UNIVERSIDAD CATÓLICA DE CUENCA

UNIVERSIDAD CATÓLICA DE CUENCA

Comunidad Educativa al Servicio del Pueblo

UNIDAD ACADÉMICA INFORMÁTICA, CIENCIAS DE LA COMPUTACIÓN E INNOVACIÓN TECNOLÓGICA

CARRERA DE INGENIERÍA DE SISTEMAS DE INFORMACIÓN

ANALISIS DE RIESGOS Y VULNERABILIDADES DE TI PARA GAD EL TAMBO, MANUALES Y POLITICAS, EN BASE ALA NORMA ISO 27002

PROYECTO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS DE INFORMACIÓN

AUTOR: OSCAR FABIAN ANGAMARCA POMAVILLA

DIRECTOR: ING. CRISTHIAN HUMBERTO FLORES URGILÉS.

CAÑAR - ECUADOR

2024

DIOS, PATRIA, CULTURA Y DESARROLLO

UNIVERSIDAD CATÓLICA DE CUENCA

Comunidad Educativa al Servicio del Pueblo

UNIDAD ACADÉMICA INFORMÁTICA, CIENCIAS DE LA COMPUTACIÓN E INNOVACIÓN TECNOLÓGICA

CARRERA DE INGENIERÍA DE SISTEMAS DE INFORMACIÓN

ANALISIS DE RIESGOS Y VULNERABILIDADES DE TI PARA GAD EL TAMBO, MANUALES Y POLITICAS, EN BASE ALA NORMA ISO 27002

PROYECTO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS DE INFORMACIÓN

AUTOR: OSCAR FABIAN ANGAMARCA POMAVILLA

DIRECTOR: ING. CRISTHIAN HUMBERTO FLORES URGILÉS.

CAÑAR - ECUADOR

2024

PATRIA, CULTURA Y DESARROLLO

DECLARATORIA DE AUTORÍA Y RESPONSABILIDAD

Oscar Fabián Angamarca portador de la cédula de ciudadanía **N.º 0302578331** Declaro ser el autor de la obra: **Análisis de riesgos y vulnerabilidades de TI para el GAD el Tambo, manuales y políticas, en base a la norma ISO 27002**, sobre la cual me hago responsable sobre sobre las opiniones, versiones e ideas expresadas. Declaro que la misma ha sido elaborada respetando los derechos de propiedad intelectual de terceros y eximo a la Universidad Católica de Cuenca sobre cualquier reclamación que pudiera existir al respecto. Declaro finalmente que mi obra ha sido realizada cumpliendo con todos los requisitos legales, éticos y bioéticos de investigación, que la misma no incumple con la normativa nacional e internacional en el área específica de investigación, sobre la que también me responsabilizo y eximo a la Universidad Católica de Cuenca de toda reclamación al respecto.

Cañar, 18 de noviembre de 2024

Oscar Fabián Angamarca

C.I. 0302578331

CERTIFICACIÓN PREVIA REVISIÓN DE LECTORES

Cañar, 24 de septiembre del 2024

En mi calidad de director del Trabajo de Titulación: **Análisis de riesgos y vulnerabilidades de TI para el GAD el Tambo, manuales y políticas, en base a la norma ISO 27002**, elaborado por Oscar Fabián Angamarca portador de la cédula de ciudadanía Nº 0302578331, estudiante de la Carrera de Ingeniería en Sistemas en la Unidad Académica de Informática, Ciencias de la Computación, e Innovación Tecnológica;

Certifico:

Que, el Trabajo de Titulación está apto para el proceso de revisión de los lectores designados por Dirección de Carrera.

Ing. Cristhian Flores Urgilés, Mgs

DIRECTOR DEL TRABAJO INVESTIGATIVO

DEDICATORIA

A Dios por permitirme llegar hasta este ciclo de mi formación profesional, que me ayudó a aprender de mis errores y a corregirlos para mejores días venideros como persona y como profesional.

A mis padres Eloy Angamarca y María Pomavilla por el apoyo brindado día a día en mi carrera universitaria, por ser la razón de mi vida, mi inspiración de seguir adelante y guiarme por el camino.

A mi hermano Remigio Angamarca por apoyarme de forma incondicional, moral y éticamente a cumplir mis sueños académicos y ser un ejemplo a seguir. Por último, dedico a toda mi familia en general por sus valiosos consejos, oraciones y estima.

Dios continúe bendiciendo de gran manera.

AGRADECIMIENTO

Agradezco a Dios, fuente de sabiduría y fortaleza, por permitirme culminar con éxito esta etapa de mi formación académica, brindándome siempre su guía y apoyo.

Expreso mi más sincero agradecimiento a mi director de tesis, al Ing Cristhian Humberto Flores Urgiles, Mgs, por su valiosa orientación, paciencia y compromiso durante todo el desarrollo de este trabajo. Su dedicación y conocimiento fueron fundamentales para el éxito de esta investigación.

Agradezco también a mis padres, Eloy Angamarca y María Pomavilla, por su apoyo incondicional y por inculcarme los valores del esfuerzo y la perseverancia.

Finalmente, mi gratitud hacia todos mis profesores, compañeros, y seres queridos, quienes de alguna manera contribuyeron al logro de este objetivo.

.

RESUMEN

El presente trabajo investigativo titulado “Análisis de Riesgos y Vulnerabilidades de TI para el Departamento Informático del GAD El Tambo”, tiene como objetivo principal desarrollar una propuesta integral para la gestión de riesgos y vulnerabilidades en el departamento de TI, asegurando la protección de los activos tecnológicos y la continuidad de las operaciones del municipio. Esta propuesta se fundamenta en la implementación de un marco de trabajo basado en la norma ISO 27001, con el fin de mejorar la seguridad de la información y alinear las prácticas de TI con los estándares internacionales. El punto de partida fue un análisis detallado de la situación actual del departamento de TI del GAD El Tambo, incluyendo la identificación de activos críticos y la evaluación de los riesgos asociados a cada uno de ellos. Además, se realizó una revisión exhaustiva de las mejores prácticas y controles sugeridos por la ISO 27001 y la ISO 27002, adaptando estas normativas a las necesidades específicas del municipio. A partir de este análisis, se desarrolló un modelo de gestión de riesgos que busca mitigar las amenazas identificadas y fortalecer la resiliencia del departamento frente a posibles incidentes de seguridad.

Palabras clave: análisis de riesgos, gestión de información, vulnerabilidad de TI.

ABSTRACT

This research work entitled "IT Risk and Vulnerability Analysis for the Information Technology Department of GAD El Tambo" aims to develop a comprehensive proposal for risk and vulnerability management in the IT department, ensuring the protection of technological assets and the continuity of municipal operations. This proposal is based on implementing a framework based on the ISO 27001 standard to improve information security and align IT practices with international standards. The starting point was a detailed analysis of the current situation of GAD El Tambo's IT department, including identifying critical assets and assessing the associated risks. In addition, an exhaustive review of the best practices and controls suggested by ISO 27001 and ISO 27002 was conducted, adapting these regulations to the specific needs of the municipality. Based on this analysis, a risk management model was developed to mitigate the identified threats and strengthen the department's resilience to potential security incidents.

Key words: risk analysis, information management, IT vulnerability.

CONTENIDO

1. **ÍNDICE DE ILUSTRACIONES**

2. ÍNDICE DE TABLAS

INTRODUCCIÓN

La creciente dependencia de las tecnologías de la información (TI) en las operaciones del sector público ha transformado significativamente la gestión y la prestación de servicios gubernamentales. En este contexto, el departamento informático del Gobierno Autónomo Descentralizado (GAD) de El Tambo desempeña un papel crucial en el aseguramiento de la integridad, confidencialidad y disponibilidad de la información crítica. Sin embargo, con el aumento de la sofisticación de las amenazas cibernéticas, este departamento enfrenta desafíos constantes para proteger sus sistemas de información contra posibles riesgos y vulnerabilidades.

El objetivo de esta tesis es llevar a cabo un análisis de riesgos y vulnerabilidades en el departamento informático del GAD El Tambo, utilizando como referencia la metodología establecida por la norma ISO 27001. El propósito debería ser no solo identificar las amenazas existentes sino también desarrollar un manual de políticas robusto que refuerce la seguridad de la información y mejore la capacidad de respuesta organizacional frente a incidentes de TI. Este estudio busca cerrar la brecha entre las prácticas actuales y las mejores prácticas recomendadas a nivel internacional, proporcionando así una base sólida para futuras iniciativas de seguridad.

Mediante la aplicación de esta norma internacional y el análisis detallado de la situación actual del departamento, se espera ofrecer un conjunto de directrices claras y aplicables que contribuyan significativamente a la creación de un entorno digital seguro. Al abordar estas cuestiones, el trabajo contribuirá a la literatura existente y servirá como referencia para futuras investigaciones en la seguridad de TI en entidades gubernamentales similares. Con esto en mente, la tesis se propone no solo abordar los desafíos técnicos sino también fomentar una cultura de seguridad de la información que sea sostenible y efectiva a largo plazo.

CAPITULO I

MARCO REFERENCIAL

1.1 Planteamiento del Problema

En el departamento informático del GAD El Tambo, la gestión adecuada de la seguridad de la información se ha convertido en una prioridad dada la creciente dependencia de los procesos tecnológicos que soportan sus operaciones cotidianas. Frente a este escenario, surge la necesidad de evaluar los riesgos y vulnerabilidades a los que está expuesta la infraestructura tecnológica para asegurar la integridad, disponibilidad y confidencialidad de la información manejada.

Esta evaluación es fundamental no solo para prevenir incidentes de seguridad que podrían tener consecuencias devastadoras sobre la operatividad del GAD El Tambo sino también para establecer un marco de políticas que guíe el manejo de estas tecnologías alineado con las mejores prácticas y estándares internacionales. Sin embargo, la falta de un manual de políticas específicas para el manejo de riesgos y la mitigación de vulnerabilidades en TI limita la capacidad del departamento para responder eficazmente ante potenciales amenazas, lo que aumenta la susceptibilidad a ataques externos e internos que podrían comprometer la seguridad de toda la organización. Dado este contexto, se identifica una brecha crítica en la gestión de la seguridad de TI que debe ser abordada mediante un estudio detallado y la posterior implementación de un manual robusto de políticas de seguridad.

1.2.1 Formulación del Problema

- ¿Cuáles son los conceptos fundamentales y las mejores prácticas en seguridad de la información, análisis de riesgos y gestión de vulnerabilidades, y cómo se han aplicado

estas prácticas en el contexto de entidades gubernamentales según la norma ISO 27001?

- ¿Cuáles son los principales riesgos y vulnerabilidades presentes en el departamento informático del GAD El Tambo y cómo se pueden evaluar adecuadamente estos riesgos utilizando las herramientas y técnicas recomendadas por la norma ISO 27001?
- ¿Cómo se puede diseñar un manual de políticas de seguridad de TI que integre efectivamente las estrategias de mitigación de riesgos, asegure el cumplimiento con la norma ISO 27001 y fomente una cultura de seguridad robusta dentro del departamento informático?

1.3**Antecedentes de la Investigación**

El presente proyecto se basa en una cuidadosa revisión de trabajos previos relacionados con el análisis de riesgos y vulnerabilidades de tecnologías de la información (TI) en entornos gubernamentales.

Roberth Baque desarrollo un trabajo investigativo en la Universidad Estatal del Sur de Manabí, con título “DISEÑO DE UNA ESTACIÓN DE TRABAJO PARA DETECCIÓN DE VULNERABILIDADES DE SERVIDORES WEB, PARA MITIGAR CIBERATAQUES ", este proyecto se enfoca específicamente en los laboratorios de cómputo de la Carrera de Ingeniería en Computación y Redes, donde la implementación de una estación de trabajo para la detección de vulnerabilidades de servidores web se presenta como una medida preventiva fundamental para proteger los activos de tecnología de la información y garantizar la continuidad de las operaciones en este entorno académico. (Baque Villegas, 2020)

Este documento proporcionará una base sólida para construir el marco teórico ya que presenta una revisión de la literatura existente relacionada con la detección de vulnerabilidades en servidores web, sistemas, dispositivos, etc.

Balcazar Lalangui realizo un estudio titulado "Propuesta metodológica para mitigar el riesgo de seguridad informática con el uso de técnicas OSINT[1]", de la Universidad de las Fuerzas Armadas ESPE, destaca la importancia de abordar los desafíos actuales en seguridad informática, especialmente en el contexto de la proliferación de ataques en la red debido al desconocimiento de técnicas de protección por parte de los usuarios. Se resalta que las redes sociales y el acceso a la red desde diferentes dispositivos representan un gran riesgo para la seguridad de la información, ya que estas plataformas son frecuentemente blanco de ciberataques. (Balcázar Lalangui, 2020)

Este documento ofrece una propuesta metodológica, herramientas específicas y consideraciones éticas para llevar a cabo la investigación.

Otro estudio realizado por Renata Toasa de la

Julio Pilla de la Universidad Israel con título "PROPUESTA DE UN MANUAL DE POLÍTICAS DE SEGURIDAD INFORMÁTICA MEDIANTE LA APLICACIÓN DENORMAS ISO/IEC 38500 E ISO/IEC 27001 ALINEADAS AL COMPONENTE HUMANO PARA LA EMPRESA WILPRO S. A", se enfoca en el diseño e implementación de una política de seguridad informática que tiene como objetivo mitigar posibles vulnerabilidades en los sistemas de información de la cooperativa. El estudio abarca desde un análisis detallado de la gestión de seguridad de la información hasta la

[1] Open Source INTelligence (Inteligencia de Fuentes Abiertas)

evaluación de riesgos de los activos de TI, siguiendo normativas internacionales y modelos de gestión de seguridad.

Este análisis sirve de base para la creación de una política de seguridad ajustada a las necesidades específicas de la organización, alineada con los estándares internacionales de ciberseguridad, en particular con la norma ISO/IEC 27002:2013, que proporciona directrices para la gestión de la seguridad de la información y la implementación de controles que mitiguen los riesgos identificados.

1.4 Justificación de la Investigación

En la era digital actual, las instituciones gubernamentales enfrentan desafíos significativos en materia de seguridad de la información, con frecuentes incidentes que comprometen datos sensibles y afectan la continuidad de las operaciones, el departamento informático del GAD El Tambo no es la excepción. La implementación de un análisis riguroso de riesgos y vulnerabilidades se vuelve indispensable para identificar y mitigar posibles amenazas que podrían tener impactos adversos, tanto a nivel operativo como en la percepción pública de la entidad. Utilizando la metodología de la norma ISO 27001, este estudio se propone establecer un marco de acción que no solo mejore la seguridad, sino que también fortalezca la confianza de los ciudadanos en la capacidad del GAD para proteger su información.

Además, el desarrollo de un manual de políticas específicas basado en los resultados del análisis ayudará a formalizar los procesos y respuestas ante incidentes de seguridad, creando un ambiente más controlado y sistemático. La falta de tales políticas actualmente limita la capacidad de respuesta del departamento frente a incidentes, lo que podría resultar en pérdidas de información crítica o fallos en los servicios ofrecidos a la comunidad. Este proyecto tiene el potencial de transformar la gestión de la seguridad de

TI del GAD El Tambo, volviéndola más proactiva y alineada con estándares internacionales, lo cual es fundamental para garantizar una gestión efectiva y segura en el contexto actual de amenazas cibernéticas en constante evolución.

1.5 **Objetivos**

1.5.1 **Objetivo General.**

Realizar un análisis de los riesgos y vulnerabilidades en el departamento informático del GAD El Tambo, utilizando basados en la metodología de la norma ISO 27001, con el fin de proponer mejoras en la gestión de la seguridad de la información.

1.5.2 **Objetivos Específicos**

- Elaborar un marco teórico que consolide los conceptos fundamentales y las mejores prácticas sobre la seguridad de la información, análisis de riesgos y la gestión de vulnerabilidades, destacando las contribuciones de la norma ISO 27001 y su aplicación en entidades gubernamentales.
- Realizar un diagnóstico detallado de los riesgos y vulnerabilidades actuales en el departamento informático del GAD El Tambo, empleando herramientas y técnicas de evaluación conforme a los principios establecidos por la norma ISO 27001
- Diseñar un manual de políticas de seguridad de TI que integre las estrategias de mitigación de riesgos identificadas, garantizando el cumplimiento de las directrices de la ISO 27001 y fomentando una cultura de seguridad robusta dentro del departamento

1.6 **Limitaciones**

- **Acceso ilimitado a datos completos y actualizados:** Dado que la investigación depende en gran medida de la disponibilidad de información detallada y

actualizada sobre la infraestructura de TI, las políticas existentes y los procedimientos del departamento informático, cualquier restricción en el acceso a estos datos podría limitar la profundidad del análisis de riesgos y vulnerabilidades.

- **Cambios en la tecnología y amenazas de TI:** El campo de la tecnología de la información es altamente dinámico, con nuevas vulnerabilidades y amenazas que emergen continuamente.

1.7 **Delimitaciones**

- La investigación se centrará exclusivamente en el departamento informático del GAD El Tambo, limitando el análisis a las políticas, procedimientos y sistemas de TI específicos de esta entidad gubernamental
- El estudio se enfocará en los aspectos de seguridad de la información relacionados con amenazas cibernéticas y vulnerabilidades internas de los sistemas de información. Se excluyen otros aspectos de TI como hardware físico o telecomunicaciones, salvo en la medida en que interfieran directamente con la seguridad de la información.

CAPITULO II

2. MARCO TEORICO

2.1 Seguridad de la información

Abarca las medidas y prácticas destinadas a proteger la confidencialidad, integridad y disponibilidad de los datos en un entorno digital, mediante la implementación de controles de acceso, cifrado, monitorización y gestión de riesgos, con el fin de prevenir y mitigar amenazas como ciberataques, robo de datos y fallos de seguridad, garantizando así la protección y confianza en la información almacenada y transmitida por sistemas informáticos y redes. (Gumucio Suares, 2021)

2.1.1 Pilares de la Seguridad de la información

Son los fundamentos esenciales que sustentan la protección de los datos en entornos digitales, comprendiendo la confidencialidad, integridad y disponibilidad de la información, así como la autenticación, control de acceso, y gestión de riesgos, que en conjunto aseguran la preservación de la información frente a amenazas cibernéticas, garantizando su protección y fiabilidad para los usuarios y sistemas involucrados. (Carvajal Artunduaga, 2021)

2.1.1.1 Confidencialidad

Es el principio que garantiza que la información sensible se encuentra protegida contra accesos no autorizados, asegurando que solo aquellos usuarios o sistemas autorizados puedan acceder a la información protegida. (Correa Murillo , 2022)

2.1.1.2 Integridad

Se refiere a la propiedad de la información de mantenerse completa, exacta y no alterada durante su almacenamiento, procesamiento o transmisión. Garantiza que los datos no han sido modificados de manera no autorizada o accidental. (Ramirez Agudelo, 2021)

2.1.1.3 **Disponibilidad**

Es el principio que asegura que la información esté accesible y utilizable por aquellos usuarios autorizados que la requieran, en el momento en que sea necesario. Implica la implementación de medidas para prevenir interrupciones o caídas en los sistemas que puedan afectar el acceso a la información. (Correa Murillo , 2022)

2.2 **Amenazas**

Una amenaza en el contexto de la seguridad de la información se refiere a cualquier circunstancia o evento con el potencial de causar daño a un sistema informático, interrumpiendo sus operaciones y comprometiendo la integridad, disponibilidad o confidencialidad de los datos almacenados, incluye desde ataques cibernéticos hasta desastres naturales y errores humanos, siendo crucial su identificación para el desarrollo de estrategias de mitigación efectivas. (Rodríguez Guzmán, 2023)

2.2.1 **Clasificación de Amenazas**

- **Internas:** Provienen de dentro de la organización y pueden ser causadas tanto de manera intencionada como no intencionada; en el primer caso, involucran actos deliberados por parte de empleados, como el robo de información confidencial o sabotaje de sistemas, mientras que las amenazas no intencionadas usualmente resultan de errores involuntarios, falta de conocimiento adecuado o descuidos que pueden llevar a pérdidas de datos o fallos de seguridad, destacando la importancia de programas de capacitación y vigilancia interna para mitigar estos riesgos. (Aillón Carrasco , 2021)
- **Externas:** Son aquellas que se originan fuera de la organización e incluyen actores como hackers, criminales cibernéticos y competidores malintencionados; estos agentes pueden lanzar ataques como phishing, inyección de malware y otros tipos de intrusiones digitales con el objetivo de robar datos, causar daños

operativos o incluso extorsionar a la empresa, haciendo esencial la implementación de robustas medidas de seguridad como firewalls, sistemas de detección de intrusos y políticas de acceso seguro para proteger los activos de la organización. (Borbor Toala, 2021)

2.3 **Vulnerabilidades**

Se refieren a debilidades en un sistema que pueden ser explotadas por amenazas para causar un daño o realizar acciones no autorizadas, abarcan fallos en el software como errores de programación, configuraciones inadecuadas de sistemas y redes, así como la falta de procedimientos de seguridad actualizados, siendo fundamental realizar pruebas de penetración, actualizaciones regulares y capacitaciones en ciberseguridad para identificar y mitigar estas debilidades antes de que sean explotadas por agentes externos o internos. (Balcázar Lalangui, 2020)

2.3.1 **Clasificación de las Vulnerabilidades**

- **Según su Origen:**

Vulnerabilidades de Software: Estas vulnerabilidades representan errores o fallos en el código de programas y aplicaciones, incluyendo inyecciones SQL, desbordamientos de buffer y problemas en la gestión de autenticaciones y sesiones, son susceptibles a ataques que buscan explotar estos errores para obtener acceso no autorizado o causar daños. (Muñoz Aguirre, 2022)

Vulnerabilidades de Hardware: Se relacionan con debilidades en los componentes físicos de los dispositivos como microchips y discos duros, causadas por defectos de diseño, fallos de fabricación o vulnerabilidades que pueden ser explotadas para interceptar datos, alterar operaciones del dispositivo o causar daños físicos, siendo Spectre y Meltdown ejemplos recientes que afectan a los procesadores modernos. (Borbor Toala, 2021)

- **Según el Impacto:**

Vulnerabilidades Criticas: Son las amenazas más graves para los sistemas, cuya explotación puede tener un impacto severo en la confidencialidad, integridad o disponibilidad de la información o los sistemas, permitiendo a los atacantes obtener control total sobre sistemas críticos, acceder a grandes volúmenes de datos sensibles o incluso causar la caída de redes completas, debido a su potencial para causar daños extensos, su mitigación es prioritaria y urgente. (Aillón Carrasco , 2021)

Vulnerabilidades Importantes: No alcanzan la severidad de las críticas, pero su explotación puede tener consecuencias significativas, afectando la funcionalidad del sistema, la integridad de los datos o la privacidad de los usuarios, generalmente con limitaciones que reducen el alcance del daño; la mitigación de estas vulnerabilidades sigue siendo importante, pero puede ser prioritaria después de abordar cualquier vulnerabilidad crítica. (Muñoz Aguirre, 2022)

Vulnerabilidades Moderados: Representan riesgos menos inmediatos o severos pero su explotación puede ser perjudicial a un nivel funcional o de información menos crítico, permitiendo a los atacantes realizar acciones que perturban los procesos operativos sin comprometer directamente datos esenciales o causar daños extensos, a menudo ofrecen medidas de mitigación más sencillas o menos urgentes y se manejan en una fase posterior en el proceso de gestión de vulnerabilidades. (Catuto Pilay, 2021)

- **Según la Facilidad de Explotación**

Difíciles de Explotar: Requieren condiciones muy específicas para ser explotadas incluyendo que el atacante tenga acceso privilegiado o condiciones particulares del sistema, además de conocimientos técnicos avanzados y en algunos casos acceso físico

al dispositivo, la complejidad y los requerimientos específicos reducen la probabilidad de explotación. (Muñoz Aguirre, 2022)

Dificultad Media para Explotar: No son tan fáciles de explotar como las de alto nivel ni tan difíciles como las de bajo nivel, pueden requerir condiciones como interacción del usuario, como hacer clic en un enlace malicioso, o que el sistema tenga una configuración poco común, la explotación puede necesitar conocimientos técnicos, pero no extremadamente especializados. (Aillón Carrasco , 2021)

Fáciles de Explotar: Pueden ser explotadas fácilmente a menudo de manera automatizada como a través de un script o usando herramientas de explotación disponibles públicamente sin requerir condiciones especiales no necesitan interacción significativa por parte del usuario conocimientos especializados profundos ni acceso físico al dispositivo son las más peligrosas porque cualquier atacante incluso con habilidades limitadas puede explotarlas rápidamente. (Ramirez Agudelo, 2021)

2.4 **Riesgos**

Se refiere a la posibilidad de que amenazas exploten vulnerabilidades dentro de sistemas y redes, lo que puede llevar a daños o pérdidas de información crucial, siendo crucial su gestión para proteger la integridad, disponibilidad y confidencialidad de los datos de una organización, abarcando desde la identificación y análisis de posibles amenazas hasta la implementación de estrategias de mitigación y revisión constante para adaptarse a un entorno de amenazas en evolución. (Hidalgo Maldonado, 2019)

2.4.1 **Clasificación de los Riesgos**

Es una técnica de seguridad esencial que transforma la información clara en un formato cifrado, haciendo que sea incomprensible sin la clave de descifrado

adecuada. Este método protege la confidencialidad e integridad de los datos, asegurando que incluso si se produce un acceso no autorizado, la información no pueda ser entendida ni utilizada maliciosamente (Collaguazo Quinatoa & Toapanta Chilig , 2020)

- **Según su naturaleza:**

Riesgos estratégicos: Impactan las decisiones a largo plazo y la dirección general de la organización emergiendo de cambios en el entorno de negocios como nuevas regulaciones cambios en las preferencias de los consumidores evolución del mercado y competencia afectando la capacidad de la organización para alcanzar sus objetivos estratégicos y pudiendo tener repercusiones duraderas si no se gestionan adecuadamente. (Rodríguez Matías, 2021)

Riesgos operativos: Se relacionan con peligros asociados a los procesos internos personal y sistemas de una organización que pueden causar fallos en las operaciones diarias incluyendo fallos de sistemas errores humanos interrupciones del proceso de negocio y fraudes internos con impactos que varían desde interrupciones menores hasta eventos que podrían detener completamente las operaciones empresariales. (Pantoja Miño , 2020)

Riesgos financieros: Involucran la posibilidad de que una organización sufra pérdidas financieras originándose por fluctuaciones en los mercados financieros fallas en los procesos financieros internos insuficiencias en la gestión de créditos o como resultado de operaciones de inversión inadecuadas estando a menudo asociados con la gestión del flujo de caja las inversiones la financiación las tasas de interés y los cambios en los precios de mercado. (Fierro Alvares, 2022)

- **Según su probabilidad de ocurrencia**

Riesgos de alta probabilidad: Son aquellos con gran posibilidad de ocurrir en un futuro cercano debido a factores bien identificados y condiciones existentes que hacen muy probable que el evento de riesgo se materialice requiriendo atención inmediata y estrategias de mitigación efectivas porque su impacto puede ser inminente. (Pantoja Miño , 2020)

Probabilidad media: Tienen una oportunidad moderada de ocurrir generalmente debido a que existen factores desencadenantes, pero también hay medidas de control en lugar que podrían evitar o minimizar su ocurrencia requiriendo un monitoreo continuo y preparación para actuar en caso de que las condiciones cambien y la probabilidad de ocurrencia aumente. (Rodríguez Matías, 2021)

Probabilidad baja: Tienen pocas posibilidades de materializarse surgiendo en circunstancias altamente específicas y poco comunes o donde existen controles muy robustos y eficaces que reducen su probabilidad a casi nula, aunque aún requieren reconocimiento y monitoreo continúo dado que las condiciones subyacentes podrían cambiar con el tiempo. (Fierro Alvares, 2022)

- **Según su impacto**

Alto impacto: Son aquellas cuya explotación puede causar daños extremadamente graves a la organización incluyendo pérdida significativa de datos sensibles interrupciones a gran escala de las operaciones críticas o severos daños financieros y a la reputación pueden ser explotadas fácilmente a menudo de manera automatizada elevando el riesgo de ataques y haciendo urgente la necesidad de medidas de mitigación. (Catuto Pilay, 2021)

Impacto medio: Cuya explotación puede causar problemas moderados en la organización incluyendo interrupciones limitadas que afecten ciertos servicios no críticos pérdida de datos no esenciales o daños a la imagen pública que aunque notables pueden

ser gestionados sin una crisis completa estas vulnerabilidades a menudo explotables fácilmente demandan atención para evitar que escalen a problemas mayores. (Fierro Alvares, 2022)

Bajo impacto: Son aquellas cuya explotación no tendría más que un efecto menor en la organización pueden incluir inconvenientes menores como degradaciones temporales de la performance que no afectan significativamente las operaciones del negocio o no comprometen datos importantes, aunque pueden ser explotadas fácilmente a menudo de manera automatizada sus efectos son fácilmente manejables y tienen pocas consecuencias a largo plazo. (Rodríguez Matías, 2021)

- **Según su origen**

Riesgos internos: Estos provienen de dentro de la propia organización y están asociados con empleados procesos internos tecnologías y sistemas internos o la cultura organizacional pueden incluir errores involuntarios de empleados fraudes internos fallos de software no detectados durante las pruebas o deficiencias en los procedimientos de seguridad interna son particularmente peligrosos porque el acceso a información sensible ya está concedido a nivel interno lo que puede facilitar incidentes de seguridad. (Pantoja Miño , 2020)

Riesgos externos: Son aquellos que provienen de fuera de la organización incluyen amenazas de actores maliciosos como hackers ataques cibernéticos espionaje industrial competencia desleal, así como desastres naturales como terremotos o inundaciones también pueden surgir de cambios en el entorno legal y regulatorio que afecten las operaciones de la empresa son impredecibles en gran medida y pueden requerir una vigilancia y preparación constantes para mitigar su impacto. (Catuto Pilay, 2021)

- **Según su control**

Riesgos controlables: Son aquellos sobre los cuales la organización tiene cierto grado de influencia o autoridad para gestionar o mitigar a menudo surgen de procesos internos operaciones decisiones estratégicas o comportamientos dentro de la empresa mediante la implementación de políticas efectivas controles internos y medidas de seguridad adecuadas la organización puede efectivamente reducir su probabilidad de ocurrencia o su impacto ejemplos incluyen fallos operativos procedimientos de seguridad deficiente y errores de gestión. (Fierro Alvares, 2022)

Riesgos no controlables: Corresponden a aquellos sobre los cuales la organización tiene poco o ningún control y no pueden ser gestionados o influenciados fácilmente por decisiones internas, incluyen factores externos como desastres naturales, cambios en la política gubernamental, fluctuaciones económicas globales o acciones de competidores; para estos riesgos, la organización puede prepararse y planificar estrategias de contingencia pero no puede alterar su probabilidad de ocurrencia, la gestión de estos riesgos se enfoca en la preparación y la respuesta más que en la prevención. (Catuto Pilay, 2021)

2.5 **Normas y estándares de la seguridad de la información**

Ofrecen lineamientos clave y mejores prácticas para proteger la integridad confidencialidad y disponibilidad de los datos incluyen un conjunto de normativas que definen cómo establecer y mantener un sistema de gestión de seguridad ofrecen recomendaciones sobre controles de seguridad efectivos. (Catuto Pilay, 2021)

2.5.1 **ISO 27001**

ISO 27001 es un estándar internacional que proporciona el marco para un sistema de gestión de seguridad de la información (SGSI). Este estándar es parte de la serie más amplia ISO/IEC 27000, que incluye lineamientos y requisitos específicos para establecer, implementar, mantener y mejorar continuamente un SGSI. ISO 27001

ayuda a las organizaciones a proteger su información de manera sistemática y rentable mediante la adopción de un proceso de gestión de riesgo que es integral y a la vez adaptativo a los cambios en el entorno de seguridad. (Aillón Carrasco , 2021)

El corazón de este estándar es la necesidad de evaluar sistemáticamente los riesgos de información identificando amenazas y vulnerabilidades que pueden afectar los activos de información, y luego diseñar e implementar un conjunto de controles de seguridad personalizados para abordar los riesgos identificados. (Farinango Farinango , 2023)

Este proceso involucra un enfoque cíclico conocido como Planificar-Hacer-Verificar-Actuar (PDCA), que asegura que el sistema de gestión de seguridad se revisa y mejora de manera continua, manteniendo la seguridad alineada con las necesidades cambiantes de la organización. (Rea Guaman , 2020)

2.5.2 **NIST**

El Instituto Nacional de Estándares y Tecnología (NIST) de Estados Unidos ofrece un conjunto de estándares y lineamientos destinados a mejorar la seguridad de la información y las infraestructuras de TI; entre los documentos más relevantes del NIST en el ámbito de la seguridad de la información se encuentra la serie NIST SP 800, que cubre amplios aspectos de la gestión de la seguridad de la información y la respuesta a incidentes. (Narváez Guerrón, 2024)

Estos documentos no solo proporcionan directrices prácticas y detalladas para asegurar los sistemas de información sino que también ofrecen marcos de referencia que ayudan a las organizaciones a entender y mejorar sus controles de seguridad; los temas tratados incluyen evaluación de riesgos seguridad cibernética gestión de identidades y acceso y protección de infraestructuras críticas entre otros. Uno de los marcos más influyentes de NIST es el Framework for Improving Critical Infrastructure Cybersecurity

comúnmente conocido como el Marco de Ciberseguridad de NIST. (Balcázar Lalangui, 2020)

2.5.3 **COBIT**

COBIT[2] es un marco de referencia desarrollado por ISACA [3]para la gestión y el gobierno de las tecnologías de la información (TI); COBIT proporciona principios, prácticas, herramientas y modelos de referencia globalmente aceptados para ayudar a las organizaciones a desarrollar, implementar y mejorar sus sistemas de control y gestión de TI, asegurando que la tecnología de la información se alinee con los objetivos de negocio. (Pantoja Miño , 2020)

El marco de COBIT está estructurado en varios componentes clave que incluyen:

- **Principios de Gobierno y Gestión:** Proporcionan directrices para alinear las prácticas de TI con los objetivos estratégicos y operativos de la organización incluyen la definición de roles y responsabilidades claras la creación de políticas y procedimientos de gobernanza y la promoción de una cultura organizacional que valore la gestión efectiva de TI además enfatizan la importancia de la transparencia la responsabilidad y la ética en el manejo de la información y la tecnología. (Carvajal Artunduaga, 2021)
- **Objetivos de Gobierno y Gestión:** Describen lo que se espera de la gestión de TI y los resultados que deben alcanzarse para asegurar que la tecnología de la información apoye efectivamente los objetivos del negocio estos objetivos se dividen en dominios específicos como alineación estratégica entrega de valor gestión de riesgos gestión de recursos y medición del rendimiento cada objetivo se vincula con metas organizacionales más amplias asegurando que todas las

[2] Control Objectives for Information and Related Technologies
[3] Information Systems Audit and Control Association

actividades de TI contribuyan al éxito general de la organización (Pantoja Miño , 2020)

- **Procesos y Prácticas de Gestión:** Detallan las actividades y tareas específicas necesarias para cumplir con los objetivos de gobierno y gestión de TI estos procesos incluyen la planificación y organización de recursos de TI la adquisición e implementación de soluciones tecnológicas, la entrega de servicios de TI, el monitoreo y evaluación del rendimiento de TI; las prácticas de gestión abarcan desde la gestión de proyectos, la garantía de calidad hasta la seguridad de la información y la gestión de cambios proporcionando un marco integral para gestionar todas las facetas de la TI. (Correa Murillo , 2022)
- **Modelos de Madurez y Capacidades:** Ayudan a las organizaciones a desarrollar un plan de acción para elevar sus prácticas de gestión de TI a niveles superiores de madurez, facilitando la mejora continua y la adaptación a cambios tecnológicos y de negocio; también permiten la comparación con mejores prácticas y estándares de la industria, ayudando a las organizaciones a mantenerse competitivas y alineadas con las tendencias actuales. (Pantoja Miño , 2020)

2.6 **Metodologías para Análisis de Riesgos de TI**

Las metodologías para el análisis de riesgos de TI son esenciales para identificar, evaluar y gestionar los riesgos que pueden afectar los sistemas y datos de una organización. (Narváez Guerrón, 2024)

2.6.1 **OCTAVE**

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) es una metodología para la gestión de riesgos de seguridad de la información desarrollada por el Software Engineering Institute (SEI) de la Universidad Carnegie Mellon. Está diseñada para ayudar a las organizaciones a identificar, evaluar y mitigar los riesgos de

seguridad mediante un enfoque sistemático y centrado en la organización. (Farinango Farinango , 2023)

Desarrollar un Perfil de Amenazas de la Organización:

- En esta fase, se identifican los activos críticos de la organización y se evalúan las amenazas potenciales que podrían afectarlos. Esto implica comprender el contexto organizativo, las necesidades de seguridad, y los impactos potenciales de las amenazas. (Muñoz Gutiérrez , 2022)

Identificación de Vulnerabilidades y Evaluación de Riesgos:

- Aquí se identifican y analizan las vulnerabilidades que podrían ser explotadas por las amenazas identificadas en la primera fase. Se evalúan los riesgos asociados a estas vulnerabilidades y se priorizan en función de su probabilidad de ocurrencia y el impacto potencial. (Farinango Farinango , 2023)

Planificación y Mitigación de Riesgos:

- En esta última fase, se desarrollan e implementan planes de mitigación para abordar los riesgos identificados. Esto incluye la selección de controles y medidas de seguridad específicas para reducir la probabilidad y el impacto de los riesgos, así como la implementación de políticas y procedimientos para gestionar la seguridad de la información de manera continua. (Muñoz Aguirre, 2022)

2.6.2 **CRAMM**[4]

Es una metodología desarrollada por la Central Computer and Telecommunications Agency del Reino Unido diseñada para el análisis y gestión de riesgos de seguridad de la información proporciona un enfoque estructurado y sistemático para identificar evaluar y gestionar riesgos asegurando que se implementen controles adecuados para proteger los activos de información. (Ayala Salguero, 2021)

CRAMM consta de tres fases principales:

Identificación y Valoración de Activos:

En esta fase, se identifican todos los activos de información críticos para la organización y se les asigna un valor en función de su importancia y la sensibilidad de los datos que contienen. Esto ayuda a priorizar los activos que necesitan mayor protección. (Muñoz Aguirre, 2022)

Análisis de Amenazas y Vulnerabilidades:

Se identifican y analizan las amenazas que pueden afectar a los activos de información y las vulnerabilidades que podrían ser explotadas por estas amenazas. Esta fase incluye la evaluación de la probabilidad de que las amenazas se materialicen y el impacto potencial en caso de que lo hagan. (Ayala Salguero, 2021)

Selección e Implementación de Controles:

Basado en el análisis de riesgos, se seleccionan los controles de seguridad adecuados para mitigar los riesgos identificados. Esta fase implica desarrollar e implementar políticas, procedimientos y medidas técnicas para reducir la probabilidad de

[4] Information Systems Audit and Control Association

que las amenazas se materialicen y minimizar el impacto si ocurren. (Correa Murillo , 2022)

2.6.3 **ISO 27005**

ISO 27005 es una norma internacional que proporciona directrices específicas para la gestión de riesgos en la seguridad de la información y es parte de la serie ISO/IEC 27000; se centra en ayudar a las organizaciones a implementar un enfoque sistemático para identificar, evaluar y gestionar los riesgos de seguridad de la información. (Pinto Auz, 2021)

2.6.3.1 **Objetivos de la ISO 27005**

- **Proporcionar un marco para la gestión de riesgos:** Ayuda a las organizaciones a establecer un proceso continuo y sistemático para la gestión de riesgos de seguridad de la información; este marco estructurado asegura que todas las actividades relacionadas con la gestión de riesgos sean coherentes, repetibles y efectivas en todas las áreas de la organización. (Ayala Salguero, 2021)
- **Facilitar la identificación de riesgos:** Proporciona métodos y herramientas para identificar riesgos potenciales que puedan afectar la confidencialidad, integridad y disponibilidad de la información; esto incluye la identificación de amenazas, vulnerabilidades y activos críticos, permitiendo a las organizaciones anticipar posibles incidentes de seguridad. (Borbor Toala, 2021)
- **Evaluación de riesgos:** Define criterios y procedimientos para evaluar la probabilidad e impacto de los riesgos identificados, permitiendo priorizarlos adecuadamente; esta evaluación sistemática ayuda a las organizaciones a enfocarse en los riesgos más significativos y a tomar decisiones informadas sobre cómo gestionarlos. (Pinto Auz, 2021)

- **Tratamiento de riesgos:** Ofrece estrategias y opciones para mitigar, transferir, aceptar o evitar riesgos, asegurando que las medidas de control sean adecuadas y efectivas; esto incluye la selección e implementación de controles de seguridad específicos para reducir los riesgos a un nivel aceptable, alineado con los objetivos de la organización. (Borbor Toala, 2021)
- **Monitoreo y revisión:** Establece la necesidad de monitorear continuamente los riesgos y revisar regularmente el proceso de gestión de riesgos para adaptarse a los cambios en el entorno de seguridad; este enfoque dinámico asegura que la gestión de riesgos se mantenga relevante y eficaz frente a nuevas amenazas, vulnerabilidades y cambios en el contexto organizacional. (Muñoz Aguirre, 2022)

2.6.3.2 **Estructura de la ISO 27005**

- **Introducción y Alcance:** En esta Define el propósito de la norma y su aplicabilidad en diversas organizaciones, estableciendo el contexto y los objetivos principales de la gestión de riesgos de seguridad de la información. (Pinto Auz, 2021)
- **Términos y Definiciones:** Proporciona una lista de términos clave y sus definiciones para asegurar una comprensión común entre todos los involucrados en el proceso de gestión de riesgos, facilitando la comunicación y la coherencia en la aplicación de la norma. (Balcázar Lalangui, 2020)
- **Proceso de Gestión de Riesgos:** Detalla los pasos específicos para la gestión de riesgos, incluyendo la identificación, evaluación, tratamiento, aceptación, comunicación y monitoreo de riesgos, ofreciendo un marco estructurado y sistemático para gestionar los riesgos de manera continua. (Aillón Carrasco , 2021)

- **Identificación de Riesgos:** Métodos y herramientas para identificar amenazas, vulnerabilidades y activos que necesitan protección, permitiendo a las organizaciones detectar posibles riesgos que puedan afectar la seguridad de la información. (Catuto Pilay, 2021)
- **Evaluación de Riesgos:** Procedimientos para evaluar la probabilidad y el impacto de los riesgos identificados, utilizando métodos cualitativos y cuantitativos, con el fin de priorizar los riesgos y tomar decisiones informadas sobre su gestión.
- **Tratamiento de Riesgos:** Opciones y estrategias para abordar los riesgos, seleccionando controles adecuados y planificando su implementación, asegurando que los riesgos sean mitigados, transferidos, evitados o aceptados de manera efectiva. (Patiño Castrillon & Bedoya Velasquez, 2023)
- **Aceptación de Riesgos:** Criterios y procedimientos para decidir cuándo aceptar riesgos residuales basados en una evaluación de costo-beneficio, determinando cuáles riesgos son aceptables para la organización y bajo qué condiciones. (Farinango Farinango , 2023)
- **Monitoreo y Revisión:** Métodos para monitorear continuamente los riesgos y revisar el proceso de gestión de riesgos para asegurar su efectividad y relevancia, garantizando que el enfoque de gestión de riesgos se mantenga actualizado y alineado con los cambios en el entorno y las operaciones de la organización. (Pinto Auz, 2021)

2.6.4 **Análisis comparativo entre OCAVE, CRAMM, ISO27005**

En la siguiente tabla se realiza un análisis comparativo.

Tabla 1 Análisis comparativo entre OCAVE, CRAMM, ISO27005

Característica	**OCTAVE**	**CRAMM**	**ISO 27005**

Enfoque	Centrado en la organización y orientado a la gestión de riesgos estratégicos.	Centrado en controles y evaluación de conformidad.	Centrado en la gestión de riesgos de la seguridad de la información.
Objetivo Principal	Identificar activos críticos y proteger la información según su valor.	Evaluar los controles existentes y recomendar mejoras.	Proveer un modelo de riesgo para la implementación de un SGSI (Sistema de Gestión de Seguridad de la Información).
Metodología	Análisis cualitativo principalmente, con opciones para cuantitativo.	Combinación de análisis cuantitativo y cualitativo.	Flexible; admite tanto análisis cualitativo como cuantitativo.
Usuarios	Adaptado para medianas y grandes empresas.	Originalmente desarrollado para el gobierno del Reino Unido, aplicable a varios sectores.	Diseñado para organizaciones que necesitan alinearse con la norma ISO 27001.
Herramientas	Herramientas propias que facilitan la realización del análisis.	Herramientas software específicas para asistir en el análisis y la documentación.	No prescribe herramientas específicas; flexible en herramientas según las necesidades de la organización.
Documentación	Guías detalladas disponibles para facilitar la implementación.	Guías y documentación extensa para implementación y gestión.	Documentación que se alinea con otros estándares ISO para una integración fluida.
Adopción	Fuerte en sectores que valoran enfoques personalizados y basados en la comunidad interna.	Ampliamente utilizado en Europa, especialmente en sectores regulados.	Globalmente reconocido y utilizado en diversas industrias.

Ciberseguridad

La ciberseguridad es un campo multidisciplinario que se centra en proteger los sistemas informáticos, redes y datos contra una amplia gama de amenazas cibernéticas. Esto incluye la protección contra malware, ataques de denegación de servicio (DDoS), robos de datos, intrusiones y otras formas de actividad maliciosa que buscan comprometer la seguridad y la privacidad de la información digital. (Rea Guaman , 2020)

Abarca la implementación de medidas proactivas, como firewalls, sistemas de detección de intrusiones y cifrado de datos, así como la gestión de incidentes, la respuesta ante emergencias y la recuperación de desastres para minimizar el impacto de posibles ataques y asegurar la continuidad del negocio. (Patiño Castrillon & Bedoya Velasquez, 2023)

Amenazas Cibernéticas

Son intentos maliciosos de infiltrarse o dañar un sistema de información o robar datos privados, incluyen ataques como malware, phishing y ataques de ingeniería social, diseñados para explotar vulnerabilidades de seguridad y pueden ser ejecutados por individuos o grupos con diversos motivos, desde el crimen organizado hasta el espionaje. (Paredes Díaz, 2022)

Tipos de Amenazas Cibernéticas

- **Malware**

El malware, abreviatura de software malicioso, engloba varios tipos de programas dañinos diseñados para infiltrarse y dañar sistemas informáticos sin el consentimiento del usuario, incluye virus, gusanos, troyanos y ransomware, cada uno con métodos específicos para afectar el rendimiento, robar información o ganar acceso no autorizado, representando una amenaza constante tanto para usuarios individuales como para

organizaciones, y requiriendo medidas proactivas de seguridad para su detección y eliminación efectiva. (Chulde Obando, 2021)

- **Phishing**

Es una técnica de fraude en la que los atacantes engañan a las víctimas para que entreguen información sensible como contraseñas y detalles de tarjetas de crédito, mediante el uso de comunicaciones falsificadas que aparentan ser de fuentes confiables como bancos o servicios populares en línea, a menudo involucra correos electrónicos, mensajes de texto o sitios web fraudulentos diseñados para imitar los legítimos, y es uno de los métodos más comunes y efectivos de ciberataque debido a su aprovechamiento de la ingeniería social. (Paredes Díaz, 2022)

- **Ataques de Ingeniería Social**

Son estrategias utilizadas por ciberdelincuentes que manipulan psicológicamente a las personas para que realicen acciones o divulguen información confidencial, estos ataques explotan la naturaleza confiada o menos precavida de los individuos, utilizando pretextos, manipulación emocional o falsas urgencias para obtener acceso no autorizado a datos importantes, son especialmente peligrosos porque se basan en el error humano más que en vulnerabilidades técnicas, lo que los hace difíciles de prevenir solo con medidas tecnológicas. (Chulde Obando, 2021)

- **Ataques de Denegacion de Servicio (DoS)**

Conocidos como DoS, son intentos malintencionados de interrumpir el funcionamiento normal de un sitio web o servicio en línea, inundándolo con tráfico excesivo hasta sobrecargar sus recursos y hacerlo inaccesible para los usuarios legítimos, estos ataques pueden originarse desde un único punto o distribuirse a través de múltiples sistemas infectados en un ataque de denegación de servicio distribuido, conocido como DDoS,

representando una amenaza seria para la continuidad de las operaciones en línea y la disponibilidad de servicios críticos. (Quispe García , 2021)

- **Ataques Man-in-the-Middle**

Conocidos como MitM, ocurren cuando un atacante intercepta y posiblemente altera la comunicación entre dos partes que creen que están comunicándose directamente entre sí, estos ataques son particularmente peligrosos porque pueden ser difíciles de detectar y permiten al atacante capturar, modificar y redirigir información sin el conocimiento de las partes involucradas, siendo utilizados para robar datos personales, credenciales de acceso y realizar fraudes financieros, requiriendo una vigilancia constante y el uso de comunicaciones cifradas para su prevención.

Estrategias de defensa

- **Defensa en Profundidad**

Es una estrategia de seguridad cibernética que utiliza múltiples capas de protección distribuidas a lo largo de los sistemas de información y redes para asegurar que si un nivel es comprometido, los siguientes puedan seguir ofreciendo resistencia, similar a las capas de una cebolla, esta táctica abarca desde controles físicos, como seguridad en el acceso a edificios, hasta controles de software como firewalls, antivirus y encriptación, siendo esencial para crear un entorno robusto que dificulte significativamente que los atacantes alcancen sus objetivos finales. (Quispe García , 2021)

- **Prevención de Amenaza**

Conocidos involucra el uso de herramientas como antivirus, firewalls, y sistemas de detección y prevención de intrusiones, junto con prácticas como actualizaciones de seguridad y educación de usuarios, para bloquear proactivamente actividades maliciosas antes de que afecten los sistemas, constituyendo una barrera esencial contra ataques y

protegiendo los activos de información de riesgos tanto externos como internos. (Balcázar Lalangui, 2020)

- **Seguridad de Aplicaciones**

Se enfoca en asegurar que el software esté protegido contra vulnerabilidades explotables mediante prácticas de codificación segura, pruebas de penetración y auditorías de seguridad, técnicas como controles de acceso, cifrado de datos y validación de entrada fortalecen las aplicaciones mientras que la educación continua de desarrolladores sobre amenazas y protecciones actualizadas es crucial para mantener la integridad y confidencialidad a lo largo del ciclo de vida de la aplicación. (Quispe García , 2021)

- **Capacitación y Concienciación**

Es vital para empoderar a los empleados como la primera línea de defensa de una organización, mediante programas regulares que enseñan sobre amenazas actuales, reconocimiento de phishing, gestión segura de contraseñas y manejo adecuado de datos sensibles, buscando no solo mejorar el conocimiento técnico sino también fomentar una cultura de seguridad que promueva comportamientos responsables y preventivos para reducir el riesgo de brechas de seguridad originadas por errores humanos. (Rodríguez Matías, 2021)

- **Gestión de Parches y Vulnerabilidades**

Es crucial para la ciberseguridad, enfocándose en el proceso de identificar, clasificar, priorizar y aplicar actualizaciones de software para corregir fallos y proteger los sistemas contra amenazas conocidas, además incluye la evaluación continua de la infraestructura de TI para detectar y remediar fallos de seguridad de manera oportuna, asegurando que todas las componentes del sistema, desde el sistema operativo hasta las aplicaciones de terceros, estén constantemente actualizadas y protegidas. (Pinto Auz, 2021)

3. CAPITULO III

3. MARCO METODOLOGICO

3.1 **Enfoque de la Investigación**

La presente investigación adopta un enfoque mixto que combina métodos cualitativos y cuantitativos para obtener una visión integral de los riesgos y vulnerabilidades de TI en el departamento informático del GAD El Tambo. Este enfoque permitirá no solo identificar las amenazas potenciales, sino también comprender las percepciones y experiencias del personal relacionadas con la seguridad de la información.

3.2 **Nivel de Investigación**

El nivel de investigación será **descriptivo y exploratorio.** La investigación descriptiva se centrará en detallar los riesgos y vulnerabilidades actuales del departamento de TI del GAD El Tambo, proporcionando una visión clara y precisa del estado actual de la seguridad de la información. Esto incluye la descripción de las prácticas, políticas y procedimientos existentes, así como la identificación de debilidades y áreas de mejora. Por otro lado, la investigación exploratoria permitirá indagar en nuevas áreas y dimensiones de riesgos y vulnerabilidades que no hayan sido previamente identificadas. Este enfoque exploratorio es crucial para descubrir amenazas emergentes y desarrollar estrategias innovadoras para mitigar riesgos futuros, asegurando así una protección integral de la infraestructura de TI del GAD El Tambo.

3.3 **Población**

La población de estudio se centrará en el gerente del departamento de TI del GAD El Tambo, quien proporciona una visión integral y detallada de las políticas, prácticas y desafíos de seguridad de la información. La muestra, por lo tanto, se limitará a este único

individuo, garantizando una recolección de datos directa y específica de la gestión de riesgos y vulnerabilidades en la infraestructura tecnológica.

3.4 **Técnicas e Instrumentos de Recolección**

Para la recolección de datos se utilizará una única técnica: una encuesta estructurada dirigida al gerente del departamento de TI del GAD El Tambo. Este cuestionario estará diseñado con preguntas cerradas para recolectar información detallada sobre las prácticas actuales de seguridad, las vulnerabilidades percibidas y las medidas de mitigación implementadas.

3.5 **Tratamiento de la Información**

La información recopilada a través de la encuesta será organizada sistemáticamente para facilitar su análisis. Posteriormente, se llevará a cabo un análisis exhaustivo e interpretación de los resultados obtenidos.

3.6 **Resultados**

Para evaluar el estado de la seguridad de la información en el GAD El Tambo, se empleará un enfoque de recopilación de datos a través de una encuesta. Una vez formuladas las preguntas clave, se procederá con la ejecución de las mismas. Finalmente, se realizará un análisis minucioso y la interpretación de los datos obtenidos.

3.6.1. Encuesta

Se realizará una encuesta al gerente de TI del GAD El Tambo con el objetivo de recopilar datos para llevar a cabo un análisis exhaustivo sobre los riesgos y vulnerabilidades en el departamento informático.

PREGUNTAS CLASIFICADAS POR DOMINIOS DE LA ISO 27001:2013

Tabla 2 Respuestas de la encuesta. Fuente: Autoría Propia.

Área de Evaluación	**Encuesta**	**SI**	**NO**	**EN PROCESO**
Contexto de la Organización	El GAD El Tambo ha identificado las partes interesadas relevantes para la seguridad de la información.	X		
	Se ha definido claramente el alcance del SGSI para el departamento informático.		X	
	Se han identificado y documentado los activos de información críticos.		X	
	Se ha realizado un análisis de riesgos de seguridad de la información recientemente.		X	
Liderazgo	La alta dirección demuestra compromiso y liderazgo en seguridad de la información.	X		
	Se han establecido políticas y objetivos claros de seguridad de la información.	X		

	Se asignan roles y responsabilidades específicas para la gestión de la seguridad de la información.	X		
	La alta dirección participa activamente en revisiones periódicas del SGSI.		X	
Planificación	Se realiza una evaluación regular de los riesgos de seguridad de la información.		X	
	Se implementan planes de tratamiento de riesgos para abordar las vulnerabilidades.	X		
	Se revisan y actualizan periódicamente los controles de seguridad de la información.		X	
	Se definen objetivos de seguridad de la información SMART. (**S**pecific, **M**easurable, **A**chievable, **R**elevant, **T**ime-bound)		X	
Soporte	El departamento informático cuenta con los recursos necesarios para implementar y mantener el SGSI.			X
	El personal recibe formación adecuada en seguridad de la información.		X	
	Existencia de procedimientos claros de comunicación interna y externa sobre seguridad de la información.		X	

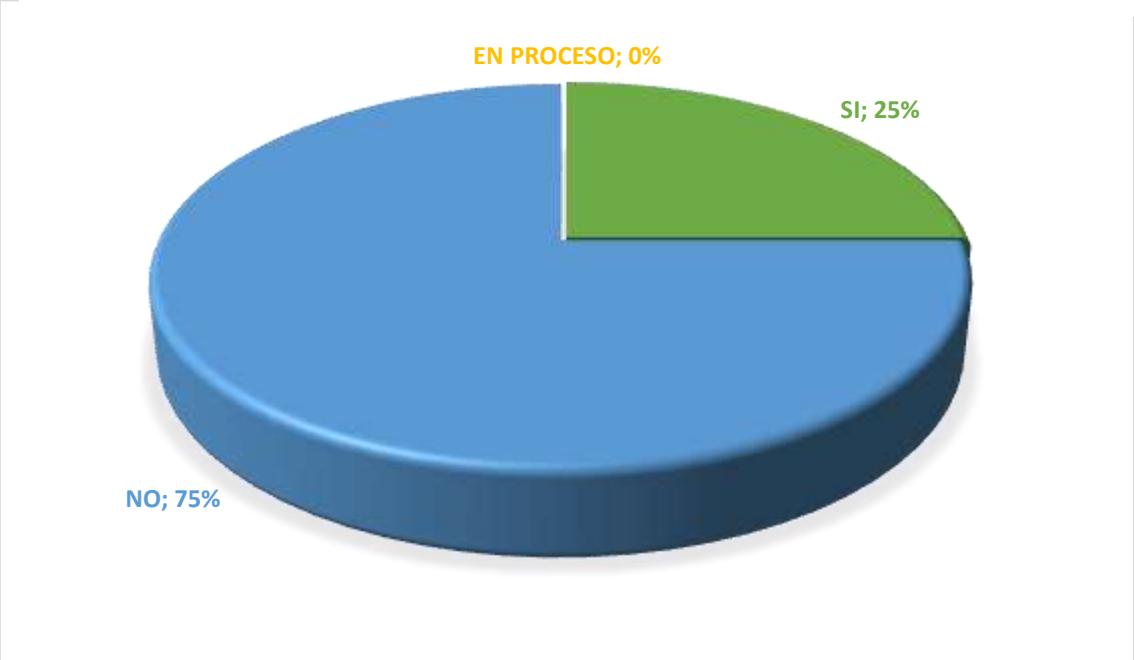
Operación	Se asignan presupuestos específicos para la seguridad de la información.	X		
	Se implementan controles efectivos de seguridad de la información en las operaciones diarias.		X	
	Se monitorea y audita regularmente el cumplimiento de los controles de seguridad.	X		
	Procedimientos documentados para la gestión de incidentes de seguridad.	X		
	Realización de pruebas de penetración o evaluaciones de vulnerabilidades periódicamente.		X	
Evaluación del Desempeño	Se realizan auditorías internas periódicas para evaluar el desempeño del SGSI.	X		
	Uso de indicadores clave de desempeño para medir la eficacia de los controles.	X		
	Implementación de acciones correctivas y preventivas basadas en auditorías.	X		
	Realización de revisiones post-incidente después de incidentes significativos.		X	
Mejora Continua	El departamento busca continuamente mejorar la eficacia del SGSI y la gestión de riesgos.		X	
	Revisión y actualización regular de procedimientos y controles de seguridad.	X		

Fomento de una cultura organizacional que promueva la conciencia en seguridad de la información.	X		
Evaluaciones periódicas de la satisfacción de los usuarios internos sobre seguridad de la información.	X		

A partir de la encuesta aplicada al gerente del departamento de Tecnologías de la Información del GAD El Tambo, donde se evaluaron los 7 dominios definidos en la norma ISO 7001:2013, se procedio realizar un análisis cuantitativo para determinar el nivel de conformidad con dichos dominios.

3.6.1. DOMINIO: Contexto de la Organización.

Gráfico 1 Dominio: Contexto de la Organización Autoría Propia

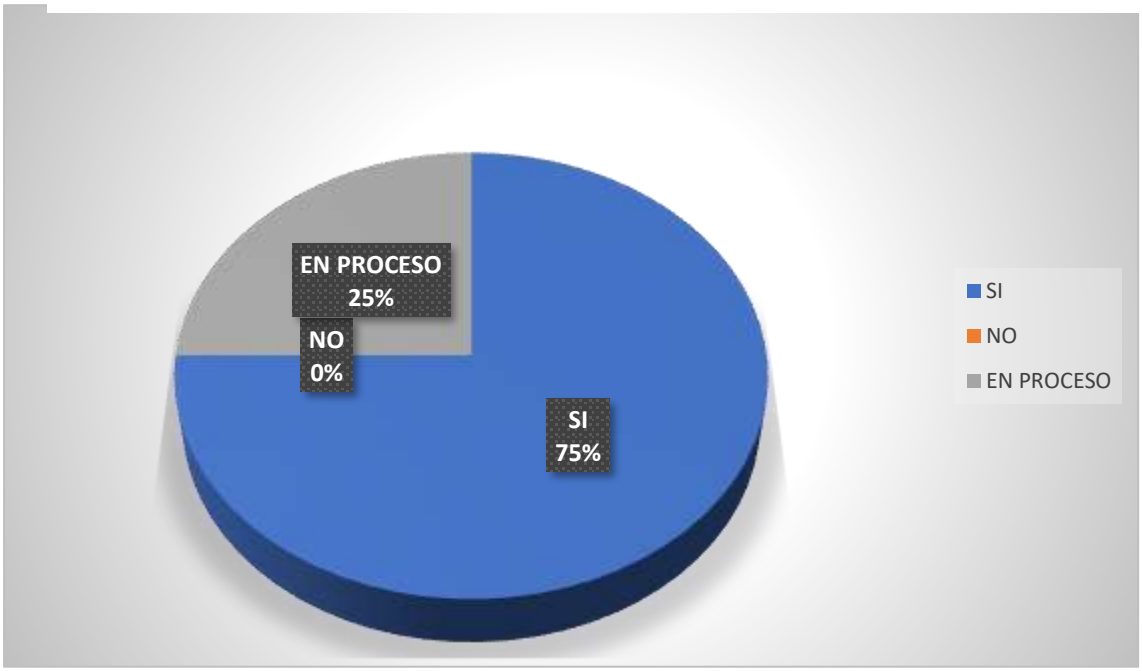


Muestra que el 25% de los ítems se han completado satisfactoriamente, indicando que el GAD El Tambo ha identificado las partes interesadas relevantes para la seguridad de la información. Sin embargo, el 75% de los ítems en este dominio aún no están implementados completamente. Esto incluye la falta de definición clara del alcance del Sistema de Gestión de Seguridad de la Información (SGSI), la no identificación y documentación de los activos de información críticos, y la ausencia de un análisis de riesgos reciente. No se reportan ítems en proceso, lo que sugiere que estos aspectos requieren atención y

desarrollo para alcanzar una mayor madurez en la gestión del contexto organizacional relacionado con la seguridad de la información.

3.6.2. DOMINIO: Liderazgo

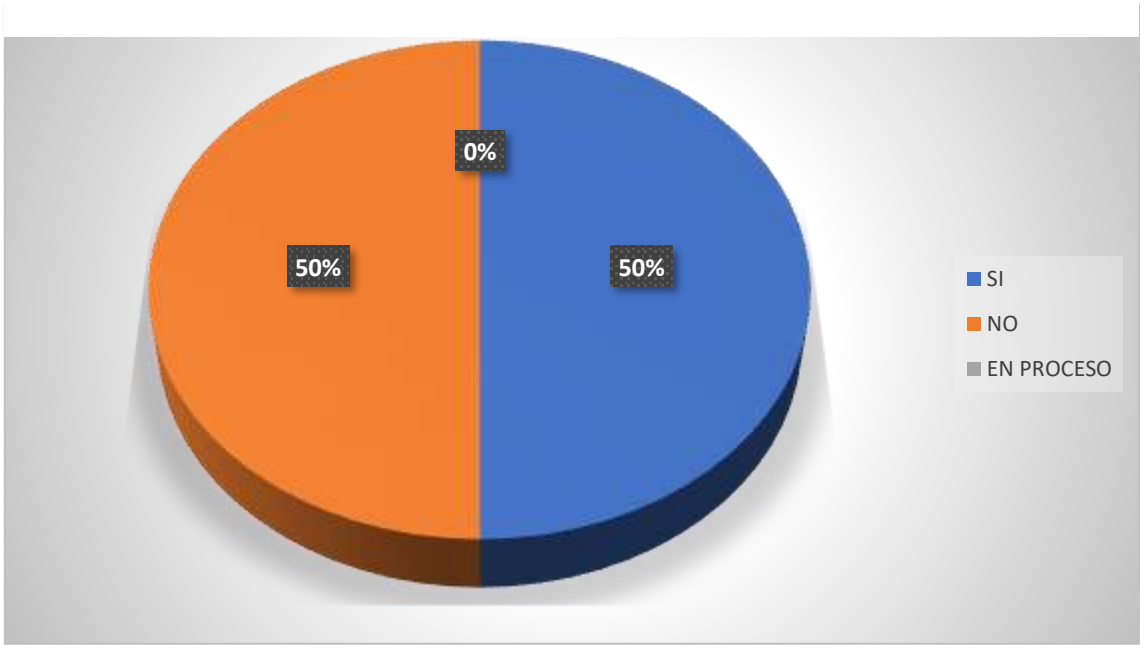
Gráfico 2 DOMINIO: Liderazgo. Fuente: Autoría Propia.



El análisis del dominio de "Liderazgo" que la alta dirección demuestra un compromiso y liderazgo adecuados en la seguridad de la información, y que se han establecido políticas y objetivos claros, además de asignar roles y responsabilidades específicas para la gestión de la seguridad de la información. Sin embargo, se señala que la alta dirección no participa activamente en las revisiones periódicas del Sistema de Gestión de Seguridad de la Información (SGSI), lo que sugiere que este aspecto aún está en proceso de implementación. No se reporta ninguna deficiencia importante en términos de liderazgo, ya que no hay respuestas negativas en este dominio.

3.6.3. DOMINIO: Planificación

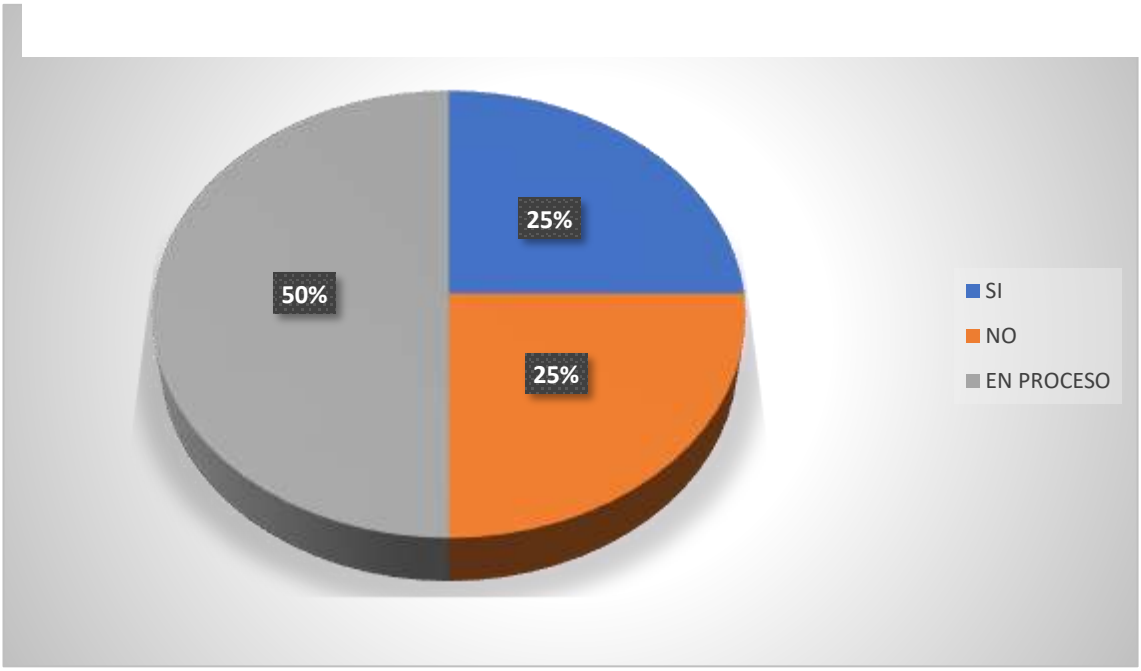
Gráfico 3 DOMINIO: Planificación. Fuente: Autoría Propia.



El GAD El Tambo muestra un equilibrio en el cumplimiento de los aspectos evaluados, con un 50% de los ítems cumplidos y otro 50% no cumplidos. La organización ha logrado implementar planes de tratamiento de riesgos y definir objetivos de seguridad SMART, lo cual es positivo. Sin embargo, la falta de evaluación regular de riesgos y la ausencia de revisión periódica de controles indican debilidades significativas. Estos déficits podrían afectar la capacidad de la organización para adaptar sus controles a nuevas amenazas y mantener la efectividad del SGSI. Se recomienda fortalecer la planificación mediante la implementación de evaluaciones de riesgos y revisiones periódicas de controles para mejorar la resiliencia del sistema de gestión de seguridad de la información.

3.6.4. DOMINIO: Soporte

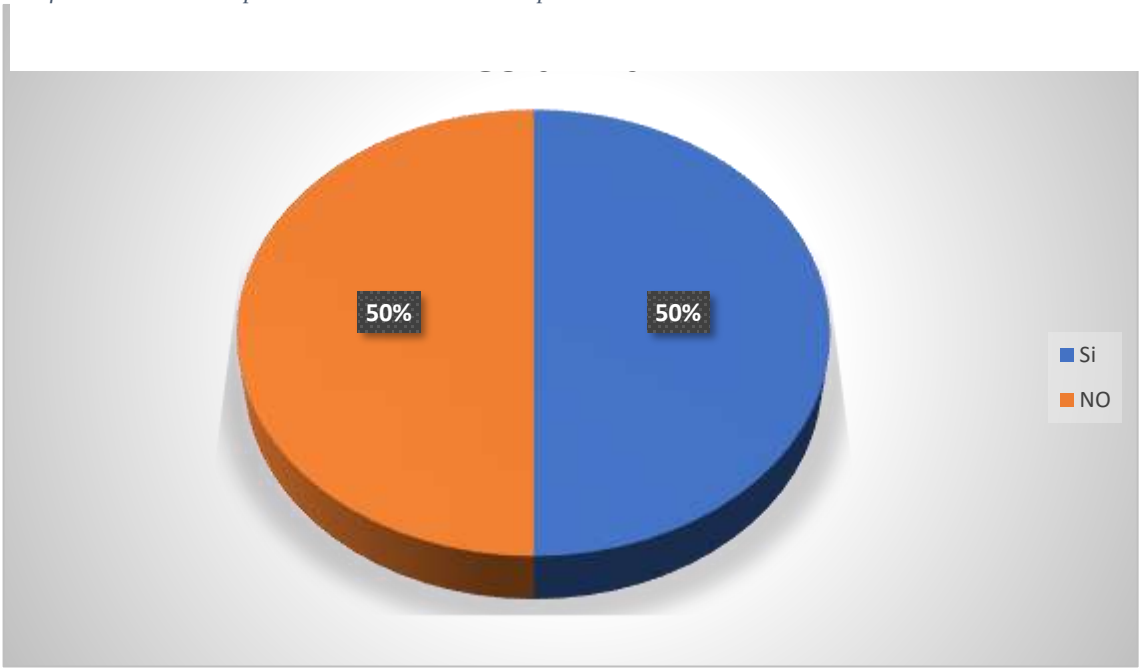
Gráfico 4 DOMINIO: Soporte. Fuente: Autoría Propia.



Implementación de medidas de seguridad de la información. Mientras que un 25% de los ítems, como la asignación de presupuestos específicos para la seguridad y la formación del personal en seguridad de la información, están en cumplimiento, el 50% de los ítems aún están en proceso y un 25% no se han abordado. La falta de recursos necesarios para implementar y mantener el SGSI y la existencia de procedimientos claros de comunicación sobre seguridad reflejan áreas críticas que necesitan atención. La falta de progreso en estos aspectos puede comprometer la capacidad del GAD El Tambo para establecer un soporte robusto y efectivo para su SGSI. Se recomienda priorizar la asignación de recursos adecuados, mejorar la comunicación interna y externa, y asegurar una formación continua del personal para fortalecer el soporte del sistema de gestión de seguridad de la información.

3.6.5. DOMINIO: Operación

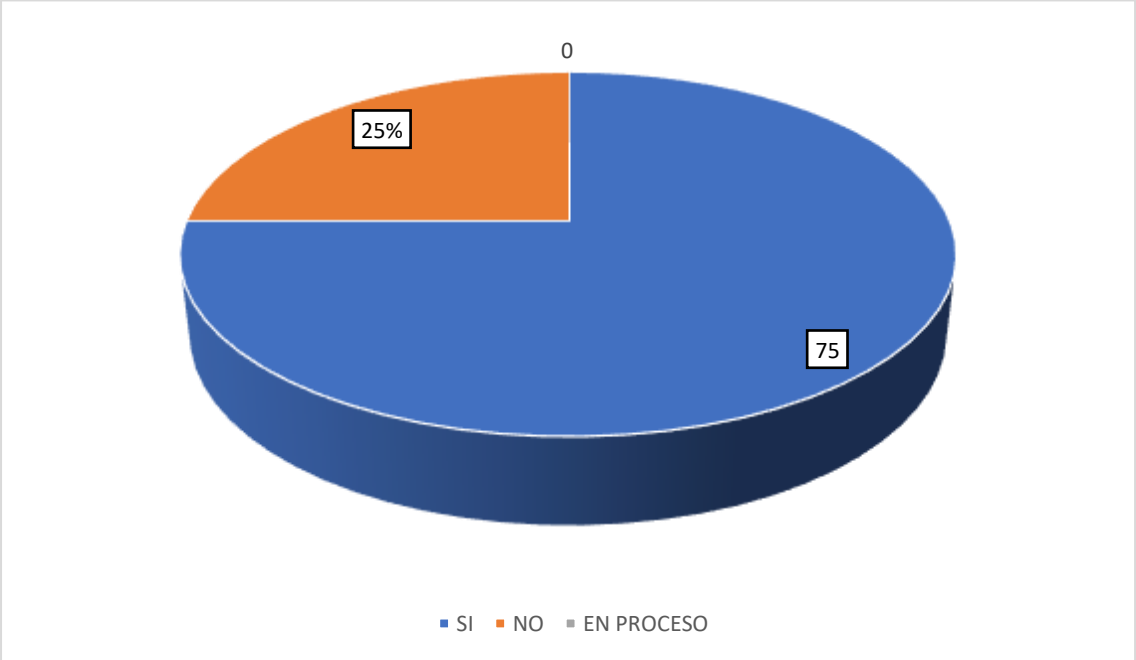
Gráfico 5 DOMINIO: Operación. Fuente: Autoría Propia.



El GAD El Tambo ha demostrado un cumplimiento parcial con un 50% de los ítems cubiertos, que incluyen la auditoría y monitoreo de controles de seguridad, así como la existencia de procedimientos documentados para la gestión de incidentes. Sin embargo, el 50% restante de los ítems no ha sido implementado, lo que incluye la implementación de controles efectivos en las operaciones diarias y la realización de pruebas de penetración. La ausencia de estas prácticas críticas indica una brecha significativa en la seguridad operativa, sugiriendo que, aunque se han establecido procedimientos, es esencial que el GAD El Tambo avance en la implementación efectiva de controles y en la realización de pruebas regulares para fortalecer la seguridad y mitigar riesgos en sus operaciones diarias.

3.6.6. DOMINIO: Evaluación del desempeño

Gráfico 6 DOMINIO: Evaluación del desempeño. Fuente: Autoría Propia.

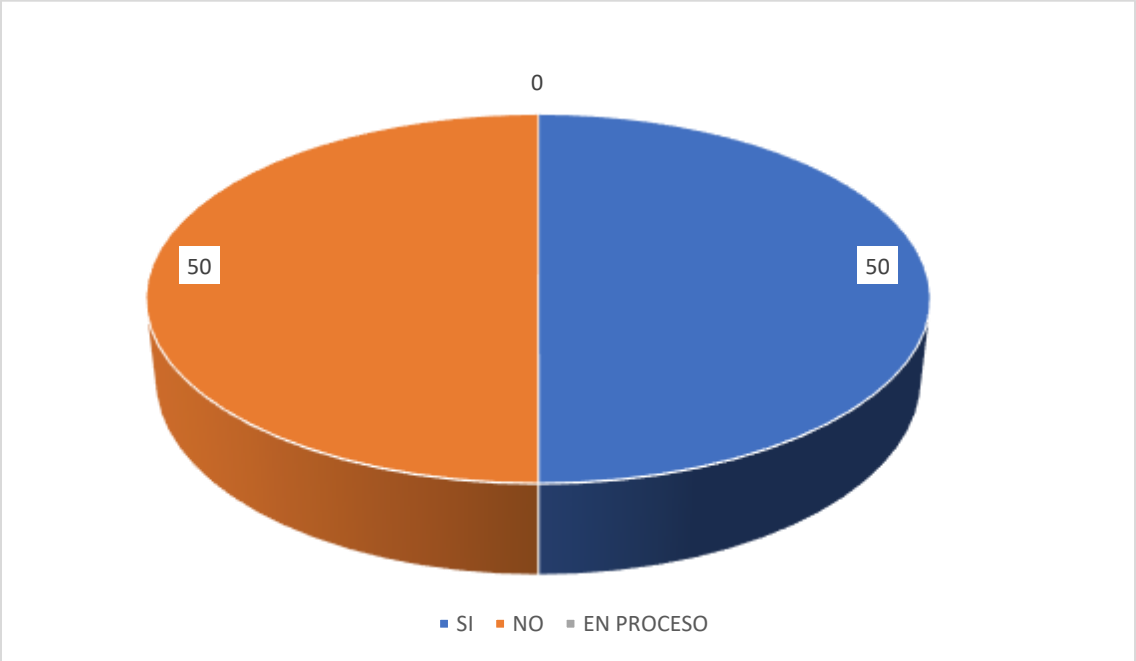


En el dominio Evaluación del Desempeño, el GAD El Tambo demuestra un sólido cumplimiento en la mayoría de las áreas evaluadas. Con un 75% de los ítems cumpliendo los requisitos, la organización realiza auditorías internas periódicas, utiliza indicadores clave de desempeño para medir la eficacia de los controles y aplica acciones correctivas basadas en los resultados de las auditorías. Estos aspectos reflejan un enfoque proactivo y estructurado para la evaluación del desempeño del Sistema de Gestión de Seguridad de la Información (SGSI). Sin embargo, el 25% de los ítems que no se cumplen está relacionado con la realización de revisiones post-incidente después de incidentes significativos. Este déficit sugiere que, aunque el GAD El Tambo cuenta con mecanismos de evaluación del desempeño robustos, existe una oportunidad significativa para mejorar la gestión post-incidente. Implementar revisiones sistemáticas después de incidentes

ayudará a identificar lecciones aprendidas y ajustar los controles y procedimientos para evitar futuros problemas, contribuyendo así a una mejora continua más efectiva en la seguridad de la información.

3.6.7. DOMINIO: Mejora Continua

Grafico 7 DOMINIO: Mejora Continua. Fuente: Autoría Propia.



El GAD El Tambo presenta un panorama mixto. Con un 50% de los ítems en cumplimiento, la organización está activamente involucrada en la revisión y actualización de procedimientos de seguridad, así como en el fomento de una cultura organizacional que promueve la conciencia sobre seguridad de la información. Estos aspectos son indicativos de un esfuerzo en curso para mantener y mejorar los estándares de seguridad. Sin embargo, el 50% de los ítems que no se cumplen indica áreas críticas de mejora. La falta de enfoque en la mejora continua de la eficacia del Sistema de Gestión de Seguridad de la Información (SGSI) y en la realización de evaluaciones periódicas de la satisfacción de los usuarios sugiere que el GAD El Tambo necesita adoptar un enfoque más proactivo.

Integrar una estrategia sistemática para la evaluación continua del SGSI y de la satisfacción del personal no solo fortalecerá el sistema de seguridad, sino que también contribuirá a una adaptación más efectiva a los cambios y desafíos en el entorno de seguridad. Esto ayudará a garantizar que el SGSI siga siendo relevante y eficaz en la protección de los activos de información.

3.7. **Análisis General de la encuesta.**

La seguridad de la información en el GAD El Tambo presenta tanto aspectos positivos como áreas que requieren atención. Se han logrado avances en aspectos como la identificación de las partes interesadas y la asignación de roles específicos para la gestión de la seguridad. Sin embargo, persisten desafíos significativos, como la necesidad de una mayor claridad en la definición del alcance del Sistema de Gestión de Seguridad de la Información (SGSI), la falta de recursos suficientes para su adecuada implementación, y la carencia de un enfoque sistemático en la evaluación y mitigación de riesgos. Asimismo, la implementación de controles de seguridad no es completamente efectiva en las operaciones diarias, y la falta de revisiones post-incidente limita la capacidad de mejorar continuamente el sistema.

Aunque el GAD El Tambo ha demostrado un compromiso inicial con la seguridad de la información, es crucial abordar las deficiencias identificadas. Esto incluye clarificar el alcance del SGSI, asegurar la realización de evaluaciones y auditorías regulares, proporcionar los recursos necesarios, y reforzar los controles de seguridad en todas las áreas operativas. Al centrarse en estas mejoras, el GAD El Tambo podrá fortalecer su sistema de seguridad de la información y proteger más eficazmente sus activos y datos críticos.

CAPITULO IV

PROPUESTA

4.1 Organigrama Institucional del GADMIC El Tambo

El organigrama presentado ilustra la estructura organizativa del Gobierno Autónomo Descentralizado (GAD) Municipal de El Tambo, detallando las diferentes dependencias, áreas y funciones que componen la entidad. En la parte superior se encuentra el Concejo Municipal y la Alcaldía, que son los órganos máximos de decisión y dirección dentro del GAD. Directamente subordinados a la Alcaldía están la Procuraduría y la Auditoría Interna, que juegan roles cruciales en la supervisión legal y la transparencia.

Las principales áreas operativas están divididas en varias direcciones clave, como el área Administrativa, Financiera, Secretaría General, Fiscalización General, y Comisaría Municipal y Seguridad Ciudadana. Cada una de estas áreas abarca diferentes departamentos específicos, como Talento Humano, Tesorería, Informática, Obras y Servicios Públicos, entre otros, que se encargan de gestionar y ejecutar las políticas y proyectos municipales.

Adicionalmente, el organigrama muestra las comisiones y consejos de participación, la Mancomunidad, y las empresas públicas asociadas, que interactúan y colaboran en la planificación y ejecución de los proyectos del GAD. Este organigrama refleja una estructura compleja y multidisciplinaria que permite al GAD El Tambo cumplir con sus funciones administrativas, financieras, sociales y de desarrollo comunitario de manera eficiente.

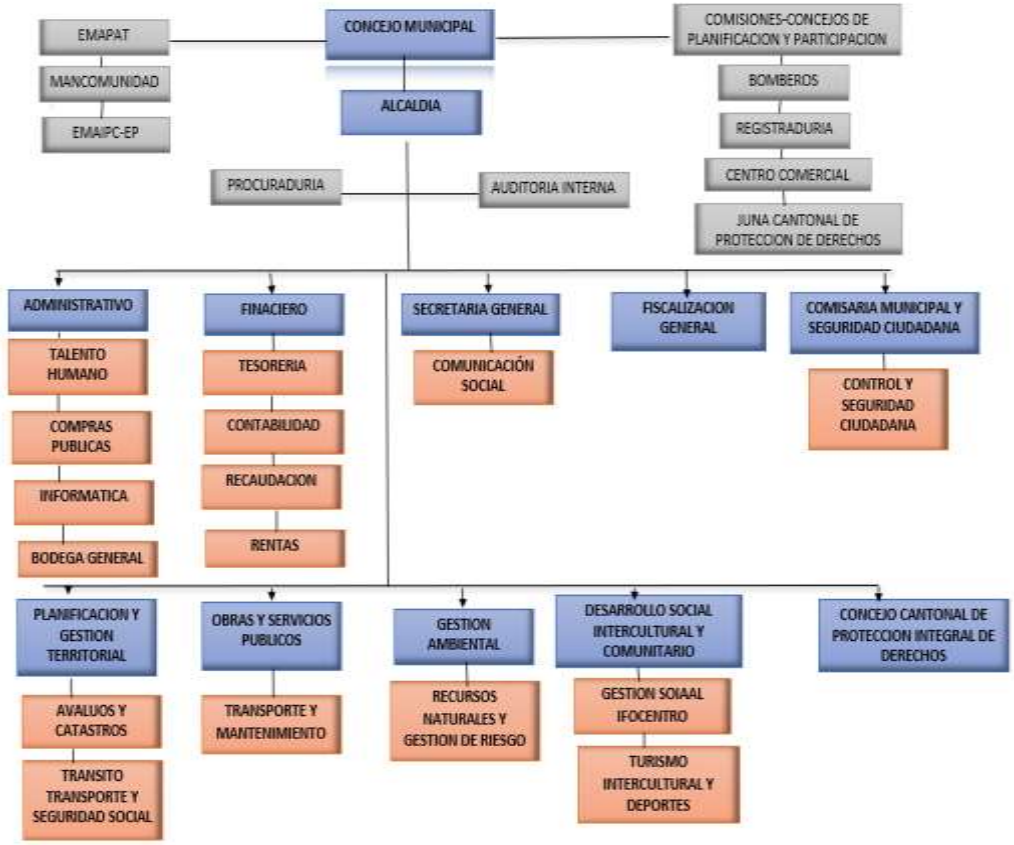


Ilustración 1 Estructura Organizacional

4.1.1 Objetivos Estratégicos

Cada unidad tiene un objetivo específico que contribuye al logro de los objetivos estratégicos del GAD, desde la elaboración y ejecución de políticas públicas hasta la gestión de recursos financieros y humanos.

El Concejo Cantonal se enfoca en ejercer la facultad legislativa cantonal, estableciendo ordenanzas y resoluciones que determinan la dirección política y las metas de la entidad municipal. La Unidad de Comunicación Social está encargada de diseñar y ejecutar estrategias de comunicación para fortalecer la imagen institucional y fomentar la participación ciudadana.

La Procuraduría Síndica juega un papel crucial en la asesoría legal y jurídica para garantizar la seguridad jurídica en los procesos institucionales. La Dirección Administrativa y la Dirección Financiera son responsables de brindar soporte logístico,

manejar recursos financieros y asegurar la eficiencia operativa de la municipalidad. Por último, la Unidad de Talento Humano se dedica al desarrollo profesional y personal de los servidores municipales, asegurando que cuenten con las capacidades necesarias para cumplir con sus funciones de manera efectiva.

UNIDAD	OBJETIVO
Concejo Cantonal	Ejercer la facultad legislativa cantonal a través de ordenanzas, dictar acuerdo resoluciones, de conformidad con sus competencias; determinar la política a seguirse y fijar las metas de la entidad Municipal.
Comunicación Social	Diseñar y ejecutar estrategias de comunicación que permitan de manera oportuna y veraz la gestión de la Municipalidad. Fortalecimiento la imagen institucional con la participación ciudadana
Procuraduría Sindica	Asesorar en los procesos institucionales a nivel Municipal, en materia Legal y Jurídica orientados a garantizar la seguridad Jurídica
Dirección Administrativa	Brindar con eficiencia y eficacia productos y servicios apoyo logístico, la entrega oportuna de materiales demandados, por diferentes unidades y procesos.
Dirección Financiera	Administrar y controlar los recursos financieros para apoyar la Dirección Institucional de conformidad a la normativa vigente y proveer información para la toma oportuna de decisiones.
Unidad de Talento Humano	Proponer el desarrollo profesional. Técnico, y personal de las y los servidores del Gad Municipal, mediante una adecuada selección y valoración, así como capacitación que permita lograr servicios con eficiencia.
Unidad de Tecnologías de Información	Laborar e implementar el Plan integral de Sistemas Informáticos y de Comunicación, brindando el soporte técnico y de mantenimiento necesario para un adecuado funcionamiento tecnológico.
Secretaria del Concejo	Certificar los actos administrativos y normativos expedidos por la institución; administrar custodiar y salvaguardar la

	documentación interna y externa, prestar atención eficiente a usuarios.

Tabla 3 Objetivos Estratégicos Institucionales Fuente: (GADMIET, s.f.)

4.2 **Departamento de TI**

El Departamento de Tecnologías de la Información y Comunicación (TIC) del GAD Intercultural El Tambo juega un rol crucial en la administración y gestión de los recursos tecnológicos de la entidad. Este departamento es responsable de garantizar la integridad, disponibilidad, y confidencialidad de la información manejada por el GAD, alineando sus actividades con las estrategias institucionales para cumplir con los objetivos organizacionales.

Entre sus principales funciones se encuentran la gestión de la infraestructura tecnológica, la administración de redes y sistemas informáticos, la implementación de políticas de seguridad de la información, y el soporte técnico a los demás departamentos del GAD. El departamento de TIC también tiene la responsabilidad de realizar un seguimiento continuo de la seguridad de la información, gestionar las vulnerabilidades técnicas, y asegurar que los sistemas de información estén protegidos contra amenazas internas y externas.

Además, el departamento de TIC debe promover la capacitación del personal en temas de seguridad de la información, asegurando que todos los funcionarios del GAD estén conscientes de las políticas de seguridad y las apliquen en sus actividades diarias. Este enfoque integral permite al departamento de TIC no solo mantener la operatividad tecnológica de la institución, sino también proteger sus activos de información frente a posibles riesgos y amenazas.

4.2.1 Estructura Organizativa

Este diseño organizativo resalta cómo el departamento de Informática está integrado dentro de la estructura administrativa, asegurando que las decisiones y políticas estratégicas fluyan desde los niveles más altos de gobierno municipal hasta la gestión de la tecnología y sistemas de información. La alineación directa de Informática bajo la dirección Administrativa subraya la importancia de la tecnología en la ejecución de las funciones administrativas y en el soporte de los servicios públicos que dependen de una infraestructura tecnológica robusta y eficiente.

Ilustración 2 Organigrama de TI: Fuente Autor Propio

4.2.2 Roles y Responsabilidades

Las responsabilidades están orientadas hacia la gestión eficaz de la tecnología y la protección de la información, lo que incluye desde el mantenimiento de la infraestructura tecnológica hasta la implementación de políticas de seguridad robustas. El objetivo es garantizar que todos los sistemas del GAD funcionen de manera eficiente y que la información esté protegida contra amenazas internas y externas.

Esta estructura organizativa permite al Departamento de TI del GAD Intercultural El Tambo no solo soportar las operaciones diarias del municipio, sino también implementar mejoras continuas en sus sistemas tecnológicos, alineando sus actividades con las metas estratégicas de la organización.

4.2.3 Identificación de Activos Críticos

En el contexto del Departamento de Tecnologías de la Información (TI) del GAD Intercultural El Tambo, los activos críticos son aquellos componentes tecnológicos fundamentales para el funcionamiento continuo y eficiente de las operaciones municipales.

Estos activos de TI son esenciales para garantizar la prestación de servicios públicos, la gestión administrativa y financiera, y la seguridad de la información manejada por el GAD.

TIPO DE ACTIVO	CODIGO	DESCRIPCIÓN
PERSONAL	A1	Analista informativo
SOFTWARE	A2	Licencia Windows 7 Pro. 32 bitt
	A3	Licencia de Checkpoint
	A4	SINAT - Sistema Nacional de Administracion

	A5	Caja Unica
HARDWARE	A6	CPU NEGRO, serie MXL1411J6Z
	A7	Lector biométrico
	A8	Equipo de Cómputo CPU INTEL CELERON 4 GB-1TB-2.0 GHZ QC PASS
	A9	Servidor HP con dos tarjetas de red SERVER HP, DL360E-Gen 8
	A10	Servidor, Intel XEON E5-2609, 1.9 MHZ, 32MB memoria, disco de 300 GB
	A11	Disco Duro externo Toshiba
	A12	intel XEON E5-2609

Tabla 4 Identificación de Activos Fuente: Autor propio

4.2.3.1 **Infraestructura de Redes**

Incluye la red interna de comunicaciones, routers, switches, puntos de acceso, y los sistemas de cableado que interconectan los diferentes departamentos del GAD. Esta infraestructura es crucial para asegurar la conectividad continua y segura entre todos los sistemas y usuarios dentro de la organización.

4.2.3.2 Servidores y Sistemas de Almacenamiento

Comprende los sistemas y procedimientos implementados para realizar copias de seguridad de los datos y garantizar la recuperación de la información en caso de desastres o fallos críticos. Estos sistemas son vitales para mantener la continuidad operativa en situaciones adversas.

4.2.3.3 Equipos de Usuario Final (Workstations)

En Incluye las computadoras de escritorio, laptops, y otros dispositivos utilizados por el personal del GAD para llevar a cabo tareas diarias. Estos equipos son la primera línea de interacción con los sistemas de TI y deben estar protegidos con medidas de seguridad adecuadas.

4.2.3.4 Bases de Datos

Las bases de datos alojan información crítica relacionada con ciudadanos, propiedades, finanzas, y otros datos esenciales para la operación del GAD. Estas bases de datos son un activo de TI altamente sensible y deben estar protegidas contra cualquier tipo de amenaza que pueda comprometer su integridad, confidencialidad o disponibilidad.

4.2.3.5 Sistemas de Respaldo y Recuperación

Comprende los sistemas y procedimientos implementados para realizar copias de seguridad de los datos y garantizar la recuperación de la información en caso de desastres o fallos críticos. Estos sistemas son vitales para mantener la continuidad operativa en situaciones adversas.

4.2.4 Situación Actual de la Seguridad de la Información

La seguridad de la información en el Departamento de TI enfrenta desafíos significativos debido a la falta de personal capacitado y recursos dedicados. Aunque existen medidas básicas de seguridad como controles de acceso y respaldos de

información, se han identificado áreas críticas que requieren mejoras, como la actualización de licencias de software, implementación de planes de contingencia y fortalecimiento de políticas de seguridad.

El análisis revela que, aunque se cuenta con algunas medidas preventivas, la infraestructura tecnológica es vulnerable a ataques cibernéticos, desastres naturales y fallas en la gestión operativa, lo que podría comprometer la confidencialidad, integridad y disponibilidad de la información.

4.2.5 **Análisis de Riesgos**

En esta sección, se identifican y valoran los riesgos asociados, determinando su probabilidad de ocurrencia y el impacto que podrían tener en la operación del GAD El Tambo. Este análisis permite priorizar las amenazas y establecer estrategias de mitigación efectivas para proteger la integridad, confidencialidad y disponibilidad de los activos de información.

4.2.5.1 **Valoración de la probabilidad**

La probabilidad se refiere a la posibilidad de que ocurra un evento no deseado relacionado con la seguridad de la información.

A continuación, se presenta un gráfico que muestra el rango de evaluación de la probabilidad.

Este rango clasifica los riesgos en tres categorías: bajo, medio y alto, cada una definida por un intervalo de valores. Este enfoque permite una evaluación clara y estructurada de los riesgos, facilitando la identificación de aquellos activos que requieren atención prioritaria para la implementación de medidas de mitigación adecuadas.

Rango para establecer el nivel de Riesgo		
Valor Inferior	Valor Superior	Grado de riesgo
1	4	Bajo
5	7	Medio
8	11	Alto

Tabla 5 Rango para el Nivel de Riesgo Fuente Autor Propio

En función de los niveles de valoración del activo y el riesgo, se elabora una matriz de riesgo en la que se identifican todos los activos que serán objeto de análisis, así como las posibles amenazas a las que podrían estar expuestos. En la siguiente tabla se muestra los cálculos realizados, se ha determinado que existen activos críticos que requieren protección a través de un tratamiento adecuado y la implementación de controles de seguridad.

4.2.5.2 **Valoración para los activos**

Esta valoración se realiza evaluando cómo la confidencialidad, integridad y disponibilidad de cada activo pueden verse afectadas en diferentes niveles de riesgo, desde muy bajo hasta alto.

Al comprender el impacto potencial de estas amenazas, la organización puede implementar medidas de seguridad adecuadas para proteger sus activos más valiosos y garantizar la continuidad operativa.

NIVEL	VALOR	Confidencialidad	Integridad	Disponibilidad
Muy Bajo	1	No se produce ningún efecto negativo	No se produce ningún efecto negativo	No se produce ningún efecto negativo

Bajo	2	Genera un impacto negativo leve	Genera un impacto negativo leve	Genera un impacto negativo leve
Medio	3	Genera un impacto negativo moderado	Genera un impacto negativo moderado	Genera un impacto negativo moderado
Alto	4	Genera un impacto negativo significativo para la entidad	Genera un impacto negativo significativo para la entidad	Genera un impacto negativo significativo para la entidad

Tabla 6 Valoración para los activos Fuente: Autor Propi

	MATRIZ DE ANALISIS DE RIESGOS					PROBABILIDAD DE AMENAZA							
TIPO DE ACTIVO	**Activos**	Confidencialidad	Integridad	Disponibilidad	Magnitud de Daño	Compromiso de las Funciones	Compromiso de la Información	Acciones no Autorizadas	Daño Físico	Eventos Naturales	Fallos Técnicos	Pérdida de Servicios Esenciales	Fallos no Intencionado
PERONAL	Analista Informatico	2	2	2	Medio	2	4	2	4	3	3	4	2
SOFTWARE	Licencia windows 7 Pro. 32 bits	2	2	2	Bajo	2	4	2	4	3	3	4	2
	Licencia windows 7 Pro. 32 bits	2	4	4	Alto	6	8	4	6	4	4	5	4
	Licencia de Checkpoint	3	2	2	Medio	5	8	3	5	3	3	5	3
	SINAT - Sistema Nacional de Administracion	3	3	3	Bajo	1	2	2	3	2	2	3	2
	Caja Unica	1	1	1	Bajo	2	2	2	3	2	2	3	2
	CPU NEGRO, serie MXL1411J6Z	2	4	2	Medio	3	4	3	4	3	3	4	3

HARDWARE	Lector biométrico	4	3	2	Medio	4	5	4	5	4	3	4	3	
	Equipo de Computo CPU INTEL CELERON 4 GB 1TB-2.0 GHZ QC PASS	3	2	4	Medio	3	6	5	5	4	3	4	4	
	Servidor HP con dos tarjetas de red	4	3	3	Medio	3	5	4	6	3	3	4	4	
	Servidor, intel XEON E5-2609	4	3	2	Medio	2	2	2	3	2	2	3	2	
	Disco Duro externo Toshiba	2	3	2	Medio	3	4	3	4	3	3	4	3	
	Servidor doble núcleo core 2 DUO 2.93 GHZ	4	4	4	Alto	8	6	5	8	7	8	9	7	

Tabla 7 Matriz de riesgo Fuente: Autor Propio

4.3 **Desarrollo del Manual de Políticas de Seguridad de la información**

El Departamento de Tecnologías de la Información y Comunicación (TIC) del GAD Intercultural desempeña un papel crucial en la protección y gestión de los activos de información de la institución. Con el objetivo de fortalecer la seguridad de la información y garantizar el cumplimiento de las normativas internacionales, se ha desarrollado un Manual de Políticas de Seguridad de la Información. Este manual proporciona directrices claras y procedimientos específicos para gestionar los riesgos y salvaguardar la integridad, confidencialidad y disponibilidad de la información en el entorno del GAD Intercultural. A continuación, se detallan los pasos seguidos en el proceso de desarrollo y las principales políticas establecidas en el manual.

4.3.1 **Cumplimiento y Responsabilidad**

Considerando que este manual es únicamente una propuesta para el GAD El Tambo establecen ciertas responsabilidades en caso de que se decida implementarlo.

- **Alta Gerencia**: La alta dirección del GADMICET será la encargada de respaldar el proceso de implementación de las políticas de seguridad de la información.
- **Departamento de TIC:** El jefe del departamento de TIC será responsable de monitorear la implementación de las políticas, supervisar al personal bajo su mando para asegurar su cumplimiento y proporcionar el apoyo necesario.
- **Compromiso de Divulgación:** El departamento de TIC se comprometerá a divulgar este manual de políticas a todos los empleados de la institución.
- **Verificación Periódica:** El departamento de TIC deberá realizar verificaciones periódicas para asegurar que las políticas de seguridad de la información se estén cumpliendo correctamente.

- **Revisión y Actualización:** Además, el departamento de TIC tendrá la responsabilidad de revisar este manual regularmente para realizar actualizaciones o mejoras cuando sea necesario.

4.3.2 Políticas de Seguridad

4.3.2.1 Directrices para la gestión de la seguridad de la información

La alta dirección del GADMICET tiene la responsabilidad de liderar y apoyar activamente las iniciativas de seguridad de la información. Esto implica asegurar que todos los esfuerzos en materia de seguridad estén alineados con los objetivos estratégicos de la organización y que se cumplan estrictamente todas las leyes y regulaciones vigentes.

Además, la alta dirección debe promover una cultura organizacional que valore y respalde la protección de la información, garantizando que los recursos necesarios, tanto financieros como humanos, estén disponibles para implementar y mantener un entorno seguro.

- **Conjunto de políticas para la seguridad de la información**

Las políticas de seguridad de la información deben ser desarrolladas teniendo en cuenta las necesidades y riesgos específicos identificados a través del análisis de riesgos realizado en la institución. Estas políticas deben abordar todos los aspectos críticos de la seguridad, incluyendo la protección de datos, el acceso a la información y la continuidad operativa. Una vez elaboradas, es esencial que las políticas sean formalmente aprobadas por la alta dirección del GAD El Tambo y luego comunicadas de manera efectiva a todo el personal involucrado,

tanto dentro de la institución como a los contratistas y colaboradores externo.

- **Revisión de las políticas para la seguridad de la información**

La revisión de las políticas de seguridad de la información es un proceso continuo y crítico, este control se implementa para asegurar que las políticas estén no solo definidas e implementadas correctamente, sino también que se mantengan actualizadas frente a los cambios en el entorno tecnológico, regulatorio y de amenazas. Es responsabilidad del departamento de TIC llevar a cabo revisiones periódicas de estas políticas, evaluando su eficacia y relevancia. Las revisiones deben ser documentadas y cualquier cambio o actualización debe ser comunicado oportunamente a todo el personal afectado.

4.3.3 Aspectos Organizativos de la Seguridad de la Información

4.3.3.1 Organización Interna

- El municipio debe diseñar un marco de seguridad de la información que defina claramente los roles y responsabilidades esenciales para una gestión eficaz de la seguridad de la información. Este diseño debe asegurar que cada área tenga un entendimiento claro de sus obligaciones para proteger los activos de información.
- El departamento informático debe establecer y mantener relaciones con organizaciones externas especializadas en seguridad de la información. Estas relaciones son vitales para intercambiar

conocimientos, mejores prácticas y recibir apoyo en la gestión de riesgos que puedan surgir.

- En la implementación de nuevos proyectos dentro de la institución, es imprescindible que se incorpore una gestión de riesgos integral. Esto permite identificar y evaluar los riesgos desde el inicio del proyecto y establecer planes de acción adecuados para su mitigación.
- **Asignación de Responsabilidades para la Seguridad de la Información**

Cada recurso de información debe tener un responsable asignado que se encargue de garantizar su seguridad. Los responsables, también denominados "propietarios de la información", tienen la autoridad exclusiva para garantizar que la información gestionada dentro de la institución esté resguardada conforme a las políticas vigentes.

- **Contactos con las Autoridades**

Los responsables de la seguridad de la información deben mantener una comunicación constante con las autoridades especializadas en esta área. Estas relaciones son esenciales para recibir apoyo y orientación en la resolución de cualquier incidente relacionado con la seguridad de la información que pueda surgir en la institución.

- **Seguridad de la Información en la Gestión de Proyectos**

En la gestión de nuevos proyectos dentro del GAD El Tambo, es fundamental involucrar al área de seguridad de la información desde las primeras etapas. Esto permitirá analizar y evaluar los riesgos inherentes a cada proyecto,

convirtiendo la seguridad de la información en un componente esencial para la ejecución exitosa del mismo.

- **Teletrabajo**

El departamento de TIC debe asegurar que las conexiones utilizadas para el teletrabajo sean seguras. Esto implica que toda la información manejada remotamente esté protegida, utilizando los softwares necesarios para defenderla contra posibles ataques y garantizar la integridad y confidencialidad de los datos durante el trabajo a distancia.

4.3.4 Seguridad Ligada a los Recursos Humanos

4.3.4.1 Antes de la Contratación

- **Investigación de antecedentes**

Antes de que un candidato sea contratado para un puesto en el municipio, deberá someterse a un riguroso proceso de verificación de antecedentes. Este proceso incluirá la revisión de su historial laboral, referencias, antecedentes penales y cualquier otro registro relevante, con el fin de garantizar que el candidato cumple con los estándares éticos y profesionales requeridos por el municipio. Además, la verificación deberá realizarse en cumplimiento con todas las leyes y regulaciones aplicables, asegurando que el proceso sea justo, transparente y respetuoso de los derechos de los candidatos

- **Términos y Condiciones de contratación**

Este contrato informará a los nuevos empleados sobre la existencia de las políticas de seguridad contenidas en el presente Manual y les especificará las responsabilidades que se les asignan en relación con la protección de la

información. Además, se garantizará que el contrato, junto con todos los documentos relacionados con la contratación, esté debidamente archivado como parte de los registros oficiales de la institución

4.3.4.2 Durante la contratación

- **Responsabilidades de gestión**

El departamento de TI tiene la responsabilidad de educar a todo el personal del municipio sobre la importancia de la seguridad de la información. Esta educación debe incluir la concientización sobre las responsabilidades de seguridad que cada empleado debe asumir desde su ingreso hasta su salida de la institución, asegurando el cumplimiento continuo de las políticas, normas y estándares establecidos. Además, es fundamental que el departamento de TIC fomente una cultura de seguridad en la que cada miembro del personal entienda y valore su papel en la protección de los activos de información de la institución.

- **Concienciación, educación y capacitación en seguridad de la información**
- La alta dirección, junto con el departamento de TIC, debe organizar programas de capacitación y sesiones de concienciación relacionadas con la seguridad de la información. Estas actividades deberán llevarse a cabo al menos una vez al año y repetirse con mayor frecuencia si se introducen actualizaciones en las políticas o procedimientos de seguridad. Además, es fundamental que todos los empleados que manejan información como parte de sus funciones en la institución participen en estas capacitaciones y sigan las directrices establecidas en este manual

4.3.4.3 Cambio de puesto de trabajo

- **Investigación de antecedentes**

Es fundamental que cada empleado esté debidamente informado sobre las responsabilidades que debe asumir en caso de un cambio de puesto o al finalizar su relación laboral con el GAD El Tambo. Estas responsabilidades incluyen la correcta entrega de los activos de información, el acceso a sistemas, y cualquier otro recurso que haya manejado durante su empleo. Además, es obligación del líder o jefe de departamento notificar inmediatamente al departamento de Recursos Humanos sobre cualquier cambio en el puesto o la salida de un empleado.

Esta notificación debe incluir todos los detalles relevantes para que se puedan tomar las decisiones adecuadas y garantizar que se sigan los procedimientos establecidos para la protección de la información.

4.3.5 **Gestión de Activos**

4.3.5.1 **Responsabilidad sobre los activos**

Es esencial identificar y catalogar todos los activos, tanto del departamento de TIC como de la institución en su conjunto; cada activo debe ser asignado a un miembro del personal responsable, quien será encargado de su protección y gestión. Estos deben ser cuidadosamente documentados, inventariados, y clasificados según su importancia y el nivel de seguridad requerido, es crucial mantener un registro actualizado de estos activos, asegurando que se gestionen de manera eficiente y se protejan contra cualquier amenaza o riesgo que pueda comprometer su integridad o disponibilidad.

- **Inventario de Activos**

Este inventario debe incluir todos los activos relevantes, asegurando que cada uno esté debidamente documentado; el encargado de estos activos debe clasificarlos según criterios como su valor, el riesgo asociado a su pérdida, o los requisitos legales que puedan aplicarse.

Esta clasificación es esencial para priorizar la protección de los activos más críticos y garantizar que se gestionen de acuerdo con las políticas de seguridad de la institución.

- **Propiedad de los activos**

El área de TI llevará a cabo la inspección correspondiente del inventario de activos de información, lo que incluye realizar actualizaciones necesarias y asignar claramente las responsabilidades sobre cada activo. Es fundamental que todos los activos de información sean utilizados por la institución en alineación con las políticas establecidas en este manual y con las normativas internas vigentes, asegurando así que se minimicen los riesgos y se eviten impactos negativos en dichos activos.

- **Devolución de los activos**

Al finalizar o dejar su puesto, cada funcionario tiene la obligación de devolver todos los activos de información que le fueron entregados al asumir su cargo y se procederá a la firma de un acta de entrega por ambas partes involucradas, garantizando así la formalidad y el cumplimiento de este proceso. Este procedimiento asegura que los activos retornados se encuentren en buen estado y que se complete la transferencia de responsabilidad de manera adecuada.

4.3.5.2 Clasificación de la Información

La entidad establecerá los niveles adecuados para clasificar su información, considerando la importancia de cada activo. El departamento de TIC se encargará de definir y aplicar los controles necesarios para proteger esta información, asegurando que se mantenga la confidencialidad, integridad y disponibilidad de todos los activos clasificados

- **Directrices de clasificación**

Para garantizar una clasificación adecuada de la información, se han establecido las siguientes categorías prioritarias:

Pública: Información que puede ser compartida libremente con todos los usuarios tanto dentro como fuera de la municipalidad, sin restricciones de acceso.

Uso Interno: Información destinada exclusivamente para uso institucional, accesible únicamente a los empleados de la municipalidad, y no debe ser divulgada fuera de la organización.

Confidencial: Información altamente sensible, restringida solo a departamentos específicos que tienen un interés directo y justificado en su acceso, con medidas de seguridad adicionales para protegerla de accesos no autorizados

- **Manipulación de Activos**

Cada activo de información clasificada debe incluir los siguientes detalles: el nombre del activo, el proceso en el que está involucrado, y su nivel de sensibilidad. En caso de que un activo esté clasificado en diferentes niveles, el jefe del departamento de TIC tendrá la autoridad para determinar y unificar su

clasificación de manera coherente, asegurando que se aplique el nivel de protección adecuado.

4.3.6 Control de Acceso

4.3.6.1 Responsabilidad sobre los activos

El departamento informático debe implementar medidas estrictas para restringir el acceso de terceras personas a las instalaciones donde se procesan y almacenan datos e información crítica. Este control es esencial para proteger los sistemas y la información de accesos no autorizados, garantizando que solo el personal autorizado tenga acceso a áreas sensibles.

- **Políticas de control de acceso**

La municipalidad se compromete a asegurar la implementación y el mantenimiento adecuado de los mecanismos de seguridad física que incluyen controles rigurosos para el acceso físico y la gestión de las condiciones ambientales necesarias para el funcionamiento óptimo de las plataformas tecnológicas, esto permitirá mitigar las amenazas físicas y prevenir accesos no autorizados.

Se establecerán medidas específicas para garantizar que solo el personal autorizado pueda ingresar a áreas sensibles y que los sistemas tecnológicos operen en un entorno seguro, minimizando los riesgos asociados a factores externos y vulnerabilidades de seguridad.

- **Control de acceso a las redes y servicios asociados**

Estos mecanismos deben ser diseñados para garantizar que solo los usuarios debidamente autorizados puedan conectarse a la red, salvaguardando así la integridad y seguridad de los datos y servicios asociados. Además, cualquier usuario externo o funcionario de la institución que desee conectar sus dispositivos personales a la red de la entidad deberá cumplir con todos los requisitos de autenticación establecidos para asegurar un acceso seguro. Se deben establecer procedimientos claros para la evaluación y autorización de estos dispositivos, asegurando que no representen un riesgo para la seguridad de la red institucional.

4.3.6.2 Gestión de acceso de usuarios

- **Gestión de altas y bajas en el registro de usuarios**

El departamento informático debe implementar procedimientos claros para asegurar la revocación o bloqueo inmediato de los privilegios de acceso a los sistemas y servicios de información cuando un usuario ya no requiere dichos accesos. Esto incluye la desactivación o eliminación de cuentas de usuario asignadas a recursos tecnológicos, garantizando que no permanezcan accesibles a personas no autorizado.

- **Gestión de los derechos de acceso con privilegios especiales.**

Los usuarios con acceso a servicios tecnológicos con privilegios especiales tienen la responsabilidad de utilizar estos servicios de manera segura y adecuada; es su deber proteger la información a la que tienen acceso autorizado, asegurando que las credenciales y claves de acceso se mantengan confidenciales y no se compartan bajo ninguna circunstancia.

Además, deben seguir todas las políticas de seguridad establecidas por la institución, incluyendo el uso de medidas adicionales de protección cuando manejen datos sensibles.

4.3.6.3 Gestión Responsabilidades del usuario

- **Uso de información confidencial para la autenticación**

Cada usuario que tenga autorización para acceder a los recursos tecnológicos de la institución es responsable de todas las actividades que realice en dichos recursos, por lo tanto, es esencial que la identificación de cada usuario se establezca de manera única y segura para garantizar la integridad de las operaciones y la protección de los sistemas tecnológicos de la organización.

4.3.6.4 Control de acceso a sistemas y aplicaciones

- **Restricción del acceso a la información**

Los usuarios que trabaje dentro de la institución, así como cualquier tercera persona a la que se le haya otorgado credenciales para acceder a los servicios de red, tiene la responsabilidad de utilizar estos recursos de manera adecuada y conforme a las políticas de seguridad establecidas

Es crucial que el acceso a la infraestructura tecnológica del GAD El Tambo esté estrictamente controlado, y que cada persona que ingrese a las instalaciones, especialmente aquellas con acceso a sistemas críticos, posea un identificador único y personalizado para garantizar la trazabilidad y seguridad de todas las actividades realizadas en los sistemas de la organización.

- **Procedimientos seguros de inicio de sesión**

El departamento informático debe establecer e implementar mecanismos robustos que protejan los servicios tecnológicos contra intentos de inicio de sesión no autorizados, incluidos ataques de fuerza bruta.

Estos mecanismos deben incluir restricciones sobre la cantidad de intentos fallidos permitidos y, tras alcanzar este límite, el sistema debe desplegar un mensaje de advertencia que informe al usuario que no tiene los permisos necesarios para acceder a los servicios solicitados, también se recomienda que estos sistemas incluyan medidas adicionales, como el bloqueo temporal de cuentas o la notificación al administrador de seguridad, para fortalecer la protección contra accesos no autorizados y mejorar la seguridad general de la infraestructura tecnológica.

- **Gestión de contraseñas de usuario**

Al crear una contraseña, es fundamental que esta cumpla con ciertos requisitos que aseguren un nivel adecuado de complejidad. Las contraseñas deben estar compuestas por un mínimo de 8 a 10 caracteres alfanuméricos y evitar el uso de palabras relacionadas con información personal.

Se recomienda que los usuarios cambien regularmente sus contraseñas de acceso a la red y a otros sistemas de información para reducir el riesgo de compromisos de seguridad.

También el departamento de TIC debe implementar controles que aseguren el bloqueo automático del acceso a la red después de tres intentos fallidos de ingreso de la contraseña, reforzando así la seguridad de los sistemas y previniendo accesos no autorizados.

4.3.7 Seguridad Física y Ambiental

4.3.7.1 Áreas Seguras

Es fundamental que se implementen controles para gestionar tanto las amenazas internas como externas de origen físico, asegurando que las áreas críticas estén resguardadas contra cualquier posible riesgo. Estas medidas deben ser diseñadas para mantener la integridad y seguridad de las instalaciones, previniendo incidentes que puedan comprometer los recursos y la información de la organización.

- **Protección contra amenazas externas y ambientales**

La institución debe contar con sistemas robustos de control ambiental que gestionen la temperatura, humedad, y detección de incendios. Es esencial disponer de sistemas de protección contra descargas eléctricas y un monitoreo continuo mediante vigilancia y alarmas, especialmente en situaciones de fenómenos climáticos que puedan causar daños a las instalaciones.

El personal responsable de los centros de procesamiento de datos y de cableado debe asegurar que todos los componentes de la plataforma tecnológica estén protegidos contra fallas o interrupciones eléctricas.

4.3.7.2 Seguridad de los Equipos

- **Emplazamiento y protección de equipos**

Es fundamental que todos los recursos tecnológicos de la institución estén equipados con medidas de seguridad física que los protejan contra accesos no autorizados y amenazas ambientales. Estas medidas deben ser diseñadas para prevenir daños o pérdidas de activos, asegurando que los equipos tecnológicos

estén resguardados adecuadamente y operen en un entorno seguro que minimice cualquier riesgo potencia

- **Seguridad del cableado**

El departamento informático deberá disponer de un modelo detallado que represente las conexiones de cableado, lo cual permitirá una identificación clara de los elementos conectados y reducirá el riesgo de desconexiones accidentales. Es esencial asegurar que los centros de cableado estén ubicados en áreas protegidas, lejos de zonas que puedan estar en riesgo de inundaciones o incendios. Esta medida garantizará la integridad y continuidad del servicio, evitando interrupciones que puedan afectar las operaciones de la institución.

- **Mantenimiento de los equipos**

El departamento informático, junto con los técnicos autorizados, será responsable exclusivo de realizar los servicios de mantenimiento y reparación de los equipos informáticos de la entidad. Es esencial que cualquier empleado que gestione información crítica para el funcionamiento de la institución asegure la realización de un respaldo de esa información. Esto es especialmente importante en caso de que los equipos informáticos presenten fallos o deterioro, para evitar la pérdida de datos y garantizar la continuidad operativa de la entidad.

4.3.8 Seguridad en la Operativa

4.3.8.1 Protección contra códigos maliciosos

- **Controles contra el código malicioso**

Cada equipo de cómputo de la institución deberá contar con un software antivirus licenciado y actualizado, asegurando la protección integral de la información.

Es necesario que se realicen chequeos periódicos a través del software antivirus para verificar que los archivos almacenados en estos equipos estén libres de virus y protegidos contra cualquier ataque de software malicioso. En caso de que el personal del municipio sospeche la presencia de un virus en los equipos, deberá suspender inmediatamente sus actividades e informar al departamento de TIC, quien se encargará de realizar la limpieza y eliminación del virus, garantizando la seguridad y estabilidad de los sistemas informáticos.

4.3.8.2 Copias de seguridad

La entidad municipal, en colaboración con el área de TI, tiene la responsabilidad de ejecutar copias de respaldo de la información confidencial, asegurando su almacenamiento seguro.

Es fundamental establecer las operaciones y estrategias necesarias para cumplir con estas actividades de manera efectiva. El departamento de TIC debe garantizar la integridad física de estos respaldos, implementando medidas que protejan la información en caso de robo, destrucción o pérdida.

4.3.8.3 Registro de actividades y supervisión

- **Registro de gestión de eventos de actividad**

El departamento de TIC establecerá un cronograma para realizar el monitoreo regular de los registros de auditoría, asegurando que los aplicativos donde se ejecutan los procesos de la institución sean revisados de manera efectiva

y en el tiempo que se considere adecuado. Esta supervisión es esencial para detectar y abordar cualquier uso inapropiado o irregularidades en los sistemas, garantizando la seguridad y eficiencia operativa.

- **Protección de los registros de información**

  Los registros de auditoría generados en la entidad deben estar protegidos de manera rigurosa y solo podrán ser accedidos por personal autorizado. Este control es esencial para asegurar que la integridad y disponibilidad de los registros se mantengan intactas, previniendo cualquier alteración no autorizada o pérdida de datos críticos.

4.3.8.4 Control de Software en explotación

- **Instalación del software en sistemas en producción**

  El área de TI designará a un personal responsable que llevará un control exhaustivo sobre la instalación de software en los equipos informáticos de la institución; este personal será encargado de supervisar todas las instalaciones, asegurando que se cumplan los protocolos establecidos.

  Cuando se presenten nuevas versiones de software, será necesario realizar pruebas de actualización para verificar y certificar que los sistemas de información y las herramientas de software funcionen correctamente en los equipos antes de implementarlas en producción**.**

4.3.8.5 Gestión de la vulnerabilidad técnica

- **Gestión de las vulnerabilidades técnicas**

El municipio y el departamento de TI realizarán un monitoreo constante y programado de sistemas y aplicaciones para detectar vulnerabilidades. Una vez identificadas, se implementarán rápidamente estrategias de mitigación y actualizaciones necesarias para proteger los sistemas y minimizar riesgos críticos, garantizando así la seguridad del entorno tecnológico de la organización.

- **Restricción sobre la instalación de software**

Cualquier software que se pretenda instalar en los equipos informáticos de la institución deberá contar con la previa autorización del departamento de TIC. Alternativamente, se puede solicitar que el propio departamento de TIC se encargue de realizar la instalación correspondiente. Esta medida asegura que todos los programas instalados cumplan con los estándares de seguridad y compatibilidad establecidos por la institución, minimizando riesgos asociados a software no autorizado o potencialmente peligroso.

4.3.9 Seguridad en las Telecomunicaciones

4.3.9.1 Gestión de seguridad en las redes

- **Controles de Red**

Estos mecanismos estarán diseñados para salvaguardar la integridad y confidencialidad de la información transmitida a través de las redes de datos. Además, el departamento de TIC deberá establecer controles específicos para mitigar los riesgos asociados con la información transportada por la red. Todos los servicios, protocolos y puertos autorizados en la red de la institución deberán ser rigurosamente documentados y monitoreados para garantizar su seguridad y conformidad con las políticas establecidas.

4.3.9.2 Intercambio de información con partes externas

Es fundamental que todo el intercambio de mensajes esté cifrado para proteger la información contra riesgos como la suplantación de identidad.

La identificación de cada usuario debe generarse de manera segura, lo que implica que tanto los nombres de usuario como las contraseñas sean enviados y almacenados con un cifrado robusto. El departamento informático también debe implementar medidas adicionales, como la autenticación de dos factores, para reforzar la seguridad del acceso a las cuentas de mensajería y evitar accesos no autorizado

- **Mensajería electrónica**

Es fundamental que todo el intercambio de mensajes esté cifrado para proteger la información contra riesgos como la suplantación de identidad. Además, la identificación de cada usuario debe generarse de manera segura, lo que implica que tanto los nombres de usuario como las contraseñas sean enviados y almacenados con un cifrado robusto. El departamento de TIC también debe implementar medidas adicionales, como la autenticación de dos factores, para reforzar la seguridad del acceso a las cuentas de mensajería y evitar accesos no autorizados.

4.3.10 Gestión de Incidentes en la Seguridad de la Información

4.3.10.1 Gestión de incidentes de seguridad de la información y mejoras.

- **Responsabilidades y procedimientos.**

En cuanto al manejo de estos incidentes, el municipio designará a un responsable calificado que se encargará de gestionar, investigar y resolver los problemas reportados relacionados con la seguridad de la información. Este personal tendrá la responsabilidad exclusiva de comunicar los incidentes de seguridad a las autoridades competentes, garantizando que se sigan los procedimientos adecuados y que la respuesta sea oportuna y efectiva.

También se establecerán protocolos claros para la documentación y seguimiento de cada incidente, asegurando que las lecciones aprendidas se apliquen para fortalecer las políticas de seguridad de la institución.

- **Notificación de los eventos de seguridad de la información**

Esta notificación urgente es crucial para prevenir que los incidentes potenciales se materialicen y causen daños mayores. El departamento informático actuará rápidamente para evaluar la situación y tomar las medidas necesarias para mitigar cualquier riesgo asociado, asegurando la protección continua de la información.

4.3.11 Cumplimiento

4.3.11.1 Cumplimiento de los requisitos legales y contractuales

Se debe mantener una documentación exhaustiva de todos los requisitos legales y contractuales relacionados con la seguridad de la información que son aplicables a la institución. Así mismo la institución como el área de TI tiene la responsabilidad de asegurar que se cumplan todas las legislaciones pertinentes, incluyendo aquellas relacionadas con derechos de autor y propiedad intelectual.

Esto implica que todo el software utilizado en la municipalidad debe estar legalmente protegido y contar con las licencias de uso correspondientes, garantizando así que la institución opere dentro del marco legal y evite cualquier infracción que pueda poner en riesgo la seguridad de la información o la reputación de la entidad.

- **Identificación de la legislación aplicable**

Tanto la entidad como el departamento informático tienen la responsabilidad de asegurar que se cumplan todas las legislaciones pertinentes, incluyendo aquellas relacionadas con derechos de autor y propiedad intelectual. Esto implica que todo el software utilizado en la municipalidad debe estar legalmente protegido y contar con las licencias de uso correspondientes, garantizando así que la institución opere dentro del marco legal y evite cualquier infracción que pueda poner en riesgo la seguridad de la información o la reputación de la entidad.

- **Protección de los registros de la organización**

La alta gerencia es responsable de garantizar que los requisitos legales y contractuales de la organización se mantengan siempre actualizados. Este esfuerzo es crucial para prevenir la pérdida, destrucción o falsificación de registros importantes, al asegurar que todos los registros de la organización estén debidamente protegidos y alineados con las normativas vigentes.

- **Protección de datos y privacidad de la información personal**

La municipalidad se compromete a garantizar la seguridad y confidencialidad de la información personal de todos los funcionarios y usuarios registrados en sus bases de datos.

Esta información será utilizada exclusivamente para funciones legítimas y operativas de la entidad, y se implementarán medidas estrictas para protegerla contra cualquier acceso no autorizado, divulgación, o uso indebido.

Así mismo la institución asegurará que todos los procesos relacionados con el manejo de datos personales cumplan con las normativas y legislaciones vigentes sobre privacidad, reforzando la confianza y seguridad en la gestión de la información.

4.3.11.2 Revisiones de la seguridad de la información

- **Revisión independiente de la seguridad de la información**

La institución junto con el departamento de TIC tiene la responsabilidad de realizar revisiones periódicas de las políticas de seguridad de la información, evaluando su efectividad y relevancia para determinar si se requieren actualizaciones. Los controles que se implementen deben alinearse con la norma ISO 27001, bajo la cual se desarrolló este manual, y seguir las recomendaciones de la guía de buenas prácticas ISO 27002. Estas revisiones son esenciales para mantener la seguridad de la información en conformidad con los estándares internacionales y asegurar que las políticas sigan siendo adecuadas frente a nuevas amenazas y cambios en el entorno tecnológico.

- **Cumplimiento de las políticas y normas de seguridad**

El departamento de Tecnología de Información y Comunicación (TIC) tiene la responsabilidad de asegurar que se cumpla estrictamente el manual de políticas de seguridad de la información, vigilando que todas las directrices sean seguidas correctamente. En caso de que se produzca una violación de las políticas de seguridad, la institución adoptará las medidas necesarias conforme a la gravedad de la situación, aplicando las sanciones o correcciones pertinentes para reforzar el cumplimiento y proteger la integridad de la información. Además, se evaluará la necesidad de implementar medidas adicionales para prevenir futuras infracciones y fortalecer la cultura de seguridad dentro de la organización.

Conclusiones

- La elaboración del marco teórico ha permitido consolidar los conceptos clave de seguridad de la información, análisis de riesgos y gestión de vulnerabilidades, proporcionando una base sólida para su aplicación en el GAD El Tambo.
- La aplicación de la metodología ISO 27005 permitió identificar de manera efectiva los riesgos y vulnerabilidades más críticos en el departamento informático del GAD El Tambo. Esto proporcionó una base sólida para el desarrollo de estrategias de mitigación que aumentarán la seguridad de los activos de TI más valiosos.
- Se concluye que la norma ISO 27001 es fundamental para guiar las mejores prácticas en la gestión de seguridad de la información, especialmente en entornos gubernamentales, donde la protección de datos es crítica.

Recomendaciones

- Se recomienda establecer un programa de capacitación continua para el personal, centrado en la seguridad de la información y en la correcta implementación de las políticas descritas en el manual. Esto garantizará que todos los empleados estén actualizados con las mejores prácticas y conscientes de sus responsabilidades en la gestión de riesgos.
- Es fundamental que el manual de políticas de seguridad de la información sea revisado y actualizado de forma periódica para adaptarse a los cambios tecnológicos y nuevos riesgos que puedan surgir. Este proceso debe incluir la evaluación de la efectividad de las políticas y la incorporación de mejoras continuas.
- Se debe establecer un sistema de monitoreo y evaluación continua de los riesgos y vulnerabilidades identificados. Este sistema permitirá una respuesta rápida a cualquier cambio en el entorno de seguridad y asegurará que las medidas de mitigación sigan siendo efectivas y relevantes en el tiempo.

REFERENCIAS

Hidalgo Maldonado, M. E. (2019). *repositorio.uasb.edu.ec.* Obtenido de repositorio.uasb.edu.ec: https://repositorio.uasb.edu.ec/bitstream/10644/8057/1/T3492-MGFARF-Hidalgo-Gestion.pdf

Muñoz Gutiérrez , C. A. (9 de 2022). *repositorio.uisrael.edu.ec.* Obtenido de repositorio.uisrael.edu.ec: https://repositorio.uisrael.edu.ec/bitstream/47000/3363/1/UISRAEL-EC-MASTER-SEG-INF%20-378.242-2022-006.pdf

Narváez Guerrón, J. P. (2024). *repositorio.utn.edu.ec.* Obtenido de repositorio.utn.edu.ec: https://repositorio.utn.edu.ec/bitstream/123456789/15944/2/PG%201823%20TRABAJO%20DE%20GRADO.pdf

Pantoja Miño , Y. E. (2020). *repositorio.upec.edu.ec.* Obtenido de repositorio.upec.edu.ec: http://repositorio.upec.edu.ec/bitstream/123456789/969/1/002-%20PANTOJA%20MI%C3%91O%20YULY%20ESTEFAN%C3%8DA.pdf

Quispe García , C. P. (09 de 2021). *repositorio.uta.edu.ec.* Obtenido de repositorio.uta.edu.ec: https://repositorio.uta.edu.ec/bitstream/123456789/33703/1/t1877si.pdf

Rodríguez Guzmán, D. P. (2023). *repositorio.puce.edu.ec.* Obtenido de repositorio.puce.edu.ec: https://repositorio.puce.edu.ec/server/api/core/bitstreams/8e3c7fa8-e01b-487f-88ab-e5af3614fe18/content

Aillón Carrasco , M. E. (09 de 2021). *repositorio.uta.edu.ec.* Obtenido de repositorio.uta.edu.ec: https://repositorio.uta.edu.ec/bitstream/123456789/33718/1/t1886si.pdf

Ayala Salguero, C. X. (2021). *dspace.ups.edu.ec.* Obtenido de dspace.ups.edu.ec: https://dspace.ups.edu.ec/bitstream/123456789/21396/1/UPS-CT009402.pdf

Balcázar Lalangui, M. (16 de 01 de 2020). *repositorio.espe.edu.ec.* Obtenido de repositorio.espe.edu.ec: https://repositorio.espe.edu.ec/bitstream/21000/22805/1/T-ESPE-044010.pdf

Borbor Toala, J. A. (2021). *repositorio.upse.edu.ec.* Obtenido de repositorio.upse.edu.ec: https://repositorio.upse.edu.ec/bitstream/46000/8645/1/UPSE-TTI-2022-0029.pdf

Carvajal Artunduaga, J. F. (2021). *repository.ucc.edu.co.* Obtenido de repository.ucc.edu.co: https://repository.ucc.edu.co/server/api/core/bitstreams/cea12143-38ff-40c1-b716-233316570ba7/content

Catuto Pilay, R. M. (2021). *repositorio.upse.edu.ec.* Obtenido de repositorio.upse.edu.ec: https://repositorio.upse.edu.ec/bitstream/46000/5754/1/UPSE-TTI-2021-0007.pdf

Chulde Obando, L. E. (03 de 2021). *repositorio.uisek.edu.ec.* Obtenido de repositorio.uisek.edu.ec: https://repositorio.uisek.edu.ec/bitstream/123456789/4192/1/Lorena%20Elizabeth%20Chulde%20Obando.pdf

Collaguazo Quinatoa, M. B., & Toapanta Chilig , D. N. (02 de 2020). *repositorio.utc.edu.ec.* Obtenido de repositorio.utc.edu.ec: https://repositorio.utc.edu.ec/bitstream/27000/6664/1/T-001493.pdf

Correa Murillo , N. I. (09 de 2022). *repositorio.ug.edu.ec.* Obtenido de repositorio.ug.edu.ec: https://repositorio.ug.edu.ec/server/api/core/bitstreams/40baa2e7-1eb6-498d-8301-990bbb625f10/content

Farinango Farinango , M. F. (2023). *repositorio.utn.edu.ec.* Obtenido de repositorio.utn.edu.ec: https://repositorio.utn.edu.ec/bitstream/123456789/14762/2/04%20RED%20362%20TRABAJO%20GRADO.pdf

Fierro Alvares, M. A. (2022). *dspace.unach.edu.ec.* Obtenido de dspace.unach.edu.ec: http://dspace.unach.edu.ec/bitstream/51000/10055/1/Fierro%20%C3%81lvarez%2C%20M%20%282022%29%20Propuesta%20de%20implementaci%C3%B3n%20de%20un%20sistema%20de%20gesti%C3%B3n%20de%20la%20seguridad%20y%20salud%20en%20el%20trabajo%20en%20el%20edificio%20centra

GADMIET. (s.f.). *municipioeltambo.gob.ec*. Obtenido de municipioeltambo.gob.ec: https://municipioeltambo.gob.ec/

GADMIET. (s.f.). *municipioeltambo.gob.ec*. Obtenido de municipioeltambo.gob.ec: https://municipioeltambo.gob.ec/

Gumucio Suares, J. L. (2021). *repositorio.uchile.cl.* Obtenido de repositorio.uchile.cl: https://repositorio.uchile.cl/bitstream/handle/2250/180169/Guia-de-implementacion-de-un-programa-de-gestion-de-riesgos-de-ciberseguridad-en-entidades-de-intermediacion-financiera.pdf?sequence=1&isAllowed=y

Muñoz Aguirre, V. F. (2022). *dspace.utb.edu.ec.* Obtenido de dspace.utb.edu.ec: http://dspace.utb.edu.ec/bitstream/handle/49000/12672/E-UTB-FAFI-SIST.INF-000068.pdf?sequence=1&isAllowed=y

Paredes Díaz, K. V. (2022). *dspace.unach.edu.ec.* Obtenido de dspace.unach.edu.ec: http://dspace.unach.edu.ec/bitstream/51000/8918/1/Paredes%20D.%2C%20%20Karen%20V.%20%282022%29%20GU%C3%8DA%20DE%20IMPLEMENTACI%C3%93N%20DE%20POL%C3%8DTICAS%20%281%29.pdf

Patiño Castrillon , J. I., & Bedoya Velasquez, J. E. (2023). *dspace.tdea.edu.co.* Obtenido de dspace.tdea.edu.co: https://dspace.tdea.edu.co/bitstream/handle/tdea/3576/Plan%20estrat%C3%

A9gico%20para%20la%20identificaci%C3%B3n%20de%20riesgos%20y%20vulnerabilidades%20en%20la%20seguridad%20de%20la%20informaci%C3%B3n%20de%20los%20datos%20personales%20en%20una%20empresa.p

Pinto Auz, D. J. (30 de 09 de 2021). *repositorio.espe.edu.ec.* Obtenido de repositorio.espe.edu.ec: http://repositorio.espe.edu.ec/bitstream/21000/26482/1/T-ESPE-050862.pdf

Ramirez Agudelo, J. F. (2021). *repository.upb.edu.co.* Obtenido de repository.upb.edu.co: https://repository.upb.edu.co/bitstream/handle/20.500.11912/8216/Estrategia%20a%20partir%20de%20un%20an%C3%A1lisis%20de%20vulnerabilidades%20para%20evaluar%20la%20seguridad.pdf?sequence=1&isAllowed=y

Rea Guaman , A. M. (2020). *oa.upm.es.* Obtenido de oa.upm.es: https://oa.upm.es/65871/1/ANGEL_MARCELO_REA_GUAMAN.pdf

Rodríguez Matías, L. A. (2021). *repositorio.upse.edu.ec.* Obtenido de repositorio.upse.edu.ec: https://repositorio.upse.edu.ec/bitstream/46000/5977/1/UPSE-TTI-2021-0026.pdf

4. ANEXOS

4.1.

4.2. Anexo 1. Protocolo de Investigación

/A. TÍTULO
Análisis de riesgos y vulnerabilidades de TI para el departamento informático del GAD El Tambo

Marcar dependiendo el tema y a que campo se relaciona.

B. DOMINIO, LÍNEA Y ÁMBITOS DE INVESTIGACIÓN			
Tecnologías de Información y Comunicación	**Ciencias exactas, naturales y tecnológicas**	Inteligencia de Negocios	
		Sistemas de Información	
		Gobierno y administración de tecnologías de información	
		Auditoría Informática	
		Seguridad Informática	
		Redes y comunicación	
		Arquitectura de Hardware	
		Arquitectura de desarrollo de software	
		Ingeniería de Software	
		Gestión y gobierno de proyectos de tecnología informática	X
		Ingeniería de requerimientos	
		Algoritmos y programación	
		Ciencias exactas y naturales (Matemáticas, Física, Química, Biología, etc.)	
		Modelaje y simulación	

C. PLANTEAMIENTO DEL PROBLEMA

En el departamento informático del GAD El Tambo, la gestión adecuada de la seguridad de la información se ha convertido en una prioridad dada la creciente dependencia de los procesos tecnológicos que soportan sus operaciones cotidianas. Frente a este escenario, surge la necesidad de evaluar los riesgos y vulnerabilidades a los que está expuesta la infraestructura tecnológica para asegurar la integridad, disponibilidad y confidencialidad de la información manejada. Esta evaluación es fundamental no solo para prevenir incidentes de seguridad que podrían tener consecuencias devastadoras sobre la operatividad del GAD, sino también para establecer un marco de políticas que guíe el manejo de estas tecnologías alineado con las mejores prácticas y estándares internacionales. Sin embargo, la falta de un manual de políticas específicas para el manejo de riesgos y la mitigación de vulnerabilidades en TI limita la capacidad del departamento para responder eficazmente ante potenciales amenazas, lo que aumenta la susceptibilidad a ataques externos e internos que podrían comprometer la seguridad de toda la organización. Dado este contexto, se identifica una brecha crítica en la gestión de la seguridad de TI que debe ser abordada mediante un estudio detallado y la posterior implementación de un manual robusto de políticas de seguridad.

D. OBJETIVO GENERAL

Realizar un análisis de los riesgos y vulnerabilidades en el departamento informático del GAD El Tambo, utilizando basados en la metodología de la norma ISO 27001, con el propósito de elaborar un manual de políticas que refuerce la seguridad de la información y mejore la respuesta organizacional ante amenazas de TI

E. OBJETIVOS ESPECÍFICOS

1.	Elaborar un marco teórico que consolide los conceptos fundamentales y las mejores prácticas sobre la seguridad de la información, análisis de riesgos y la gestión de vulnerabilidades, destacando las contribuciones de la norma ISO 27001 y su aplicación en entidades gubernamentales.
2.	Realizar un diagnóstico detallado de los riesgos y vulnerabilidades actuales en el departamento informático del GAD El Tambo, empleando herramientas y técnicas de evaluación conforme a los principios establecidos por la norma ISO 27001
3.	Diseñar un manual de políticas de seguridad de TI que integre las estrategias de mitigación de riesgos identificadas, garantizando el cumplimiento de las directrices de la ISO 27001 y fomentando una cultura de seguridad robusta dentro del departamento
a)	
b)	

F. JUSTIFICACIÓN

En la era digital actual, las instituciones gubernamentales enfrentan desafíos significativos en materia de seguridad de la información, con frecuentes incidentes que comprometen datos sensibles y afectan la continuidad de las operaciones, el departamento informático del GAD El Tambo no es la excepción. La implementación de un análisis riguroso de riesgos y vulnerabilidades se vuelve indispensable para identificar y mitigar posibles amenazas que podrían tener impactos adversos, tanto a nivel operativo como en la percepción pública de la entidad. Utilizando la metodología de la norma ISO 27001, este estudio se propone establecer un marco de acción que no solo mejore la seguridad, sino que también fortalezca la confianza de los ciudadanos en la capacidad del GAD para proteger su información.

Además, el desarrollo de un manual de políticas específicas basado en los resultados del análisis ayudará a formalizar los procesos y respuestas ante incidentes de seguridad, creando un

ambiente más controlado y sistemático. La falta de tales políticas actualmente limita la capacidad de respuesta del departamento frente a incidentes, lo que podría resultar en pérdidas de información crítica o fallos en los servicios ofrecidos a la comunidad. Este proyecto tiene el potencial de transformar la gestión de la seguridad de TI del GAD El Tambo, volviéndola más proactiva y alineada con estándares internacionales, lo cual es fundamental para garantizar una gestión efectiva y segura en el contexto actual de amenazas cibernéticas en constante evolución.

G. ALCANCE

El alcance de esta investigación abarca un análisis exhaustivo de los riesgos y vulnerabilidades asociados a la seguridad de la información en el departamento informático del GAD El Tambo, centrándose en la identificación, evaluación y propuesta de medidas de mitigación conforme a la norma ISO 27001; se incluirá la elaboración de un manual de políticas específico que servirá como guía para el manejo de incidentes de seguridad y la protección de datos.

H. CONCEPTOS RELACIONADOS

Seguridad informática

La seguridad informática se refiere al conjunto de medidas y técnicas destinadas a proteger la confidencialidad, integridad y disponibilidad de la información en sistemas informáticos y redes, mediante la implementación de controles de acceso, encriptación, detección de intrusiones y políticas de seguridad, con el objetivo de prevenir y mitigar riesgos asociados a ciberataques, malware, robo de datos y otras amenazas digitales. (Carvajal Artunduaga, 2021)

En un entorno donde la información es esencial para las organizaciones, la seguridad informática se vuelve crucial para su operatividad y reputación en el mercado. La protección de datos confidenciales es vital debido a las posibles repercusiones económicas y de imagen; esto implica la implementación de medidas técnicas y organizativas, así como la formación del personal, la

vigilancia continua de la red y la adaptación constante de las políticas de seguridad para enfrentar las nuevas amenazas digitales. (Rea Guaman , 2020)

Seguridad de la Información

Abarca las medidas y prácticas destinadas a proteger la confidencialidad, integridad y disponibilidad de los datos en un entorno digital, mediante la implementación de controles de acceso, cifrado, monitorización y gestión de riesgos, con el fin de prevenir y mitigar amenazas como ciberataques, robo de datos y fallos de seguridad, garantizando así la protección y confianza en la información almacenada y transmitida por sistemas informáticos y redes. (Gumucio Suares, 2021)

Pilares de la seguridad de la información

Son los fundamentos esenciales que sustentan la protección de los datos en entornos digitales, comprendiendo la confidencialidad, integridad y disponibilidad de la información, así como la autenticación, control de acceso, y gestión de riesgos, que en conjunto aseguran la preservación de la información frente a amenazas cibernéticas, garantizando su protección y fiabilidad para los usuarios y sistemas involucrados. (Carvajal Artunduaga, 2021)

- **Confidencialidad**

  Es el principio que garantiza que la información sensible se encuentra protegida contra accesos no autorizados, asegurando que solo aquellos usuarios o sistemas autorizados puedan acceder a la información protegida.

- **Integridad** (Correa Murillo , 2022)

  Se refiere a la propiedad de la información de mantenerse completa, exacta y no alterada durante su almacenamiento, procesamiento o transmisión. Garantiza que los datos no han sido modificados de manera no autorizada o accidental. (Ramirez Agudelo, 2021)

- **Disponibilidad**

  Es el principio que asegura que la información esté accesible y utilizable por aquellos usuarios autorizados que la requieran, en el momento en que sea necesario. Implica la implementación de medidas para prevenir interrupciones o caídas en los sistemas que puedan afectar el acceso a la información. (Correa Murillo , 2022)

Ciberseguridad

La ciberseguridad es un campo multidisciplinario que se centra en proteger los sistemas informáticos, redes y datos contra una amplia gama de amenazas cibernéticas. Esto incluye la protección contra malware, ataques de denegación de servicio (DDoS), robos de datos, intrusiones y otras formas de actividad maliciosa que buscan comprometer la seguridad y la privacidad de la información digital. (Rea Guaman , 2020)

Abarca la implementación de medidas proactivas, como firewalls, sistemas de detección de intrusiones y cifrado de datos, así como la gestión de incidentes, la respuesta ante emergencias y la recuperación de desastres para minimizar el impacto de posibles ataques y asegurar la continuidad del negocio (Patiño Castrillon & Bedoya Velasquez, 2023)

Riesgos

En el contexto de la seguridad informática representan las posibles amenazas y vulnerabilidades que pueden comprometer la confidencialidad, integridad y disponibilidad de la información en sistemas informáticos y redes. Estos riesgos pueden surgir de diversas fuentes, como ataques cibernéticos, errores humanos, fallas en los sistemas, desastres naturales o acciones malintencionadas, y tienen el potencial de causar daños significativos a los activos digitales y a la reputación de las organizaciones si no son gestionados adecuadamente (Puga Jacome, 2019)

Tipos de riesgos

Estos incluyen riesgos de seguridad cibernética, como ataques de malware, phishing, ingeniería social y vulnerabilidades de software, así como riesgos físicos, como desastres naturales, fallos de infraestructura y acceso no autorizado a instalaciones. Además, los riesgos relacionados con el cumplimiento normativo, la privacidad de los datos y la gestión de la cadena de suministro también son consideraciones importantes en la evaluación y gestión de los riesgos en seguridad informática. (Balcázar Lalangui, 2020)

Análisis de Riesgos

Es un proceso sistemático que busca identificar, evaluar y mitigar las posibles amenazas y vulnerabilidades que pueden afectar la seguridad de la información en un sistema informático o una organización. Consiste en identificar los activos de información, determinar las posibles amenazas y evaluar la probabilidad de que ocurran, así como el impacto que tendrían en caso de materializarse. (Patiño Castrillon & Bedoya Velasquez, 2023)

Vulnerabilidad

Una vulnerabilidad se refiere a una debilidad o fallo en un sistema informático, una red o una aplicación que puede ser explotada por un atacante para comprometer la seguridad y obtener acceso no autorizado, modificar datos o causar daños. Estas vulnerabilidades pueden surgir debido a errores de programación, configuraciones inseguras, falta de actualizaciones de seguridad o diseño deficiente del sistema, y representan puntos de entrada potenciales para ataques cibernéticos y explotación por parte de individuos malintencionados (Ramirez Agudelo, 2021)

Amenazas

Las amenazas en el contexto de la seguridad informática son cualquier tipo de acción, evento o situación que tiene el potencial de causar daño, comprometer la integridad o la disponibilidad de la información, o violar la privacidad de los sistemas y los datos. Estas amenazas pueden manifestarse de diversas formas, incluyendo ataques de malware, ataques de denegación de servicio (DDoS), phishing, ingeniería social, robo de datos, fallos de seguridad y desastres naturales, entre otros. Identificar y mitigar las amenazas es esencial para proteger los activos de información y mantener la seguridad y la integridad de los sistemas y las redes informáticas. (Balcázar Lalangui, 2020)

I. TRABAJOS RELACIONADOS

El presente proyecto se basa en una cuidadosa revisión de trabajos previos relacionados con el análisis de riesgos y vulnerabilidades de tecnologías de la información (TI) en entornos gubernamentales.

Roberth Baque desarrollo un trabajo investigativo en la Universidad Estatal del Sur de Manabí, con título “DISEÑO DE UNA ESTACIÓN DE TRABAJO PARA DETECCIÓN DE VULNERABILIDADES DE SERVIDORES WEB, PARA MITIGAR CIBERATAQUES ", este proyecto se enfoca específicamente en los laboratorios de cómputo de la Carrera de

Ingeniería en Computación y Redes, donde la implementación de una estación de trabajo para la detección de vulnerabilidades de servidores web se presenta como una medida preventiva fundamental para proteger los activos de tecnología de la información y garantizar la continuidad de las operaciones en este entorno académico. (Baque Villegas, 2020)

Este documento proporcionará una base sólida para construir el marco teórico ya que presenta una revisión de la literatura existente relacionada con la detección de vulnerabilidades en servidores web, sistemas, dispositivos, etc

Otro estudio realizado por Martha Pantoja de la Universidad Técnica Del Norte con título "EVALUACIÓN TÉCNICA INFORMÁTICA DE LAS VULNERABILIDADES EN CIBERSEGURIDAD EN LOS LABORATORIOS DE COMPUTACIÓN DE LA UNIVERSIDAD TÉCNICA DEL NORTE CON BASE EN COBIT 2019 ", este estudio se centra en una metodología de evaluación técnica informática que aborda diversos aspectos de seguridad, incluida la identificación de riesgos, la evaluación de controles de seguridad existentes, la detección de vulnerabilidades y la recomendación de medidas de mitigación. Para llevar a cabo esta evaluación, se realizará un análisis exhaustivo de los laboratorios de computación, considerando tanto los aspectos técnicos como los procesos y políticas de seguridad implementados. (Pantoja Mejía, 2023)

Esto servirá como referencia de una estructura metodológica sólida para llevar a cabo la evaluación de riesgos y vulnerabilidades en el departamento de TI. Esto te permite contar con un marco de trabajo bien definido desde el cual desarrollar y ejecutar la presente investigación.

Balcazar Lalangui realizo un estudio titulado "Propuesta metodológica para mitigar el riesgo de seguridad informática con el uso de técnicas OSINT", de la Universidad de las Fuerzas Armadas ESPE, destaca la importancia de abordar los desafíos actuales en seguridad informática, especialmente en el contexto de la proliferación de ataques en la red debido al desconocimiento de técnicas de protección por parte de los usuarios. Se resalta que las redes sociales y el acceso a la red desde diferentes dispositivos representan un gran riesgo para la seguridad de la información, ya que estas plataformas son frecuentemente blanco de ciberataques. (Balcázar Lalangui, 2020)

Este documento ofrece una propuesta metodológica, herramientas específicas y consideraciones éticas para llevar a cabo la investigación.

J. METODOLOGÍA

Enfoque de la Investigación

El enfoque de esta investigación es mixto, combinando métodos cualitativos y cuantitativos para obtener una comprensión completa de los riesgos y vulnerabilidades a los que está expuesto el departamento informático del GAD El Tambo; los métodos cualitativos incluirán entrevistas y revisión de documentos que proporcionarán una visión detallada de las percepciones y prácticas actuales, mientras que los métodos cuantitativos emplearán análisis estadístico para validar y cuantificar los riesgos identificados durante la fase cualitativa, ofreciendo así una perspectiva integral y robusta de la situación.

Nivel de Investigación

En cuanto al nivel de la investigación, se clasificará como aplicada ya que se enfocará en resolver un problema específico mediante la implementación de un manual de políticas de seguridad de TI; este nivel permite no solo generar conocimiento sobre las vulnerabilidades y riesgos en el contexto específico del GAD El Tambo sino también aplicar este conocimiento de manera práctica para mejorar la seguridad y eficiencia de la organización, buscando resultados que tengan un impacto directo y medible en la gestión de la seguridad de la información dentro del departamento.

K. CRONOGRAMA DE ACTIVIDADES

N°	ACTIVIDAD	MES						MEDIOS DE VERIFICACIÓN
		I	II	III	IV	V	VI	
1	Fundamentación Teórica	x						Revisión de la literatura existente sobre seguridad informática, ciberseguridad, análisis de riesgos, vulnerabilidades, y otros temas relacionados. Identificación y selección de teorías, modelos y marcos conceptuales relevantes para fundamentar tu investigación.
2	Diagnóstico Situacional		x					Recopilación de datos sobre la situación actual de la seguridad informática en la

								organización o contexto de estudio. Identificación de activos de información, riesgos y vulnerabilidades presentes en el entorno analizado. Análisis de brechas y puntos críticos que requieran atención y acción inmediata.
3	Metodología de la investigación			x	x			Selección de enfoque metodológico (cualitativo, cuantitativo o mixto) y justificación de la elección.
4	Desarrollo de la propuesta				x	x		Desarrollo de una propuesta de mejora basada en los hallazgos del diagnóstico situacional y la fundamentación teórica. Diseño de estrategias y medidas específicas para abordar los riesgos y vulnerabilidades identificados. .
5	Conclusiones y recomendaciones						x	Desarrollo de las conclusiones y recomendaciones de la Tesis.

L. DECLARACIÓN FINAL

Los abajo firmantes declaramos bajo juramento que el proyecto descrito en este documento no ha sido presentado a otra institución nacional o internacional para su financiamiento, no causa perjuicio al ambiente, es de nuestra autoría y no transgrede norma ética alguna.

M. PARTICIPANTES

DIRECTOR:	
ESTUDIANTE 1	
ESTUDIANTE 2	

N. FIRMAS DE RESPONSABILIDAD

Lugar:	

Fecha:	

Firmas:

Nombre: CC: **Director del Proyecto**	Nombre: C.C.: **Estudiante / Egresado**

O. APROBACIÓN

Firmas:

Nombre: CC: **Primer Par Revisor**	Nombre: C.C.: **Segundo Par Revisor**

P. REFERENCIAS

5.

Balcázar Lalangui, M. (16 de 01 de 2020). *repositorio.espe.edu.ec.* Obtenido de repositorio.espe.edu.ec: https://repositorio.espe.edu.ec/bitstream/21000/22805/1/T-ESPE-044010.pdf

Baque Villegas, R. A. (2020). *repositorio.unesum.edu.ec.* Obtenido de repositorio.unesum.edu.ec: https://repositorio.unesum.edu.ec/bitstream/53000/3186/1/BAQUE%20VILLEGAS%20ROBERTH%20ANDR%C3%89S.pdf

Carvajal Artunduaga, J. F. (2021). *repository.ucc.edu.co.* Obtenido de repository.ucc.edu.co: https://repository.ucc.edu.co/server/api/core/bitstreams/cea12143-38ff-40c1-b716-233316570ba7/content

Correa Murillo , N. I. (09 de 2022). *repositorio.ug.edu.ec.* Obtenido de repositorio.ug.edu.ec: https://repositorio.ug.edu.ec/server/api/core/bitstreams/40baa2e7-1eb6-498d-8301-990bbb625f10/content

Gumucio Suares, J. L. (2021). *repositorio.uchile.cl.* Obtenido de repositorio.uchile.cl: https://repositorio.uchile.cl/bitstream/handle/2250/180169/Guia-de-implementacion-de-un-programa-de-gestion-de-riesgos-de-ciberseguridad-en-entidades-de-intermediacion-financiera.pdf?sequence=1&isAllowed=y

Pantoja Mejía, M. C. (2023). *repositorio.utn.edu.ec.* Obtenido de repositorio.utn.edu.ec: https://repositorio.utn.edu.ec/bitstream/123456789/15300/2/PG%201680%20TRABAJO%20GRADO.pdf

Patiño Castrillon , J. I., & Bedoya Velasquez, J. E. (2023). *dspace.tdea.edu.co.* Obtenido de dspace.tdea.edu.co: https://dspace.tdea.edu.co/bitstream/handle/tdea/3576/Plan%20estrat%C3%A9gico%20para%20la%20identificaci%C3%B3n%20de%20riesgos%20y%20vulnerabilidades%20en%20la%20seguridad%20de%20la%20informaci%C3%B3n%20de%20los%20datos%20personales%20en%20una%20empresa.p

Puga Jacome, C. E. (21 de 03 de 2019). *repositorio.uisek.edu.ec.* Obtenido de repositorio.uisek.edu.ec: https://repositorio.uisek.edu.ec/bitstream/123456789/3343/1/TESIS%20MTI%20EDUARDO%20PUGA.pdf

Ramirez Agudelo, J. F. (2021). *repository.upb.edu.co.* Obtenido de repository.upb.edu.co: https://repository.upb.edu.co/bitstream/handle/20.500.11912/8216/Estrategia%20a%20partir%20de%20un%20an%C3%A1lisis%20de%20vulnerabilidades%20para%20evaluar%20la%20seguridad.pdf?sequence=1&isAllowed=y

Rea Guaman , A. M. (2020). *oa.upm.es.* Obtenido de oa.upm.es: https://oa.upm.es/65871/1/ANGEL_MARCELO_REA_GUAMAN.pdf

6.

6.1. Anexo 3. Traducción del Resumen de el Centro de Idiomas

ABSTRACT

This research work entitled "IT Risk and Vulnerability Analysis for the Information Technology Department of GAD El Tambo" aims to develop a comprehensive proposal for risk and vulnerability management in the IT department, ensuring the protection of technological assets and the continuity of municipal operations. This proposal is based on implementing a framework based on the ISO 27001 standard to improve information security and align IT practices with international standards. The starting point was a detailed analysis of the current situation of GAD El Tambo's IT department, including identifying critical assets and assessing the associated risks. In addition, an exhaustive review of the best practices and controls suggested by ISO 27001 and ISO 27002 was conducted, adapting these regulations to the specific needs of the municipality. Based on this analysis, a risk management model was developed to mitigate the identified threats and strengthen the department's resilience to potential security incidents.

Key words: risk analysis, information management, IT vulnerability.

6.2. Anexo 2. Certificado Turniting

Tesis

INFORME DE ORIGINALIDAD

9%	7%	3%	3%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	blog.bitso.com Fuente de Internet	<1%
2	www.risti.xyz Fuente de Internet	<1%
3	Submitted to Universidad Mariano Gálvez de Guatemala Trabajo del estudiante	<1%
4	seguridadinfoperu.blogspot.com Fuente de Internet	<1%
5	www.slideshare.net Fuente de Internet	<1%
6	Submitted to Universidad Tecnológica Centroamericana UNITEC Trabajo del estudiante	<1%
7	Submitted to Universidad Autónoma de Bucaramanga,UNAB Trabajo del estudiante	<1%
8	dspace.uazuay.edu.ec Fuente de Internet	<1%

Universidad Católica de Cuenca

AUTORIZACIÓN DE PUBLICACIÓN EN EL REPOSITORIO INSTITUCIONAL

Oscar Fabian Angamarca Pomavilla portador(a) de la cédula de ciudadanía Nº **0302578331** En calidad de autor/a y titular de los derechos patrimoniales del trabajo de titulación **"Análisis de riesgos y vulnerabilidades de TI para el GAD el Tambo, manuales y políticas, en base a la norma ISO 27002"** de conformidad a lo establecido en el artículo 114 Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación, reconozco a favor de la Universidad Católica de Cuenca una licencia gratuita, intransferible y no exclusiva para el uso no comercial de la obra, con fines estrictamente académicos y no comerciales. Autorizo además a la Universidad Católica de Cuenca, para que realice la publicación de éste trabajo de titulación en el Repositorio Institucional de conformidad a lo dispuesto en el artículo 144 de la Ley Orgánica de Educación Superior.

Cañar, **21 de noviembre de 2024**

F: .....

Oscar Fabian Angamarca Pomavilla

C.I. **0302578331**