UNIVERSIDAD TECNICA DEL NORTE

FACULTAD DE POSTGRADO

MAESTRÍA EN COMPUTACION MENCION EN SEGURIDAD INFORMATICA

TEMA:

PROPUESTA METODOLOGICA DE GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN PARA LA COORDINACION DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓNES DE LA ASOCIACION DE MUNICIPALIDADES ECUATORIANAS (AME), TOMANDO COMO REFERENCIA LA NORMATIVA NTE INEN ISO/IEC 27005.

Trabajo de Titulación previo a la obtención del Título de

Magíster en Computación con Mención en Seguridad Informática.

AUTOR: Ing. Marcelo Renán Proaño Santacruz

DIRECTOR: PhD. Ángel Jaramillo Alcázar

ASESOR: Msc. Mauricio Rea Peñafiel

IBARRA - ECUADOR

2024

DEDICATORIA

Querida esposa e hijos,

En este importante momento de mi vida, quiero dedicar el trabajo de investigación a ustedes, mi mayor fuente de inspiración y apoyo incondicional. A lo largo de este arduo viaje académico, ustedes han sido mi roca, mi motivación y mi razón para esforzarme cada día.

Han compartido conmigo las alegrías de los logros y han sido mi consuelo en los momentos de desafío. Su amor y paciencia infinitos han hecho posible que alcance este importante hito en mi carrera.

No solo es un testimonio de mi dedicación y esfuerzo, sino también de su compromiso inquebrantable y apoyo constante.

Cada página escrita y cada descubrimiento realizado están impregnados de gratitud hacia ustedes por ser la familia maravillosa que son.

Espero que no solo sea un logro personal, sino también un tributo a la unidad y fortaleza de nuestra familia. Que sirva como un recordatorio de que juntos, podemos superar cualquier desafío que la vida nos presente.

Con amor y agradecimiento eterno,

Marcelo Renán

AGRADECIMIENTOS

Hoy, en este significativo momento de mi vida académica, deseo expresar mi más profundo agradecimiento a todos ustedes. Este logro no habría sido posible sin su valiosa contribución, orientación y apoyo.

En primer lugar, quiero agradecer a mi director y asesor de tesis, el PhD. Ángel Jaramillo y al Msc. Mauricio Rea, por su dedicación incansable, sabiduría y paciencia a lo largo de este proceso. Su guía experta y sus comentarios críticos fueron fundamentales para dar forma a esta investigación.

A todos mis profesores y mentores a lo largo de mi trayecto académico, les agradezco por compartir su conocimiento y ayudarme a crecer como estudiante e investigador.

A mis amigos y compañeros de clase, les agradezco por el apoyo emocional, las conversaciones estimulantes y el sentido de comunidad que compartimos durante este viaje.

A mi familia, especialmente a mi cónyuge, hijos y padres, le estoy profundamente agradecido por su amor incondicional, su comprensión y su apoyo constante. Son mi razón de ser y la fuente de mi motivación.

Este logro es el resultado de un esfuerzo conjunto y de la generosidad de muchos. Espero que mi trabajo no solo contribuya al campo de estudio, sino que también sea un reflejo de la gratitud que siento hacia todos ustedes.

CONSTANCIA DE APROBACIÓN DEL TUTOR

En calidad de tutor del Trabajo de Grado: “PROPUESTA METODOLOGICA DE GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN PARA LA COORDINACION DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓNES DE LA ASOCIACION DE MUNICIPALIDADES ECUATORIANAS (AME), TOMANDO COMO REFERENCIA LA NORMATIVA NTE INEN ISO/IEC 27005, presentado por el Ing. Marcelo Renán Proaño Santacruz, para optar por el grado de Magister en Computación mención Seguridad Informática, doy fe que dicho trabajo reúne los requisitos y méritos suficientes para ser sometido a presentación y evaluación por parte del jurado examinador que se designe.

Atentamente,

Firmado electrónicamente por:
ANGEL GABRIEL
JARAMILLO ALCAZAR

PhD. Ángel Jaramillo Alcázar

Tutor

UNIVERSIDAD TÉCNICA DEL NORTE

BIBLIOTECA UNIVERSITARIA

AUTORIZACIÓN DE USO Y PUBLICACIÓN

A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

1. IDENTIFICACIÓN DE LA OBRA

En cumplimiento del Art. 144 de la Ley de Educación Superior, hago la entrega del presente trabajo a la Universidad Técnica del Norte para que sea publicado en el Repositorio Digital Institucional, para lo cual pongo a disposición la siguiente información:

DATOS DE CONTACTO			
CÉDULA DE IDENTIDAD	1710586742		
APELLIDOS Y NOMBRES	Proaño Santacruz Marcelo Renán		
DIRECCIÓN	Yaruquí, Simón Bolívar N1-228 y Abdón Calderón		
EMAIL	mrproanos@utn.edu.ec		
TELÉFONO FIJO	022-777093	**TELÉFONO MÓVIL:**	**0999596259**
DATOS DE LA OBRA			
TÍTULO:	"PROPUESTA METODOLOGICA DE GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN PARA LA COORDINACION DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓNES DE LA ASOCIACION DE MUNICIPALIDADES ECUATORIANAS (AME), TOMANDO COMO REFERENCIA LA NORMATIVA NTE INEN ISO/IEC 27005"		
AUTOR (ES):	Proaño Santacruz Marcelo Renán		
FECHA: DD/MM/AAAA	25/11/2024		
SOLO PARA TRABAJOS DE GRADO			
PROGRAMA DE POSGRADO			
TITULO POR EL QUE OPTA	MAESTRÍA EN COMPUTACION MENCIÓN SEGURIDAD INFORMATICA		
ASESOR/TUTOR	MsC. Mauricio Rea Peñafiel PhD. Ángel Jaramillo Alcázar		

2. CONSTANCIAS

El autor manifiesta que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto, la obra es original y que es el titular de los derechos patrimoniales, por lo que asume la responsabilidad sobre elcontenido de la misma y saldrá en defensa de la Universidad en caso de reclamación porparte de terceros.

Ibarra, a los 25 días del mes de noviembre de 2024

EL AUTOR:

Firmado electrónicamente por:
MARCELO RENAN
PROANO SANTACRUZ

Ing. Marcelo Renán Proaño Santacruz.
C.I: 1710586742

RESUMEN

La investigación, se centra en la gestión de riesgos en sistemas de información, específicamente en el contexto de la Coordinación de Tecnologías de la Información y Comunicaciones de la Asociación de Municipalidades Ecuatorianas; quien enfrenta desafíos críticos relacionados con la seguridad de la información y la continuidad operativa, lo que resalta la necesidad de desarrollar una propuesta metodológica para abordar estos riesgos.

El objetivo principal de esta investigación es desarrollar una propuesta metodológica adaptada a las necesidades específicas de la Coordinación de Tecnologías de la Información y Comunicaciones de la Asociación de Municipalidades Ecuatorianas.

Adicionalmente, la propuesta metodológica tiene como propósito identificar, evaluar y mitigar los riesgos en sistemas tecnológicos, asegurando la seguridad y protección de la información crítica.

Para lograr una gestión efectiva de riesgos, se ha tomado como referencia la normativa NTE INEN ISO/IEC 27005. Este estándar sirve como base sólida para la creación de la propuesta metodológica.

La adaptación efectiva de organizaciones como la Asociación de Municipalidades Ecuatorianas, es crucial en este contexto. Además, se destaca la importancia de aprovechar experiencias previas de organizaciones comparables en la implementación de propuestas metodológicas de gestión de riesgos en sistemas de información.

En conclusión, este estudio aborda la gestión de riesgos en sistemas de información relacionados con los procesos críticos de la CTIC, destacando la importancia de considerar tanto las regulaciones locales como internacionales.

La propuesta metodológica ofrece una estrategia sólida para garantizar la integridad y confidencialidad de los datos en el contexto de la Coordinación de tecnologías de la Información y Comunicaciones de la Asociación de Municipalidades Ecuatorianas, contribuyendo así a la modernización y seguridad de sus procesos.

Palabras clave: Gestión de riesgos, seguridad de la información, Tecnologías de la Información y Comunicaciones, Asociación de Municipalidades Ecuatorianas, NTE INEN ISO/IEC 27005

ABSTRACT

The research focuses on risk management in information systems, specifically in the context of the Coordination of Information and Communications Technologies of the Association of Ecuadorian Municipalities; who faces critical challenges related to information security and operational continuity, which highlights the need to develop a methodological proposal to address these risks.

The main objective of this research is to develop a methodological proposal adapted to the specific needs of the Information and Communications Technologies Coordination of the Association of Ecuadorian Municipalities.

Additionally, the purpose of the methodological proposal is to identify, evaluate and mitigate risks in technological systems, ensuring the security and protection of critical information.

To achieve effective risk management, the NTE INEN ISO/IEC 27005 standard has been taken as a reference. This standard serves as a solid basis for the creation of the methodological proposal.

The effective adaptation of organizations such as the Association of Ecuadorian Municipalities is crucial in this context. Furthermore, the importance of taking advantage of previous experiences of comparable organizations in the implementation of methodological proposals for risk management in information systems is highlighted.

In conclusion, this study addresses risk management in information systems related to critical CTIC processes, highlighting the importance of considering both local and international regulations.

The methodological proposal offers a solid strategy to guarantee the integrity and confidentiality of data in the context of the Coordination of Information and Communications Technologies of the Association of Ecuadorian Municipalities, thus contributing to the modernization and security of its processes.

Key words: Risk management, information security, Information and Communication Technologies, Association of Ecuadorian Municipalities, NTE INEN ISO/IEC 27005.

INDICE DE CONTENIDO

INDICE DE TABLAS

INDICE DE FIGURAS

INTRODUCCIÓN

En el entorno digital actual, la seguridad de la información se ha convertido en un aspecto importante para las organizaciones, especialmente en aquellas que manejan datos sensibles como la Asociación de Municipalidades Ecuatorianas (AME), por lo que se requiere de una adecuada estrategia de gestión de riesgos para proteger la confidencialidad, integridad y disponibilidad de la información. Frente a ello la norma NTE INEN ISO/IEC 27005 ofrece un marco metodológico para gestionar eficazmente los riesgos asociados a la seguridad de la información, proporcionando directrices para identificar, evaluar y tratar estos riesgos de manera sistemática (Organización Internacional de Normalización, 2022).

Es así, que el principal problema que enfrenta la AME es la falta de un enfoque unificado y estandarizado para gestionar los riesgos de seguridad de la información, lo cual aumenta la exposición a amenazas que podrían comprometer la seguridad de los datos. Esta situación es especialmente crítica debido a la creciente dependencia de las TIC para la prestación de servicios municipales y la gestión de la información pública. Sin un marco claro y aplicado uniformemente, las municipalidades afiliadas corren el riesgo de sufrir incidentes de seguridad que pueden resultar en la interrupción de servicios esenciales para la ciudadanía.

En este contexto, es fundamental entender los conceptos de amenaza, riesgo y vulnerabilidad, donde una amenaza se refiere a cualquier potencial evento o acción que pueda explotar una debilidad en un sistema, causando un impacto negativo en la confidencialidad, integridad o disponibilidad de la información. Mientras que el riesgo es la probabilidad de que una amenaza se materialice y cause un daño, considerando tanto la probabilidad como la severidad del impacto. Y la vulnerabilidad, por su parte, es una

debilidad inherente en un sistema que puede ser explotada por una amenaza, aumentando la posibilidad de que ocurra un incidente de seguridad.

Es por ello, que la presente propuesta es relevante para asegurar que la AME y sus municipalidades afiliadas puedan gestionar los riesgos de seguridad de la información de manera proactiva y eficiente. Ya que al implementar una metodología basada en la norma NTE INEN ISO/IEC 27005 permitirá a la AME fortalecer sus capacidades para prevenir, detectar y responder a incidentes de seguridad, minimizando el impacto de posibles amenazas. Además, esta intervención contribuirá a una mayor confianza en los sistemas de información municipales, mejorando así la calidad de los servicios ofrecidos a los ciudadanos y promoviendo un entorno digital más seguro.

CAPITULO I

EL PROBLEMA

1.1. Problema de Investigación

La Asociación de Municipalidades Ecuatorianas (AME) es una institución que promueve la construcción de un modelo de gestión local descentralizado y autónomo basado en la planificación articulada y la gestión participativa del territorio (Asociación de Municipalidades Ecuatorianas, 2014). Dentro de su estructura se encuentra la Coordinación de Tecnologías de la Información y Comunicaciones (CTIC) que se encarga de preservar la integridad, confidencialidad y disponibilidad de la información asociada a la provisión de servicios ofrecidos a los Gobiernos Autónomos Descentralizados Municipales, misma que es gestionada a través de diversas herramientas informáticas por lo que manifiesta la necesidad de implementar una metodología robusta de seguridad de dicha información.

Al respecto, la CTIC carece de una metodología adecuada para gestionar los riesgos asociados con sus sistemas de información, lo que pone en riesgo tanto la seguridad como la eficiencia de dichos sistemas. En donde la ausencia de un enfoque estructurado expone a la organización a una serie de amenazas potenciales, incluyendo la pérdida de información, ataques cibernéticos y divulgación no autorizada, entre otras. Estas vulnerabilidades no solo comprometen la seguridad de los sistemas de información, sino que también afectan la capacidad de la CTIC para cumplir con su misión de brindar asistencia técnica de calidad y coordinación eficiente con otros niveles de gobierno y organismos del Estado.

Por lo tanto, es crucial que la CTIC adopte una metodología específica y efectiva para la gestión de riesgos de seguridad de la información, para lo cual, puede alinearse con la normativa NTE INEN ISO/IEC 27005, que proporciona directrices para la implementación

de un sistema de gestión de seguridad de la información mediante un enfoque sistemático y estructurado para la identificación, evaluación y tratamiento de los riesgos de seguridad de la información.

1.2. Interrogantes de la Investigación

RQ1: ¿Qué procesos y requisitos de la norma NTE INEN ISO/IEC 27005 son relevantes en el contexto de la Coordinación de Tecnologías de la Información y Comunicaciones de la Asociación de Municipalidades Ecuatorianas (AME)?

RQ2: ¿Cuál es la situación actual de la Coordinación de Tecnologías de la Información y Comunicaciones (CTIC) de la Asociación de Municipalidades Ecuatorianas (AME) en relación a la gestión de riesgos de seguridad de la información?

RQ3: ¿De qué manera se puede mejorar la gestión de riesgos de seguridad de la información de la Coordinación de Tecnologías de la Información y Comunicaciones de la AME?

1.3. Objetivos de la Investigación

1.3.1. Objetivo General

Elaborar una propuesta metodológica de gestión de riesgos de seguridad de la información para la Coordinación de Tecnologías de la Información y Comunicaciones de la Asociación de Municipalidades Ecuatorianas (AME), tomando como referencia la norma NTE INEN ISO/IEC 27005.

Hipótesis

La implementación de una propuesta metodológica basada en la NORMATIVA NTE INEN ISO/IEC 27005 mejorará significativamente la gestión de riesgos de seguridad de la información en la Coordinación de Tecnologías de la Información y Comunicaciones de la Asociación de Municipalidades Ecuatorianas (AME).

Hipótesis Alternativa

La implementación de una propuesta metodológica basada en la NORMATIVA NTE INEN ISO/IEC 27005 mejorará significativamente la gestión de riesgos de seguridad de la información en la Coordinación de Tecnologías de la Información y Comunicaciones de la Asociación de Municipalidades Ecuatorianas (AME).

Categorización de Variables

Variable independiente: Propuesta metodológica basada en la NORMATIVA NTE INEN ISO/IEC 27005

Variable dependiente: Gestión de riesgos de seguridad de la información.

1.3.2 Objetivos Específicos

OE1: Analizar la situación actual de la Coordinación de Tecnologías de la Información y Comunicaciones (CTIC) de la Asociación de Municipalidades Ecuatorianas (AME) en relación a la gestión de riesgos de seguridad de la información.

OE2: Revisar y adaptar los procesos y requisitos de la norma NTE INEN ISO/IEC 27005 en el contexto de la Coordinación de Tecnologías de la Información y Comunicaciones de la Asociación de Municipalidades Ecuatorianas (AME).

OE3: Elaborar y validar la guía metodológica de gestión de riesgos de seguridad de la información de la Coordinación de Tecnologías de la Información y Comunicaciones de la AME, alineada a los mejores elementos de la NTE INEN ISO/IEC 27005, y su aplicación en los activos de información más críticos.

1.4. Justificación

La presente investigación se justifica desde distintos enfoques como:

Aportes al Área de Conocimiento

El desarrollo de la presente investigación contribuye significativamente al área de la seguridad de la información, especialmente en el contexto de instituciones públicas. Pues la adaptación y aplicación de la normativa NTE INEN ISO/IEC 27005 en la AME proporcionará un caso práctico valioso que puede servir de referencia para otras instituciones similares en el país y la región. Además, el desarrollo de una metodología para la gestión de riesgos de seguridad de la información enriquecerá la literatura académica y práctica en el campo de la ciberseguridad.

Beneficiarios

Los principales beneficiarios de esta propuesta son la Asociación de Municipalidades Ecuatorianas (AME) y los Gobiernos Autónomos Descentralizados Municipales (GADM). En cuanto a la AME, se fortalecerá la protección de sus activos informáticos, mejorando la integridad, confidencialidad y disponibilidad de la información, lo cual aumentará la confianza en su gestión. Mientras los GADM, que reciben servicios y soporte tecnológico de la AME, se beneficiarán al contar con una infraestructura de información más segura y confiable, permitiendo una gestión más eficiente y segura de sus operaciones y datos municipales.

Repercusión en el Desarrollo Nacional

La implementación de esta propuesta metodológica tiene una repercusión significativa en el desarrollo nacional, pues según el Plan de Desarrollo para el Nuevo Ecuador, en su objetivo 14, indica: “Propender la construcción de un Estado eficiente, transparente y orientado al bienestar social”. Por lo que este estudio, contribuirá a

garantizar una gestión eficiente y segura de la información, en donde se alineará con los esfuerzos nacionales para mejorar la eficiencia y autonomía de los procesos estatales, promoviendo así un entorno más seguro y confiable para la administración pública.

Impacto en la Calidad de Vida

El diseño de una metodología personalizada para el análisis y gestión de riesgos en los sistemas de información robusto en la Asociación de Municipalidades Ecuatorianas (AME), puede mejorar la calidad de vida de los ciudadanos al asegurar que los servicios municipales se gestionen de manera más segura. Esto permitirá contar con la protección adecuada de la información sensible evitará problemas como la pérdida de datos, el fraude y otros incidentes de seguridad que podrían afectar directamente a los ciudadanos, fortaleciendo la confianza de los ciudadanos en las instituciones gubernamentales en la gestión de sus datos.

CAPITULO II

MARCO REFERENCIAL

2.1. Marco Teórico

Tras una revisión documental se pudo identificar diversos aspectos de relevancia para el desarrollo del presente trabajo, aunque cabe mencionar que no existen trabajos similares orientados a una organización como la del objeto de estudio; pero sí se encuentran elementos que pueden adaptarse a este sector. En este sentido, se describen dimensiones necesarias para la mejora de la gestión de sus riesgos informáticos.

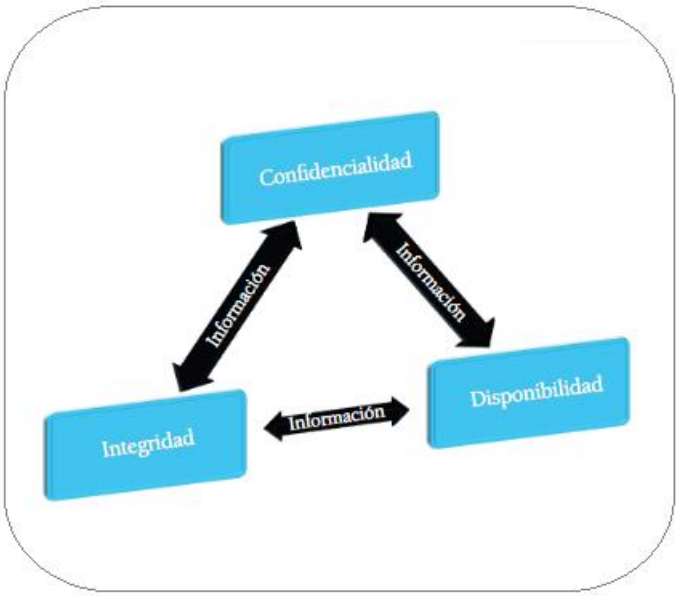
2.1.1. Gestión del riesgo informático

Para comprenderla gestión de riesgo, es importante entender este concepto se basa en la combinación de probabilidad de que una amenaza se concrete (Kowask et al., 2018), por lo que la gestión del riesgo tendría por objeto evitar esta ocurrencia y proteger los activos ante atacantes, desastres naturales o diversas situaciones que se pueden presentar (Vega, 2021).

Por lo que, en contraparte, la seguridad de la información puede definirse como la protección de la información en relación con varios tipos de amenazas, a fin de garantizar la continuidad del negocio, minimizando los riesgos que puedan comprometerlo, y maximizando el retorno sobre las inversiones y las oportunidades de la organización Kowask et al., (2018). Lo que se puede lograr mediante la implementación de un conjunto de controles, políticas, procesos, procedimientos, estructuras organizacionales.

Mientras que Valencia (2021) considera que la seguridad de la información se asocia a tres factores basados en confidencialidad, integridad y disponibilidad, por lo que estos determinan la base para plantear los objetivos que se deben alcanzar en función de un adecuado sistema de gestión de seguridad de la información:

Figura 1. *Triada de la seguridad de la Información*



Fuente: Valencia (2021)

Según Valencia (2021), estos componentes son fundamentales en la gestión de la seguridad de la información, ya que la confidencialidad implica que la información debe ser accesible únicamente por las personas, entidades o mecanismos autorizados, protegiendo así los datos sensibles de accesos no autorizados. Por otra parte, la integridad se refiere a la propiedad de salvaguardar la exactitud y consistencia de la información y de los activos tecnológicos, garantizando que no sean modificados o destruidos de manera no autorizada. En cuanto a la disponibilidad, se requiere que los datos permanezcan precisos y completos y accesibles.

2.1.2. Estándares de la Seguridad de la Información

La seguridad de la información se consigue mediante un conjunto de controles, políticas, procesos, procedimientos, estructuras organizativas y funciones de software y hardware. Lo que se logra estableciendo, implementando, monitorizando, revisando y

mejorando estos controles para asegurar que se cumplan los objetivos de seguridad de la organización. Por lo tanto, a continuación, se revisan los aportes desde distintas normas:

Tabla 1. *Resumen comparativo entre las normas*

Norma	Título	Objetivo	Observación
27001	Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos	Especificar los requisitos para establecer, implementar, operar, monitorear, analizar críticamente, mantener y mejorar un SGSI documentado en el contexto de los riesgos de negocio globales de la organización. Especifica requisitos para la implementación de controles de seguridad personalizados para las necesidades individuales de organizaciones o de sus partes. Cubre todos los tipos de organización (emprendimientos comerciales, agencias gubernamentales, organizaciones sin fines lucrativos, entre diversas otras).	Tratar más específicamente de directrices y principios para un sistema de gestión de seguridad de la información.
27002	Tecnología de la información. Técnicas de seguridad.	Establece directrices y principios generales para iniciar, implementar,	Enfocada a controles de seguridad.

	Código de práctica para la de gestión de seguridad de	mantener y mejorar la gestión de seguridad de la información. Los objetivos definidos en esta norma establecen directrices generales para las metas y mejores prácticas para la gestión de la seguridad de la información.	
27005	Tecnología de la información. Técnicas de seguridad. Gestión del riesgo de seguridad de	Presenta un sistema de gestión del riesgo de seguridad de la información con énfasis en tecnología de la información.	Aclara como realizar la gestión del riesgo de seguridad de información
31000	Gestión del riesgo. Principios y directrices.	Norma que presenta principios y directrices básicas para la gestión del riesgo en general en cualquier tipo de ambiente.	Editada en 2009, de este año en delante las demás normas de gestión del riesgo deben estar alineadas a esta.
31010	Gestión del riesgo. Técnicas para el proceso de evaluación del riesgo.	Describe las diversas técnicas y herramientas de análisis d	Editada en 2012.
GUIDE 73	Gestión del riesgo. Vocabulario	Presenta las definiciones de términos genéricos relacionados con la gestión del riesgo.	Editada en 2009.

Fuente: Kowask et al, (2018)

Puede observarse por ejemplo que la NTE INEN ISO/IEC 27001 especifica los requisitos para establecer, implementar, operar, monitorear y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI), lo que garantizará la adopción de controles personalizados y adaptados a las necesidades de la organización. Mientras que la NTE INEN ISO/IEC 27002 complementa esta norma al proporcionar directrices y principios para mejorar la seguridad de la información. En cuanto a la NTE INEN ISO/IEC 27005, base principal de la propuesta metodológica, presenta un sistema de gestión del riesgo de seguridad de la información con énfasis en tecnología, aclarando cómo realizar la gestión del riesgo, crucial para identificar, evaluar y tratar los riesgos que afectan la seguridad de la información sensible.

Por otra parte, la ISO 31000, aunque no específica para TI, ofrece principios y directrices básicas para la gestión del riesgo en cualquier ambiente, proporcionando un marco adicional para una metodología robusta. Finalmente, la ISO 31010 describe técnicas y herramientas de análisis del riesgo, proporcionando métodos prácticos que pueden ser integrados en la propuesta para identificar y mitigar los riesgos de manera más efectiva.

Así también, Castro y Bayona (2011), considera los estándares ISO 31000 e ISO 27005 en donde menciona que estos:

> Proveen lineamientos generales, pero hace falta una guía más precisa que ofrezca pautas sobre la forma de lograr los aspectos de seguridad requeridos; adicionalmente este marco hace referencia a la gestión sobre los riesgos como concepto global y deja de lado el análisis de riesgos específicos como el tecnológico, lo más cercano es la administración del riesgo operativo en el que se relaciona de forma tangencial el riesgo tecnológico. (p.57)

2.1.3. Normativa NTE INEN ISO/IEC 27005

Antecedentes

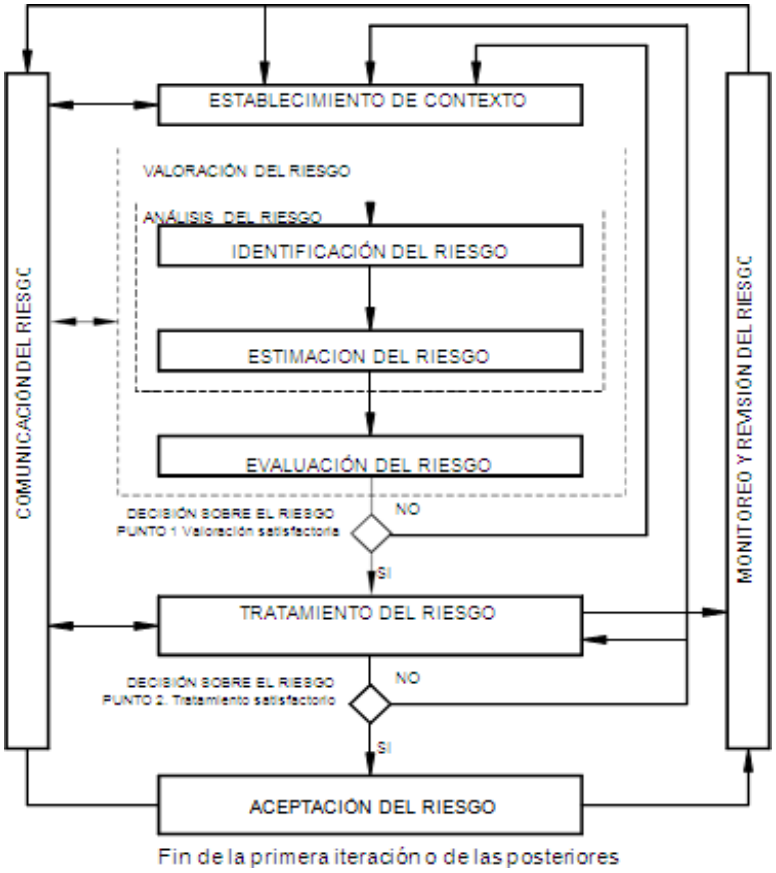
La normativa ISO/IEC 27005 ha experimentado una evolución significativa desde su última actualización en 2022. Esta revisión introdujo el documento bajo el nuevo nombre de “ISO/IEC 27005:2022 – Seguridad de la información, ciberseguridad y protección de la privacidad: directrices para la gestión de riesgos de seguridad de la información”, reemplazando a la versión anterior de 2018. La actualización alineó el texto con la normativa ISO/IEC 27001:2022 y la ISO 31000:2018, ajustando tanto la terminología como la estructura de las cláusulas para reflejar estos cambios. Se incorporaron conceptos adicionales como "escenarios de riesgo" y se ofreció una nueva directriz para contrastar enfoques en la identificación de riesgos, consolidando además los anexos en uno solo que ofrece criterios y técnicas prácticas para la gestión de riesgos (Audetic, 2023).

El alcance de la ISO/IEC 27005:2022 es proporcionar una guía integral para implementar los requisitos de gestión de riesgos especificados en la ISO/IEC 27001, y para complementar la gestión de riesgos en el contexto de la seguridad de la información con orientación adicional basada en ISO 31000. Aunque esta normativa no se presenta como una metodología específica, proporciona una base sólida para construir una metodología adaptada a las necesidades particulares de las organizaciones. Su aplicabilidad es universal, sirviendo tanto a organizaciones que buscan establecer o mejorar sus sistemas de gestión de seguridad de la información como a profesionales involucrados en la gestión de riesgos en este ámbito (Audetic, 2023).

En el país, esta norma ha sido adoptada como NTE INEN-ISO/IEC 27005:2012 por el Instituto Ecuatoriano de Normalización (INEN), la cual, es compatible con los conceptos de ISO/IEC 27001 y está diseñada para apoyar la implementación de un Sistema de Gestión

de Seguridad de la Información (SGSI) basado en un enfoque de gestión de riesgos. Por lo que exige un proceso estructurado, sistemático y riguroso de análisis para elaborar el plan de tratamiento de riesgos y determinar la probabilidad de una organización para enfrentar un riesgo que exceda el impacto permitido.

Figura 2. *Componentes NTE INEN ISO/IEC 27005*



Fuente: INEN (2008)

Por lo tanto, se estiman los siguientes procesos:

1. Establecimiento del Contexto

Este parte de la definición de criterios básicos de evaluación del riesgo, de impacto, y la aceptación del riesgo. Lo que permitirá a la AME establecer un marco sólido para

evaluar y gestionar los riesgos específicos a su entorno. Posteriormente se debe definir el alcance y los límites de la gestión de riesgos para asegurar que todos los activos y procesos críticos estén cubiertos. Finalmente, se procede a organizar la gestión del riesgo de la seguridad de la información lo que implica asignar roles y responsabilidades claras dentro de la CTIC, garantizando que todos los niveles de la AME estén involucrados en la protección continua de la información.

2. Valoración del riesgo

Esta valoración del riesgo involucra la identificación detallada de los riesgos que enfrenta la institución. Lo que abarca la identificación de activos, amenazas, controles existentes, vulnerabilidades y las posibles consecuencias de estos riesgos. Después de esta actividad se debe realizar la estimación del riesgo a través de metodologías específicas para valorar las consecuencias y la probabilidad de incidentes, estableciendo un nivel de riesgo. Finalmente, se procede a la evaluación del riesgo, que compara los niveles de riesgo estimados con los criterios predefinidos para determinar si los riesgos son aceptables o requieren mitigación.

3. Tratamiento del riesgo

Al respeto, este proceso se enfoca en que se va a realizar con los riesgos encontrados, por lo que estos pueden asumirse desde una acción de reducción, retención, evitación o transferencia del riesgo, lo que implica implementar medidas para disminuir la probabilidad o mitigar el impacto de los riesgos identificados, aceptar ciertos riesgos dentro de límites aceptables sin intervención adicional, modificar actividades o sistemas para eliminar riesgos potenciales o transferir la responsabilidad del riesgo a terceros cuando sea adecuado. Por lo que estas acciones pueden contribuir a que la Coordinación de

Tecnologías de la Información y Comunicaciones (CTIC) maneje eficazmente los riesgos de seguridad de la información, protegiendo los activos y garantizando la continuidad operativa frente a amenazas potenciales.

4. Aceptación del riesgo

El proceso de aceptación del riesgo implica la decisión consciente de la AME de asumir ciertos riesgos identificados sin aplicar medidas adicionales para mitigarlos. Esta decisión se basa en evaluaciones que indican que los costos de mitigación pueden superar los beneficios esperados o que el riesgo residual es considerado aceptable dentro de los límites establecidos.

5. Comunicación de los Riesgos

La comunicación de los riesgos hallados involucra la transmisión clara y efectiva de información sobre los riesgos de seguridad de la información dentro de la AME. Lo que incluye identificar, documentar y comunicar los riesgos de manera comprensible a todas las partes interesadas, asegurando que se comprendan las implicaciones y las acciones necesarias para manejarlos de forma adecuada.

6. Monitoreo y Revisión del Riesgo

Este proceso, parte del monitoreo y revisión de los factores del riesgo, gracias al control continuo de los factores que contribuyen a los riesgos de seguridad identificados, como cambios en el entorno tecnológico, nuevas amenazas, o debilidades en los controles implementados. Luego este proceso de debe enfocar al monitoreo, revisión y mejora de la gestión de riesgos, lo que incluye revisar la eficacia de los controles existentes, identificar áreas de mejora, y ajustar las estrategias de mitigación según sea necesario para garantizar una gestión de riesgos continua y eficiente en la institución.

2.2.4. Metodologías de Gestión de Riesgos Informáticos

La norma ISO/IEC 27005: 2012 no especifica instrumentos orientados a la evaluación de riesgos, por lo que su selección y uso son decisión de cada entidad acorde a su naturaleza y necesidades. Al respecto puede mencionarse la NIST SP 800-30 que es un enfoque reconocido internacionalmente para la evaluación y gestión de riesgos de seguridad de la información (National Institute of Standards and Technology , 2012).

Así mismo, otra metodología utilizada para la gestión de riesgos informáticos es la basada en MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Públicas) desarrollada por el MINTEL, la que está orientada a todas las instituciones del sector público ecuatoriano. Esta metodología implementa la gestión de riesgos para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información.

2.2. Marco legal

Es importante considerar tanto las regulaciones locales como las normativas internacionales relacionadas con la gestión de riesgos en sistemas de información proporcionan el marco legal en el que opera la Coordinación de Tecnologías de la Información y Comunicaciones de la Asociación de Municipalidades Ecuatorianas para influir en los requisitos de seguridad y gestión de riesgos que debe cumplir.

2.2.1. Regulaciones y Normativas Internacionales

Norma ISO 27001

La norma ISO 27001 establece un marco internacional reconocido para la gestión de la seguridad de la información en las organizaciones, enfocándose en proteger los datos contra amenazas internas y externas. Por lo que este estándar se orienta a la gestión de riesgos, que implica identificar, evaluar y abordar de manera sistemática los riesgos de

seguridad. Para ello usa el ciclo PDCA (Planificar-Hacer-Verificar-Actuar) para garantizar mejoras continuas, donde se planifican medidas de seguridad, se implementan controles adecuados, se monitorea el desempeño a través de auditorías y se ajusta el sistema según sea necesario (NQA, 2022).

Por lo que este enfoque sistemático y adaptable hace que la ISO 27001 sea fundamental para cualquier organización como la Ame, en su búsqueda de asegurar la protección de sus activos de información y manejar los riesgos de seguridad de manera efectiva.

Marco de Ciberseguridad del Instituto Nacional de Estándares y Tecnología

El Marco de Ciberseguridad es propuesto por el Instituto Nacional de Estándares y Tecnología (NIST, una entidad dependiente del Departamento de Comercio de EE. UU. Este Marco de Ciberseguridad está orientado a prestar ayuda a los negocios de todo tamaño a comprender mejor sus riesgos de ciberseguridad, administrar y reducir sus riesgos, y proteger sus redes y datos. Sin embargo, cabe mencionar que este instrumento es voluntario, pero puede brindar a una organización una reseña de las mejores prácticas para ayudarlo a decidir dónde tiene que concentrar su tiempo y su dinero en cuestiones de protección de ciberseguridad desde cinco áreas: identificación protección, detección, respuesta y recuperación (Comisión Federal de Comercio, 2022).

Reglamento General de Protección de Datos

El Reglamento General de Protección de Datos (RGPD) es una regulación de la Unión Europea (UE) que tiene repercusiones significativas a nivel mundial en la gestión de riesgos informáticos. Aunque se centra en la protección de la privacidad de los datos personales dentro de la UE, su alcance se extiende más allá de sus fronteras debido a su impacto en las prácticas globales de manejo de datos (Unión Europea, 2016).

Para la aplicación del RGPD, se exige que las organizaciones implementen medidas rigurosas para proteger la información personal, lo cual incluye no solo datos de ciudadanos, sino también de cualquier individuo cuyos datos personales sean procesados por organizaciones sujetas al RGPD. Esto implica adoptar prácticas de gestión de datos transparentes, segura y ética, asegurando así la privacidad y la integridad de la información en un entorno digital cada vez más interconectado y vulnerable a amenazas.

Estrategia Interamericana Integral para Combatir las Amenazas a la Seguridad Cibernética

Esta estrategia se aprobó desde el año 2004 por los países de la OEA, por lo que ha sido adoptada por sus varios países, quienes han implementado acciones y regulaciones específicas que abordan la gestión de riesgos informáticos de manera integral (Organización de Estados Americanos, 2004).

Por otra parte, además de las disposiciones sobre gestión de riesgos informáticos, estas regulaciones suelen incluir medidas para fortalecer la protección de datos personales, fomentar la colaboración público-privada en materia de ciberseguridad y establecer mecanismos de supervisión y cumplimiento para asegurar el cumplimiento de las normativas establecidas.

2.3.1. Leyes y Normativas Nacionales

Plan de Desarrollo para el Nuevo Ecuador 2024-2025

En concordancia con su objetivo 9 que indica: “Propender la construcción de un Estado eficiente, transparente y orientado al bienestar social”, se establece la necesidad de desarrollar y fortalecer herramientas de información centradas en las Tecnologías de la Información y la Comunicación (TIC) (Secretaría Nacional de Planificación , 2024).

Este enfoque es fundamental para mejorar la capacidad del Estado de gestionar y utilizar la información de manera efectiva, facilitando la toma de decisiones informadas y la prestación de servicios públicos de alta calidad, integrando soluciones se promueve la eficiencia administrativa, se optimizan los recursos y se mejoran los procesos internos, lo cual contribuye a la transparencia gubernamental.

Además, el fortalecimiento de estas herramientas de gestión de la información permite una mayor participación ciudadana, proporcionando plataformas para la interacción y el acceso a la información pública. De este modo, se impulsa el bienestar social al asegurar que las políticas y servicios estén alineados con las necesidades y expectativas de la población.

2.3.1.2. Ley Orgánica de Protección de Datos Personales

La Ley Orgánica de Protección de Datos Personales, aprobada en el registro oficial 459 de fecha 26 de mayo de 2021, señala: “Art. 1.-Objeto y finalidad.- El objeto y finalidad de la presente ley es garantizar el ejercicio del derecho a la protección de datos personales, que incluye el acceso y decisión sobre información y datos de este carácter, así como su correspondiente protección, Para dicho efecto regula, prevé y desarrolla principios, derechos, obligaciones y mecanismos de tutela.”, las cuales todas las entidades están obligadas a cumplir, por lo que en base a dichos lineamientos se deben establecer metodologías, procedimientos y políticas internas que permitan dar el cumplimiento a la misma (Ley Orgánica de Protección de Datos Personales, 2021, Art. 1).

2.3.1.3. Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos

La Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, Registro Oficial 557 de 17 de abril de 2002, señala: “Art. 1. Objeto de la Ley. - Esta Ley regula los mensajes de datos, la firma electrónica, los servicios de certificación, la contratación

electrónica y telemática, la prestación de servicios electrónicos a través de redes de información, incluido el comercio electrónico y la protección a los usuarios de estos sistemas". (Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, 2002, Art. 1).

2.3.1.5. Estatuto de la Asociación de Municipalidades Ecuatorianas.

Este estatuto establece el marco normativo y organizacional que rige el funcionamiento de la institución. Conforme a su finalidad de promover la colaboración y el desarrollo de los municipios del Ecuador, la AME tiene la responsabilidad de desarrollar políticas específicas para el manejo de la información que administra (Estatuto de la Asociación de Municipalidades Ecuatorianas, 2014).

Esto incluye la creación de procedimientos rigurosos para la recopilación, almacenamiento, protección y uso de datos, asegurando su integridad, confidencialidad y disponibilidad. Por lo que sus políticas deben alinearse con las mejores prácticas internacionales y normativas locales sobre gestión de información y ciberseguridad, garantizando así que la AME pueda cumplir con sus objetivos de manera eficiente y transparente.

CAPITULO III

MARCO METODOLÓGICO

3.1. Descripción del área de estudio

La presente investigación se llevó a cabo en la Asociación de Municipalidades Ecuatorianas, una instancia asociativa que agrupa a Gobiernos Autónomos Descentralizados Municipales y Metropolitanos. La asociación está ubicada en la ciudad de Quito, Ecuador, y desempeña un papel fundamental en la promoción de un modelo de gestión local descentralizado y autónomo.

La Asociación de Municipalidades Ecuatorianas dada su naturaleza asociativa y su enfoque en la planificación articulada y la gestión participativa del territorio, maneja información vital de todo tipo en sus diversos sistemas y herramientas tecnológicas en ámbitos administrativos, financieros, tributarios, etc.

3.2. Contexto de la Organización.

La Asociación de Municipalidades Ecuatorianas, puede contextualizarse desde su misión y visión, tal como se lo expresa a continuación:

Misión

La Asociación de Municipalidades Ecuatorianas es una instancia asociativa de los Gobiernos Autónomos Descentralizados Municipales y Metropolitanos que promueve la construcción de un modelo de gestión local descentralizado y autónomo, con base en la planificación articulada y la gestión participativa del territorio, a través del ejercicio de la representación institucional, asistencia técnica de calidad y la coordinación con otros niveles de gobierno y organismos del Estado. (Asociación de Municipalidades Ecuatorianas, 2022).

Visión

La Asociación de Municipalidades Ecuatorianas es una instancia asociativa de los Gobiernos Autónomos Descentralizados Municipales y Metropolitanos que promueve la construcción de un modelo de gestión local descentralizado y autónomo, con base en la planificación articulada y la gestión participativa del territorio, a través del ejercicio de la representación institucional, asistencia técnica de calidad y la coordinación con otros niveles de gobierno y organismos del Estado .(Asociación de Municipalidades Ecuatorianas, 2022)

3.3. Enfoque y tipo de investigación

3.2.1. Enfoque y Tipo de Investigación

El enfoque asumido para abordar el problema de investigación es principalmente cualitativo, con elementos de enfoque mixto para complementar y enriquecer la comprensión del fenómeno estudiado. A continuación, se detalla la elección de este enfoque y se describe el tipo de investigación adoptado.

3.2.2. Enfoque Cualitativo

El enfoque cualitativo fue seleccionado debido a la naturaleza exploratoria y comprensiva de la investigación, dado que el estudio se centra en la implementación de una Metodología para el Análisis y Gestión de Riesgos de los sistemas de información en la entidad asociativa de los Gobiernos Autónomos Descentralizados y se enfoca en la percepción de los participantes, por lo que este enfoque es idóneo para capturar las complejidades del tema. Además, este enfoque permitió profundizar en las experiencias, perspectivas y desafíos de los actores involucrados, y se adapta al estudio de realidades subjetivas en diferentes contextos.

3.2.3. Enfoque Mixto

Se integran elementos del enfoque mixto al utilizar tanto datos cualitativos como cuantitativos. Aunque el énfasis principal es cualitativo, se recopilarán algunos datos cuantitativos para respaldar y contextualizar ciertos aspectos de la investigación.

3.2.4. Tipo de Investigación: Exploratorio y Descriptivo:

En cuanto al tipo de investigación, se adopta un enfoque exploratorio y descriptivo. En donde la fase exploratoria tiene como objetivo explorar en profundidad el contexto y comprender las necesidades y desafíos específicos de la Coordinación de Tecnologías de la Información y Comunicaciones (CTIC) de la Asociación de Municipalidades Ecuatorianas (AME), en relación con la seguridad de la información. Esta fase permite la identificación de factores clave que luego serán abordados diseño y en la implementación. Posteriormente, la fase descriptiva se centra en la implementación concreta de la metodología y en la descripción detallada de los resultados obtenidos.

3.3. Procedimiento de investigación

El procedimiento de investigación que se llevará a cabo se estructura en varias fases para abordar de manera efectiva el tema propuesto. Cada fase se desarrollará en función de los objetivos específicos de la investigación, de esta manera:

OE1: Se realizará una revisión preliminar de literatura en donde se recopile y analice la información existente sobre la normativa NTE INEN ISO/IEC 27005, identificando los aspectos clave a considerar en la elaboración de la metodología de la asociación.

OE2: Se realizará el proceso de recolección de datos aplicando técnicas como encuestas, revisión de documentación y registros de la organización para obtener la información sobre la coordinación de tecnologías de la información y comunicaciones de la Asociación de Municipalidades Ecuatorianas (AME) y su entorno.

OE3: Se definirá el marco de trabajo a ser utilizado en base al análisis realizado, se validará la guía metodológica a través de su aplicación en los activos de información más críticos identificados de la coordinación de tecnologías de la información y comunicaciones de la Asociación de Municipalidades Ecuatorianas (AME).

De igual forma, se tiene previsto desarrollar la investigación con las siguientes fases:

Fase 1: Planteamiento y definición del problema: en esta etapa, se identificará el problema relacionado con la gestión de riesgos de la Coordinación de Tecnologías de la Información y Comunicaciones (CTIC), para lo que se llevará a cabo una revisión de la literatura existente, centrándose en la gestión de riesgos en sistemas de información. Esta fase también involucra la formulación de las preguntas de investigación pertinentes y la definición de los objetivos específicos de la investigación.

Fase 2: Diseño de los instrumentos, recopilación de datos y validación: se procede a la recopilación de datos siguiendo los métodos y el cronograma establecidos. Se recopilan datos de manera precisa y sistemática a través de encuestas, entrevistas y análisis de documentos, y se almacenan de forma segura para su análisis posterior. Durante esta fase, se presta especial atención a la calidad y la integridad de los datos recopilados.

Fase 3: Análisis de datos: se realiza su procesamiento y análisis, lo que incluye la limpieza de los datos, análisis cualitativos según corresponda. Este análisis es fundamental para responder a las preguntas de investigación y extraer conclusiones basadas en evidencia.

Fase 4: Diseño de la propuesta: en esta fase, se procede al diseño de una metodología personalizada para la gestión de riesgos en la Coordinación de Tecnologías

de la Información y Comunicaciones (CTIC) de la Asociación de Municipalidades Ecuatorianas (AME) a partir de los resultados obtenidos en la fase anterior.

Fase 5: Validación y evaluación de la metodología: la metodología propuesta se somete a una fase de validación se validará la guía metodológica a través de su aplicación en dos activos de información más críticos identificados de la coordinación de tecnologías de la información y comunicaciones de la Asociación de Municipalidades Ecuatorianas (AME), garantizando que la metodología sea efectiva y viable.

Fase 6: Conclusiones y recomendaciones: se resumen las principales conclusiones de la investigación y se destacan las contribuciones al campo de la gestión de riesgos en sistemas de información. A continuación, se formulan recomendaciones finales para la implementación de la metodología en la Asociación de Municipalidades Ecuatorianas y se sugieren posibles direcciones para futuras investigaciones en este ámbito.

3.4. Consideraciones bioéticas

El proyecto de investigación en cuestión no hará uso, modificación o experimentación con elementos naturales y/o su información genética.

Conforme a lo dispuesto en la Ley Orgánica de Servicio Público la Institución tiene la potestad de disponer la colaboración de los servidores públicos en actividades concernientes a la misma.

3.5. Instrumentos

Se plantea aplicar un modelo de cuestionario basado en la metodología COSO que aborda los niveles de madurez respecto a la gestión de riesgos de seguridad de la información para la Coordinación de Tecnologías de la Información y Comunicaciones de

la Asociación de Municipalidades Ecuatorianas (AME). En donde se considera la siguiente escala:

Tabla 2. *Nivel de madurez*

Nivel de madurez	Interpretación
0	No se evidencia proceso alguno con respecto a la gestión de riesgo.
1	La evaluación del riesgo se lo hace según la necesidad, por lo que este proceso no es replicable en otras circunstancias
2	En este nivel el proceso puede ser replicable, pero se aplica solo en proyectos de importancia o para solucionar problemas específicos
3	Existe un proceso documentado para la evaluación de riesgo
4	A más de la documentación del proceso existe medición y control de sus resultados
5	Existe un proceso optimizado

Fuente: Fernández y Monteros (2014)

La población del estudio estuvo conformada por el coordinador de la CTIC y 1 funcionario del área de infraestructura tecnológica, 1 funcionario del área de desarrollo de software y 1 funcionario del área de soporte tecnológico lo que permitió garantizar la confiabilidad de los resultados.

Los datos recopilados durante la encuesta no se compartirán sin su consentimiento y sus respuestas se mantendrán completamente confidenciales.

CAPITULO IV

ANÁLISIS DE RESULTADOS

A continuación, se describen los principales resultados obtenidos considerando el nivel de madurez para cada área de estudio (AME, 2024).

4.1. Políticas y prácticas de gerencia de riesgos

Tabla 3. *Políticas y prácticas de gerencia de riesgos*

Pregunta	Resultado	Nivel de madurez	Promedio
1.¿La Asociación de Municipalidades Ecuatorianas (AME) dispone de una política general para la gestión de riesgos tecnológicos, y ha sido esta comunicada internamente?	1	0.2	
2.¿La Asociación de Municipalidades Ecuatorianas (AME) cuenta con un mapa de riesgos que incluya la identificación, descripción y priorización de los mismos?	2	0.4	0.486
3. ¿La Asociación de Municipalidades Ecuatorianas (AME) ha implementado un proceso formal de gestión de riesgos?	2	0.4	
4. ¿En la Asociación de Municipalidades Ecuatorianas (AME) se ha adoptado alguno de los marcos de referencia como COBIT, COSO, ISO, MAGERIT u otros?	2	0.4	
5. ¿La Asociación de Municipalidades Ecuatorianas (AME) realiza alguna actividad de auditoría informática?	3	0.6	
6. En caso de existir una, ¿cómo describiría usted la relación entre la gestión de riesgos y la función de auditoría?	2	0.4	

7.Según su perspectiva, ¿qué grado de participación tiene la gestión de riesgos en las actividades de control interno realizadas para cumplir con los requisitos regulatorios?	5	0.6

Fuente: Elaboración propia

Respecto al uso de políticas para la Gestión de Riesgos Tecnológicos y Comunicación Interna, la Asociación de Municipalidades Ecuatorianas (AME) evalúa el riesgo según sus necesidades lo que indica que no existe un proceso estructurado y replicable para la gestión de riesgos tecnológicos. En donde la falta de una política general establecida y comunicada internamente sugiere una gestión reactiva más que proactiva debido a una falta de concienciación sobre la importancia de la gestión de riesgos o a una ausencia de recursos y formación adecuados para desarrollar e implementar políticas efectivas.

Referente al uso de algún tipo de mapa de riesgos, se halló que la entidad posee un proceso para su elaboración, el cual es replicable, pero se usa únicamente en proyectos importantes o para solucionar problemas específicos. Aunque hay un reconocimiento de la necesidad de identificar y priorizar riesgos, la implementación limitada sugiere que la organización aún no ha integrado completamente esta práctica en su cultura organizacional posiblemente por falta de interés de la dirección o de recursos insuficientes para una implementación más amplia.

Se consideró también la existencia de un proceso formal de gestión de riesgos, que similar al mapa de riesgos, este es replicable solo en circunstancias específicas, por lo que la ausencia de un enfoque sistemático y continuo para la gestión del riesgo puede aumentar la vulnerabilidad de la organización ante amenazas imprevistas a causa de una falta de

priorización de la gestión de riesgos en la agenda estratégica de la organización o por barreras operativas que dificultan la implementación de un proceso formalizado.

Además, que la adopción de algún marco de referencia es limitada, y se orientan también a proyectos importantes o problemas específicos, lo que refleja una integración parcial de estándares reconocidos en la gestión de riesgos, lo cual puede limitar la eficacia y consistencia del proceso lo que destaca una falta de capacitación especializada en estos marcos o una resistencia al cambio dentro de la organización.

Sobre la existencia de un proceso documentado para la auditoría informática, este es un punto positivo, indicando así la presencia de un nivel de madurez más avanzado en comparación con las otras dimensiones evaluadas. Sin embargo, esta documentación por sí sola no garantiza la efectividad del proceso si no se acompaña de una implementación rigurosa y de la correspondiente retroalimentación para mejoras continuas.

En cuanto, a la relación entre la gestión de riesgos y la función de auditoría se encuentra un nivel de madurez bajo, lo que sugiere una falta de integración y coordinación entre ambas funciones, lo cual puede afectar la capacidad de la organización para identificar y mitigar los riesgos de manera efectiva, que puede estar influenciada por una comunicación inadecuada entre las diferentes áreas de la AME.

Respecto a la participación de la gestión del riesgo en el control interno, se halló que tiene una participación documentada, lo cual es un avance significativo. Sin embargo, la efectividad de esta participación dependerá de la calidad de la documentación y de la forma en que se implemente y supervise este control, lo que podría estar relacionada con iniciativas recientes para fortalecer el control interno, aunque aún haya espacio para mejoras en términos de medición y control de resultados.

Figura 3. *Políticas y prácticas de gerencia de riesgo*

Fuente: Elaboración propia

De manera general, con respecto a la dimensión de políticas y prácticas de gerencia de riesgos, los resultados obtenidos reflejan una gestión que se encuentra en un estado de madurez intermedio, con varios procesos replicables, pero no completamente integrados ni optimizados. En donde la principal afectación es la vulnerabilidad ante riesgos no gestionados de manera sistemática, lo cual puede tener consecuencias negativas para la seguridad de la información y la continuidad operativa. Puede identificarse causas que incluyen una falta de políticas claras y comunicadas, una implementación limitada de marcos de referencia reconocidos y una coordinación insuficiente entre la gestión de riesgos y otras funciones clave como la auditoría; para avanzar hacia niveles más altos de madurez, la AME deberá priorizar la formalización y documentación de sus procesos, así como la integración de la gestión de riesgos en todos los niveles de la organización.

4.2. Comunicación

Tabla 4. *Comunicación*

Dimensión	Resultado	Nivel de madurez	Promedio
1. Según su opinión, ¿la Asociación de Municipalidades Ecuatorianas (AME) comunica eficazmente sus políticas y acciones de gestión de riesgos?	2	0.4	
2. ¿Hasta qué punto la Asociación de Municipalidades Ecuatorianas (AME) divulga sus riesgos en sus informes (reporte anual, documentos de referencia, etc.)?	2	0.4	
3. ¿En qué medida la Asociación de Municipalidades Ecuatorianas (AME) incluye información sobre sus programas de seguros en sus reportes financieros?	5	1	0.50
4. ¿Existe una política de seguridad de la información?	2	0.4	
5. En caso de existir, ¿considera usted que la Asociación de Municipalidades Ecuatorianas (AME) comunica adecuadamente las políticas de seguridad de la información a todo el personal?	2	0.4	
6. Según su opinión, ¿el personal está consciente de las posibles consecuencias y responsabilidades en caso de incumplir las normativas de seguridad?	2	0.4	

Fuente: Elaboración propia

Respecto al ámbito de la Comunicación de Políticas y Acciones de Gestión de Riesgos se halló que la AME no comunica sus políticas y acciones de gestión de riesgos de manera eficiente acorde a un grado de madurez bajo, por lo que esta falta de

comunicación puede llevar a una percepción limitada sobre la importancia de la gestión de riesgos entre los empleados y partes interesadas, lo que refleja una estrategia de comunicación deficiente, falta de recursos dedicados a la divulgación o un enfoque limitado a situaciones críticas.

En cuanto a divulgación, la AME divulga sus riesgos en informes anuales y documentos de referencia de manera replicable, pero de nuevo, principalmente en proyectos importantes. Esto sugiere que la organización no ha integrado plenamente la divulgación de riesgos en su cultura de transparencia y rendición de cuentas. La divulgación limitada podría deberse a una falta de normativas internas que obliguen a una divulgación más exhaustiva o a una percepción de que dicha divulgación podría tener impactos negativos.

Otro aspecto considerado es la inclusión de información sobre programas de seguros en donde se encontró que reportes financieros están documentados, lo que indica un paso adelante en la formalización de la gestión de riesgos. Sin embargo, es importante que a más de documentar la información esta se debe acompañar de un análisis riguroso y una comprensión clara por parte de todos los actores involucrados, destacando el reconocimiento de la necesidad de transparencia de la información, aunque la implementación de programas de seguros aún puede estar en proceso de optimización.

Se indagó también sobre la existencia de políticas de seguridad de la información, la cual demostró un nivel de madurez, bajo por lo que está replicada en proyectos importantes, pero no es una práctica extendida a toda la organización. Esto puede indicar una falta de compromiso institucional hacia la seguridad de la información, posiblemente debido a una falta de comprensión de los riesgos asociados o a una carencia de liderazgo en esta área.

Respecto a la comunicación adecuada de las políticas de seguridad de la información al personal, tampoco tiene un nivel de madurez adecuado, ya que se replica en circunstancias específicas, sin estar generalizada. Esto puede llevar a una falta de comprensión y cumplimiento de las políticas de seguridad por parte de los empleados, incrementando así los riesgos de seguridad. En problema se profundiza por una estrategia de comunicación interna insuficiente, falta de capacitación continua o una baja prioridad dada a la comunicación de políticas.

Respecto a la conciencia del personal sobre las consecuencias y responsabilidades en caso de incumplir las normativas de seguridad, puede llevar a incumplimientos no intencionados y a un aumento en los incidentes de seguridad. Lo que puede estar influenciado por una falta de formación continua, ausencia de programas de sensibilización sobre seguridad o una cultura organizacional que no enfatiza la importancia de la seguridad de la información.

Figura 4. *Comunicación*

Fuente: Elaboración propia

A manera de resumen, los resultados obtenidos respecto al ámbito comunicativo reflejan una gestión de riesgos de seguridad de la información en la AME que se encuentra en un nivel de madurez bajo a intermedio. Por lo que estas prácticas son replicables pero limitadas a circunstancias específicas, lo que indica una falta de integración y sistematización en la gestión de riesgos. Las principales afectaciones derivadas de estos resultados pueden fomentar una mayor vulnerabilidad a incidentes de seguridad, una baja conciencia y cumplimiento de políticas de seguridad entre el personal, y una divulgación limitada de riesgos que podría afectar la transparencia y la confianza de las partes interesadas.

4.3. Amenazas y riesgos

Tabla 5. *Amenazas y riesgos*

Dimensión	Resultado	Nivel de madurez	Promedio
1. En el contexto económico actual, ¿ha observado cambios en las amenazas que enfrenta su organización?	5	1	
2. Con las tendencias actuales hacia el uso de redes sociales, computación en la nube y dispositivos móviles personales en las organizaciones, ¿ha notado cambios en el entorno de riesgos que enfrenta su organización?	2	0.4	0.533
3. ¿Dispone su organización de un programa establecido de gestión de riesgos de TI para manejar los riesgos asociados con el uso de redes sociales, computación en la nube y dispositivos móviles personales?	1	0.2	

Fuente: Elaboración propia

Sobre los cambios en las amenazas que enfrenta la organización en el ámbito económico, los resultados muestran un nivel de madurez bajo, por lo que la organización podría estar reaccionando de manera tardía a los cambios en el entorno económico, lo que

puede resultar en una preparación inadecuada para mitigar los riesgos emergentes. Además, la falta de proactividad puede llevar a vulnerabilidades y a una gestión de crisis menos eficaz. Este es un problema que se acentúa por la ausencia de un proceso formalizado y continuo para evaluar los cambios en el contexto económico.

En el ámbito tecnológico, se encontró que la AME reconoce y evalúa los riesgos derivados de las tendencias tecnológicas actuales, como el uso de redes sociales, computación en la nube y dispositivos móviles, pero lo hace de manera esporádica o sólo cuando se considera necesario. Esto puede resultar en vulnerabilidades no anticipadas, afectando la seguridad de la información y los sistemas.

En cuanto al uso de algún programa de gestión de riesgos, se obtuvo un resultado de madurez bajo bajos, ya que la AME tiene un programa de gestión de riesgos de TI que se utiliza según la necesidad, pero no es replicable en diferentes circunstancias o situaciones, lo que puede llevar a una gestión inconsistente de los riesgos de TI, dejando a la organización vulnerable a una amplia gama de amenazas con un nivel de respuesta a incidentes ineficaz y descoordinado.

Figura 5. *Amenazas y riesgos*

Fuente: Elaboración propia

De manera general se encuentra una mayor deficiencia en el uso de programas de gestión de riesgos, por lo que existe una necesidad urgente de formalizar y estandarizar los procesos de evaluación de riesgos tanto económicos como tecnológicos, siendo la implementación de un proceso continuo es crucial para mejorar la preparación y la respuesta de la organización ante los cambios en estos contextos. De esta manera es importante desarrollar un programa de gestión de riesgos que sea replicable y aplicable en diversas circunstancias. Mismo que debe estar bien documentado y ser parte integral de la estrategia de seguridad de la información de la organización. Además, es importante el invertir en la capacitación del personal y en la asignación de recursos adecuados para la gestión de riesgos, además la adopción de tecnologías de soporte puede ayudar a elevar el nivel de madurez en estas áreas.

4.4. Herramientas y tecnología

Tabla 6. *Herramientas y tecnología*

Dimensión	Resultado	Nivel de madurez	Promedio
1. ¿Su organización emplea alguna tecnología particular para respaldar el proceso de gestión de riesgos?	2	0.4	
2. ¿La Asociación de Municipalidades Ecuatorianas (AME) utiliza actualmente tecnologías de virtualización?	3	0.6	0.667
3. ¿Su organización dispone de un software o control específico de gestión de accesos e identidades que reduzca los riesgos asociados con los derechos de acceso a sus datos y sistemas?	5	1	

Fuente: Elaboración propia

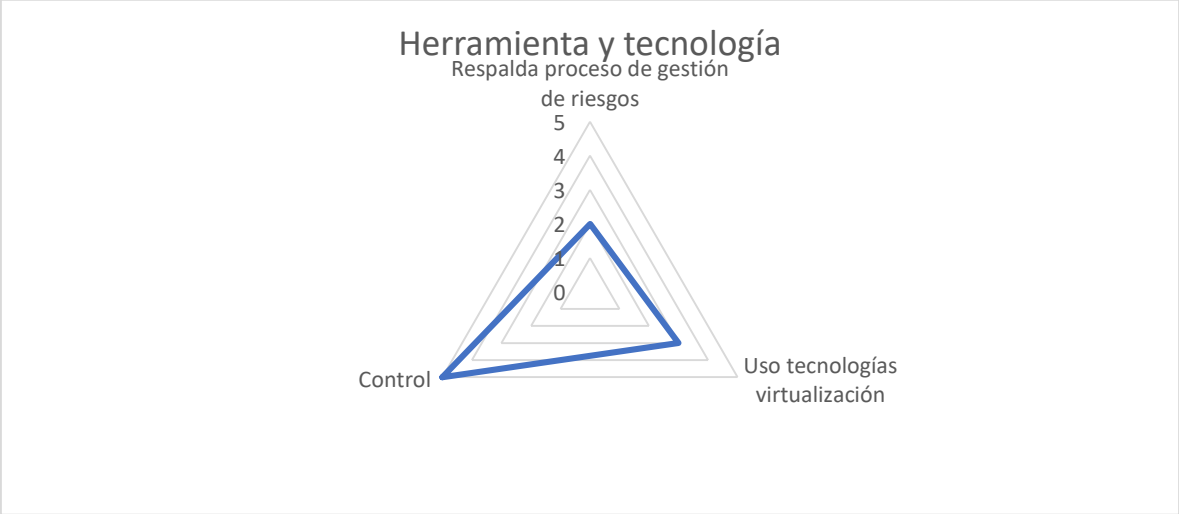
Con relación al empleo de tecnología para la gestión de riesgos, existe un nivel de madurez bajo, ya que la evaluación revela que la AME emplea tecnologías específicas para respaldar el proceso de gestión de riesgos, pero de manera replicable únicamente en situaciones específicas o proyectos importantes. Lo que sugiere, aunque la organización reconoce la importancia de utilizar tecnología para la gestión de riesgos, su implementación no es uniforme ni consistente en todas las áreas de la organización a causa de limitaciones presupuestarias, falta de personal especializado en tecnología de gestión de riesgos, y falta de una estrategia clara para la integración de estas tecnologías a nivel organizacional.

Se consideró también el uso de tecnologías de virtualización en donde se halló un nivel de madurez medio lo que refleja una adopción más formal y estructurada de tecnologías, que son esenciales para mejorar la eficiencia, la flexibilidad y la seguridad de las operaciones de TI. La documentación de este proceso sugiere que la organización está comprometida con la optimización de su infraestructura tecnológica, aunque todavía puede haber margen para mejoras en la medición y control de resultados para una mayor eficiencia operativa y una reducción en los costos de infraestructura, aunque la falta de un proceso completamente optimizado puede limitar el pleno aprovechamiento de estos beneficios.

En cuanto a la gestión de accesos e identidades, la AME dispone medios de control específico para la gestión de accesos e identidades, lo que también está documentado. Esto indica que la organización reconoce la importancia de controlar y mitigar los riesgos asociados con los derechos de acceso a datos y sistemas. Sin embargo, al igual que con las tecnologías de virtualización, la existencia de documentación sugiere un nivel de formalización y estructura, aunque puede faltar una optimización completa del proceso. En busca de una mayor seguridad en el acceso a la información y una reducción en los

incidentes de seguridad relacionados con accesos no autorizados, pero la falta de optimización puede significar que aún hay vulnerabilidades por abordar.

Figura 6. *Herramientas y tecnología*



Fuente: Elaboración propia

Como resultados generales, se observa que existe una adopción y uso de tecnologías para la gestión de riesgos en la AME que se encuentra en un nivel de madurez intermedio. Hay una implementación formal y documentada de tecnologías de virtualización y gestión de accesos e identidades, lo que indica una base sólida sobre la cual construir. Sin embargo, el uso de tecnologías para respaldar el proceso de gestión de riesgos es replicable sólo en circunstancias específicas, lo que sugiere la necesidad de una mayor integración y uniformidad en toda la organización.

4.5. Gobierno y control

Tabla 7. *Gobierno y control*

Dimensión	Resultado	Nivel de madurez	Promedio
1. ¿Ha implementado su organización un sistema de gestión de la seguridad de la información que incluya su administración general?	5	1	
2. ¿La Asociación de Municipalidades Ecuatorianas (AME) cuenta con un comité de seguridad de la información (CSI)?	1	0.2	
3. ¿La Asociación de Municipalidades Ecuatorianas (AME) dispone de un plan de respuesta a incidentes de seguridad?	2	0.4	
4. ¿Se ha llevado a cabo una evaluación de riesgos tecnológicos?	2	0.4	
5. ¿La Asociación de Municipalidades Ecuatorianas (AME) ha contratado una póliza contra delitos informáticos?	1	0.2	0.433
6. ¿La Asociación de Municipalidades Ecuatorianas (AME) tiene establecidos planes de contingencia?	2	0.4	

Fuente: Elaboración propia

Se indagó sobre la implementación de algún sistema de gestión de la seguridad de la información, en donde un nivel de madurez bajo, pues se halla que la AME ha implementado un sistema de gestión de la seguridad de la información que se aplica de manera replicable solo en proyectos importantes o para solucionar problemas específicos. Esto indica que, aunque existe un sistema, su aplicación no es uniforme ni extendida en toda la organización debido a la falta de una estrategia clara y una cultura organizacional que no prioriza la seguridad de la información de manera integral.

Se encontró también que la AME no cuenta con un comité de seguridad de la información formalmente establecido, lo que sugiere una falta de un enfoque estructurado e interés en la gestión de la seguridad de la información a nivel organizacional. Por lo que su ausencia puede afectar la capacidad de la organización para coordinar y supervisar eficazmente las iniciativas de seguridad de la información, así como para responder a incidentes de manera rápida y coherente.

También la AME dispone de un plan de respuesta a incidentes de seguridad que se aplica ante problemas específicos, lo que indica, aunque hay un plan en marcha, su aplicación no es uniforme ni generalizada por falta de entrenamiento adecuado del personal, la ausencia de simulacros regulares de respuesta a incidentes o una falta de actualización continua del plan para reflejar nuevas amenazas y vulnerabilidades.

En cuanto a la evaluación de riesgos tecnológicos la AME ha llevado a cabo evaluaciones en proyectos importantes o para solucionar problemas específicos. Lo que sugiere, aunque se reconocen los riesgos tecnológicos, la evaluación no es una práctica estándar ni continua en toda la organización, lo que puede ocasionar una incapacidad para identificar y mitigar de manera proactiva nuevos riesgos emergentes.

Respecto a uso de alguna póliza contra delitos informáticos, la AME no usa ni ha contratado algún tipo de póliza, lo que indica una falta de protección financiera ante posibles incidentes de ciberseguridad, lo que puede dejar a la organización vulnerable a pérdidas financieras significativas en caso de un ataque, lo que puede generar una falta de percepción del riesgo, consideraciones presupuestarias o una falta de conocimiento sobre la disponibilidad y beneficios de tales pólizas.

Finalmente, con respecto al uso de planes de contingencia, la AME si posee planes de contingencia, pero su aplicación no es uniforme ni extendida, ya que se usan en

situaciones específicas lo que responde a un nivel de madurez bajo. Lo que se puede relacionar con una falta de simulacros regulares, la falta de actualización de los planes o una falta de capacitación adecuada del personal sobre su implementación.

Figura 7. *Gobierno y control*

Fuente: Elaboración propia

Los resultados generales de la dimensión de gobierno y control, refleja un nivel de madurez intermedio en el gobierno y control de la gestión de seguridad de la información en la AME. Aunque existen ciertos elementos y procesos en marcha, su aplicación no es uniforme ni generalizada en toda la organización. Por lo que la falta de un comité de seguridad de la información y de una póliza contra delitos informáticos son áreas críticas que requieren atención urgente.

4.6. Resumen de hallazgos

A continuación, se hace un análisis general de todas las dimensiones abordadas según el nivel de madurez de la gestión de riesgos de seguridad de la información en la AME:

Figura 8. *Resumen de hallazgos*

Fuente: Elaboración propia

Las políticas y prácticas de gestión de riesgos en la AME se encuentran en un nivel intermedio de madurez, lo que sugiere que existen ciertas políticas y prácticas documentadas, pero no están completamente integradas ni optimizadas. En cuanto a la comunicación de las políticas y acciones de gestión de riesgos en la AME también muestra un nivel de madurez intermedio. Aunque hay esfuerzos por comunicar las políticas, estos no son completamente efectivos ni llegan a todo el personal de manera consistente.

Respecto a la identificación y evaluación de amenazas y riesgos en la AME se encuentra un nivel bajo de madurez. Esto indica que los procesos relacionados con la identificación y priorización de riesgos no están bien establecidos ni son consistentes lo que puede llevar a la organización a estar mal preparada para enfrentar incidentes de seguridad.

La dimensión de herramientas y tecnología presenta el nivel de madurez más alto entre las evaluadas, lo que sugiere que la AME ha implementado algunas tecnologías y herramientas específicas para apoyar la gestión de riesgos. Sin embargo, aún hay margen

para optimizar y mejorar la integración de estas tecnologías en los procesos generales de gestión de riesgos.

En cuanto al gobierno y control de la gestión de la seguridad de la información en la AME también se encuentra en un nivel bajo de madurez, por lo que hay una falta de estructuras de gobierno robustas y de control efectivo sobre los procesos de seguridad de la información. La ausencia de comités dedicados, planes de respuesta a incidentes y evaluaciones de riesgos tecnológicas contribuye a esta baja madurez.

CAPÍTULO V

PROPUESTA

Una vez determinado el proceso de diagnóstico con respecto al nivel de madurez de la gestión de riesgos de seguridad de la información dentro de la CTIC, se encontró deficiencias en los ámbitos de:

1. Gestión de amenazas y riesgos
2. Gobierno y control

Con respecto a ellos, se procede a desarrollar cada uno de los procesos establecidos en la NTE INEN-ISO/IEC 27005:2022, mismos que se alinean al Esquema Gubernamental de Seguridad de la Información (EGSI) versión 3.0, aspectos que se describen a continuación:

5.1. Establecimiento del Contexto

Para poder desarrollar este proceso, es necesario identificar en primer lugar los activos que gestiona la Coordinación de Tecnologías de la Información y Comunicaciones, los cuáles son los siguientes:

Tabla 8. *Servicios*

N° Activo	Proceso Macro	Subproceso	Tipo de activo	Nombre activo	Descripción activo	Propietario activo
A1	Coordinación general de TIC	Servicios	Software	Internet	Red global de comunicación	CTIC
A2	Coordinación general de TIC	Servicios	Software	Página web	Documentos accesibles a través de la web	CTIC

A3	Coordinación general de TIC	Servicios	Software	SIGAME	Sistema de gestión administrativa	CTIC
A4	Coordinación general de TIC	Servicios	Software	QUIPUX	Plataforma de gestión documental	CTIC
A5	Coordinación general de TIC	Servicios	Software	Correo Electrónico	Servicio digital de mensajería	CTIC
A6	Coordinación general de TIC	Servicios	Software	Mesa de Ayuda	Sistema de soporte técnico	CTIC
A7	Coordinación general de TIC	Servicios	Software	Plataforma Documental	Aclaración de dudas en normas procesos y procedimientos	CTIC

Fuente: Elaboración propia

Tabla 9. *Datos información*

N° Activo	Proceso Macro	Subproceso	Tipo de activo	Nombre activo	Descripción activo	Propieta-rio activo
A8	Coordinación general de TIC	Datos información	Software	Ficheros	Conjuntos de datos o documentos	CTIC
A9	Coordinación general de TIC	Datos información	Software	Contratos proveedores	acuerdos legales entre la institución y sus proveedores	CTIC

A10	Coordinación general de TIC	Datos información	Software	Copias respaldo	Réplicas de seguridad de datos críticos	CTIC
A11	Coordinación general de TIC	Datos información	Software	Archivo de copias de seguridad de la información	Repositorio de las copias de respaldo,	CTIC

Fuente: Elaboración propia

Tabla 10. *Aplicaciones informáticas*

N° Activo	Proceso Macro	Subproceso	Tipo de activo	Nombre activo	Descripción activo	Propietario activo
A12	Coordinación general de TIC	Aplicaciones informáticas	Software	SIGAMEE	Sistema Administrativo Financiero	CTIC
A13	Coordinación general de TIC	Aplicaciones informáticas	Software	EGAD	Sistema de Gestión POA	CTIC
A14	Coordinación general de TIC	Aplicaciones informáticas	Software	GCS (GESTION DE COMERCIALIZACIÓN DE SERVICIOS)	Sistema gestión catastros	CTIC
A 15	Coordinación general de TIC	Aplicaciones informáticas	Software	SISTEMA INTEGRAL DE	Sistema gestión predios urbanos y rurales	CTIC

				CATASTROS SIC		
A16	Coordinación general de TIC	Aplicaciones informáticas	Software	PLATAFORMA TECNOLÓGICA	Sistema de gestión en línea	CTIC
A17	Coordinación general de TIC	Aplicaciones informáticas	Software	SICOM	Sistema para registro de proyectos de cooperación	CTIC
A18	Coordinación general de TIC	Aplicaciones informáticas	Software	SGIDS	Sistema Integral de Desechos Sólidos	CTIC
A19	Coordinación general de TIC	Aplicaciones informáticas	Software	SISTEMA DE COMPROBANTES ELECTRÓNICOS	Sistema de gestión de comprobantes electrónicos	CTIC
A20	Coordinación general de TIC	Aplicaciones informáticas	Software	FACTURADOR UNIVERSAL	Sistema de facturación universal	CTIC
A21	Coordinación general de TIC	Aplicaciones informáticas	Software	MESA DE AYUDA	Herramienta de asistencia	CTIC
A22	Coordinación general de TIC	Aplicaciones informáticas	Software	SIOC - SISTEMA DE INFORMACIÓN DE OFERTA DE	Acceso a ofertas de cooperación no reembolsable	CTIC

				COOPERACIÓN		
A23	Coordinación general de TIC	Aplicaciones informáticas	Software	CONSULTA VEHICULAR	Herramienta de consulta los datos más importantes de un vehículo	CTIC
A24	Coordinación general de TIC	Aplicaciones informáticas	Software	FULLTIME	Sistema para el control de asistencia,	CTIC

Fuente: Elaboración propia

Tabla 11. *Equipos informáticos*

N° Activo	Proceso Macro	Subproceso	Tipo de activo	Nombre activo	Descripción activo	Propietario activo
A25	Coordinación general de TIC	Equipos informáticos	Hardware	Computadores	Dispositivos para procesar, almacenar y transmitir información.	CTIC
A26	Coordinación general de TIC	Equipos informáticos	Hardware	Switches, Router, Firewall, Access Point	Dispositivos de red que conectan múltiples dispositivos	CTIC
A27	Coordinación general de TIC	Equipos informáticos	Hardware	Central telefónica	Sistema que gestiona las comunicaciones telefónicas	CTIC
A28	Coordinación general de TIC	Equipos informáticos	Hardware	Impresoras	Dispositivos para la impresión de textos, imágenes, y otros	CTIC

					materiales gráficos	

Fuente: Elaboración propia

Tabla 12. *Soportes de información*

N° Activo	Proceso Macro	Subproceso	Tipo de activo	Nombre activo	Descripción activo	Propietario activo
A29	Coordinación general de TIC	Soportes de información	Hardware	Discos, SAN, NAS, discos duros extraíbles de respaldo de información	Dispositivos de almacenamiento de datos	CTIC

Fuente: Elaboración propia

Tabla 13. *Redes de comunicaciones*

N° Activo	Proceso Macro	Subproceso	Tipo de activo	Nombre activo	Descripción activo	Propietario activo
A30	Coordinación general de TIC	Redes de comunicaciones	Infraestructura de red	Red local LAN	Red de comunicación	CTIC
A31	Coordinación general de TIC	Redes de comunicaciones	Infraestructura de red	Red MPLS (Enlaces de datos)	Tecnología de red que optimiza el enrutamiento de datos en	CTIC

					redes de área extensa	
A32	Coordinación general de TIC	Redes de comunicaciones	Infraestructura de red	WAN	Red de comunicación	CTIC

Fuente: Elaboración propia

Tabla 14. *Equipo auxiliar*

N° Activo	Proceso Macro	Subproceso	Tipo de activo	Nombre activo	Descripción activo	Propietario activo
A33	Coordinación general de TIC	Equipo auxiliar	Fijo	Mobiliario	Elementos del entorno de trabajo	8
A34	Coordinación general de TIC	Equipo auxiliar	Fijo	Estantes	Estructura de almacenaje	8

Fuente: Elaboración propia

Tabla 15. *Instalaciones/recursos humanos*

N° Activo	Proceso Macro	Subproceso	Tipo de activo	Nombre activo	Descripción activo	Propietario activo
A35	Coordinación general de TIC	Instalaciones /recursos humanos	Instalaciones	Rack de Comunicaciones.	Estructura para organizar y montar equipos de red	CTIC

A36	Coordinación general de TIC	Instalaciones /recursos humanos	Instalaciones	Data Center	Instalación física que alberga servidores y otros	CTIC
A37	Coordinación general de TIC	Instalaciones /recursos humanos	Recursos humanos	Administradores de sistemas, Analistas, Proveedores	Profesionales de TI	CTIC

Fuente: Elaboración propia

Es así que se procede a analizar cada uno de ellos en sus componentes y cuantificar su valor en función de tres criterios y una escala cualitativa y cuantitativa:

- **Confidencialidad:** Protección de la información contra el acceso no autorizado, garantizando que solo las personas con los permisos adecuados puedan visualizar o utilizar los datos.

Tabla 16. *Escala confidencialidad*

Situación	Resultado	Calificación
Libre acceso	Muy bajo	1
Acceso limitado solo a personal de la institución	Bajo	2
Acceso limitado solo a responsables del proceso	Medio	3
Acceso limitado solo a Gerencia	Alto	4
Acceso limitado solo a la Dirección	Muy alto	5

Fuente: Elaboración propia

- **Integridad:** Aseguramiento de que la información es precisa, completa y no ha sido alterada de manera no autorizada, manteniendo su validez y fiabilidad.

Tabla 17. *Escala integridad*

Situación	Resultado	Calificación
Modificación libre	Muy bajo	1
Modificación limitada a personal de la institución	Bajo	2
Modificación limitada a responsables del proceso	Medio	3
Modificación limitada a Gerencia	Alto	4
Modificación limitada a la Dirección	Muy alto	5

Fuente: Elaboración propia

- **Disponibilidad:** Garantía de que la información y los sistemas de procesamiento de datos están accesibles y utilizables cuando se necesiten, asegurando un servicio continuo y sin interrupciones indebidas.

Tabla 18. *Escala disponibilidad*

Situación	Resultado	Calificación
La no disponibilidad de hasta una semana no afecta a la entidad	Muy bajo	1
La no disponibilidad de hasta 3 días y no afecta a la entidad	Bajo	2
La no disponibilidad de hasta 1 día no afecta a la entidad.	Medio	3
La no disponibilidad de hasta 1 hora no afecta la entidad	Alto	4

El activo debe estar siempre disponible	Muy alto	5

Fuente: Elaboración propia

Por lo tanto, se procede a valorar los activos mencionados:

Tabla 19. *Servicios*

N° Activo	Nombre del activo	Tipo de soporte	Propietario activo	Valoración de impacto			
				Confidencialidad	Integridad	Disponibilidad	VA
A1	Internet	Virtual	CTIC	2	2	5	3
A2	Página web	Virtual	CTIC	2	2	5	3
A3	SIGAME	Virtual	CTIC	3	3	3	3
A4	QUIPUX	Virtual	CTIC	2	2	3	2.33
A5	Correo Electrónico	Virtual	CTIC	2	2	3	2.33
A6	Mesa de Ayuda	Virtual	CTIC	1	2	2	1.67
A7	Plataforma Documental	Virtual	CTIC	1	2	3	2

Fuente: Elaboración propia

Tabla 20. *Datos información*

N° Activo	Nombre del activo	Tipo de soporte	Propietario activo	Valoración de impacto			
				Confidencialidad	Integridad	Disponibilidad	VA
A8	Ficheros	Virtual	CTIC	2	2	2	2

A9	Contratos proveedores	Virtual	CTIC	3	3	3	3
A10	Copias respaldo	Virtual	CTIC	2	2	2	2
A11	Archivo de copias de seguridad de la información	Virtual	CTIC	2	2	2	2

Fuente: Elaboración propia

Tabla 21. *Aplicaciones informáticas*

N° Activo	Nombre del activo	Tipo de soporte	Propietario Activo	Valoración de impacto			
				Confidencialidad	Integridad	Disponibilidad	VA
A12	SIGAMEE	Virtual	CTIC	3	3	2	2.66
A13	EGAD	Virtual	CTIC	3	3	2	2.66
A14	GCS (GESTION DE COMERCIALIZACIÓN DE SERVICIOS)	Virtual	CTIC	3	3	3	3
A 15	SISTEMA INTEGRAL DE CATASTROS SIC	Virtual	CTIC	3	3	3	3

A16	PLATAFORMA TECNOLÓGICA	Virtual	CTIC	1	3	3	2.33
A17	SICOM	Virtual	CTIC	3	3	3	3
A18	SGIDS	Virtual	CTIC	3	3	3	3
A19	SISTEMA DE COMPROBANTES ELECTRÓNICOS	Virtual	CTIC	3	3	3	3
A20	FACTURADOR UNIVERSAL	Virtual	CTIC	3	3	3	3
A21	MESA DE AYUDA	Virtual	CTIC	3	3	3	3
A22	SIOC - SISTEMA DE INFORMACIÓN DE OFERTA DE COOPERACIÓN	Virtual	CTIC	3	3	3	3
A23	CONSULTA VEHICULAR	Virtual	CTIC	3	3	3	3
A24	FULLTIME	Virtual	CTIC	3	3	3	3

Fuente: Elaboración propia

Tabla 22. *Equipos informáticos*

N° Activo	Nombre del activo	Tipo de soporte	Propietario Activo	Valoración del activo			
				Confidencialidad	Integridad	Disponibilidad	VA
A25	Computadores	Físico	CTIC	2	3	5	3.33
A26	Switches, Router, Firewall, Access Point	Físico	CTIC	3	3	5	3.66

A27	Central telefónica	Físico	CTIC	3	3	5	3.66
A28	Impresoras	Físico	CTIC	2	2	2	2

Fuente: Elaboración propia

Tabla 23. Soportes de información

N° Activo	Nombre del activo	Tipo de soporte	Propietario activo	Valoración del activo			
				Confidencialidad	Integridad	Disponibilidad	VA
A29	Discos, SAN, NAS, discos duros extraíbles de respaldo de información	CTIC		3	3	5	3.66

Fuente: Elaboración propia

Tabla 24. *Redes de comunicaciones*

N° Activo	Nombre del activo	Tipo de soporte	Propietario activo	Valoración del activo			
				Confidencialidad	Integridad	Disponibilidad	VA
A30	Red local LAN	Virtual	CTIC	2	3	5	3.33
A31	Red MPLS (Enlaces de datos)	Virtual	CTIC	2	3	5	3.33
A32	WAN	Virtual	CTIC	2	3	5	3.33

Fuente: Elaboración propia

Tabla 25. *Equipo auxiliar*

N° Activo	Nombre del activo	Tipo de soporte	Propietario activo	Valoración del activo			
				Confidencialidad	Integridad	Disponibilidad	VA
A33	Mobiliario	Físico	CTIC	2	3	3	2.66
A34	Estantes	Físico	CTIC	2	3	3	2.66

Fuente: Elaboración propia

Tabla 26. *Instalaciones/recursos humanos*

N° Activo	Nombre del activo	Tipo de soporte	Propietario activo	Valoración del activo			
				Confidencialidad	Integridad	Disponibilidad	VA
A35	Rack de Comunicaciones.	Físico	CTIC	3	3	5	3.66
A36	Data Center	Físico	CTIC	3	3	5	3.66
A37	Administradores de sistemas, Analistas, Proveedores	Físico	CTIC	3	3	5	3.66

Fuente: Elaboración propia

5.2. Valoración del riesgo

A continuación, se establece de manera detallada los riesgos que enfrenta la institución con respecto a sus activos, para este fin se estiman dos criterios:

- **Impacto de amenaza**

Tabla 27. *Escala de impacto*

Situación	Resultado	Calificación
Probabilidad de más del 50%	Alto	3
Probabilidad de menos del 50%	Medio	2
Probabilidad 0-49%	Bajo	1

Fuente: Elaboración propia

- **Alcance vulnerabilidad**

Tabla 28. *Escala de probabilidad*

Situación	Resultado	Calificación
No existe ninguna medida de seguridad	Alto	3
Existen medidas de seguridad pero no son efectivas	Medio	2
Existen medidas de seguridad adecuadas	Bajo	1

Fuente: Elaboración propia

Por lo tanto, se procede a determinar los riesgos asociados a cada tipo de activo según su valor, nivel de impacto y probabilidad acorde a este rango:

Tabla 29. *Escala de riesgo*

Valor	Nivel riesgo	Acciones
1-3	Bajo	Retención y monitoreo
4-8	Medio	Aplicación de controles para disminuir el riesgo

9-27	Alto	Atención inmediata para modificar el riesgo

Fuente: Elaboración propia

Tabla 30. *Nivel de riesgo servicios*

Análisis de riesgos				Evaluación de riesgos					
				Impacto (I)	Exposición				
N° Activo	Activo	Amenaza	Vulnerabilidad	CID	Nivel de amenaza	Nivel de vulnerabilidad	Controles complementarios	Cálculo evaluación de	Nivel de riesgo
A1	Internet	Fallos de proveedores del servicio	Interrupciones en la conectividad	3	1	1	Monitoreo continuo	3	Bajo
A2	Página web	Modificación no autorizada del sitio web,	Integridad de la información publicada.	3	1	1	Monitoreo continuo	3	Bajo
A3	SIGAME (sistema administrativo financiero)	Acceso no autorizado a datos financieros sensibles,	Confidencialidad de la información.	3	2	2	Monitoreo continuo	12	Atto
A4	QUIPUX	Ataques maliciosos	Integridad y disponibilidad de los documentos	2.33	2	2	Monitoreo continuo	9.32	Alto
A5	Correo Electrónico	Phishing	Confidencialidad de la información y facilitando el acceso no autorizado a sistemas internos.	2.33	2	2	Monitoreo continuo	9.32	Alto
A6	Mesa de Ayuda	Uso indebido del sistema	Solicitudes falsas, comprometiendo la integridad de	1.67	2	2	Monitoreo continuo	6.68	Medio

			la información y la eficiencia del servicio.						
A7	Plataforma Documental	Accesos no autorizados	Fuga de información sensible a través	2	2	2	Monitoreo continuo	8	Medio

Fuente: Elaboración propia

Tabla 31. *Datos información*

Análisis de riesgos				Evaluación de riesgos					
				Impacto (I)	Exposición				
N° Activo	Activo	Amenaza	Vulnerabilidad	CID	Nivel de amenaza	Nivel de vulnerabilidad	Controles complementarios	Cálculo evaluación de riesgo	Nivel de riesgo
A8	Ficheros	Acceso no autorizado a ficheros,	Confidencialidad y la integridad de la información almacenada.	2	2	2	Monitoreo continuo	8	Medio
A9	Contratos proveedores	Robo de información contractual	Sistema deficiente de seguridad	3	1	1	Monitoreo continuo	3	Medio
A10	Copias respaldo	Fallo en el almacenamiento o corrupción de datos	, Disponibilidad de la información respaldada	2	2	2	Monitoreo continuo	8	Medio
A11	Archivo de copias de seguridad de la información	Pérdida o robo de copias de seguridad	Confidencialidad, integridad y disponibilidad de la información crítica.	2	2	2	Monitoreo continuo	8	Medio

Fuente: Elaboración propia

Tabla 32. *Aplicaciones informáticas*

Análisis de riesgos				Evaluación de riesgos					
				Impacto (I)	Exposición				
N° Activo	Activo	Amenaza	Vulnerabilidad	CID	Nivel de amenaza	Nivel de vulnerabilidad	Controles complementarios	Cálculo evaluación de riesgo	Nivel de riesgo
A12	SIGAMEE	Robo de datos financieros sensibles	Confidencialidad y la integridad de la información financiera.	2.66	3	3	Monitoreo continuo	23.94	Alto
A13	EGAD	Acceso no autorizado	Alteración de la planificación y ejecución de programas y proyectos	2.66	3	3	Monitoreo continuo	23.94	Alto
A14	GCS (GESTION DE COMERCIALIZACIÓN DE SERVICIOS)	Fallo en la automatización de procesos	Errores en la gestión y facturación de servicios, afectando la integridad de los datos comerciales	3	2	2	Monitoreo continuo	12	Alto
A 15	SISTEMA INTEGRAL DE CATASTROS SIC	Manipulación incorrecta de datos	Errores en la valoración y cobro de predios, comprometiendo la integridad y disponibilidad de los datos	3	3	3	Monitoreo continuo	27	Alto

A16	PLATAFORMA TECNOLÓGICA	Interrupción del servicio	acceso a los servicios municipales, afectando la disponibilidad de la información	2.33	2	2	Monitoreo continuo	9.32	Alto
A17	SICOM	Pérdida de datos de proyectos de cooperación	Continuidad y seguimiento de los proyectos, afectando la integridad y disponibilidad de la información	3	2	2	Monitoreo continuo	12	Alto
A18	SGIDS	Fallo en la gestión de desechos sólidos,	Problemas ambientales y sanitarios, afectando la integridad y disponibilidad de los datos de gestión	3	2	2	Monitoreo continuo	12	Alto
A19	SISTEMA DE COMPROBANTES ELECTRÓNICOS	Errores en la emisión de comprobantes electrónicos	Legalidad y validez de las transacciones, afectando la integridad y disponibilidad de los comprobantes	3	2	2	Monitoreo continuo	12	Alto
A20	FACTURADOR UNIVERSAL	Fallas en la facturación	Errores en los cobros y generación de cartera	3	3	3	Monitoreo continuo	27	Alto

			vencida, comprometiendo la integridad y disponibilidad de los datos de facturación						
A21	MESA DE AYUDA	Fallo en la gestión de solicitudes de soporte	Demoras en la resolución de incidencias tecnológicas	3	2	2	Monitoreo continuo	12	Alto
A22	SIOC - SISTEMA DE INFORMACIÓN DE OFERTA DE COOPERACIÓN	Pérdida de acceso a información	Pérdidas de oportunidades de financiamiento y apoyo externo.	3	2	2	Monitoreo continuo	12	Alto
A23	CONSULTA VEHICULAR	Errores en la consulta de datos vehiculares	Problemas en la recaudación de impuestos,	3	3	3	Monitoreo continuo	27	Alto
A24	FULLTIME	Manipulación indebida de registros	Integridad de los datos de recursos humanos y afectando la gestión del personal	3	2	2	Monitoreo continuo	12	Alto

Fuente: Elaboración propia

Tabla 33. *Equipos informáticos*

Análisis de riesgos				Evaluación de riesgos					
				Impacto (I)	Exposición				
N° Activo	Activo	Amenaza	Vulnerabilidad	CID	Nivel de amenaza	Nivel de vulnerabilidad	Controles complementarios	Cálculo evaluación de riesgo	Nivel de riesgo
A25	Computadores	Infección por malware	Confidencialidad, integridad y disponibilidad de los datos almacenados y procesados en los equipos.	3.33	3	3	Monitoreo continuo	29.97	Alto
A26	Switches, Router, Firewall, Access Point	Accesos no autorizados	Integridad y disponibilidad de la red, permitiendo.	3.66	3	3	Monitoreo continuo	32.94	Alto
A27	Central telefónica	Intercepción de comunicaciones	Se puede comprometer la confidencialidad de las llamadas y mensajes,	3.66	1	1	Monitoreo continuo	3.66	Bajo
A28	Impresoras	Acceso no autorizado a impresiones	Confidencialidad de documentos impresos, permitiendo el acceso a información sensible	2	1	1	Monitoreo continuo	2	Bajo

Fuente: Elaboración propia

Tabla 34. *Soportes de información*

Análisis de riesgos				Evaluación de riesgos				
N° Activo	Activo	Amenaza	Vulnerabilidad	Impacto (I)	Exposición	Controles com	Cálculo eval	Nivel de

				CID	Nivel de amenaza	Nivel de vulnerabilidad			
A29	Discos, SAN, NAS, discos duros extraíbles de respaldo de información	Pérdida de datos por fallos físicos, humanos, desastres naturales	Disponibilidad de la información	3.66	3	3	Monitoreo continuo	32.94	Alto

Fuente: Elaboración propia

Tabla 35. *Redes de comunicaciones*

Análisis de riesgos				Evaluación de riesgos					
				Impacto (I)	Exposición				
N° Activo	Activo	Amenaza	Vulnerabilidad	CID	Nivel de amenaza	Nivel de vulnerabilidad	Controles complementarios	Cálculo evaluación de riesgo	Nivel de riesgo
A30	Red local LAN	Fallos de hardware o software,	Interrupciones del servicio.	3.33	3	3	Monitoreo continuo	29.97	Alto
A31	Red MPLS (Enlaces de datos)	Interrupciones en los enlaces	Afectación a la comunicación entre distintas ubicaciones, comprometiendo la disponibilidad del servicio	3.33	3	3	Monitoreo continuo	29.97	
A32	WAN	Fallos de proveedores de servicios	Interrupciones en la conectividad	3.33	3	3	Monitoreo continuo	29.97	Alto

Fuente: Elaboración propia

Tabla 36. *Equipo auxiliar*

Análisis de riesgos				Evaluación de riesgos					
				Impacto (I)	Exposición				
N° Activo	Activo	Amenaza	Vulnerabilidad	CID	Nivel de amenaza	Nivel de vulnerabilidad	Controles complementarios	Cálculo evaluación de riesgo	Nivel de riesgo
A33	Mobiliario	Accidentes laborales	Seguridad física del personal	2.66	3	3	Monitoreo continuo	23.94	Alto
A34	Estantes	Desorganización o etiquetado inadecuado	Localización y acceso a documentos o equipos, afectando la eficiencia operativa	2.66	3	3	Monitoreo continuo	23.94	Alto

Fuente: Elaboración propia

Tabla 37. *Instalaciones/recursos humanos*

Análisis de riesgos				Evaluación de riesgos					
				Impacto (I)	Exposición				
N° Activo	Activo	Amenaza	Vulnerabilidad	CID	Nivel de amenaza	Nivel de vulnerabilidad	Controles complementarios	Cálculo evaluación de riesgo	Nivel de riesgo
A35	Rack de Comunicaciones.	Fallas eléctricas	Daño a los equipos de comunicación.	3.66	3	3	Monitoreo continuo	32.94	Alto
A36	Data Center	Fallas en sistemas de climatización	Sobrecalentamiento y daños en los equipos	3.66	3	3	Monitoreo continuo	32.94	Alto
A37	Administradores de sistemas, Analistas, Proveedores	Falta de actualización en conocimientos	Gestión ineficaz de los datos y sistemas	3.66	3	3	Monitoreo continuo	32.94	Alto

Fuente: Elaboración propia

5.3. Tratamiento del riesgo

Se determina las acciones a realizar en cada uno de los riesgos encontrados, Esto implica implementar medidas para disminuir la probabilidad o mitigar el impacto de los riesgos identificados, aceptar ciertos riesgos dentro de límites aceptables sin intervención adicional, modificar actividades o sistemas para eliminar riesgos potenciales o transferir la responsabilidad del riesgo a terceros cuando sea adecuado.

Por lo tanto, se consideran los riesgos que se deben abordar a corto plazo y de manera inmediata, siendo los siguientes:

Tabla 38. *Tratamiento de riesgos servicios*

Evaluación de riesgos								Tratamiento de riesgos							Riesgo residual
N° Activo	Activo	Impacto (I)	Probabilidad		Controles complementarios	Cálculo evaluación de	Nivel de riesgo	Método de tratamiento de Riesgos	Tipo de control	Controles a Implementar	Nivel de amenaza	Nivel de vulnerabilidad	Cálculo de Evaluación Riesgo con el control implementado	Nivel de Riesgo con el control Implementado	
		CID	Nivel de amenaza	Nivel de vulnerabilidad											
A1	Internet	3	1	1	Monitoreo continuo	3	Bajo	Retención	No aplica	Implementar un contrato con otro proveedor para asegurar la continuidad del servicio.	1	1	3	Bajo	Aceptable
A2	Página web	3	1	1	Monitoreo continuo	3	Bajo	Retención	No aplica	Implementar autenticación, controles de acceso estrictos y monitoreo continuo de las actividades de los usuarios.	1	1	3	Bajo	Aceptable
A3	SIGAME (sistema administrativo financiero)	3	2	2	Monitoreo continuo	12	Atto	Modificar	Control correctivo	Realizar copias de seguridad regulares, implementar medidas de protección.	1	1	3	Bajo	Aceptable
A4	QUIPUX	2.33	2	2	Monitoreo continuo	9.32	Alto	Modificar	Control correctivo	Capacitar a los empleados sobre la detección de correos de phishing	1	1	2.33	Bajo	Aceptable

A5	Correo Electrónico	2.33	2	2	Monitoreo continuo	9.32	Alto	Modificar	Control correctivo	Implementar autenticación y autorización para la generación de solicitudes, y monitorear y el uso del sistema.	1	1	2.33	Bajo	Aceptable
A6	Mesa de Ayuda	1.67	2	2	Monitoreo continuo	6.68	Medio	Prevención	Control preventivo	Implementar controles de acceso basados en roles, cifrado de datos y monitoreo continuo de los accesos a la plataforma.	1	1	1.67	Bajo	Aceptable
A7	Plataforma Documental	2	2	2	Monitoreo continuo	8	Medio	Prevención	Control preventivo	Implementar un contrato con otro proveedor para asegurar la continuidad del servicio.	1	1	2	Bajo	Aceptable

Fuente: Elaboración propia

Tabla 39. *Datos / información*

Evaluación de riesgos								Tratamiento de riesgos							Riesgo residual
N° Activo	Activo	Impacto (I)	Probabilidad		Controles complementarios	Cálculo evaluación de	Nivel de riesgo	Método de tratamiento de Riesgos	Tipo de control	Control a Implementar	Nivel de amenaza	Nivel de vulnerabilidad	Cálculo de Evaluación Riesgo con el control implementado	Nivel de Riesgo con el control Implementado	
		CID	Nivel de amenaza	Nivel de vulnerabilidad											
A8	Ficheros	2	2	2	Monitoreo continuo	8	Medio	Prevención	Control preventivo	Implementar controles de acceso estrictos y autenticación para todos los usuarios	1	1	2	Bajo	Aceptable

A9	Contratos proveedores	3	1	1	Monitoreo continuo	3	Medio	Prevención	Control preventivo	Implementar un sistema de respaldo automatizado con múltiples copias en ubicaciones distintas.	1	1	3	Bajo	Aceptable
A10	Copias respaldo	2	2	2	Monitoreo continuo	8	Medio	Prevención	Control preventivo	Implementar un sistema de respaldo	1	1	2	Bajo	Aceptable
A11	Archivo de copias de seguridad de la información	2	2	2	Monitoreo continuo	8	Medio	Prevención	Control preventivo	Implementar un sistema de respaldo	1	1	2	Bajo	Aceptable

Fuente: Elaboración propia

Tabla 40. *Aplicaciones informáticas*

Evaluación de riesgos								Tratamiento de riesgos							Riesgo residual
N° Activo	Activo	Impacto (I)	Probabilidad		Controles complementarios	Cálculo evaluación	Nivel de riesgo	Método de tratamiento de Riesgos	Tipo de control	Controles a Implementar	Nivel de amenaza	Nivel de vulnerabilidad	Cálculo de Evaluación Riesgo con el control implementado	Nivel de Riesgo con el control Implementado	
		CID	Nivel de amenaza	Nivel de vulnerabilidad											
A12	SIGAMEE	2.66	3	3	Monitoreo continuo	23.94	Alto	Modificar	Control correctivo	Implementar controles de acceso estrictos.	1	1	2.66	Bajo	Aceptable

A13	EGAD	2.66	3	3	Monitoreo continuo	23.94	Alto	Modificar	Control correctivo	Implementar controles de acceso estrictos.	1	1	2.66	Bajo	Aceptable
A14	GCS (GESTION DE COMERCIALIZACIÓN DE SERVICIOS)	3	2	2	Monitoreo continuo	12	Alto	Modificar	Control correctivo	Implementar controles de acceso estrictos.	1	1	3	Bajo	Aceptable
A 15	SISTEMA INTEGRAL DE CATASTROS SIC	3	3	3	Monitoreo continuo	27	Alto	Modificar	Control correctivo	Implementar controles de acceso estrictos.	1	1	3	Bajo	Aceptable
A16	PLATAFORMA TECNOLÓGICA	2.33	2	2	Monitoreo continuo	9.32	Alto	Modificar	Control correctivo	Monitorear el sistema para identificar y corregir fallos rápidamente.	1	1	2.33	Bajo	Aceptable
A17	SICOM	3	2	2	Monitoreo continuo	12	Alto	Modificar	Control correctivo	Asegurar la realización de copias de seguridad periódicas y mantener un sistema de recuperación de datos efectivo.	1	1	3	Bajo	Aceptable
A18	SGIDS	3	2	2	Monitoreo continuo	12	Alto	Modificar	Control correctivo	Implementar controles de acceso estrictos.	1	1	3	Bajo	Aceptable

A19	SISTEMA DE COMPROBANTES ELECTRÓNICOS	3	2	2	Monitoreo continuo	12	Alto	Modificar	Control correctivo	Implementar un sistema de validación y verificación de comprobantes electrónicos	1	1	3	Bajo	Aceptable
A20	FACTURADOR UNIVERSAL	3	3	3	Monitoreo continuo	27	Alto	Modificar	Control correctivo	Asegurar un sistema de facturación confiable con controles y validaciones integrados.	1	1	3	Bajo	Aceptable
A21	MESA DE AYUDA	3	2	2	Monitoreo continuo	12	Alto	Modificar	Control correctivo	Establecer un sistema de gestión de incidencias eficiente y realizar capacitaciones regulares al personal	1	1	3	Bajo	Aceptable
A22	SIOC - SISTEMA DE INFORMACIÓN DE OFERTA DE COOPERACIÓN	3	2	2	Monitoreo continuo	12	Alto	Modificar	Control correctivo	Implementar medidas de seguridad para proteger el acceso a la información y realizar copias de seguridad regulares.	1	1	3	Bajo	Aceptable

A23	CONSULTA VEHICULAR	3	3	3	Monitoreo continuo	27	Alto	Modificar	Control correctivo	Asegurar la integridad de los datos mediante validaciones y controles rigurosos.	1	1	3	Bajo	Aceptable
A24	FULLTIME	3	2	2	Monitoreo continuo	12	Alto	Modificar	Control correctivo	Implementar controles y auditorías de registros de asistencia y permisos.	1	1	3	Bajo	Aceptable

Fuente: Elaboración propia

Tabla 41. *Equipos informáticos*

Evaluación de riesgos								Tratamiento de riesgos							Riesgo residual
N° Activo	Activo	Impacto (I)	Probabilidad		Controles complementarios	Cálculo evaluación de riesgo	Nivel de riesgo	Método de tratamiento de Riesgos	Tipo de control	Controles a Implementar	Nivel de amenaza	Nivel de vulnerabilidad	Cálculo de Evaluación Riesgo con el control implementado	Nivel de Riesgo con el control Implementado	
		CID	Nivel de amenaza	Nivel de vulnerabilidad											
A25	Computadores	3.33	3	3	Monitoreo continuo	29.97	Alto	Modificar	Control correctivo	Realizar escaneos periódicos	1	1	3.33	Bajo	Aceptable

A26	Switches, Router, Firewall, Access Point	3.66	3	3	Monitoreo continuo	32.94	Alto	Modificar	Control correctivo	Configurar adecuadamente los dispositivos de red con políticas de acceso estrictas para proteger las comunicaciones.	1	1	3.66	Bajo	Aceptable
A27	Central telefónica	3.66	1	1	Monitoreo continuo	3.66	Bajo	Retención	No aplica		1	1	3.66	Bajo	Aceptable
A28	Impresoras	2	1	1		2	Bajo	Retención	No aplica		1	1	2	Bajo	Aceptable

Fuente: Elaboración propia

Tabla 42. *Soportes de información*

Evaluación de riesgos								Tratamiento de riesgos							Riesgo residual
N° Activo	Activo	Impacto (I)	Probabilidad		Controles complementarios	Cálculo evaluación	Nivel de riesgo	Método de tratamiento de Riesgos	Tipo de control	Controles a Implementar	Nivel de amenaza	Nivel de vulnerabilidad	Cálculo de Evaluación Riesgo con el control implementado	Nivel de Riesgo con el control Implementado	
		CID	Nivel de amenaza	Nivel de vulnerabilidad											
A29	Discos, SAN, NAS, discos duros extraíbles de respaldo de información	3.66	3	3	Monitoreo continuo	32.94	Alto	Modificar	Control correctivo	Realizar pruebas de restauración periódicas y mantener registros de respaldo actualizados.	1	1	3.66	Bajo	Aceptable

Fuente: Elaboración propia

Tabla 43. *Redes de comunicaciones*

Evaluación de riesgos								Tratamiento de riesgos							Riesgo residual
N° Activo	Activo	Impacto (I)	Probabilidad		Controles complementarios	Cálculo evaluación	Nivel de riesgo	Método de tratamiento de Riesgos	Tipo de control	Controles a Implementar	Nivel de amenaza	Nivel de vulnerabilidad	Cálculo de Evaluación Riesgo con el control implementado	Nivel de Riesgo con el control Implementado	
		CID	Nivel de amenaza	Nivel de vulnerabilidad											
A30	Red local LAN	3.33	3	3	Monitoreo continuo	29.97	Alto	Modificar	Control correctivo	Implementar controles en hardware y software, y establecer procedimientos de mantenimiento preventivo.	1	1	3.33	Bajo	Aceptable
A31	Red MPLS (Enlaces de datos)	3.33	3	3	Monitoreo continuo	29.97	Alto	Modificar	Control correctivo	Implementar enlaces de respaldo y realizar pruebas de conmutación por error periódicamente.	1	1	3.33	Bajo	Aceptable
A32	WAN	3.33	3	3	Monitoreo continuo	29.97	Alto	Modificar	Control correctivo	Utilizar múltiples proveedores de servicios para garantizar la conectividad	1	1	3.33	Bajo	Aceptable

Fuente: Elaboración propia

Tabla 44. *Equipo auxiliar*

Evaluación de riesgos								Tratamiento de riesgos							Riesgo residual
N° Activo	Activo	Impacto (I) CID	Probabilidad Nivel de amenaza	Probabilidad Nivel de vulnerabilidad	Controles complementarios	Cálculo evaluación	Nivel de riesgo	Método de tratamiento de Riesgos	Tipo de control	Controles a Implementar	Nivel de amenaza	Nivel de vulnerabilidad	Cálculo de Evaluación Riesgo con el control implementado	Nivel de Riesgo con el control Implementado	
A33	Mobiliario	2.66	3	3	Monitoreo continuo	23.94	Alto	Modificar	Control correctivo	Realizar una evaluación de riesgos para la disposición del mobiliario y seguir las normas de ergonomía y seguridad.	1	1	2.66	Bajo	Aceptable
A34	Estantes	2.66	3	3	Monitoreo continuo	23.94	Alto	Modificar	Control correctivo	Establecer un sistema de organización y etiquetado claro para estante.	1	1	2.66	Bajo	Aceptable

Fuente: Elaboración propia

Tabla 45. *Instalaciones/recursos humanos*

Evaluación de riesgos								Tratamiento de riesgos							Riesgo residual
N° Activo	Activo	Impacto (I) CID	Probabilidad: Nivel de amenaza	Probabilidad: Nivel de vulnerabilidad	Controles complementarios	Cálculo evaluación	Nivel de riesgo	Método de tratamiento de Riesgos	Tipo de control	Controles a Implementar	Nivel de amenaza	Nivel de vulnerabilidad	Cálculo de Evaluación Riesgo con el control implementado	Nivel de Riesgo con el control Implementado	
A35	Rack de Comunicaciones.	3.66	3	3	Monitoreo continuo	32.94	Alto	Modificar	Control correctivo	Instalar sistemas de alimentación ininterrumpida (UPS) y protección contra sobre tensiones.	1	1	3.66	Bajo	Aceptable
A36	Data Center	3.66	3	3	Monitoreo continuo	32.94	Alto	Modificar	Control correctivo	Realizar mantenimiento preventivo y revisiones periódicas del sistema de climatización.	1	1	3.66	Bajo	Aceptable
A37	Administradores de sistemas, Analistas, Proveedores	3.66	3	3	Monitoreo continuo	32.94	Alto	Modificar	Control correctivo	Proveer formación continua y actualizaciones regulares sobre tecnologías y mejores prácticas.	1	1	3.66	Bajo	Aceptable

Fuente: Elaboración propia

5.4. Aceptación del riesgo

Este proceso implica la decisión de la AME de asumir ciertos riesgos identificados sin aplicar medidas adicionales para mitigarlos, ya que estos riesgos no implican afectaciones importantes para la entidad.

Tabla 46. *Aceptación de riesgos*

N° Activo	Activo	Afectaciones menores a la institución	Beneficios mayores sobre el riesgo	Costo de modificación muy alto	Requisito contractual	Compromiso de tratarlo a futuro
A1	Página web				X	
A2	Ficheros	X				
A27	Central telefónica				X	
A28	Impresoras			X		

Fuente: Elaboración propia

5.5. Comunicación de los Riesgos

La comunicación de los riesgos hallados involucra la transmisión clara y efectiva de información dentro de la AME. Lo que incluye identificar el mensaje, el medio y a quien se va a informar.

Tabla 47. *Plan de comunicación*

Riesgo a Comunicar	Mensaje	Canal	Destinatario
Interrupciones en la conectividad de Internet	Informar sobre el riesgo de interrupciones de conectividad y la implementación de un contrato con un	Correo Electrónico / Reuniones	Equipo de Infraestructura Tecnológica

	proveedor adicional para asegurar la continuidad.		
Acceso no autorizado a SIGAME	Avisar sobre el riesgo de acceso no autorizado a datos financieros sensibles y las medidas de autenticación multifactor y monitoreo continuo que se implementarán.	Correo Electrónico / Reuniones	Equipo de Desarrollo de Sistemas
Pérdida de datos en QUIPUX	Comunicar el riesgo de pérdida de datos debido a errores o ataques y las medidas de respaldo regular y protección a implementar.	Correo Electrónico / Reuniones	Equipo de Desarrollo de Sistemas
Phishing en Correo Electrónico	Informar sobre el riesgo de phishing y las capacitaciones sobre detección de correos sospechosos para los empleados.	Correo Electrónico / Capacitaciones	Empleados de la organización
Uso indebido en la Mesa de Ayuda	Comunicar el riesgo de solicitudes falsas y las nuevas medidas de autenticación y monitoreo del sistema de solicitudes.	Correo Electrónico / Reuniones	Personal de Soporte Tecnológico

Fuga de información en Plataforma Documental	Notificar sobre el riesgo de fuga de información y las nuevas políticas de control de acceso y cifrado de datos.	Correo Electrónico / Reuniones	Equipos de Desarrollo de Sistemas y de Infraestructura Tecnológica
Robo de información contractual	Comunicar el riesgo de robo de datos contractuales y las nuevas medidas de control de acceso y autenticación que se implementarán.	Correo Electrónico / Reuniones	Equipos de Infraestructura Tecnológica y Desarrollo de Sistemas
Fallo en el almacenamiento de Copias de Respaldo	Informar sobre el riesgo de fallo en el almacenamiento de copias de respaldo y la implementación de un sistema automatizado con múltiples copias.	Correo Electrónico / Reuniones	Equipo de Infraestructura Tecnológica
Robo de datos en SIGAMEE	Comunicar el riesgo de robo de datos financieros y las medidas de acceso restringido que se implementarán.	Correo Electrónico / Reuniones	Equipo de Infraestructura Tecnológica y Desarrollo de Sistemas
Acceso no autorizado en EGAD	Notificar el riesgo de acceso no autorizado a EGAD y las nuevas medidas de control de acceso.	Correo Electrónico / Reuniones	Equipo de Infraestructura Tecnológica y Desarrollo de Sistemas

Fallo en la automatización en GCS	Informar sobre el riesgo de fallos en la automatización de procesos y las medidas para asegurar la correcta gestión y facturación.	Correo Electrónico / Reuniones	Equipo de Infraestructura Tecnológica y Desarrollo de Sistemas
Manipulación incorrecta en el Sistema Integral de Catastros SIC	Comunicar el riesgo de manipulación incorrecta de datos catastrales y las medidas de control de acceso.	Correo Electrónico / Reuniones	Equipo de Infraestructura Tecnológica y Desarrollo de Sistemas
interrupción en la Plataforma Tecnológica	Avisar sobre el riesgo de interrupción del servicio y las acciones de monitoreo para corregir fallos.	Correo Electrónico / Reuniones	Equipo de Infraestructura Tecnológica
Pérdida de datos en SICOM	Comunicar el riesgo de pérdida de datos de proyectos y las medidas de copias de seguridad y recuperación de datos.	Correo Electrónico / Reuniones	Equipo de Desarrollo de Sistemas
Fallo en la gestión de SGIDS	Informar sobre el riesgo de fallo en la gestión de desechos y las medidas para asegurar el control de acceso.	Correo Electrónico / Reuniones	Equipo de Infraestructura Tecnológica y Desarrollo de Sistemas

Errores en el Sistema de Comprobantes Electrónicos	Notificar el riesgo de errores en la emisión de comprobantes y las medidas de validación y verificación.	Correo Electrónico / Reuniones	Equipo de Desarrollo de Sistemas
Fallas en el Facturador Universal	Comunicar el riesgo de fallas en la facturación y las medidas de aseguramiento del sistema de facturación.	Correo Electrónico / Reuniones	Equipo de Desarrollo de Sistemas
Fallo en la gestión de solicitudes en la Mesa de Ayuda	Informar sobre el riesgo de fallos en la gestión de solicitudes y las mejoras en el sistema de gestión de incidencias.	Correo Electrónico / Reuniones	Personal de Soporte Tecnológico
Pérdida de acceso a SIOC	Comunicar el riesgo de pérdida de acceso a información sobre cooperación y las medidas de seguridad y respaldo.	Correo Electrónico / Reuniones	Coordinación y Asistente
Errores en la Consulta Vehicular	Notificar el riesgo de errores en la consulta de datos vehiculares y las medidas para asegurar la integridad de los datos.	Correo Electrónico / Reuniones	Equipo de Desarrollo de Sistemas

Manipulación indebida en FULLTIME	Comunicar el riesgo de manipulación de registros de asistencia y las medidas de control y auditoría a implementar.	Correo Electrónico / Reuniones	Recursos Humanos / Desarrollo de Sistemas
Infección por malware en Computadores	Informar sobre el riesgo de malware y las medidas de escaneo y mantenimiento de software antivirus.	Correo Electrónico / Reuniones	Equipo de Infraestructura Tecnológica
Pérdida de datos en Discos, SAN, NAS, discos duros extraíbles	Comunicar el riesgo de pérdida de datos y las pruebas de restauración periódicas a implementar.	Correo Electrónico / Reuniones	Equipo de Infraestructura Tecnológica
Interrupciones en la Red local LAN	Informar sobre el riesgo de interrupciones en la red y las medidas de control en hardware y software.	Correo Electrónico / Reuniones	Equipo de Infraestructura Tecnológica
Interrupciones en la Red MPLS	Notificar el riesgo de interrupciones en enlaces y las medidas de enlace de respaldo a implementar.	Correo Electrónico / Reuniones	Equipo de Infraestructura Tecnológica

Interrupciones en la WAN	Comunicar el riesgo de interrupciones en la conectividad y las acciones para utilizar múltiples proveedores.	Correo Electrónico / Reuniones	Equipo de Infraestructura Tecnológica
Inadecuada disposición del Mobiliario	Informar sobre el riesgo de accidentes laborales y las evaluaciones de riesgos y normas de seguridad a implementar.	Correo Electrónico / Reuniones	Recursos Humanos
Desorganización en Estantes	Comunicar el riesgo de desorganización y las medidas de etiquetado y organización a establecer.	Correo Electrónico / Reuniones	Coordinador de TI / Desarrollo de Sistemas
Fallas eléctricas en Rack de Comunicaciones	Notificar el riesgo de fallas eléctricas y las medidas de instalación de UPS y protección contra sobretensiones.	Correo Electrónico / Reuniones	Equipo de Infraestructura Tecnológica
Fallas en sistemas de climatización en Data Center	Informar sobre el riesgo de fallas en la climatización y las medidas de mantenimiento preventivo.	Correo Electrónico / Reuniones	Equipo de Infraestructura Tecnológica

Falta de actualización en Administradores, Analistas, Proveedores	Comunicar el riesgo de falta de actualización de conocimientos y las medidas de formación continua a implementar.	Correo Electrónico / Recursos Humanos Reuniones

Fuente: Elaboración propia

5.6. Monitoreo y Revisión del Riesgo

El proceso de monitoreo y revisión debe ser continuo y eficaz, lo que implica la vigilancia constante de los sistemas y procesos para detectar anomalías y brechas en tiempo real, Adicionalmente, por lo que el uso de herramientas avanzadas de monitoreo y análisis de datos puede ayudar a identificar patrones sospechosos o incidentes de seguridad. En donde la revisión periódica de los controles de seguridad también es crucial, ya que permite ajustar las estrategias en función de los cambios en el entorno y las lecciones aprendidas de incidentes previos.

Para garantizar una gestión de riesgos continua y efectiva, es fundamental evaluar la eficacia de los controles existentes. Examinar cómo están funcionando los controles y si están cumpliendo sus objetivos puede revelar deficiencias y áreas que necesitan refuerzo. Identificar oportunidades de mejora basadas en esta evaluación y en los hallazgos del monitoreo y revisión permite actualizar las medidas de seguridad y políticas de gestión de riesgos. Ajustar las estrategias de mitigación en respuesta a los riesgos identificados asegura que se mantengan efectivas frente a nuevos desafíos.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones.

Respecto al primer objetivo, se encontró que en referencia a los requisitos de la norma NTE INEN ISO/IEC 27005, se requirió realizar una valoración del riesgo que implica la identificación detallada de activos, amenazas, controles, vulnerabilidades, seguida de la estimación y evaluación de estos riesgos. En cuanto al tratamiento del riesgo se propusieron acciones de reducción, retención, evitación o transferencia, asegurando que la CTIC pueda manejar eficazmente los riesgos de seguridad, protegiendo los activos y garantizando la continuidad operativa. La aceptación del riesgo, por su parte, fue una decisión consciente de asumir ciertos riesgos dentro de límites aceptables.

Respecto al segundo objetivo existen niveles bajos de madurez en los procesos de identificación y evaluación de amenazas y riesgos, lo que indica que estos no están bien establecidos ni son consistentes lo que puede llevar a la organización a estar mal preparada para enfrentar incidentes de seguridad. Así también, en cuanto a la dimensión de gobierno y control de la gestión de la seguridad de la información, también se encuentra en un nivel bajo de madurez, por lo que hay una falta de estructuras de gobierno robustas y de control efectivo sobre los procesos de seguridad de la información.

En cuanto al tercer objetivo planteado, se desarrollaron propuestas específicas de mejora en la gestión de riesgos de seguridad para aquellos activos que presentan un mayor nivel de riesgo. Estas propuestas incluyeron acciones de mitigación y controles adicionales basados en los procesos establecidos por la NTE INEN ISO/IEC 27005, tales como la implementación de medidas preventivas, la actualización de políticas de seguridad y la capacitación del personal. Además, se llevó a cabo una evaluación detallada para determinar los riesgos aceptables que no requieren intervención adicional.

Recomendaciones.

En cuanto al primer objetivo, se recomienda implementar un programa continuo de evaluación y gestión de riesgos que se alinee con la norma NTE INEN ISO/IEC 27005, asegurando la actualización periódica de la identificación de activos, amenazas y vulnerabilidades. Además, establecer un comité de gestión de riesgos que supervise las acciones de tratamiento de riesgos, asegurando que las medidas de mitigación, retención, evitación y transferencia sean efectivas y se ajusten a los cambios en el entorno de amenazas.

Respecto al segundo objetivo se sugiere desarrollar e implementar un plan de mejora de la madurez de los procesos de gestión de riesgos y gobierno de la seguridad de la información. Esto incluye la capacitación de personal clave, la adopción de mejores prácticas y estándares internacionales, y la creación de una estructura de gobierno robusta que supervise y controle todos los aspectos de la seguridad de la información. Realizar auditorías regulares para evaluar el progreso y ajustar las estrategias según sea necesario.

Referente al tercer objetivo se sugiere ejecutar las propuestas de mejora identificadas para los activos de alto riesgo de manera prioritaria, asegurando la implementación de medidas preventivas y controles adicionales. Actualizar regularmente las políticas de seguridad de la información y proporcionar capacitación continua al personal para fortalecer la cultura de seguridad en la organización. Monitorear y revisar constantemente los riesgos aceptados para asegurar que se mantengan dentro de límites aceptables y ajustar las estrategias de tratamiento de riesgos según sea necesario.

BIBLIOGRAFÍA

National Institute of Standards and Technology . (2012). Guide for conducting risk assessments (NIST Special Publication 800-30 Rev. 1). . *U.S. Department of Commerce*. doi:https://doi.org/10.6028/NIST.SP.800-30r1

AME, P. d. (2024). Encuesta. (M. Proaño, Entrevistador)

Asamblea Nacional del Ecuador. (2021). *Ley Orgánica de Protección de Datos Personales*. Obtenido de https://www.finanzaspopulares.gob.ec/wp-content/uploads/2021/07/ley_organica_de_proteccion_de_datos_personales.pdf

Asociación de Municipalidades Ecuatorianas. (2014). *Estatuto de la Asociación de Municipalidades Ecuatorianas*. Obtenido de https://ame.gob.ec/wp-content/uploads/2019/12/ESTATUTO-DE-LA-AME-2014.pdf

Asociación de Municipalidades Ecuatorianas. (2022). *Misión y Visión*. Obtenido de https://ame.gob.ec/institucion/mision-y-vision/

Audetic. (2023). *Cambios principales de la ISO/IEC 27005:2022*. Obtenido de https://audetic.io/cambios-principales-de-la-iso-iec-270052022/?v=3fd6b696867d

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

Comisión Federal de Comercio. (2022). *Marco de ciberseguridad del NIST*. Obtenido de https://www.ftc.gov/es/guia-para-negocios/protegiendo-pequenos-negocios/ciberseguridad/marco-ciberseguridad-nist

Congreso Nacional del Ecuador. (2002). *Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos*. Obtenido de https://www.telecomunicaciones.gob.ec/wp-content/uploads/downloads/2012/11/Ley-de-Comercio-Electronico-Firmas-y-Mensajes-de-Datos.pdf

Fernández, R., & Monteros, N. (2014). *Propuesta metodológica para la gestión de riesgos tecnológicos en empresas proveedoras de servicios de telecomunicaciones.* ESPE.

INEN. (2008). *NORMA TÉCNICA ECUATORIANA NTE INEN-ISO/IEC 27005:2012*. Obtenido de https://app.virtualex.ec/documentos/nte_inen_iso_iec_27005.pdf

Kowask, E., Alcantara, F., & Motta, A. (2018). *Gestión del riesgo de las TI NTC 27005.* Escuela Superior de Redes.

NQA. (2022). *ISO 27001*. Obtenido de https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/Spanish%20QRFs%20and%20PDFs/NQA-ISO-27001-Guia-de-implantacion.pdf

Organización de Estados Americanos. (2004). *Estrategia Interamericana Integral para Combatir las Amenazas a la Seguridad Cibernética*. Obtenido de https://www.oas.org/en/citel/infocitel/julio-04/ult-ciberseguridad_e.asp

Organización Internacional de Normalización. (2022). *ISO/IEC 27005:2022*. Obtenido de https://www.iso.org/obp/ui/es/#iso:std:iso-iec:27005:ed-4:v1:en

Secretaría Nacional de Planificación . (2024). *Plan de Desarrollo para el Nuevo Ecuador 2024-2025*. Obtenido de https://www.planificacion.gob.ec/plan-de-desarrollo-para-el-nuevo-ecuador-2024-2025/

Unión Europea. (2016). *Reglamento General de Protección de Datos*. Obtenido de https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016R0679

Valencia, F. (2021). *Sistema de gestión de seguridad de la información basado en la familia de normas ISO/IEC 27000.* Universidad Nacional de Colombia.

Vega, E. (2021). *Seguridad de la información.* 3Ciencias.

Anexos

Anexo 1. Propuesta de guía metodológica

Contenido

Introducción

La seguridad de la información es fundamental para el desarrollo y funcionamiento eficaz de cualquier organización en la era digital. Por lo que en el contexto de la gestión de los municipios ecuatorianos se busca garantizar la confidencialidad, integridad y disponibilidad de la información que manejan, pues esta es esencial para la prestación continua y confiable de servicios a los ciudadanos. Sobre todo, ante el creciente número de amenazas y el avance constante de la tecnología.

Es por ello, que este manual está diseñado para proporcionar una guía clara y estructurada para la aplicación de la norma NTE INEN ISO/IEC 27005 en los municipios de Ecuador, pues es una norma internacional que establece directrices para la gestión de riesgos de seguridad de la información, complementando el marco de trabajo de la ISO/IEC 27001 para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI).

Por lo que el propósito de este manual es asistir a los responsables de la seguridad de la información en los municipios, proporcionándoles las herramientas y conocimientos necesarios para identificar, evaluar, y tratar los riesgos que puedan comprometer la seguridad de sus activos de información y estandarizar los procesos de gestión de riesgos de seguridad de la información, asegurando que todos las entidades puedan seguir un enfoque coherente y efectivo, adaptado a sus contextos y necesidades específicas.

Glosario

1. **Activo de información:** Cualquier elemento de información que tenga valor para una organización, como datos, sistemas, hardware, software, procesos, etc.
2. **Amenaza:** Cualquier circunstancia o evento que tiene el potencial de causar daño a los activos de información de una organización.
3. **Análisis de riesgos:** Proceso de comprensión de los riesgos mediante la identificación de amenazas, vulnerabilidades y posibles impactos.

4. **Auditoría de seguridad de la información:** Examen sistemático de las políticas, procedimientos y controles de seguridad de la información de una organización.
5. **Comunicación de riesgos:** Proceso de informar a las partes interesadas sobre los riesgos de seguridad de la información y las medidas de tratamiento.
6. **Consultar a las partes interesadas:** Involucrar a las partes interesadas relevantes en el proceso de gestión de riesgos para obtener su opinión y perspectiva.
7. **Criterios de evaluación de riesgos:** Estándares utilizados para evaluar la importancia y la probabilidad de los riesgos.
8. **Evaluación de riesgos:** Proceso de identificación y evaluación de los riesgos de seguridad de la información.
9. **Gestión de riesgos:** Proceso de identificar, evaluar y responder a los riesgos de seguridad de la información de una organización.
10. **Marco de gestión de riesgos:** Estructura que establece los procesos y responsabilidades para la gestión de riesgos de seguridad de la información.
11. **Mitigación de riesgos:** Acciones tomadas para reducir la probabilidad o el impacto de los riesgos.
12. **Monitorización de riesgos:** Seguimiento continuo de los riesgos de seguridad de la información para garantizar que se gestionen de manera efectiva.
13. **Plan de continuidad del negocio:** Documento que describe cómo una organización responderá a incidentes que afecten la disponibilidad de la información y los procesos críticos de negocio.
14. **Resiliencia de la información:** Capacidad de una organización para resistir, adaptarse y recuperarse de incidentes de seguridad de la información.
15. **Revisión de riesgos:** Evaluación periódica de los riesgos de seguridad de la información y las medidas de tratamiento para garantizar su eficacia.
16. **Riesgo de seguridad de la información:** Posibilidad de que una amenaza explote una vulnerabilidad y cause un impacto no deseado en la información.
17. **Riesgo residual:** Riesgo que queda después de que se han aplicado medidas de tratamiento de riesgos.

18. **Seguridad de la información:** Protección de la información contra una amplia gama de amenazas con el objetivo de preservar la confidencialidad, integridad y disponibilidad de la información.
19. **Tratamiento de riesgos:** Proceso de selección e implementación de medidas para modificar los riesgos.
20. **Vulnerabilidad:** Debilidad en un sistema de información que puede ser explotada por una amenaza para comprometer la seguridad de la información.

Objetivo

El objetivo de este manual es proporcionar una guía detallada y práctica para la aplicación de la norma NTE INEN ISO/IEC 27005 en los municipios de Ecuador, por lo que está diseñado para ayudar a los responsables de la seguridad de la información a implementar un sistema efectivo de gestión de riesgos de seguridad de la información, garantizando la protección de los activos de información y la continuidad operativa de los servicios municipales.

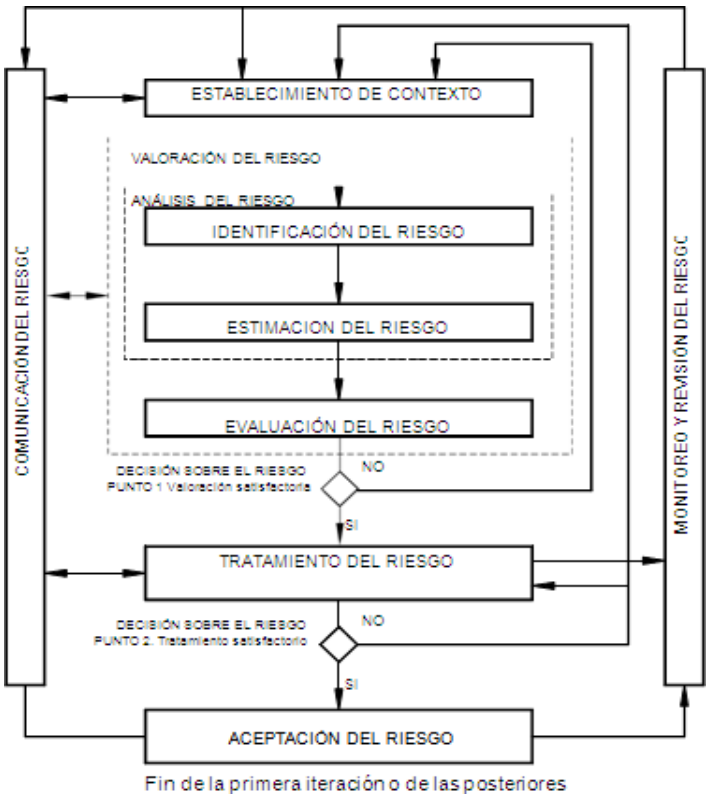
Mediante este manual, se busca:

1. **Estandarizar los procesos de gestión de riesgos**: Proporcionar una metodología clara y consistente para la identificación, evaluación y tratamiento de riesgos de seguridad de la información.
2. **Fortalecer la seguridad de la información**: Asegurar que se adopten prácticas robustas para proteger la confidencialidad, integridad y disponibilidad de la información crítica, enfrentando eficazmente las amenazas cibernéticas.
3. **Facilitar la toma de decisiones informadas**: Proveer a los responsables de la seguridad de la información con las herramientas necesarias para evaluar adecuadamente los riesgos y tomar decisiones informadas sobre las medidas de mitigación y tratamiento adecuadas.
4. **Mejorar la preparación y respuesta ante incidentes**: Establecer un marco que permita prepararse mejor y responder de manera eficiente a los incidentes de seguridad, minimizando el impacto sobre sus operaciones y servicios.
5. **Fomentar la cultura de seguridad de la información**: Promover la conciencia y la responsabilidad en todos los niveles de la administración municipal respecto a la importancia de la seguridad de la información y la gestión de riesgos.

Componentes de la NTE INEN ISO/IEC 27005

- Contexto de la organización: Este proceso implica comprender la organización y su contexto en relación con la seguridad de la información. Se trata de identificar los activos de información, las amenazas, las vulnerabilidades y los requisitos legales y reglamentarios pertinentes.
- Establecimiento del marco de gestión de riesgos: En este proceso se definen los objetivos y los límites del proceso de gestión de riesgos, así como los criterios para evaluar y tratar los riesgos.

- Evaluación de riesgos: Aquí se identifican, analizan y evalúan los riesgos de seguridad de la información que enfrenta la organización. Este proceso implica determinar la probabilidad y el impacto de los riesgos.
- Tratamiento de riesgos: En este proceso se seleccionan y aplican medidas para tratar los riesgos identificados. Puede implicar la mitigación, la transferencia, la aceptación o la evitación de los riesgos.
- Aceptación de riesgos: Este proceso implica que la organización apruebe y acepte los riesgos residuales después de aplicar las medidas de tratamiento de riesgos.
- Comunicación y consulta: Es importante comunicar de manera efectiva sobre los riesgos de seguridad de la información en toda la organización y consultar a las partes interesadas relevantes.
- Monitoreo y revisión: Se establecen procesos para monitorear y revisar continuamente la eficacia de la gestión de riesgos de la seguridad de la información en la organización.



Fin de la primera iteración o de las posteriores

01 Establecimiento del contexto

Objetivo

Identificar y comprender el entorno operativo y las circunstancias en las que la organización lleva a cabo sus actividades, con respecto a los activos que se busca precautelar en función de las partes interesadas y los requisitos legales y regulatorios.

Valoración de activos

Para este fin, se procede a identificar los principales activos que maneja la entidad, mismos que se deben cuantificar acorde a los siguientes criterios de evaluación

- **Confidencialidad:** Protección de la información contra el acceso no autorizado, garantizando que solo las personas con los permisos adecuados puedan visualizar o utilizar los datos.

Tabla 1. *Escala confidencialidad*

Situación	Resultado	Calificación
Libre acceso	Muy bajo	1
Acceso limitado solo a personal de la institución	Bajo	2
Acceso limitado solo a responsables del proceso	Medio	3
Acceso limitado solo a Gerencia	Alto	4
Acceso limitado solo a la Dirección	Muy alto	5

- **Integridad:** Aseguramiento de que la información es precisa, completa y no ha sido alterada de manera no autorizada, manteniendo su validez y fiabilidad.

Tabla 2. *Escala integridad*

Situación	Resultado	Calificación
Modificación libre	Muy bajo	1
Modificación limitada a personal de la institución	Bajo	2
Modificación limitada a responsables del proceso	Medio	3
Modificación limitada a Gerencia	Alto	4
Modificación limitada a la Dirección	Muy alto	5

- **Disponibilidad:** Garantía de que la información y los sistemas de procesamiento de datos están accesibles y utilizables cuando se necesiten, asegurando un servicio continuo y sin interrupciones indebidas.

Tabla 3. *Escala disponibilidad*

Situación	Resultado	Calificación
La no disponibilidad de hasta una semana no afecta a la entidad	Muy bajo	1
La no disponibilidad de hasta 3 días y no afecta a la entidad	Bajo	2
La no disponibilidad de hasta 1 día no afecta a la entidad.	Medio	3
La no disponibilidad de hasta 1 hora no afecta la entidad	Alto	4
El activo debe estar siempre disponible	Muy alto	5

Por lo tanto, se procede a hacer un levantamiento de información acorde a la siguiente matriz:

Activo	Responsable	Confidencialidad	Integridad	Disponibilidad	Total valor activo (C+I+D)
Activo 1	A	#	#	#	#
Activo 2	B	#	#	#	#
Activo 3	C	#	#	#	#
…					
…					
…					
…					

02 Valoración del riesgo

Objetivo

Evaluar y determinar la magnitud de los riesgos de seguridad de la información a los que está expuesta la organización, considerando la probabilidad de ocurrencia y el impacto potencial en sus activos de información.

Valoración del riesgo

A continuación, se establece de manera detallada los riesgos que enfrenta la institución con respecto a sus activos, para este fin se estiman dos criterios:

- **Impacto:** Grado de severidad de las consecuencias que un evento de riesgo puede causar a los activos de la organización, afectando la confidencialidad, integridad y disponibilidad de la información.

Tabla 4. *Escala de impacto*

Situación	Resultado	Calificación
La materialización del riesgo no genera afectaciones económicas, no daña la imagen, ni compromete el cumplimiento de objetivos.	Muy bajo	1
La materialización del riesgo genera afectaciones económicas menores, daña levemente la imagen, no compromete el cumplimiento de objetivos.	Bajo	2
La materialización del riesgo genera afectaciones	Medio	3

económicas moderadas, daña levemente la imagen, retrasa el cumplimiento de objetivos.		
La materialización del riesgo genera afectaciones económicas importantes, daña significativamente la imagen, dificulta el cumplimiento de objetivos.	Alto	4
La materialización del riesgo genera afectaciones económicas que comprometen el presupuesto institucional, daña totalmente la imagen, impide el cumplimiento de objetivos.	Muy alto	5

- **Probabilidad:** Posibilidad o frecuencia con la que un evento de riesgo específico puede ocurrir, considerando tanto factores internos como externos que podrían facilitar su materialización.

Tabla 5. *Escala de probabilidad*

Situación	Resultado	Calificación
Probabilidad de ocurrencia improbable (1% a 10%)	Muy bajo	1
Probabilidad de ocurrencia baja (11% a 30%)	Bajo	2
Probabilidad de ocurrencia media (31% a 65%)	Medio	3
Probabilidad de ocurrencia alta (66% a 89%)	Alto	4
Probabilidad de ocurrencia muy alta (90%-100%)	Muy alto	5

Por lo tanto, se procede a determinar los riesgos asociados a cada tipo de activo según su valor, nivel de impacto y probabilidad.

Tabla 6. *Nivel de riesgo servicios*

Activo	Valor Activo (VA)	Vulnerabilidad	Exposición			Nivel de Riesgo (R)=VA*FE
			Impacto (I)	Probabilidad (P)	Total factor exposición (FE)= IxP	
Activo 1	A	#	#	#	#	#
Activo 2	B	#	#	#	#	#
Activo 3	C	#	#	#	#	#
…						
…						
…						
…						

03 Tratamiento del riesgo

Objetivo

Desarrollar e implementar medidas adecuadas para modificar los riesgos de seguridad de la información identificados durante la valoración, con el fin de reducir su impacto o probabilidad, de acuerdo con los recursos y las capacidades disponibles.

Tratamiento

Se determina que se va a realizar con los riesgos encontrados, lo que implica implementar medidas para disminuir la probabilidad o mitigar el impacto de los riesgos identificados, aceptar ciertos riesgos dentro de límites aceptables sin intervención adicional, modificar actividades o sistemas para eliminar riesgos potenciales o transferir la responsabilidad del riesgo a terceros cuando sea adecuado. Para este fin se usa la siguiente escala:

Tabla7. *Nivel de riesgo*

Rango	Nivel de riesgo	Descripción
3-35	**Bajo**	Se acepta el riesgo por lo que no se realiza ninguna intervención
36-71	**Medio**	Se acepta el riesgo temporalmente, pero se lo atiende a mediano plazo
72-111	**Alto**	No se acepta el riesgo, se lo atiende a corto plazo
112-144	**Crítico**	No acepta el riesgo, se lo atiende de manera inmediata.

Por lo tanto, se consideran los riesgos que se deben abordar a corto plazo y de manera inmediata, siendo los siguientes:

Tabla 8. *Tratamiento de riesgos servicios*

Activo	Vulnerabilidad	Nivel de Riesgo	Tratamiento	Propuesta	Responsable
Activo 1	A	…	…	…	…
Activo 2	B	…	…	…	…
Activo 3	C	…	…	…	…
…					
…					
…					

04 Aceptación del riesgo

Objetivo

Evaluar y decidir conscientemente sobre la aceptación de los riesgos residuales que no se tratarán o mitigarán, considerando los beneficios potenciales y las posibles consecuencias para la entidad.

05 Comunicación de los riesgos

Objetivo

Informar de manera clara y oportuna a las partes interesadas internas y externas sobre los riesgos de seguridad de la información identificados, incluyendo su naturaleza, impacto y las medidas adoptadas para gestionarlos.

Tratamiento

Tabla 9. *Plan de comunicación*

Riesgo a Comunicar	Mensaje	Canal	Destinatario
R 1	…	…	…
R 2	…	…	…
R 3	…	…	…
…	…	…	…
…			
…			

06 Monitoreo del riesgo

Objetivo

Establecer un proceso continuo de seguimiento y revisión de los riesgos de seguridad de la información, para garantizar que las medidas de tratamiento sigan siendo efectivas y adecuadas, y para adaptarse a los cambios en el entorno operativo de la organización.

Proceso

- Establecer un marco de monitoreo:
- Definir indicadores clave de rendimiento (KPIs) y umbrales de alerta.
- Establecer un cronograma y frecuencia para el monitoreo
- Recopilar datos relevantes
- Analizar la información recopilada
- Informar a las partes interesadas
- Tomar medidas correctivas
- Retroalimentar los resultados

Anexo 2. Instrumento de Evaluación de Madurez en Administración de Riesgos Tecnológicos para la Asociación de Municipalidades Ecuatorianas (AME)

CRITERIO DE EVALUACION	NO DISPONE (0)	NO SE PIENSA EN ELLO DE MANERA ESENCIAL (1)	OCASIONAL Y/O SOLO EN CIERTOS PROYECTOS (2)	PROCEDIMIENTOS DEFINIDOS Y DOCUMENTADOS (3)	MEDIDO Y GESTIONADO (4)	OPTIMIZADO (5)
1. ¿La Asociación de Municipalidades Ecuatorianas (AME) cuenta con una política general de administración de riesgos tecnológicos y ha sido comunicada internamente?						
2. ¿La Asociación de Municipalidades Ecuatorianas (AME) tiene un mapa de riesgos (identificación, descripción y priorización)						
3. ¿La Asociación de Municipalidades Ecuatorianas (AME) tiene implantado un proceso de administración de riesgos?						
4. ¿En la Asociación de Municipalidades Ecuatorianas (AME) se ha implementado alguno de los marcos de referencia como COBIT, COSO, ISO, ¿MAGERIT u OTRO?						
5. ¿Existe alguna actividad de auditoría informática en La Asociación de Municipalidades Ecuatorianas (AME)?						
POLÍTICAS Y PRÁCTICAS DE GERENCIA DE RIESGOS.						
6. De haberla y en su opinión ¿qué tipo de relación existe entre la administración de riesgos y la función de auditoría?						
7. En su opinión, ¿Hasta qué punto está involucrada la administración de riesgos en el trabajo de control interno realizado para cumplir con los requerimientos regulatorios?						
COMUNICACIÓN						
8. En su opinión, ¿La Asociación de Municipalidades Ecuatorianas (AME) comunica sobre sus políticas y acciones de administración de riesgos?						
9. ¿Hasta qué punto la Asociación de Municipalidades Ecuatorianas (AME) revela sus riesgos en el reporte de información (reporte anual, documentos de referencia, etc.)?						
10. ¿Hasta qué punto la Asociación de Municipalidades Ecuatorianas (AME) revela sus programas de seguros en su reporte de información financiera?						
11. ¿Existe una Política de Seguridad de la Información?						
12. De existir y en su opinión, ¿La Asociación de Municipalidades Ecuatorianas (AME) difunde las políticas de seguridad de la Información satisfactoriamente al personal en general?						

13. En su opinión, ¿el personal conoce las consecuencias que se pudieran derivar y las responsabilidades en que pudieran incurrir en caso de incumplimiento de la normativa de seguridad?						
AMENAZAS Y RIESGOS						
14. ¿Considerando el ambiente económico actual, ¿ha percibido cambios en las amenazas que enfrenta su organización?						
15. ¿Dadas las tendencias actuales hacia el uso de redes sociales, cómputo en nube y dispositivos personales móviles en las organizaciones, ¿percibe cambios en el ambiente de riesgos que enfrenta su organización?						
16. ¿Cuenta con un programa de administración de riesgos de TI establecido que maneje estos riesgos derivados del uso de redes sociales, cómputo en nube y dispositivos personales móviles?						
HERRAMIENTA Y TECNOLOGÍA						
17. ¿Su organización usa alguna tecnología específica para soportar el proceso de administración de riesgos?						
18. ¿La Asociación de Municipalidades Ecuatorianas (AME) usa actualmente tecnologías de virtualización?						
19. ¿Su organización cuenta con un software o control específico de administración de accesos e identidades que mitigue los riesgos asociados con los derechos de acceso a sus datos y sistemas?						
GOBIERNO Y CONTROL						
20. ¿Su organización ha implementado un sistema de gestión de seguridad de la información que contemple la administración general de ésta?						
21. ¿La Asociación de Municipalidades Ecuatorianas (AME) cuenta con un comité de seguridad de la información (CSI)?						
22. ¿La Asociación de Municipalidades Ecuatorianas (AME) posee un plan de respuesta a incidentes de seguridad?						
23. ¿Se ha realizado una evaluación de riesgos tecnológicos?						
24. ¿La Asociación de Municipalidades Ecuatorianas (AME) ha contratado una póliza de delitos informáticos?						
25. ¿La Asociación de Municipalidades Ecuatorianas (AME) tiene planes de contingencia?						