecuadas de temperatura o humedad
	Errores del administrador
	Errores de mantenimiento / actualización de equipos (hardware)
	Caída del sistema por agotamiento de recursos
	Abuso de privilegios de acceso
	Acceso no autorizado
	Ataques de red (DOS/DDOS)
	Robo
Redes LAN	Fallo de servicios de comunicaciones
	Errores del administrador
	Alteración accidental de la información
	Revelación de información
	Caída del sistema por agotamiento de recursos
	Suplantación de la identidad del usuario
	Abuso de privilegios de acceso
	Acceso no autorizado
	Análisis de tráfico
	Ataques de red (DOS/DDOS)

Almacenamiento en red (NAS)	Terremoto
	Erupción
	Corrimiento de tierras
	Fuego
	Daños por agua
	Contaminación mecánica (vibraciones, polvo, suciedad)
	Avería de origen físico o lógico
	Corte del suministro eléctrico
	Condiciones inadecuadas de temperatura o humedad
	Errores de los usuarios
	Errores del administrador
	Alteración accidental de la información
	Revelación de información
	Errores de mantenimiento / actualización de equipos (hardware)
	Acceso no autorizado
	Robo
Sistemas de alimentación ininterrumpida (UPS)	Terremoto
	Erupción
	Corrimiento de tierras
	Fuego
	Daños por agua
	Contaminación mecánica (vibraciones, polvo, suciedad)
	Avería de origen físico o lógico
	Corte del suministro eléctrico
	Condiciones inadecuadas de temperatura o humedad
	Errores de mantenimiento / actualización de equipos (hardware)
	Acceso no autorizado
	Robo
Data center	Terremoto
	Erupción
	Corrimiento de tierras
	Fuego
	Daños por agua
	Revelación de información
	Acceso no autorizado
Administrador de sistemas	Revelación de información
	Indisponibilidad del personal
	Ingeniería social

Fuente: Adaptado de MAGERIT V3

6.8.2.4 Valoración del impacto

El impacto se calcula en términos de la máxima degradación que la amenaza ocasionaría al nivel de criticidad del activo. En la Tabla 6.10 y 6.11 se detallan los criterios tomados para realizar la valoración del impacto.

Tabla 6.10 Criterio de degradación del activo a causa de la amenaza

Criterio de Valoración - DEGRADACIÓN		
Nivel	**Peso**	**Definición**
Daño total	1	Hasta el 100%
Daño extremo	0.9	Hasta el 90%
Daño muy grave	0.8	Hasta el 80%
Daño grave	0.7	Hasta el 70%
Daño importante	0.6	Hasta el 60%
Daño medio	0.5	Hasta el 50%
Daño menor	0.4	Hasta el 40%
Daño muy bajo	0.3	Hasta el 30%
Recuperable	0.2	Hasta el 20%
No hay daño	0.1	Hasta el 10%

Fuente: Adaptado de MAGERIT v3

A cada activo se le estima su degradación causada por la posible amenaza en cada una de las tres características de disponibilidad, integridad y confidencialidad, con valores entre 0% y 100%.

Tabla 6.11 Criterio de valoración del impacto

Criterio de Valoración - IMPACTO			
	Nivel	**Peso**	**Definición**
MA	Muy alto	5	Cuando el máximo es 5.
A	Alto	4	Cuando el máximo es 4.
M	Medio	3	Cuando el máximo es 3.
B	Bajo	2	Cuando el máximo es 2.
MB	Despreciable	1	Cuando el máximo es 1.

Fuente: Adaptado de MAGERIT v3

En la Tabla 6.12, se muestra el cálculo del impacto sobre los activos de la empresa.

Tabla 6.12 Valoración del impacto sobre los activos

Activos		Amenaza	Degradación			Impacto
No.	Criticidad	Descripción	D	I	C	Total
Servicio SRTV: Sistema de revisión técnica vehicular	3.67	Errores de los usuarios	100%	50%	40%	3.67
		Errores del administrador	60%	30%	10%	2.20
		Errores de configuración	50%	20%	10%	1.84
		Alteración accidental de la información	60%	30%	30%	2.20
		Revelación de información	10%	70%	20%	2.57
		Suplantación de la identidad del usuario	20%	80%	30%	2.94
		Abuso de privilegios de acceso	30%	40%	20%	1.47
		Acceso no autorizado	50%	70%	40%	2.57
Copias de respaldo	3.67	Errores de los usuarios	0%	10%	0%	0.37
		Errores del administrador	30%	50%	40%	1.84
		Errores de configuración	20%	40%	30%	1.47
		Alteración accidental de la información	0%	10%	0%	0.37
		Revelación de información	10%	40%	30%	1.47
		Suplantación de la identidad del usuario	20%	60%	50%	2.20
		Abuso de privilegios de acceso	20%	40%	30%	1.47
		Acceso no autorizado	30%	60%	50%	2.20
Credenciales/contraseñas	3.33	Errores de los usuarios	50%	100%	80%	3.33

		Errores del administrador	10%	30%	20%	1.00
		Alteración accidental de la información	30%	50%	40%	1.67
		Revelación de información	50%	60%	40%	2.00
		Suplantación de la identidad del usuario	40%	50%	10%	1.67
		Abuso de privilegios de acceso	30%	40%	20%	1.33
		Acceso no autorizado	20%	30%	30%	1.00
Internet	3	Errores de los usuarios	40%	50%	30%	1.50
		Errores del administrador	60%	60%	50%	1.80
		Alteración accidental de la información	0%	10%	0%	0.30
		Revelación de información	10%	20%	10%	0.60
		Caída del sistema por agotamiento de recursos	100%	90%	80%	3.00
		Suplantación de la identidad del usuario	0%	10%	0%	0.30
		Abuso de privilegios de acceso	10%	20%	10%	0.60
		Acceso no autorizado	40%	30%	50%	1.50
		Ataques de red (DOS/DDOS)	80%	70%	60%	2.40
Aplicaciones (SIGAME, Recaudación, AXIS, Eurosystem, Sistema Calificador)	4.33	Avería de origen físico o lógico	100%	50%	50%	4.33
		Errores de los usuarios	100%	50%	50%	4.33
		Errores del administrador	50%	40%	40%	2.17
		Difusión de software dañino	100%	60%	90%	4.33
		Alteración accidental de la información	40%	60%	40%	2.60
		Revelación de información	10%	10%	20%	0.87
		Errores de mantenimiento / actualización de programas (software)	40%	70%	60%	3.03
		Suplantación de la identidad del usuario	40%	40%	60%	2.60

		Abuso de privilegios de acceso	40%	50%	40%	2.17
		Acceso no autorizado	30%	30%	60%	2.60
		Vulnerabilidades de los programas (software	20%	60%	40%	2.60
Firewall	4.67	Terremoto	100%	100%	20%	4.67
		Erupción	50%	30%	30%	2.34
		Corrimiento de tierras	10%	20%	30%	1.40
		Fuego	100%	100%	50%	4.67
		Daños por agua	100%	100%	50%	4.67
		Contaminación mecánica (vibraciones, polvo, suciedad)	70%	80%	50%	3.74
		Avería de origen físico o lógico	100%	100%	50%	4.67
		Corte del suministro eléctrico	70%	50%	40%	3.27
		Condiciones inadecuadas de temperatura o humedad	80%	100%	30%	4.67
		Errores del administrador	50%	60%	10%	2.80
		Errores de mantenimiento / actualización de equipos (hardware)	50%	60%	40%	2.80
		Caída del sistema por agotamiento de recursos	100%	90%	50%	4.67
		Abuso de privilegios de acceso	80%	70%	40%	3.74
		Acceso no autorizado	100%	100%	40%	4.67
		Ataques de red (DOS/DDOS)	100%	100%	50%	4.67
		Robo	100%	100%	100%	4.67
Redes LAN	4	Fallo de servicios de comunicaciones	100%	100%	50%	4.00
		Errores del administrador	80%	70%	50%	3.20
		Alteración accidental de la información	10%	20%	10%	0.80
		Revelación de información	40%	30%	50%	2.00

		Caída del sistema por agotamiento de recursos	100%	100%	40%	4.00
		Suplantación de la identidad del usuario	10%	10%	20%	0.80
		Abuso de privilegios de acceso	80%	70%	60%	3.20
		Acceso no autorizado	100%	100%	40%	4.00
		Análisis de tráfico	80%	80%	60%	3.20
		Ataques de red (DOS/DDOS)	100%	100%	60%	4.00
Almacenamiento en red (NAS)	4.33	Terremoto	100%	100%	10%	4.33
		Erupción	70%	80%	60%	3.46
		Corrimiento de tierras	10%	50%	40%	2.17
		Fuego	100%	100%	80%	4.33
		Daños por agua	100%	100%	20%	4.33
		Contaminación mecánica (vibraciones, polvo, suciedad)	70%	60%	50%	3.03
		Avería de origen físico o lógico	100%	100%	10%	4.33
		Corte del suministro eléctrico	50%	60%	30%	2.60
		Condiciones inadecuadas de temperatura o humedad	80%	60%	50%	3.46
		Errores de los usuarios	0%	0%	10%	0.43
		Errores del administrador	100%	100%	30%	4.33
		Alteración accidental de la información	80%	70%	60%	3.46
		Revelación de información	100%	100%	20%	4.33
		Errores de mantenimiento / actualización de equipos (hardware)	80%	70%	10%	3.46
		Acceso no autorizado	100%	100%	90%	4.33
		Robo	100%	100%	100%	4.33
	2.67	Terremoto	100%	100%	20%	2.67

Sistemas de alimentación ininterrumpida (UPS)		Erupción	70%	80%	30%	2.14
		Corrimiento de tierras	10%	50%	40%	1.34
		Fuego	100%	100%	50%	2.67
		Daños por agua	100%	100%	90%	2.67
		Contaminación mecánica (vibraciones, polvo, suciedad)	50%	60%	30%	1.60
		Avería de origen físico o lógico	100%	100%	10%	2.67
		Corte del suministro eléctrico	10%	0%	0%	0.27
		Condiciones inadecuadas de temperatura o humedad	80%	90%	20%	2.40
		Errores de mantenimiento / actualización de equipos (hardware)	50%	70%	30%	1.87
		Acceso no autorizado	30%	40%	20%	1.07
		Robo	100%	100%	10%	2.67
Data center	4.67	Terremoto	100%	100%	10%	4.67
		Erupción	80%	70%	40%	3.74
		Corrimiento de tierras	100%	100%	20%	4.67
		Fuego	100%	100%	10%	4.67
		Daños por agua	100%	100%	30%	4.67
		Revelación de información	50%	60%	100%	4.67
		Acceso no autorizado	100%	100%	100%	4.67
Administrador de sistemas	2.67	Revelación de información	40%	50%	100%	2.67
		Indisponibilidad del personal	60%	30%	20%	1.60
		Ingeniería social	90%	100%	100%	2.67

Fuente: Adaptado MAGERIT V3

6.8.2.5 Valoración del riesgo

En la Tabla 6.13, se establece el criterio para valorar la probabilidad de ocurrencia de una amenaza.

Tabla 6.13 Criterio de valoración de la probabilidad de ocurrencia

Criterio de valoración - PROBABILIDAD			
Nivel	**Peso**	**Probabilidad**	**Definición**
Extremo	1	100%	A diario
Muy Alto	0.9	90%	Semanalmente
Alto	0.8	80%	Mensualmente
	0.7	70%	
Medio	0.6	60%	Una vez al año
	0.5	50%	
Bajo	0.4	40%	Cada varios años
	0.3	30%	
Muy bajo	0.2	20%	Décadas
	0.1	10%	
Nula	0	0%	Nunca

Fuente: Adaptado de MAGERIT v3

En la Tabla 6.14, se establece el criterio para valorar el nivel del riesgo.

Tabla 6.14 Criterio de valoración del Riesgo

Criterio de valoración – RIESGO			
Nivel		**Peso**	**Definición**
MA	Muy alto	5	Cuando el máximo es 5.
A	Alto	4	Cuando el máximo es 4.
M	Medio	3	Cuando el máximo es 3.
B	Bajo	2	Cuando el máximo es 2.
MB	Despreciable	1	Cuando el máximo es 1.

Fuente: Adaptado de MAGERIT v3

En la Tabla 6.15, se establece la valoración del nivel del riesgo para cada uno de los activos estudiados de la empresa.

Tabla 6.15 Criterio de valoración del Riesgo

Activo	Amenaza	Probabilidad	Impacto	Riesgo
Servicio SRTV: Sistema de revisión técnica vehicular	Errores de los usuarios	100%	3.67	3.67
	Errores del administrador	70%	2.20	1.54
	Errores de configuración	60%	1.84	1.10
	Alteración accidental de la información	90%	2.20	1.98
	Revelación de información	10%	2.57	0.26
	Suplantación de la identidad del usuario	10%	2.94	0.29
	Abuso de privilegios de acceso	20%	1.47	0.29
	Acceso no autorizado	20%	2.57	0.51
Copias de respaldo	Errores de los usuarios	20%	0.37	0.07
	Errores del administrador	10%	1.84	0.18
	Errores de configuración	70%	1.47	1.03
	Alteración accidental de la información	60%	0.37	0.22
	Revelación de información	20%	1.47	0.29
	Suplantación de la identidad del usuario	30%	2.20	0.66
	Abuso de privilegios de acceso	20%	1.47	0.29
	Acceso no autorizado	10%	2.20	0.22
Credenciales/contraseñas	Errores de los usuarios	100%	3.33	3.33
	Errores del administrador	60%	1.00	0.60

	Alteración accidental de la información	40%	1.67	0.67
	Revelación de información	100%	2.00	2.00
	Suplantación de la identidad del usuario	80%	1.67	1.33
	Abuso de privilegios de acceso	60%	1.33	0.80
	Acceso no autorizado	10%	1.00	0.10
Internet	Errores de los usuarios	100%	1.50	1.50
	Errores del administrador	60%	1.80	1.08
	Alteración accidental de la información	20%	0.30	0.06
	Revelación de información	70%	0.60	0.42
	Caída del sistema por agotamiento de recursos	70%	3.00	2.10
	Suplantación de la identidad del usuario	20%	0.30	0.06
	Abuso de privilegios de acceso	20%	0.60	0.12
	Acceso no autorizado	60%	1.50	0.90
	Ataques de red (DOS/DDOS)	50%	2.40	1.20
Aplicaciones (SIGAME, Recaudación, AXIS, Eurosystem, Sistema Calificador)	Avería de origen físico o lógico	70%	4.33	3.03
	Errores de los usuarios	100%	4.33	4.33
	Errores del administrador	90%	2.17	1.95
	Difusión de software dañino	70%	4.33	3.03
	Alteración accidental de la información	60%	2.60	1.56
	Revelación de información	50%	0.87	0.43
	Errores de mantenimiento / actualización de programas (software)	80%	3.03	2.42
	Suplantación de la identidad del usuario	100%	2.60	2.60
	Abuso de privilegios de acceso	60%	2.17	1.30

	Acceso no autorizado	50%	2.60	1.30
	Vulnerabilidades de los programas (software	70%	2.60	1.82
Firewall	Terremoto	60%	4.67	2.80
	Erupción	40%	2.34	0.93
	Corrimiento de tierras	20%	1.40	0.28
	Fuego	30%	4.67	1.40
	Daños por agua	30%	4.67	1.40
	Contaminación mecánica (vibraciones, polvo, suciedad)	90%	3.74	3.36
	Avería de origen físico o lógico	100%	4.67	4.67
	Corte del suministro eléctrico	60%	3.27	1.96
	Condiciones inadecuadas de temperatura o humedad	20%	4.67	0.93
	Errores del administrador	60%	2.80	1.68
	Errores de mantenimiento / actualización de equipos (hardware)	70%	2.80	1.96
	Caída del sistema por agotamiento de recursos	80%	4.67	3.74
	Abuso de privilegios de acceso	70%	3.74	2.62
	Acceso no autorizado	90%	4.67	4.20
	Ataques de red (DOS/DDOS)	80%	4.67	3.74
	Robo	60%	4.67	2.80
Redes LAN	Fallo de servicios de comunicaciones	90%	4.00	3.60
	Errores del administrador	60%	3.20	1.92
	Alteración accidental de la información	60%	0.80	0.48
	Revelación de información	30%	2.00	0.60
	Caída del sistema por agotamiento de recursos	70%	4.00	2.80

	Suplantación de la identidad del usuario	30%	0.80	0.24
	Abuso de privilegios de acceso	40%	3.20	1.28
	Acceso no autorizado	50%	4.00	2.00
	Análisis de tráfico	80%	3.20	2.56
	Ataques de red (DOS/DDOS)	100%	4.00	4.00
Almacenamiento en red (NAS)	Terremoto	30%	4.33	1.30
	Erupción	20%	3.46	0.69
	Corrimiento de tierras	40%	2.17	0.87
	Fuego	30%	4.33	1.30
	Daños por agua	20%	4.33	0.87
	Contaminación mecánica (vibraciones, polvo, suciedad)	70%	3.03	2.12
	Avería de origen físico o lógico	100%	4.33	4.33
	Corte del suministro eléctrico	60%	2.60	1.56
	Condiciones inadecuadas de temperatura o humedad	20%	3.46	0.69
	Errores de los usuarios	20%	0.43	0.09
	Errores del administrador	70%	4.33	3.03
	Alteración accidental de la información	80%	3.46	2.77
	Revelación de información	20%	4.33	0.87
	Errores de mantenimiento / actualización de equipos (hardware)	70%	3.46	2.42
	Acceso no autorizado	40%	4.33	1.73
	Robo	70%	4.33	3.03
Sistemas de alimentación ininterrumpida (UPS)	Terremoto	30%	2.67	0.80
	Erupción	20%	2.14	0.43

	Corrimiento de tierras	40%	1.34	0.53
	Fuego	30%	2.67	0.80
	Daños por agua	20%	2.67	0.53
	Contaminación mecánica (vibraciones, polvo, suciedad)	70%	1.60	1.12
	Avería de origen físico o lógico	90%	2.67	2.40
	Corte del suministro eléctrico	30%	0.27	0.08
	Condiciones inadecuadas de temperatura o humedad	20%	2.40	0.48
	Errores de mantenimiento / actualización de equipos (hardware)	40%	1.87	0.75
	Acceso no autorizado	20%	1.07	0.21
	Robo	40%	2.67	1.07
Data center	Terremoto	70%	4.67	3.27
	Erupción	60%	3.74	2.24
	Corrimiento de tierras	30%	4.67	1.40
	Fuego	20%	4.67	0.93
	Daños por agua	20%	4.67	0.93
	Revelación de información	10%	4.67	0.47
	Acceso no autorizado	20%	4.67	0.93
Administrador de sistemas	Revelación de información	30%	2.67	0.80
	Indisponibilidad del personal	70%	1.60	1.12
	Ingeniería social	60%	2.67	1.60

Fuente: Elaboración propia

6.8.2.6 Riesgo actual y riesgo objetivo

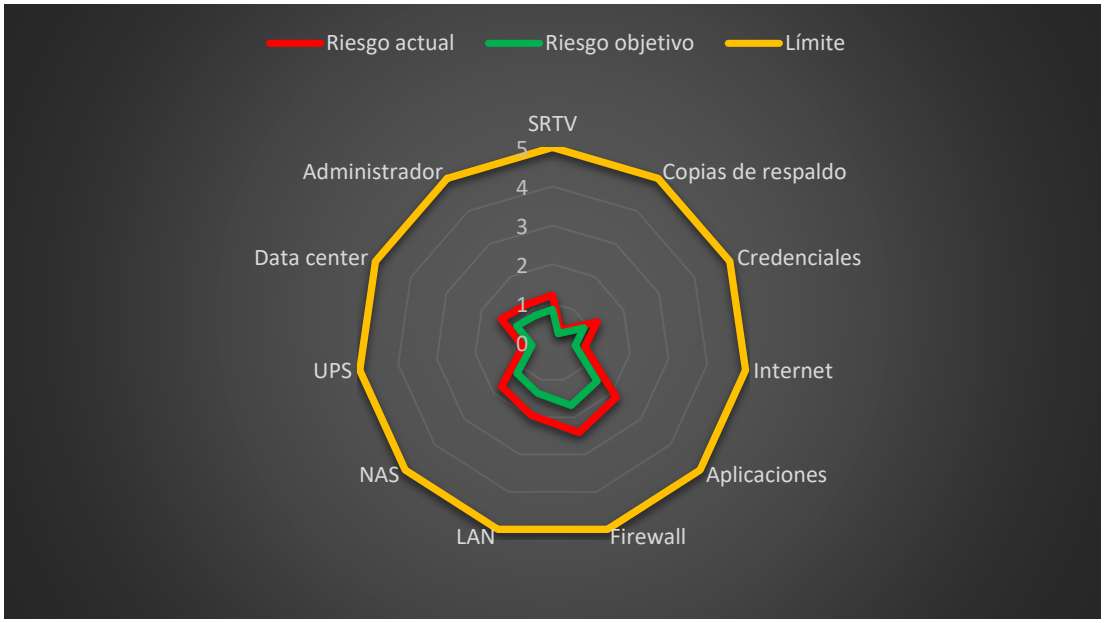
En la Tabla 6.16 se describen los riesgos actuales de cada activo crítico y cuál sería el riesgo objetivo recomendado; es decir, la reducción del riesgo en un 30% y el valor máximo o límite del riesgo al que nunca se debe llegar.

Tabla 6.16 Riesgo actual y riesgo objetivo

Activo	Riesgo actual	Riesgo objetivo	Límite
Servicio SRTV: Sistema de revisión técnica vehicular	1.21	0.85	5
Copias de respaldo	0.37	0.26	5
Credenciales/contraseñas	1.26	0.88	5
Internet	0.83	0.58	5
Aplicaciones	2.16	1.51	5
Firewall	2.41	1.69	5
Redes LAN	1.95	1.37	5
Almacenamiento en red (NAS)	1.73	1.21	5
Sistemas de alimentación ininterrumpida (UPS)	0.77	0.54	5
Data center	1.45	1.02	5
Administrador de sistemas	1.17	0.82	5

Fuente: Elaboración propia

Figura 6.3 Gráfico radar Riesgo actual y Riesgo objetivo



Fuente: Elaboración propia

6.8.2.7 Salvaguardas

En la práctica, es poco común hallar sistemas desprovistos de protección. Las salvaguardias o contramedidas comprenden procedimientos o mecanismos ya arraigados en la empresa, que se aplican de manera inconsciente para enfrentar amenazas potenciales y minimizar riesgos. Estas amenazas pueden ser contrarrestadas a través de una organización adecuada, que incluya documentación y gestión de incidentes, soluciones técnicas como programas o equipos, medidas de seguridad física en las instalaciones, así como mediante políticas establecidas.

En la Tabla 6.17 se describen los tres tipos de salvaguardas (administrativa, técnica, física) previstos para cada activo crítico de la empresa.

Tabla 6.17 Salvaguardas

Tipo de activos	Activo	Salvaguarda Administrativa	Salvaguarda Técnica	Salvaguarda Física
Activos esenciales	Servicio SRTV: Sistema de revisión técnica vehicular	• Procedimientos de operación (manuales)	• Mantenimiento • Soporte técnico proveedor y auditoria	• Seguridad física en cubículos
Datos/Información	Copias de respaldo	• Revisión de controles de acceso	• Cifrado de la información • Fechado electrónico (NTP)	
Encriptación	Credenciales/contraseñas	• Gestión de claves		
Servicios	Internet	• Disponibilidad de expertos - soporte CNT	• Mantenimiento • Red privada virtual (VPN)	
Software	Aplicaciones	• Disponibilidad de expertos	• Copias de seguridad (backup) • Actualizaciones y parches	

			• Mantenimiento • Vigencia tecnológica • Sistemas de Identity Management • FW a nivel de aplicación	
Hardware	Firewall	• Disponibilidad de expertos • Etiquetado de información	• Se aplican perfiles de seguridad • Operación • Actualizaciones y parches • Mantenimiento • Vigencia tecnológica	• Guardianía
Redes de comunicaciones	Redes LAN	• Disponibilidad de expertos • Etiquetado de información	• Protección criptográfica de la confidencialidad de los datos intercambiados • Autenticación del canal • Actualizaciones y parches • Mantenimiento • Segmentación de la red • Sistema antivirus	
Soportes de información	Almacenamiento en red (NAS)	• Etiquetado de información	• Actualizaciones y parches • Mantenimiento • Protección criptográfica del contenido	
Equipamiento auxiliar	Sistemas de alimentación ininterrumpida (UPS)	• Etiquetado de información	• Mantenimiento • Mejoramiento del suministro eléctrico	

Instalaciones	Data center	• Etiquetado de información • Inventario de activos • Seguimiento de activos	• Mantenimiento • Iluminación de emergencia • Detectores de humo	• Sistema de protección perimetral • Salidas de emergencia • Guardianía
Personal	Administrador de sistemas		• Biometría	• Gafetes • Control de visitantes

Fuente: Elaboración propia

6.8.3 Tratamiento de los riesgos

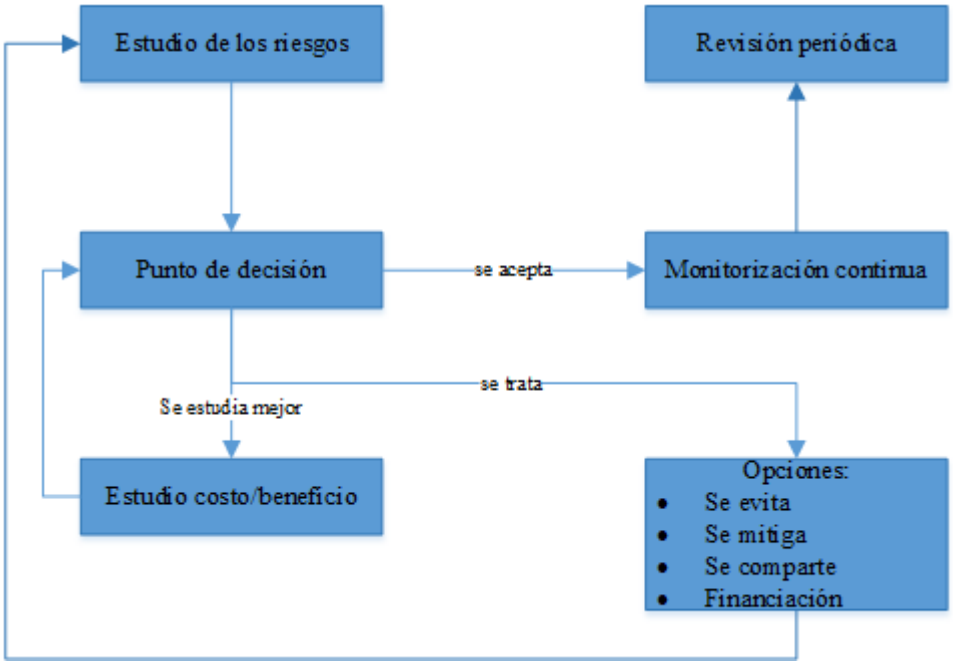
La gestión de riesgos implica tomar decisiones referentes a los diversos riesgos presentes, en línea con la estrategia de la organización, es necesario elegir medidas de control para disminuir, aceptar, prevenir o transferir los riesgos, y establecer un plan para el manejo de estos.

Existen algunas opciones disponibles para el tratamiento del riesgo:

- Aceptación del riesgo
- Evitación del riesgo
- Mitigación del riesgo
- Compartición del riesgo
- Financiación

La Figura 6.4 ilustra la actividad del tratamiento del riesgo dentro de los procesos de la gestión del riesgo:

Figura 6.4 Decisiones de tratamiento de los riesgos



Fuente: Adaptado de MAGERIT v3

En la Tabla 6.18 se describen los respectivos controles a implementar para las amenazas detectadas.

Tabla 6.18 Tratamiento de riesgos

Amenaza	Opciones de tratamiento	Tipo de control	Acciones de Tratamiento(Controles a implementar)	Dominio	Objetivo de control	Responsable	Áreas que participan
Errores de los usuarios	Aceptar	Correctivo: aplicado luego del suceso	Monitorización continua	Técnico	Revisión periódica	Oficial de seguridad de la información	Unidad Tecnológica
Errores del administrador	Mitigar	Preventivo	Capacitación	Administrativo	Seguridad de los recursos humanos	Director de tecnología	Talento humano, Unidad Tecnológica
Errores de configuración	Mitigar	Correctivo	Implementación de único usuario de administrador y desactivación de puertos que no están siendo utilizados	Técnico	Mantenimiento de equipos	Equipo de seguridad de la información	Unidad Tecnológica
Alteración accidental de la información	Aceptar	Preventivo: aplicado para evitarlo	Monitorización continua	Técnico	Revisión periódica	Oficial de seguridad de la información	Unidad Tecnológica
Revelación de información	Mitigar	Preventivo	Procedimiento disciplinario en conformidad con las leyes y códigos internos	Administrativo	Documentación de procedimientos	Talento Humano	Gerencia General, Talento Humano

Suplantación de la identidad del usuario	Mitigar	Correctivo	Uso de contraseñas temporales	Técnico	Prevención del uso inadecuado de la información	Equipo de seguridad de la información	Unidad Tecnológica
Abuso de privilegios de acceso	Mitigar	Correctivo	Credenciales de acceso por tipo de usuario	Técnico	Distribución y separación de funciones	Equipo de seguridad de la información	Unidad Tecnológica
Acceso no autorizado	Eliminar	Correctivo	Cambio de equipos con seguridad AAA: Autenticación, Autorización, Contabilización	Técnico	Mantenimiento de equipos	Director de tecnología	Gerencia General, Dirección administrativa, Unidad Tecnológica
Caída del sistema por agotamiento de recursos	Mitigar	Correctivo	Analizar programas periódicos de mantenimiento preventivo de los equipos	Administrativo	Mantenimiento de equipos	Comité de seguridad de la información	Dirección administrativa, Unidad Tecnológica
Ataques de red (DOS/DDOS)	Financiación	Preventivo	Adquisición de herramientas de ciberseguridad	Técnico	Autorización para nuevas herramientas de procesamiento de Tecnologías de la Información y Comunicación	Director de tecnología	Gerencia General, Dirección administrativa, Unidad Tecnológica

Difusión de software dañino	Mitigar	Preventivo	Instalación y actualización de antivirus	Técnico	Control contra código malicioso	Equipo de seguridad de la información	Unidad Tecnológica
Errores de mantenimiento / actualización de programas (software)	Mitigar	Preventivo	Examinar la frecuencia de los planes de mantenimiento preventivo y mejorar los procedimientos	Administrativo	Documentación de procedimientos	Oficial de seguridad de la información	Dirección administrativa, Unidad Tecnológica
Vulnerabilidades de los programas (software)	Mitigar	Correctivo	Estructurar programas periódicos de mantenimiento preventivo de los equipos	Administrativo	Documentación de procedimientos	Comité de seguridad de la información	Unidad Tecnológica
Terremoto	Mitigar	Preventivo	Elaboración de plan de emergencias ante desastres naturales	Administrativo	Documentación de procedimientos	Comité de seguridad de la información	Gerencia General, Dirección administrativa
Erupción	Mitigar	Preventivo	Elaboración de plan de emergencias ante desastres naturales	Administrativo	Documentación de procedimientos	Comité de seguridad de la información	Gerencia General, Dirección administrativa
Corrimiento de tierras	Mitigar	Preventivo	Elaboración de plan de emergencias ante desastres naturales	Administrativo	Documentación de procedimientos	Comité de seguridad de la información	Gerencia General, Dirección administrativa
Fuego	Mitigar	Preventivo	Controles de acceso y sensores de humo	Técnico	Mantenimiento de instalaciones	Equipo de seguridad de la información	Dirección administrativa,

							Unidad Tecnológica
Daños por agua	Mitigar	Preventivo	Controles de acceso y sistemas de monitoreo	Técnico	Mantenimiento de instalaciones	Equipo de seguridad de la información	Dirección administrativa, Unidad Tecnológica
Contaminación mecánica (vibraciones, polvo, suciedad)	Mitigar	Correctivo	Programas periódicos de mantenimiento preventivo de los equipos	Técnico	Mantenimiento de equipos	Equipo de seguridad de la información	Unidad Tecnológica
Avería de origen físico o lógico	Compartir	Preventivo	Mantener vigente los contratos de soporte con el fabricante	Administrativo	Mantenimiento de equipos	Comité de seguridad de la información	Dirección administrativa, Unidad Tecnológica
Corte del suministro eléctrico	Mitigar	Preventivo	Mejoramiento del sistema del generador eléctrico	Técnico	Mantenimiento de equipos	Oficial de seguridad de la información	Dirección administrativa, Unidad Tecnológica
Condiciones inadecuadas de temperatura o humedad	Mitigar	Preventivo	Instalación de aires acondicionados de precisión	Técnico	Control simultáneo de temperatura, humedad, limpieza y movimiento de aire	Oficial de seguridad de la información	Dirección administrativa, Unidad Tecnológica

Errores de mantenimiento / actualización de equipos (hardware)	Mitigar	Preventivo	Examinar la frecuencia de los planes de mantenimiento preventivo y mejorar los procedimientos	Administrativo	Documentación de procedimientos	Comité de seguridad de la información	Dirección administrativa, Unidad Tecnológica
Robo	Mitigar	Preventivo	Sistemas de control de acceso y biometría	Físico	Seguridad física y del entorno	Comité de seguridad de la información	Dirección administrativa, Unidad Tecnológica
Fallo de servicios de comunicaciones	Compartir	Preventivo	Soporte técnico con el proveedor, acuerdos de nivel de servicio (SLA)	Técnico	Monitoreo y revisión de servicios	Oficial de seguridad de la información	Dirección administrativa, Unidad Tecnológica
Análisis de tráfico	Financiación	Preventivo	Adquisición de herramientas de ciberseguridad	Técnico	Autorización para nuevas herramientas de procesamiento de Tecnologías de la Información y Comunicación	Director de tecnología	Gerencia General, Dirección administrativa, Unidad Tecnológica
Indisponibilidad del personal	Mitigar	Correctivo	Teletrabajo, accesos seguros a la red por VPN	Técnico	Seguridad de los recursos humanos	Equipo de seguridad de la información	Unidad Tecnológica

Ingeniería social	Financiación	Preventivo	Capacitación al usuario	Administrativo	Seguridad de los recursos humanos	Director de tecnología	Área administrativa y área técnica

Fuente: Elaboración propia

6.8.4 Riesgo residual

El riesgo residual se refiere al nivel de riesgo que permanece después de que se han implementado medidas o controles para mitigar o reducir los riesgos iniciales. En otras palabras, una vez que se han aplicado acciones para minimizar los riesgos identificados, el riesgo residual es el que todavía persiste. Este cálculo se realiza para evaluar la efectividad de los controles y para determinar si son adecuadas para disminuir el riesgo a un nivel que la organización considera aceptable.

En consecuencia, el riesgo residual se calcula posteriormente a la implementación de controles y puede ayudar a tomar decisiones informadas sobre la gestión de riesgos. Dado que su determinación se lleva a cabo una vez implementado el plan de tratamiento de riesgos, su cálculo quedaría reservado para un futuro estudio.

6.8.5 Comunicación y consulta

Dentro de esta fase, se propone realizar la comunicación a todo el personal de la EPMTT, informando las falencias, fortalezas y debilidades; además, establecer el cronograma para futuras capacitaciones.

6.8.6 Seguimiento y revisión

Dado que la gestión de riesgos es un proceso iterativo, es fundamental que se realice una evaluación continua y un análisis exhaustivo de todos los activos de la empresa.

El presente proyecto no contempla la realización de este trabajo. Dado que el seguimiento adecuado requiere una cantidad significativa de tiempo, no se puede llevar a cabo dentro de los límites del proyecto. No obstante, se brindan sugerencias y directrices para continuar progresando en esta área en el futuro.

6.9 Política de seguridad de la información para la Empresa Pública Mancomunidad de Tránsito de Tungurahua

Con el propósito de contribuir en la evaluación, tratamiento, seguimiento y revisión de los riesgos a los que están expuestos los activos críticos y la información de la EPMTT, se crea la siguiente política de seguridad de la información.

6.9.1 Objetivos

- Identificar los riesgos asociados a la información y los activos críticos evaluando su posible impacto en la consecución de los objetivos de la empresa.
- Implementar medidas de seguridad preventivas, de respuesta y de recuperación para salvaguardar los activos y la información críticos de la empresa, asegurando su confidencialidad, integridad y disponibilidad física y digital.
- Abordar la gestión de riesgos de seguridad de la información, tanto operativa como estratégicamente, para mantener niveles de exposición aceptables y garantizar la protección de la confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad de los activos de información.
- Difundir la política de seguridad de la información y capacitar a los empleados de la EPMTT.

6.9.2 Alcance

La Política de seguridad de la información es válida para todo el personal interno, externo y terceros que acceden a la información de la empresa, ya sea en formato físico o digital, y en cada una de sus fases de ciclo de vida.

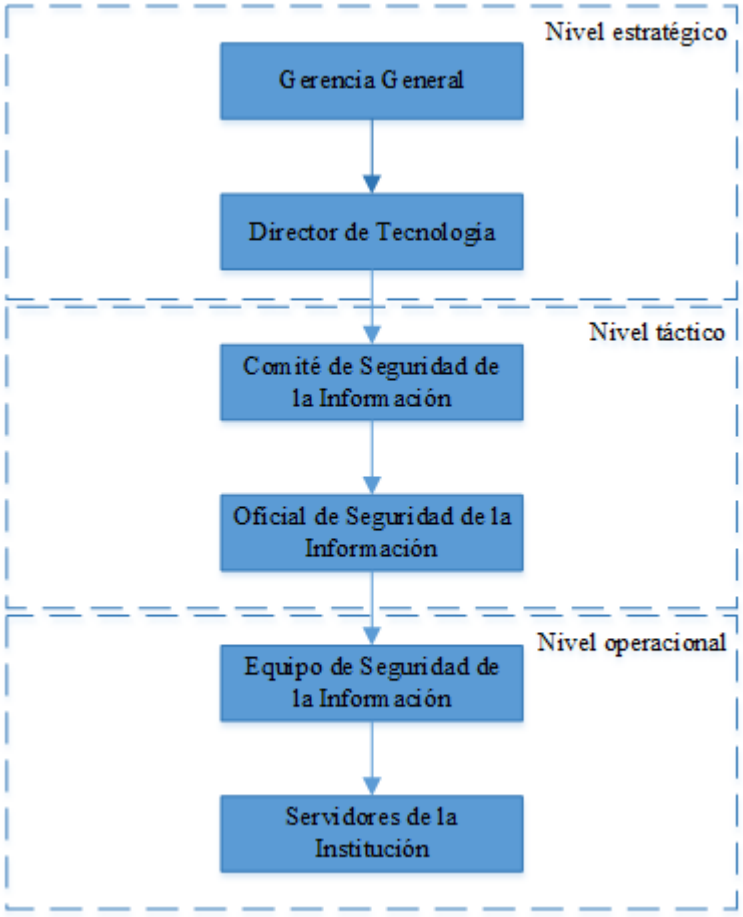
6.9.3 Roles y Responsabilidades

Todos los servidores de la entidad son responsables de la seguridad de la información, no obstante, la alta dirección y el área de tecnología tienen el compromiso de responder rápido y de forma correcta ante cualquier incidente de manera que se reduzca al mínimo el impacto de los riesgos.

Para mejorar el actual manejo de seguridad de la información en la EPMTT, es necesario establecer los roles y responsabilidades alrededor de la Unidad Tecnológica, debido a que una sola persona no es capaz de realizar todas las labores para efectuar una activa gestión de riesgos. A continuación, se definen los niveles de gestión:

- **Nivel estratégico:** Planificación para lograr los objetivos, se basa en el establecimiento de políticas, lineamientos y herramientas para lograr su efectividad.
- **Nivel táctico:** Coordinación de las actividades, así como la evaluación y la orientación para su operación.
- **Nivel operativo:** Ejecución de tareas específicas, reportar los inconvenientes y oportunidades al nivel estratégico y táctico.

Figura 6.5 Cargos por niveles de gestión



Fuente: Adaptado de MAGERIT v3

A continuación, se detallan las responsabilidades básicas de cada uno de los roles involucrados de acuerdo con el nivel de gestión en el que se ubiquen.

Tabla 6.19 Roles y responsabilidades definidos para la EPMTT

Cargo/Rol	Responsabilidad
Gerencia General	Asegurar la aplicación de los requisitos legales, directrices de organismos de control y de la normativa de seguridad de información. Apoyo para llevar los proyectos a buen fin.
Director de Tecnologías de la Información y Comunicación	Directivo de alto nivel encargado de aprobar y monitorear los planes, manuales y actividades. Informa de los resultados de la ejecución de planes de TI a la alta dirección.
Comité de Seguridad de la Información	Responsable de la planificación y organización de los planes de TI.
Oficial de Seguridad de la Información	Garantizar y facilitar la implementación de las iniciativas de seguridad de la información en EPMTT.
Equipo de Seguridad de la Información	Es responsable de la ejecución de las actividades y tareas para la adecuada gestión de la seguridad de la información, a través de los instructivos desarrollados dentro del proceso.
Servidores de la Institución	Cumplir con los lineamientos establecidos.

Fuente: Adaptado de MAGERIT v3

6.9.4 Compromisos empresariales

Para el cumplimiento de la presente política, se establecen los siguientes compromisos:

- Establecer y mantener actualizados los criterios manejados en la gestión de seguridad de la información de la EPMTT, con el propósito de fomentar una cultura empresarial que se centre en la identificación, comunicación y prevención del riesgo.
- Destinar los recursos apropiados, tanto humanos como tecnológicos, económicos y materiales, para garantizar la implementación y aplicación efectiva de las políticas establecidas.
- Garantizar una comunicación efectiva y clara para que todo el personal sea consciente y comprenda la política de gestión de riesgos, de manera que se

puedan integrar actitudes preventivas y proactivas en su comportamiento ante situaciones que puedan afectar la continuidad del negocio.

- Proporcionar liderazgo y asistencia a los funcionarios para asegurar que la política de gestión de riesgos se implemente de manera efectiva y se administre adecuadamente.
- Garantizar que la política se implemente correctamente y supervisar su cumplimiento.
- Llevar a cabo evaluaciones periódicas para verificar la aplicación de los controles de riesgos.
- Revisar y mejorar continuamente la política de gestión de riesgos en respuesta a eventos o cambios en las circunstancias para mejorar su eficacia.

6.9.5 Políticas, normas y procedimientos de seguridad

La presente política, es complemento de la gestión de riesgos de la seguridad de la información de la EPMTT, definiendo el conjunto de procedimientos y herramientas de seguridad para garantizar la protección de los activos de información.

6.9.5.1 Lineamientos generales

- Los incidentes de seguridad de la información considerados de alta o crítica gravedad, que requieren la evaluación y análisis por parte de personal especializado después del incidente, sean atendidos por personal externo contratado. Esto deberá ser llevado a cabo previa emisión de un informe por parte del Oficial de Seguridad de la Información y la aprobación del Comité de Seguridad de la Información.
- Se llevará a cabo una revisión periódica de esta política en caso de que se identifiquen modificaciones en la EPMTT, su estructura, objetivos o cualquier situación que afecte a la organización, con el fin de garantizar que siga siendo adecuada y se adapte a la misión, visión, objetivos y requisitos institucionales.

6.9.5.2 Lineamientos específicos

- Es responsabilidad de la máxima autoridad, directivos y personal de la EPMTT poner en práctica el Sistema de Gestión de Riesgos, el cual es un mecanismo estratégico que busca mejorar la administración de procesos, personas, infraestructura y tecnología, y fomentar la competitividad, la confianza de los grupos de interés, y el cumplimiento de los objetivos estratégicos y operativos de la empresa.
- La política forma parte del sistema de gestión de riesgos de la EPMTT, que se basa en normas internacionales y se lleva a cabo mediante la creación de herramientas como guías, matrices, mapas de riesgos y controles en todos los procesos de la cadena de valor. Estos recursos se guardan en un repositorio para su consulta y ayudan en la identificación y evaluación de los riesgos presentes y futuros.
- La responsabilidad de gestionar un riesgo recae en el área donde este surge, y es su deber garantizar la implementación de acciones para prevenir y reducir cualquier contingencia que pudiera afectar la realización de sus operaciones. En caso de ser necesario, también deben asegurar la recuperación y continuidad de los servicios, para así lograr los objetivos a pesar de que el riesgo se materialice.
- Es obligación del responsable del proceso elaborar planes de mitigación y contingencia para los riesgos identificados. Estos planes deben ser difundidos entre el personal de las áreas correspondientes. El responsable del proceso también debe llevar a cabo revisiones periódicas del sistema de gestión de riesgos y mantener registros de las distintas fases del proceso, que incluyen la identificación, evaluación, tratamiento, monitoreo y revisión de riesgos.
- El encargado del proceso que identificó el riesgo es responsable de monitorear el cumplimiento de los requisitos, incluyendo la política, y de realizar auditorías internas de acuerdo con el procedimiento de monitoreo y revisión de la gestión de riesgos, para verificar el cumplimiento o incumplimiento de dichos requisitos.

6.9.5.3 Seguridad de los activos esenciales

- Para garantizar la seguridad de los datos esenciales y servicios vitales del negocio, es necesario enfocarse en los procedimientos y responsabilidades operacionales. Esta política contempla la implementación de procedimientos para acceder a la información, procesarla, realizar respaldos, controlar y registrar errores, así como para contactar al soporte técnico y para reiniciar, apagar, encender y recuperar los sistemas; además, se proyectan los requisitos futuros de capacidad en procesamiento, memoria y almacenamiento, y se establecen ambientes separados para reducir los riesgos de accesos no autorizados.

6.9.5.4 Seguridad de los datos/Información

- Es fundamental crear pautas precisas para la categorización de la información, asignar responsabilidades a cada departamento y establecer procedimientos para su reorganización; así también, resulta crucial determinar las funciones de custodio y propietario. Es necesario establecer criterios para evaluar la sensibilidad de la información y su gestión.
- Se debe implementar un proceso para realizar copias de seguridad y restauración de la información, lo cual implica definir el tipo de copia de seguridad, la periodicidad de esta, el lugar donde se almacenarán, las tecnologías que se utilizarán para ello y la eliminación adecuada de las copias de seguridad.

6.9.5.5 Seguridad en la encriptación

- Se debe llevar a cabo la gestión de usuarios a fin de controlar el acceso a la información, para lo cual se requiere un procedimiento que permita crear, inhabilitar o eliminar cuentas de usuario dentro del dominio de la empresa, abarcando tanto a los usuarios internos como a los externos, así como también establecer contraseñas temporales cuando sea necesario.

- La administración de privilegios conlleva identificar los responsables de los sistemas y establecer un procedimiento para manejar cambios de puesto o función, así como realizar evaluaciones periódicas de dichos privilegios.
- Es necesario garantizar la autenticidad del usuario mediante el uso de contraseñas temporales, el bloqueo de cuentas tras varios intentos fallidos, implementando procedimientos para desbloquearlas y evitando el uso de credenciales preestablecidas.
- Cuando se utilice los servicios de red es necesario controlar sus accesos, mediante procedimientos para el uso de servicios como el correo electrónico, el acceso a internet y la gestión de usuarios externos. Además, se debe prohibir el intercambio de contraseñas y definir procedimientos para el manejo de puertos, como Telnet y SSH, así como también bloquear los puertos que no se estén utilizando.
- Implementar un mecanismo que cierre automáticamente las sesiones en los sistemas operativos después de un cierto tiempo de inactividad, con el fin de controlar el acceso a los mismos.
- Establecer el uso de VPN para trabajo remoto.
- La implementación de medidas de seguridad criptográficas para proteger la información requiere la gestión adecuada de las claves criptográficas, lo que implica establecer un proceso completo que abarque su creación, distribución, modificación, revocación, y pérdida o eliminación.

6.9.5.6 Seguridad de los servicios

- Es esencial activar y mantener registros detallados de actividades y eventos en los sistemas y servicios informáticos para realizar su seguimiento y control. Estos registros deben incluir información como fechas, direcciones IP y datos modificados, y también deben contener registros de la activación y desactivación de medidas de seguridad, es importante monitorear los equipos mediante herramientas de seguimiento de tráfico de red y alarmas, y sincronizar el reloj de los dispositivos a través del servicio NTP.
- La Unidad Tecnológica tendrá la responsabilidad de garantizar la seguridad de los procesos de desarrollo y mantenimiento de sistemas, aplicaciones y

servicios, para ello, se encargará de elaborar las directrices, procedimientos y reglamentos necesarios que se deben seguir en estos procesos.

6.9.5.7 Seguridad del software

- La Unidad Tecnológica establecerá las pautas específicas para el desarrollo de aplicaciones, y se definirán los requisitos y especificaciones técnicas tanto para software adquirido externamente como para desarrollos internos, todo ello con el objetivo de salvaguardar la propiedad intelectual.
- Para garantizar la seguridad contra la entrada de código malicioso, es necesario hacer uso de herramientas de control en equipos finales (endpoints) y servidores, esto incluye el uso de tecnologías antivirus, actualización, parches y la utilización de software legal.

6.9.5.8 Seguridad del hardware

- Es importante asumir la responsabilidad de los activos tecnológicos mediante el mantenimiento de un registro actualizado que contenga información detallada acerca de cada uno de ellos, incluyendo la marca, modelo, número de serie, código, ubicación y estado actual. Asimismo, es necesario contar con un proceso establecido para gestionar la devolución de los activos.
- La política de seguridad contempla la devolución segura de equipos y su posible reutilización, a través de la implementación de un procedimiento que incluye el retorno de los equipos, el formateo y reasignación, además de la elaboración de un informe técnico y la realización de copias de seguridad de la información relevante.
- Por último, se establece un proceso para el final de la gestión, mantenimiento y término de la vida útil de los equipos. Es necesario implementar un procedimiento seguro para retirar los equipos y contar con un protocolo de acción en caso de hurto o robo.

6.9.5.9 Seguridad de redes de comunicaciones

- Para garantizar la seguridad en las comunicaciones, es necesario crear un inventario de los equipos activos en la red, establecer indicadores de disponibilidad, utilizar encriptación en los canales de datos y establecer acuerdos de nivel de servicio (SLA). Además, se debe mantener una documentación completa que incluya esquemas físicos y lógicos de redes, inventario de equipos, esquema de direccionamiento IP, respaldo de configuración de herramientas de seguridad como PRTG, firewalls, ISE, AAA, controlador WLAN, telefonía IP, videoconferencia, switches de core, distribución y acceso.
- Para llevar a cabo la transferencia de datos entre instituciones, es imprescindible administrar el intercambio de información correspondiente a cada una, lo cual incluye la firma de acuerdos y convenios de confidencialidad. Así también, es fundamental establecer acuerdos de nivel de servicio y verificar el cumplimiento de las políticas de seguridad de cada institución.

6.9.5.10 Seguridad de Soportes de información

- Para asegurar los medios de almacenamiento de información es importante establecer contraseñas y privilegios adecuados sobre la información en las carpetas compartidas y los medios de almacenamiento extraíbles, incluyendo el uso de dispositivos como memorias USB y discos duros externos.

6.9.5.11 Seguridad de equipamiento auxiliar

- Es necesario establecer la ubicación, protección y mantenimiento del equipamiento auxiliar, implementando un plan de mantenimiento adecuado, es importante contar con instalaciones de suministro eléctrico y otros servicios operativos, incluyendo la utilización de dispositivos UPS y generadores redundantes, así como la correcta identificación del cableado de datos y eléctrico.

- La seguridad del cableado se garantiza cumpliendo con las normativas establecidas y restringiendo el acceso a ductos, racks y otros elementos.

6.9.5.12 Seguridad de instalaciones

- Para la seguridad física y del entorno es necesario implementar sistemas y procedimientos de control de acceso a las instalaciones, centros de datos y cuartos de comunicaciones, que incluyan la elaboración de un listado de personal autorizado, el uso de tecnología biométrica y la emisión de gafetes.
- Es importante garantizar la seguridad de los centros de datos o salas de comunicaciones frente a posibles amenazas externas o ambientales, para ello, se deben implementar sistemas de detección y extinción de incendios.
- Definición de áreas de acceso público y zonas para carga/descarga de bienes o servicios.
- Implementación de políticas de seguridad para documentos en el puesto de trabajo y políticas de impresión.

6.9.5.13 Seguridad de personal

- Definición de las funciones y responsabilidades de los empleados, así como la adhesión a las políticas, normas, procedimientos, tecnologías, planes y programas de seguridad de la información.
- Realización de una investigación de antecedentes para comprobar que los candidatos cumplen con los requisitos legales.
- Firmar acuerdos de confidencialidad con los empleados y proveedores.
- La empresa es responsable de capacitar y socializar periódicamente las funciones y responsabilidades en seguridad de la información.
- Se establece la responsabilidad de talento humano en la desactivación de usuarios en caso de traslados de puestos, desvinculación, licencias, comisión de servicios, etc.
- Talento humano debe establecer un procedimiento disciplinario de conformidad con normativa vigente, según el cual a los servidores públicos está prohibido utilizar, difundir, reproducir, divulgar o publicar información de

la EPMTT, ya sea de manera verbal o escrita, por medios físicos o digitales, con fines distintos a los relacionados con el cumplimiento de sus deberes y responsabilidades laborales.

6.10 Capacitación y concienciación

Se identificarán las necesidades de capacitación tanto para el personal de tecnología de la información como para los usuarios que hacen uso de los servicios. Estas necesidades serán integradas en un plan de capacitación que se creará en conjunto con la unidad de talento humano. El plan se enfocará en los cargos y requerimientos específicos de conocimiento determinados por la evaluación de desempeño e institucional. El responsable de la Unidad Tecnológica establecerá los temas prioritarios para la capacitación y los comunicará por correo electrónico. Se definirán los horarios y participantes de forma que no interrumpan la continuidad operativa del negocio.

A continuación, se detalla el temario a ser implementado en el plan de capacitación:

Tabla 6.20 Temario para la capacitación de la EPMTT

Temario	Duración (horas)
Normas y estándares de seguridad de la información	30
Amenazas y vulnerabilidades	10
Métodos de ataque cibernéticos • Difusión de software dañino (virus, gusanos, spyware, troyanos, ransomware, adware) • Ataques de red (spamming, phishing, botnets, denegación de servicio-DOS/DDOS) • Ingeniería Social (correo electrónico, wifi free, pendrive baiting, ataques controlados alta gerencia)	10
Metodologías de análisis de riesgos	20
Internet y navegación segura	5
Hacking ético	5
Fundamentos de Ciberseguridad	20
TOTAL	**100**

Fuente: Elaboración propia