UNIVERSIDAD TECNOLÓGICA ECOTEC

FACULTAD DE INGENIERÍAS, ARQUITECTURA Y CIENCIAS DE LA NATURALEZA

TÍTULO DEL TRABAJO:

PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN PARA LA UNIDAD DE TIC´S DEL GAD MUNICIPAL DEL CANTÓN PAUTE

LÍNEA DE INVESTIGACIÓN:

TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

MODALIDAD DE TITULACIÓN:

TRABAJO DE INTEGRACIÓN CURRICULAR

CARRERA:

INGENIERÍA EN SISTEMAS CON ÉNFASIS EN SISTEMAS

TÍTULO A OBTENER:

INGENIERÍA EN SISTEMAS INTELIGENTES

AUTORES (A):

ANA PAULINA CABRERA BRAVO

NAIN ALEXANDER VALLADARES SIERRA

TUTOR (A):

ING. MARCOS ANTONIO ESPINOZA MINA, PHD.

SAMBORONDÓN – ECUADOR

2024

ANEXO No. 9

PROCESO DE TITULACIÓN
CERTIFICADO DE APROBACIÓN DEL TUTOR

Samborondón, 22 de agosto de 2024

Magíster
Erika Ascencio
Facultad de Ingenierías, Arquitectura y Ciencias de la Naturaleza
Universidad Tecnológica ECOTEC

De mis consideraciones:

Por medio de la presente comunico a usted que el trabajo de titulación TITULADO: **PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN PARA LA UNIDAD DE TIC´S DEL GAD MUNICIPAL DEL CANTÓN PAUTE**, fue revisado, siendo su contenido original en su totalidad, así como el cumplimiento de los requerimientos establecidos en la guía para su elaboración, por lo que se autoriza a los estudiantes: **CABRERA BRAVO ANA PAULINA Y VALLADARES SIERRA NAIN ALEXANDER** para que procedan con la presentación oral del mismo.

ATENTAMENTE,

ING. MARCOS ANTONIO ESPINOZA MINA, PHD.

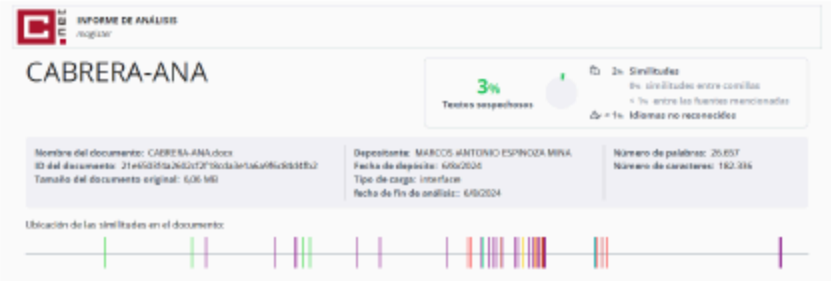
Tutor

Universidad Ecotec

ANEXO No. 10

PROCESO DE TITULACIÓN
CERTIFICADO DEL PORCENTAJE DE COINCIDENCIAS
DEL TRABAJO DE TITULACIÓN

Habiendo sido revisado el trabajo de titulación TITULADO: **PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN PARA LA UNIDAD DE TIC'S DEL GAD MUNICIPAL DEL CANTÓN PAUTE** elaborado por **CABRERA BRAVO ANA PAULINA Y VALLADARES SIERRA NAIN ALEXANDER** fue remitido al sistema de coincidencias en todo su contenido el mismo que presentó un porcentaje del 3%, mismo que cumple con el valor aceptado para su presentación que es inferior o igual al 10% sobre el total de hojas del documento. Adicional se adjunta print de pantalla de dicho resultado.



ATENTAMENTE,

MARCOS ANTONIO ESPINOZA MINA

ING. MARCOS ANTONIO ESPINOZA MINA, PHD.
Tutor

Dedicatoria

Paulina Cabrera.

A mi madre, quien con su amor incondicional y su inquebrantable dedicación me ha formado con valores y principios que han guiado cada uno de mis pasos. Su ejemplo de fortaleza y sabiduría me ha inspirado a enfrentar todos los desafíos con valentía y determinación. A mis hermanos, por ser mis compañeros de vida, por compartir risas y lágrimas, y por brindarme su apoyo incondicional en todo momento. Su presencia ha sido una fuente constante de ánimo y alegría, y juntos hemos construido recuerdos invaluables que atesoro profundamente.

A mis abuelitos, cuyas historias y sabios consejos han enriquecido mi vida de manera inmensurable. Gracias por enseñarme el verdadero significado de la perseverancia y el amor. Sus vidas son un testimonio de dedicación y fortaleza, y su cariño ha sido un pilar fundamental en mi crecimiento personal y académico. A mis sobrinos, por ser una fuente constante de alegría y renovación. Sus risas y curiosidad me han recordado la importancia de la inocencia y la maravilla de descubrir el mundo. A todos ustedes, dedico este logro con gratitud y amor eterno, reconociendo que, sin su apoyo y guía, este camino habría sido mucho más difícil de recorrer.

Nain Valladares.

Este logro se lo dedico a mi familia, mi mamá Alexandra Sierra por siempre darme su cariño y apoyo incondicional durante todos estos años. A mi papá, por esforzarse cada día por nosotros y poder traer el pan de cada día y no dejar que nos falte al menos lo necesario. A mis hermanas Nicholle Valladares, Nailyn Valladares y Nathalia Valladares. A mis abuelitas Mariana Romero y especialmente a Letty Morán, que por cosas de la vida no pude compartir este logro con ella, pero se que está en un lugar mejor y siempre me acompaña en todo momento.

Agradecimiento

Paulina Cabrera.

Agradezco a Dios, por ser mi guía constante y por darme la fortaleza para enfrentar cada desafío con esperanza y determinación. A mi familia, especialmente a mi madre, hermanos, abuelitos y sobrinos, por su amor y apoyo incondicional. Su aliento y fe en mí han sido fundamentales para alcanzar esta meta. A mi madre, por su sabiduría y sacrificio; a mis hermanos, por su compañerismo y apoyo; a mis abuelitos, por sus valiosos consejos y enseñanzas; y a mis sobrinos, por traer alegría y renovación a mi vida.

A mis profesores y mentores, por compartir su conocimiento y por guiarme con paciencia y dedicación a lo largo de mi formación académica. Y a todas aquellas personas que, de una u otra manera, han contribuido a la culminación de este logro, les estoy eternamente agradecido.

Nain Valladares.

Estoy eternamente agradecido con Dios, mi familia, compañeros, profesores y conocidos que a lo largo de todos estos años me han ayudado a convertirme en la persona que soy actualmente. Gracias a los que creyeron y creen en mí, incluso en momentos en los que dudaba de mi potencial. Solo quiero decirles que esto es solo un inicio de otro capítulo más y no los defraudaré, especialmente no me rendiré.

Gracias Totales

Resumen

En una sociedad cada vez más automatizada, las tecnologías de la información se han convertido en un componente crucial para que las instituciones operen y respalden sus actividades específicas. Esto plantea nuevos desafíos para los administradores municipales, especialmente en aspectos de eficiencia en la seguridad de la información de sus habitantes, asegurando al mismo tiempo la integridad de sus procesos y datos. Dado que el GAD Municipal del Cantón Paute está en constante evolución. Por estos motivos, pensando en el beneficio del GAD Municipal, este trabajo de integración curricular se enfoca en el diseño de un plan estratégico para la seguridad de la información en la Unidad de TIC´s. A través de una metodología cualitativa cuyo enfoque se caracterizó por la búsqueda de una comprensión profunda y detallada de la situación actual. Con resultados que parten de la falta de políticas de seguridad adecuadas, procesos formales y recursos necesarios para garantizar la protección de la información. El plan propuesto incluye la identificación, evaluación y priorización de riesgos, así como la implementación de estrategias de mitigación basadas en las mejores prácticas de la norma ISO 27001.

Palabras clave: seguridad de la información, buenas prácticas, plan estratégico, estrategias.

Abstract

In an increasingly automated society, information technologies have become a crucial component for institutions to operate and support their specific activities. This presents new challenges for municipal administrators, especially in aspects of efficiency in the security of their inhabitants' information, while simultaneously ensuring the integrity of their processes and data. Given that the GAD Municipal of the Canton Paute is constantly evolving, and thinking about its benefit, this curricular integration project focuses on designing a strategic plan for information security in the TIC Unit. Through a qualitative methodology characterized by the search for a deep and detailed understanding of the current situation, the results highlight a lack of adequate security policies, formal processes, and necessary resources to ensure information protection. The proposed plan includes the identification, evaluation, and prioritization of risks, as well as the implementation of mitigation strategies based on the best practices of the ISO 27001 standard.

Keywords: information security, best practices, strategic plan, strategies.

Tabla de Contenido

INTRODUCCIÓN **1**
Contexto histórico social 1
Antecedentes 3
Planteamiento del problema 4
Objetivos de la investigación 5
General 5
Específicos 5
Justificación 6
MARCO TEÓRICO **1**
1.1. Marco fundamental 10
1.1.1. Tecnología y seguridad de la información 10
1.1.2. Teoría de sistemas y gestión de la seguridad de la información 10
1.1.3. Sociedad de conocimiento 11
1.1.4. Desafíos en la seguridad de la información 12
1.2. Marco conceptual 14
1.2.1. Estrategia en tecnología 14
1.2.2. Técnicas de información y comunicación 14
1.2.3. La gestión del cambio 15
1.2.4. Estrategias para la gestión del cambio 16
1.2.5. La planificación estratégica 16
1.2.6. Plan estratégico de seguridad de la información (PESI) 18
1.2.7. Seguridad de la información 19
1.2.8. Principios de seguridad de la información 20
1.2.9. Riesgos 21
1.2.10. Controles. 22
1.2.11. Vulnerabilidades 23
1.2.12. Comparativa de estándares internacionales posibles 23
1.3. Marco situacional 26
1.3.1. Evolución histórica de la seguridad de la información 26
1.3.2. Derecho a la protección de los datos personales 27
1.3.3. Norma ISO 27001 28
1.3.4. Análisis FODA 29

1.3.5. Plan de acción 30
1.4. Marco contextual 30
1.4.1. Seguridad de la información en la unidad de TIC’s 30
MARCO METODOLÓGICO 10
2.1. Enfoque de la investigación 35
2.2. Alcance de la investigación 36
2.3. Delimitación de la investigación 37
2.4. Población 38
2.5. Muestra 39
2.6. Métodos empleados 39
2.6.1. Encuesta 39
2.6.2. Entrevista 41
2.7. Análisis de datos 41
ANÁLISIS E INTERPRETACIÓN DE LOS RESULTADOS 35
3.1. Descripción de los resultados 36
3.1.1. Fase 1: Visión 36
3.1.2. Fase 2: Situación actual - Análisis de la población 37
3.2. Análisis de los Resultados 45
3.2.1. Entrevistas 45
3.2.2. Encuestas 45
3.3. Discusión 47
CONCLUSIONES 50
RECOMENDACIONES 51
REFERENCIAS 52
ANEXOS 58

Índice de Tablas

Tabla 1.Comparación de Normativas de seguridad de la información 24
Tabla 2. Distribución de la muestra 39
Tabla 3.Resultados de la encuesta, variable: modo general. 40
Tabla 4.Resultados de la encuesta, variable: usuarios. 41
Tabla 5. Resultados de la encuesta, variable: autenticación. 42
Tabla 6.Resultados de la encuesta, variable: autorización. 42
Tabla 7. Resultados de la encuesta, variable: administración de sistemas. 43
Tabla 8.Resultados de la encuesta, variable: equipos informáticos. 43
Tabla 9.Resultados de la encuesta, variable: activos fijos. 44
Tabla 10. Equipos con los que cuenta la institución. 83
Tabla 11. Softwares manejados por la entidad. 83
Tabla 12. Fortalezas identificadas. 85
Tabla 13. Debilidades identificadas. 85
Tabla 14.Oportunidades identificadas. 86
Tabla 15. Amenazas identificadas. 86
Tabla 16. Priorización de riesgos del PESI 95

Índice de Figuras

Figura 1. Metodología del PESI 79
Figura 2. Organigrama del Unidad de TIC'S del GAD-Paute 80
Figura 3.Organigrama de la unidad de TIC´S 81
Figura 4. Mapa de calor de riesgos ISO 27001:2022 91
Figura 5. Matriz de riesgo de activos ISO 27001:2022 93

INTRODUCCIÓN

Contexto histórico social

En una sociedad cada vez más automatizada, las tecnologías de la información (TI) se han convertido en un componente crucial para que las instituciones operen y respalden sus actividades específicas. La gestión adecuada de la información en tiempo real a través de sistemas de información es fundamental, especialmente cuando se trata de proteger la confidencialidad, integridad y disponibilidad de los datos.

Desde hace varios años, las TI no solo se reconocen como un área de apoyo al negocio, sino también como un diferenciador que permite ofrecer nuevos y variados productos. Este es un tema relevante especialmente para las instituciones gubernamentales, donde se requiere un manejo adecuado de los datos y procesos (Franciskovic, et al., 2020). No obstante, la administración de los recursos de TI se ha convertido en una tarea compleja (Casanova y Calderón, 2020).

Así mismo, el control adecuado de las TI se identifica como un proceso difícil de manejar, que requiere la separación de funciones, la especialización del personal y la alineación de las metas con los objetivos empresariales, asegurando además que se implementen prácticas robustas para la protección de la información (Castaño, 2020). La seguridad de la información también es un tema crucial en el contexto gubernamental actual. Los sistemas de información de las instituciones públicas están expuestos a diversas amenazas que pueden comprometer la integridad, confidencialidad y disponibilidad de sus activos informáticos.

Estas amenazas representan un riesgo significativo que puede ocasionar graves daños tanto a las entidades gubernamentales como a los ciudadanos involucrados. Sin embargo,

muchas entidades se enfocan más en el control de la información que en la prevención de amenazas, lo que puede resultar en compromisos de la información resguardada.

En los últimos años, se ha observado un aumento significativo de los ataques y amenazas dirigidos a las instituciones públicas en el ámbito de la seguridad de la información (Cáceres, 2022). Esto evidencia la necesidad de contar con un plan estratégico que permita identificar y abordar de manera efectiva los riesgos y vulnerabilidades existentes y posibles amenazas a las que se expone.

En el cantón Paute, ubicado en el sector oriental de Azuay, Ecuador, el Gobierno Autónomo Descentralizado (GAD) Municipal tiene como objetivo convertir al cantón en una "ciudad" tecnológica y segura (Morocho, 2023). Paute busca el desarrollo integral del cantón a través de una planificación estratégica que incluya diversas iniciativas tecnológicas y la implementación de proyectos destinados a mejorar la calidad de vida de sus habitantes (Municipio de Paute, 2024).

La Misión Institucional del Gobierno Autónomo Descentralizado (GAD) Municipal de Cantón Paute es impulsar un desarrollo sostenible a nivel cantonal, proporcionando equipamientos accesibles que aseguren el acceso equitativo a los grupos prioritarios, enfocándose en la eficiencia y efectividad en sus competencias (Municipio de Paute, 2024). La Visión Institucional del GAD Municipal de Paute es ser un cantón innovador, equitativo, eficiente y sostenible, garantizando un ambiente sustentable y una alta calidad de vida para todos (Municipio de Paute, 2024).

Esto plantea nuevos desafíos para los administradores municipales, especialmente en aspectos de eficiencia en la seguridad de la información de sus habitantes, asegurando al mismo tiempo la integridad de sus procesos y datos. Dado que el GAD Municipal del Cantón Paute está en constante evolución (Muñoz P. , 2021). Por estos motivos y pensando en el beneficio del GAD Municipal de Cantón Paute, este trabajo de integración curricular se enfoca

en el diseño de un plan estratégico para fortalecer la seguridad de la información en la Unidad de TIC´s del GAD.

Antecedentes

En el ámbito gubernamental, el Ministerio de Trabajo ha abordado desafíos similares relacionados con la gestión eficiente de las entidades estatales y fortalecer la seguridad de la información de los servicios públicos (Ministerio del Trabajo, 2021). Este enfoque se refleja en el "Objetivo Estratégico Institucional", cuyo objetivo principal es incrementar la excelencia en la protección de los recursos de TI y la gestión segura de los recursos estatales. Este objetivo se logra mediante la implementación de tecnologías de la información y estándares de seguridad que faciliten la administración adecuada de estos recursos.

El Plan Nacional de Desarrollo subraya el compromiso con la implementación de buenas prácticas regulatorias en seguridad de la información, basadas en TI y estándares de seguridad como la ISO 27001. Estas prácticas están diseñadas para asegurar la transparencia, eficiencia y competitividad del Estado, garantizando la integridad, confidencialidad y disponibilidad de los activos de información (Ministerio del Trabajo, 2021).

Un ejemplo notable de la implementación de estándares de seguridad de la información es el Registro de la Propiedad del Distrito Metropolitano de Quito, que inició el proceso de certificación ISO 27001:2013 en julio de 2022 y concluyó en abril de 2023, como parte de su modernización institucional (Comunicación Social RPDMQ, 2022). Este proceso incluyó diagnóstico, capacitación, implementación y cierre de no conformidades y tuvo como objetivo mejorar la calidad y eficiencia de sus servicios registrales. El Registro ha obtenido dicha certificación para destacarse por ofrecer servicios en línea seguros y de alta calidad en beneficio de la ciudadanía.

La adopción de estas buenas prácticas regulatorias promueve la transparencia en la toma de decisiones y las operaciones gubernamentales. Aseguran que las regulaciones sean

eficientes, apoyen la competitividad del Estado y faciliten un entorno favorable para el desarrollo. Mejorar la seguridad y eficiencia de los servicios y productos ofrecidos por las instituciones públicas es una responsabilidad primordial de los gobiernos (Casanova Villalba et al., 2021).

Estos antecedentes proporcionan información sobre cómo las entidades gubernamentales deben buscar fortalecer su eficiencia y seguridad de servicios mediante la implementación de tecnologías de la información y estándares de seguridad de la información. Resaltando la importancia de elaborar estrategias de mejora regulatorias para cumplir con los objetivos estratégicos institucionales. Estas experiencias en el ámbito ministerial son referentes valiosos para abordar desafíos similares en el GAD Municipal de Cantón Paute, especialmente en el contexto previamente mencionado.

Planteamiento del problema

En los últimos años, las TI se han convertido en herramientas esenciales y globalmente imprescindibles. Han revolucionado la automatización de procesos, transformando nuestra forma de trabajar, comprar y comunicarnos, al hacer que los procesos sean más eficientes y rápidos. Actualmente, el auge de las TIC se ha vuelto una necesidad imperativa para la sociedad. Los continuos avances tecnológicos permiten a las organizaciones crecer y volverse más competitivas.

La creciente complejidad de las amenazas y vulnerabilidades informáticas ha generado una preocupación significativa en el GAD Municipal de Cantón Paute. Este contexto plantea un desafío en la prevención y el control adecuado de los sistemas y tecnologías de la información que manejan. Así mismo, la Unidad de TIC´s no emplea buenas prácticas establecidas por estándares internacionales, lo que agrava la situación a mediano y largo plazo, al comprometer la integridad, confidencialidad y disponibilidad de la información, con posibles consecuencias

operativas y reputacionales para la institución. Esto evidencia la necesidad de una estrategia robusta y efectiva.

Por lo tanto, es crucial el diseño de un plan estratégico para fortalecer la seguridad de la información, alineado con los estándares internacionales para mitigar estos riesgos y asegurar una gestión eficiente y segura de la información (Pazmiño, et al., 2020). El objetivo principal del PESI es diseñar un plan de tecnología informática que soporte las necesidades de información del municipio y esté fundamentalmente alineado con sus estrategias institucionales y prioridades (Acosta, et al., 2023).

Dicho plan proporciona un mecanismo para priorizar las iniciativas de seguridad de la información, permitiendo analizar, evaluar los activos actuales de la Unidad de TIC´s, se puedan manejar de manera eficiente y apoyar las metas establecidas en beneficio de la comunidad de Paute. Estas acciones son esenciales para el correcto manejo y control en la prestación de servicios públicos y construir una base tecnológica segura (Cano, 2018). Teniendo en cuenta lo anteriormente expuesto se plantea como pregunta científica:

¿Cómo se puede fortalecer la seguridad de la información en la Unidad de TIC´s en el GAD Municipal del Cantón Paute?

Objetivos de la investigación

General

Elaborar un plan estratégico para la mitigación de riesgos de seguridad de la información en la Unidad de TIC´s.

Específicos

- Revisar estudios académicos y conceptos relevantes sobre la seguridad de la información.

- Identificar la situación actual de la seguridad de la información en la Unidad de TIC´s.
- Diseñar un plan estratégico de seguridad de información que incluya la identificación, evaluación, priorización y estrategias para la mitigación de riesgos.
- Evaluar el plan estratégico con criterio de experto.

Justificación

La elaboración de un plan estratégico en instituciones gubernamentales es fundamental para asegurar que las TIC se integren de manera efectiva y segura. Sin una planificación adecuada, las instituciones corren el riesgo de perder competitividad, eficiencia y comprometer la integridad de la información, esto afecta negativamente su capacidad para cumplir con sus objetivos y responder a las demandas de la sociedad.

Este panorama se refleja en el contexto latinoamericano donde, tal como Briceño (2021) señala que muchas organizaciones carecen de una inversión adecuada en el área tecnológica, lo que impide implementar de forma efectiva estrategias. De igual manera, Cedeño y Townsend (2021) respaldan que la inversión en el área tecnológica es crucial para la competitividad de las empresas o instituciones.

La integración efectiva de las TIC en la administración pública es un desafío persistente, marcado por un desconocimiento generalizado. Este desconocimiento se traduce en la falta de capacitación y concientización del personal o procesos establecidos en un plan de acción. Esto impide que las instituciones gubernamentales aprovechen plenamente los beneficios de la tecnología, comprometiendo la seguridad de la información y la eficiencia en la prestación de servicios públicos.

Por lo tanto, es esencial elaborar un plan estratégico que aborde estas deficiencias, asegurando un manejo adecuado de la seguridad de la información y fortalecer la capacidad de la unidad de TIC´s para cumplir con sus objetivos y servir correctamente a sus habitantes. El

GAD Municipal ha comenzado un proceso de reestructuración en la Unidad de TIC´s desde la posesión de las nuevas autoridades.

Estas se enfocan en combatir la carencia de estrategias claras y adecuadas para seguridad de la información de las TIC, con el objetivo de asegurar que el cantón Paute progrese en términos de desarrollo humano y mejores estándares de vida, a través de una Unidad de TIC´s fortalecida que responda eficazmente a las necesidades tecnológicas de sus habitantes.

Además, la implementación de normas internacionales, como la ISO 27001 que ha demostrado ser crucial para reducir brechas de seguridad y aumentar la eficiencia operativa. Por ejemplo, la organización DataGuard reporta que la certificación ha ayudado a minimizar los errores humanos y optimizar los procesos de seguridad, lo cual resulta en una mayor resiliencia frente a ciberataques y una reducción significativa de incidentes de seguridad (Boutwell, 2024)

Otra ventaja importante es el aumento de la confianza entre los stakeholders y los ciudadanos. Puesto que, la ISO 27001 establece un estándar de manejo seguro de datos, lo que no solo protege contra accesos no autorizados, sino que también mejora la percepción pública de la gestión de la información. La empresa Thoropass destaca que obtener esta certificación puede servir como un diferencial competitivo en el mercado, promoviendo la confianza y facilitando la adquisición de nuevos negocios y la retención de clientes (Thoropass, 2024)

En este contexto, se plantea la necesidad de elaborar un plan estratégico para la Unidad de TIC´S. El impacto de este trabajo de integración curricular es significativo, ya que, se identifican áreas críticas que necesitan fortalecer estrategias efectivas para mitigar los riesgos, vulnerabilidades detectadas y establecer metas claras que sean alcanzables (Mera , et al., 2021). Estas metas facilitan la creación de una estructura directiva que permite supervisar y asegurar la ejecución de los planes de acción (Arévalo, et al., 2020).

En conclusión, este trabajo de integración curricular presenta un enfoque práctico, enfocado en aplicar soluciones efectivas para fortalecer la seguridad de la información en la Unidad de TIC 's, a través de un plan estratégico. Además, se complementa con una metodología analítica, que implica la elaboración de estrategias para la Unidad de TIC´s siguiendo las buenas prácticas y estándares internacionales. Por lo tanto, la investigación contribuye significativamente tanto al campo académico como al práctico, apoyando la misión y visión del Cantón Paute que apuntan hacia un futuro tecnológicamente sostenible y eficiente.

MARCO TEÓRICO

CAPÍTULO I

Capítulo I: Marco Teórico

1.1. Marco fundamental

1.1.1. Tecnología y seguridad de la información

Según Saavedra, et al., (2021), la tecnología no solo implica el uso de herramientas y sistemas para resolver problemas, sino también el manejo seguro de la información que fluye a través de estos sistemas. La tecnología moderna juega un papel crucial en la protección de datos contra accesos no autorizados y amenazas cibernéticas, mejorando así la seguridad y el bienestar humano.

La tecnología abarca un conjunto de conocimientos y procesos organizados, no solo para la producción de bienes y servicios, sino también asegurar la disponibilidad, confidencialidad e integridad de los datos (Galante y Marí, 2020). Este enfoque integra la técnica y la ciencia con consideraciones económicas, sociales y culturales, subrayando la importancia de una gestión de seguridad de la información efectiva dentro de las organizaciones.

En la última década, la adopción de tecnologías avanzadas ha transformado las operaciones organizacionales a escala global, facilitando la automatización y eficiencia; Sin embargo, la interacción humana continúa siendo indispensable, no solo para la gestión operativa sino también para la implementación de medidas de seguridad que se adapten a los desafíos emergentes y las situaciones complejas. La tecnología, particularmente en el contexto de la seguridad de la información, debe ser manejada de manera que se maximice su potencial mientras se minimizan los riesgos asociados.

1.1.2. Teoría de sistemas y gestión de la seguridad de la información

La tecnología está inmersa en un contexto que interactúa continuamente a nivel económico, social, cultural e ideológico. Comprender la tecnología y la seguridad de la información mediante la teoría de sistemas permite situar estos elementos dentro de un proceso de investigación enfocado en la problemática de seguridad en organizaciones gubernamentales.

La metodología sistemática es crucial para descubrir, analizar y abordar los problemas de seguridad que emergen en la gestión de las TIC. Asimismo, en el ámbito del aprendizaje, la teoría de los sistemas y su aplicación práctica en la realidad actúan como herramientas para comprender en profundidad la administración de los recursos en las instituciones.

En el ámbito tecnológico, el enfoque sistemático, respaldado por teóricos como Chadwick (1978), aporta herramientas y conceptos organizativos esenciales para el manejo eficiente de la seguridad de la información. Este enfoque ofrece un marco de referencia integral que permite no sólo analizar sino también organizar y mejorar los sistemas de seguridad dentro de las estructuras organizacionales con un énfasis en la seguridad.

Mediante un conjunto de procedimientos y metodologías, la teoría de sistemas permite evaluar de manera integral cómo las políticas de seguridad de la información se integran y protegen los activos informáticos, destacando la importancia de un análisis sistemático y estructurado para garantizar la integridad, confidencialidad y disponibilidad de la información.

1.1.3. Sociedad de conocimiento

Para entender la aplicación de la tecnología en diversas actividades, es esencial incorporar el término sociedad del conocimiento, que se define como la participación activa de los seres humanos en los procesos intelectuales de enseñanza y aprendizaje. La sociedad del conocimiento se refiere a aquellos entornos en los que individuos o grupos, debido a diversos

cambios sociales, políticos y culturales, utilizan herramientas para transformar y adaptar conocimientos en respuesta a los eventos.

Los enfoques que la sociedad otorga al conocimiento están guiados por los avances tecnológicos, los cuales alteran la manera en que las personas piensan y actúan (García, 2020). Los conocimientos se generan mediante la capacidad de razonamiento desplegada. Estos autores destacan que los elementos principales incluyen la generación de conocimiento, la colaboración, la gestión del cambio y la utilización de las Tecnologías de la Información y Comunicaciones (Martínez, et al., 2020).

García (2020) menciona que los rápidos avances tecnológicos y la digitalización de la información a través de Internet facilitan el progreso de grupos especializados y el desarrollo de la población, basándose en la innovación y la investigación. Por lo tanto, el conocimiento ha sido siempre el producto del proceso tecnológico, que emerge a partir de la abundante información disponible en general. En este contexto, la gestión segura de la información se convierte en una necesidad imperativa, asegurando que la transformación tecnológica se realice de manera que proteja la integridad y privacidad del conocimiento generado.

1.1.4. Desafíos en la seguridad de la información

Las regulaciones sobre seguridad de la información están en constante evolución, adaptándose a nuevas amenazas y cambiando contextos tecnológicos. Las organizaciones deben cumplir con un conjunto diverso de normativas internacionales, como la ISO 27001, para gestionar de forma segura la información y proteger los intereses de todos los actores involucrados.

Estas normativas abarcan desde la protección de datos hasta la transparencia y la responsabilidad, enfatizando la importancia de una gestión proactiva de los riesgos de información (UdeCataluña, 2024). Además, la crisis sanitaria global ha acelerado la adopción de modelos de trabajo flexibles, aumentando los riesgos asociados con el acceso remoto. Las

organizaciones deben implementar medidas de seguridad robustas, como la autenticación multifactor y redes privadas virtuales, para proteger la integridad de la información corporativa (UdeCataluña, 2024).

Simultáneamente, la falta de personal cualificado en seguridad de la información sigue siendo un desafío significativo, limitando la capacidad de las empresas para responder efectivamente a los incidentes de seguridad. Este déficit de talento hace esencial la colaboración con socios tecnológicos que aporten experiencia y conocimientos actualizados (Dubois, 2023).

La inteligencia artificial también emerge como una herramienta de doble filo en la seguridad de la información. Si bien puede anticipar y automatizar la detección de amenazas, también es utilizada por los atacantes para perfeccionar sus estrategias, lo que requiere una estrategia de seguridad integral que abarque desde la protección de accesos hasta la infraestructura de red, aplicando enfoques de "confianza cero" y utilizando las últimas tecnologías en firewalls (Dubois, 2023).

En la última década, los avances en la seguridad de la información han sido significativos, impulsados por la creciente adopción de la inteligencia artificial y el aprendizaje automático (Lugo, Carrasquero, & Gómez, 2020). Estas tecnologías permiten una detección y respuesta más rápidas y precisas a las amenazas cibernéticas, identificando patrones de comportamiento anómalos y mitigando riesgos antes de que causen daños significativos. Además, el enfoque de "confianza cero", que no da por sentado la seguridad de ningún usuario o dispositivo, ha mejorado considerablemente la protección de los sistemas y datos corporativos al requerir una verificación continua.

Otro avance importante es la implementación de medidas de seguridad robustas como la autenticación multifactor (MFA) y las redes privadas virtuales (VPN), especialmente relevantes con el aumento del trabajo remoto (Lugo, Carrasquero, & Gómez, 2020). Estas tecnologías garantizan que solo usuarios autorizados puedan acceder a los recursos

corporativos, protegiendo la integridad de la información sensible. Asimismo, el cifrado avanzado se ha convertido en una práctica estándar para proteger los datos tanto en tránsito como en reposo, asegurando que la información permanezca segura incluso en caso de interceptación. La formación continua del personal en ciberseguridad y la colaboración con expertos externos han fortalecido aún más las defensas contra amenazas cada vez más sofisticadas.

1.2. Marco conceptual

1.2.1. Estrategia en tecnología

Las estrategias pueden ser definidas según los lineamientos que guían la misión de cada organización o actividad, y que su concepción implica el uso de métodos para la planificación y dirección de operaciones a gran escala (Erbes y Roitter, 2020). A través de su integración progresiva en el mundo, estas herramientas se utilizan generalmente para demostrar acciones orientadas a objetivos derivados de la dirección, planificación y organización.

La actividad se desarrolla con el objetivo de alcanzar algo esperado por una persona o grupo, dentro de un tiempo específico y bajo ciertas condiciones, definiendo así el trabajo de varios profesionales hacia un logro común (Rueda y Rodríguez, 2020). La estrategia se utiliza como una herramienta guía para facilitar procedimientos y métodos, aplicados de manera interactiva y funcional, con el fin de contribuir activamente a una organización y lograr una mayor satisfacción en los usuarios. Para utilizar la tecnología correctamente, es necesario tomar decisiones, establecer metas, propuestas sobre su acceso y uso adecuado, mediante la implementación de servicios y funciones que deben cumplirse en las empresas u organizaciones.

1.2.2. Técnicas de información y comunicación

El papel de las TIC en el ámbito educativo, describiéndolas como herramientas que facilitan el almacenamiento, la sistematización y la presentación formal y documental de información (Moreira y Adell, 2021). Destacándose la notable evolución de estas tecnologías, que han ido reemplazando gradualmente a los medios de comunicación tradicionales como el periódico, el telégrafo, el teléfono fijo, la radio y la televisión, siendo sustituidos por dispositivos como teléfonos inteligentes y computadoras con acceso a Internet. Este cambio, ha desencadenado transformaciones significativas en la sociedad, la educación, las relaciones interpersonales y los métodos de difusión y generación de información y conocimiento.

En su investigación realizada en 2020, Escofet describe las TIC como una estructura compuesta por diversas aplicaciones, sistemas, métodos, técnicas y metodologías que se basan en la digitalización en tiempo real. Destaca que estas tecnologías poseen características como la inmaterialidad, el desequilibrio y la capacidad de innovación en los procesos de automatización, lo que facilita una mayor diversidad y conexión entre diferentes estados. El proceso de cambio en las TIC suele iniciarse en las instituciones debido a las necesidades y demandas de los usuarios. Se considera que solo aquellas entidades que reconocen sus carencias y actúan proactivamente para superarlas son capaces de innovar y transformarse.

1.2.3. La gestión del cambio

El cambio se define como la acción de abandonar una situación o condición para adoptar una nueva. Todo cambio, ya sea grande o pequeño, global o parcial, social, tecnológico o político, requiere ser gestionado adecuadamente. Todo indicio de cambio genera resistencia y temor en algunos sectores, sin embargo, las organizaciones que desean sobrevivir no pueden permitirse ser rígidas (Guevara, et al., 2021). La gestión del cambio es un campo interdisciplinario que integra conocimientos de sociología, psicología, antropología y economía (Guaman, 2022).

Al planificar un cambio, es esencial comprender profundamente el funcionamiento interno de la organización, así como entender su mentalidad y sus respuestas. Es crucial comprender los valores y la historia de la organización, conocer las expectativas del cambio, identificar a los patrocinadores y opositores, y gestionar el cambio de manera inclusiva, aceptando sugerencias, justificando decisiones y rindiendo cuentas (Guaman, 2022). Al implementar la gestión del cambio, se debe inicialmente crear un sentido de urgencia y luego contratar líderes influyentes que puedan realizar grandes cambios, ya sean a corto o largo plazo, en beneficio de la organización (Rodriguez, 2022).

1.2.4. Estrategias para la gestión del cambio

La toma de decisiones informada, basada en buenas prácticas, permite a las organizaciones alcanzar con éxito sus objetivos establecidos, mejorando así la eficiencia (Vázquez, et al., 2022). Al formular estrategias, es fundamental utilizar de manera óptima los recursos disponibles, involucrando todos los niveles de la organización y considerando las diversas dimensiones que afectan a la empresa.

Además, la implementación de estas estrategias debe ser monitoreada y ajustada continuamente para responder a los cambios del entorno y asegurar la sostenibilidad de los resultados. La comunicación efectiva y el compromiso de los empleados son cruciales para la aceptación y el éxito del cambio organizacional, creando un ambiente de colaboración y confianza que facilita la transición.

1.2.5. La planificación estratégica

La planificación estratégica es el proceso que implica organizar y tomar decisiones para obtener, procesar y analizar información interna y externa clave, con el fin de identificar, prever y determinar el futuro de la organización (Delgado, et al., 2022). Debe ser implementado de manera oportuna, teniendo en cuenta posibles cambios inesperados (Guaman, 2022). La

planificación estratégica es una función crucial en cualquier organización y se ha convertido en una herramienta indispensable para la gestión gerencial actuando como un pilar esencial en el crecimiento de la empresa (Muñiz, et al., 2022).

Una adecuada elaboración e implementación de la planificación estratégica permitirá a la empresa fortalecer su capacidad de respuesta, resolver problemas y alcanzar los objetivos y metas propuestas (Zuñiga, 2021). La planificación es fundamental para la gestión empresarial, ya que promueve la eficiencia al evitar la improvisación y funciona como un sistema de control (Gutiérrez, et al., 2021).

1.2.5.1. Principios planificación estratégica

La planificación estratégica se basa en principios que aumentan la confiabilidad y credibilidad del método:

- **Priorizar el "ser" sobre el "hacer":** se identifica y define la razón de ser de la organización, su actividad económica y los objetivos que se esperan alcanzar.
- **Priorizar el "hacer" sobre el "cómo hacerlo":** se identifican las acciones que llevan de manera efectiva a la consecución de los objetivos.
- **Visión o Enfoque sistémica:** La empresa se ve como un conjunto de subsistemas o elementos interrelacionados, que pueden tener origen interno (recurso) o externo (insumo).
- **Visión o Perspectiva del proceso:** Los sistemas son dinámicos y deben ser estudiados con una perspectiva temporal, considerando su historia.
- **Visión u Orientación hacia el futuro:** Se adopta un pensamiento estratégico proactivo para prepararse para posibles eventos futuros.
- **Compromiso con la acción y los resultados:** La planificación no se queda en el papel, sino que se analiza, actúa y evalúa, enfocándose en los logros.

- **Flexibilidad**: La capacidad de adaptarse a condiciones cambiantes y de improvisar cuando sea necesario.
- **Estabilidad**: Se busca un equilibrio dinámico que permita un crecimiento seguro, minimizando riesgos y asegurando la sostenibilidad del sistema y los procesos (González y Rodríguez, 2019)

1.2.5.2. Propósitos de la planificación estratégica

La planificación estratégica tiene varios propósitos que contribuyen al logro de los objetivos institucionales:

- Propósito protector
- Propósito afirmativo
- Propósito de coordinación

1.2.6. Plan estratégico de seguridad de la información (PESI)

Este enfoque se centra en fortalecer la protección de la información dentro de la organización, identificando y mitigando riesgos para asegurar la integridad, confidencialidad y disponibilidad de los datos. Es vital establecer políticas de seguridad claras y efectivas que respondan a las necesidades internas y los desafíos del entorno externo (Cañón, 2020). Este proceso es fundamental tanto en el ámbito profesional como académico, adaptándose a las particularidades de cada institución (Reina, 2021).

1.2.6.1. El PESI incluye varias fases para su correcto desarrollo

- **FASE I Analizar el estado actual:** Se analiza la situación actual de la seguridad de la información en la institución. Esto incluye una revisión de las políticas existentes, la efectividad de las medidas de seguridad y la conciencia de seguridad entre los empleados.

Las tareas a llevar a cabo en esta etapa son

- Alcance de la Evaluación:
    - Evaluación de las políticas de seguridad actuales.
    - Análisis de la infraestructura tecnológica en términos de seguridad.
    - Revisión del talento humano en relación con la seguridad de TI.
    - Evaluación de los gastos en seguridad de la información.

FASE II Modelo de gestión de riesgos: Desarrollo de un modelo que identifique, evalúe y gestione los riesgos asociados a la seguridad de la información. Este modelo ayuda a priorizar las amenazas y definir estrategias efectivas para mitigarlas.

- **Componentes del modelo**:
    - Identificación y análisis de amenazas.
    - Evaluación de vulnerabilidades.
    - Estrategias para mitigar riesgos identificados.

FASE III Integración de la seguridad en la estrategia TI: Formulación de un marco que alinee la seguridad de la información con la estrategia de TI general de la organización, asegurando que todas las decisiones tecnológicas refuercen las directrices de seguridad. Las actividades que conlleva son:

- **Estrategias y planificación**:
    - Integración de la seguridad en la arquitectura de TI y sistemas de información.
    - Desarrollo de un plan operativo que incluya seguridad como un pilar fundamental.

FASE IV Planificación estratégica y continuidad: Esta fase implica el desarrollo de un plan estratégico que incluya programas de formación en seguridad, procedimientos de respuesta ante incidentes y medidas para la recuperación ante desastres (Chapin & Cuenca, 2021).

1.2.7. Seguridad de la información

En el actual entorno tecnológico, la seguridad de la información se ha convertido en un pilar fundamental para la operación segura de las organizaciones. La seguridad de la información comprende un conjunto de técnicas, estrategias y políticas diseñadas para proteger la información y los sistemas de TI contra accesos, usos, divulgaciones, interrupciones, modificaciones o destrucciones no autorizadas. (Briceño, 2021)

Este conjunto de medidas busca, fundamentalmente, salvaguardar los datos y los activos tecnológicos de usos malintencionados. Por su parte, Castillo y Zavala (2019) enfatizan que la seguridad de la información asegura la disponibilidad, confidencialidad e integridad de los datos esenciales para una entidad, abarcando tanto información digital como física.

La creciente dependencia de las tecnologías de la información ha hecho que estas medidas de seguridad sean indispensables para mantener la continuidad de las operaciones y la confianza de los stakeholders en un panorama cada vez más amenazado por ataques cibernéticos (Ticona, 2021). La seguridad de la información ha ganado importancia con la evolución tecnológica y la capacidad de interconexión a través de redes, lo que ha abierto nuevas oportunidades para las instituciones de mejorar su productividad, pero también ha generado grandes preocupaciones entre los profesionales de la seguridad de la información.

1.2.8. Principios de seguridad de la información

Los principios de seguridad de la información son fundamentales para proteger los activos de datos en cualquier organización, incluidas las entidades gubernamentales como el GAD Municipal de Cantón Paute. Estos principios aseguran la integridad, confidencialidad, y disponibilidad de la información.

- **Confidencialidad**: La información debe estar disponible únicamente para las personas autorizadas. En el ámbito gubernamental, proteger la confidencialidad requiere

implementar controles de acceso y técnicas de cifrado para proteger los datos sensibles contra accesos no permitidos (Lucas, 2023).

- **Integridad**: La exactitud y completitud de la información. La integridad es esencial para preservar la precisión de los datos gubernamentales, garantizando que no se alteren sin autorización, ya sea por error o de forma intencional. Esto se consigue utilizando algoritmos de hashing y sistemas de control de versiones que detectan y evitan modificaciones no autorizadas (Ruiz, 2024).
- **Disponibilidad**: La información debe estar accesible y disponible para los usuarios autorizados cuando sea necesaria (Ruiz, 2024). Esta disponibilidad puede ser comprometida por ataques como los de denegación de servicio (DoS). Para mitigar estos riesgos, las instituciones gubernamentales deben implementar soluciones robustas de redundancia de datos y continuidad del negocio (Cabrera, 2023).

Además de estos principios fundamentales, la seguridad de la información en entidades gubernamentales debe incluir aspectos como la autenticación y autorización de usuarios, auditorías regulares de los sistemas de información y la formación continua del personal sobre las mejores prácticas de seguridad (De La Cruz, et al., 2023). Al adoptar estos principios no solo protege la información crítica del gobierno contra amenazas internas y externas, sino que también incrementa la confianza pública en el manejo de sus datos personales (Lucas, 2023).

1.2.9. Riesgos

En términos generales, la posibilidad de que ocurra un evento adverso que perjudique tanto los recursos tangibles como los intangibles, lo que a su vez puede obstaculizar el desarrollo adecuado de la labor profesional (Romero, y otros, 2018). Además, se indica que el riesgo debe comprenderse como la posibilidad de una amenaza se aproveche de dichas vulnerabilidades.

Al referirse a un efecto de riesgo, se está aludiendo a la incertidumbre o duda en relación con los objetivos establecidos. También existe una probabilidad de que ocurra un impacto que altere el resultado esperado durante el análisis, el cual puede ser positivo o negativo, dependiendo de la situación (Sánchez y Hidalgo, 2023). Finalmente, el riesgo, en su totalidad o en parte, depende de la información relevante o de la comprensión de un nuevo evento.

1.2.9.1. Evaluación de riesgos basado en activos

La evaluación de riesgos centrada en activos en el estándar ISO 27001 es una herramienta que las organizaciones que han adoptado esta normativa utilizan para identificar amenazas significativas a los objetivos de seguridad de la información. A diferencia de la evaluación basada en escenarios, esta metodología se centra en dispositivos, computadoras, software, bases de datos, estructuras para almacenar documentos en papel y algunas personas (Solarte, et al., 2015). Analizar, evaluar los riesgos, verificar controles existentes de seguridad, usar software para realizar pruebas y monitorear los sistemas, sirve para determinar cuál es el estado o situación actual en la organización y poder reconocer las causas para plantear soluciones en dichos controles para su mitigación (Ramirez, 2019).

1.2.9.2. Gestión del riesgo

La gestión del riesgo es una práctica metodológica y sistemática llevada a cabo con el propósito de identificar, evaluar, clasificar y definir los procedimientos, políticas y acciones necesarias para manejar los riesgos (Pazmiño, et al., 2020).

1.2.9.3. Objetivo

El objetivo principal de la gestión del riesgo es implementar controles efectivos que permitan abordar los riesgos de manera adecuada. Estos controles pueden tener diferentes enfoques:

1.2.10. Controles

- **Mitigar**: Reducir el impacto y la probabilidad de los riesgos mediante la implementación de medidas preventivas y correctivas específicas.
- **Evitar**: Eliminar completamente el riesgo al tomar decisiones que eviten las actividades o situaciones que puedan generarlo.
- **Transferir**: Desplazar el riesgo a un tercero, generalmente a través de contratos seguros, para que otra entidad asuma la responsabilidad del mismo.
- **Asumir**: Aceptar el riesgo y planificar estrategias para enfrentar sus consecuencias, entendiendo que algunas veces los costos de mitigación o transferencia pueden ser mayores que el impacto del riesgo mismo.

1.2.11. Vulnerabilidades

Las vulnerabilidades como fallos en los sistemas de seguridad o en las herramientas que los usuarios utilizan para realizar sus actividades, las cuales podrían permitir que una amenaza se concrete y cause problemas (Sánchez y Hidalgo, 2023). Las deficiencias en los sistemas de seguridad o en las herramientas empleadas por los usuarios en sus actividades pueden facilitar que una amenaza se materialice y genere un problema (Gómez, 2022). Además, una vulnerabilidad puede considerarse como la posibilidad de que una amenaza se realice y afecte un activo. Las vulnerabilidades que afectan a los activos incluyen debilidades en los aspectos físicos de la organización, los procedimientos, el personal, la gestión, la administración, los equipos, el software o la información.

1.2.12. Comparativa de estándares internacionales posibles

La elección adecuada de un estándar se basa en las características del entorno operativo y las necesidades específicas de la organización en estudio (Fernández y Carrera, 2019). Para seleccionar el estándar más adecuado para fortalecer la seguridad de la

información en la Unidad de TIC 's del GAD Municipal del Cantón Paute, se consideraron tres estándares: NIST SP 800-53, CIS Controls e ISO 27001. A continuación, se presenta una comparativa basada en su aplicabilidad, fortalezas y limitaciones en relación con el caso de la Unidad de TIC's, que busca fortalecer la identificación de riesgos y vulnerabilidades, así como diseñar estrategias de seguridad para proteger la información y datos personales.

1.2.12.1. NIST SP 800-53

Proporciona un conjunto exhaustivo de controles y recomendaciones para la seguridad de la información en sistemas federales de Estados Unidos. Su enfoque principal es la gestión de riesgos mediante la implementación de controles de seguridad específicos y detallados (Kurii y Opirskyy, 2022).

1.2.12.2. CIS Controls

Ofrecen una guía práctica y eficiente para la implementación de la seguridad cibernética, priorizando las mejores prácticas en 18 controles críticos. Su enfoque es práctico y está diseñado para ser fácil de implementar, proporcionando una solución efectiva para mejorar la ciberseguridad en organizaciones de diversos tamaños y sectores (Groš, 2021).

1.2.12.3. ISO 27001

La norma ISO 27001 se especializa en la seguridad de la información y es reconocida a nivel internacional. Su enfoque se basa en la implementación de buenas prácticas y recursos para proteger datos sensibles y confidenciales, asegurando el cumplimiento normativo y proporcionando estándares robustos (Bustamante, et al., 2021).

Tabla 1

Comparación de Normativas de seguridad de la información

Criterio	NIST SP 800-53	CIS Controls	ISO 27001

Enfoque	Protección y gestión de la seguridad de información	Guía práctica para la implementación de seguridad de TI	Protección integral de la información mediante buenas prácticas
Aplicabilidad	Recomendaciones y controles para la seguridad de información en sistemas federales	Prioriza las mejores prácticas de seguridad cibernética en 18 controles críticos	Aplicación de buenas prácticas y recursos para la seguridad de información
Fortalezas	Conjunto exhaustivo de controles, enfoque en gestión de riesgos	Facilidad de implementación, enfoque práctico y eficiente	Cumplimiento normativo y mejora continua de seguridad.
Limitaciones	Puede ser complejo y burocrático, más adecuado para organizaciones grandes	Menos formal, puede no cubrir todas las necesidades de organizaciones grandes	Recursos y compromiso a largo plazo para implementación y mantenimiento de buenas prácticas
Idoneidad para Paute	Medio, adecuado para entidades que requieren alto nivel de detalle en controles de seguridad	Medio, proporciona controles prácticos fáciles de implementar	Alto, ideal para protección integral y gestión continua de la seguridad de información

Nota. Elaboración basada en la comparación de normativas de seguridad de información. Elaborado por los Autores.

La selección del estándar más adecuado es una decisión que debe alinearse estrechamente con las prioridades y metas actuales de la Unidad de TIC's. Como el enfoque principal es fortalecer la seguridad de la información, la ISO 27001 emergió como la opción más adecuada, ofreciendo un marco integral para el manejo y control de la seguridad de la información, proponer instrucciones específicas para la identificación, evaluación de riesgos y la mejora continua de las prácticas de seguridad.

Puesto que la ISO 27001 se especializa en la protección de datos sensibles y confidenciales, es más adecuada para abordar las debilidades críticas identificadas en la Unidad de TIC's, como la falta de procesos de seguridad adecuados y la ausencia de auditorías regulares. A diferencia del NIST SP 800-53, que es altamente detallado y específico para entornos federales y del CIS Controls, que se enfoca en controles prácticos y básicos, la ISO

27001 ofrece un enfoque balanceado y sistemático que es reconocible y aplicable y reconocido a nivel internacional.

En conclusión, para la Unidad de TIC's, la ISO 27001 se destacó como el estándar más favorable al coincidir con la necesidad de elaborar un plan estratégico para la mitigación de riesgos de la seguridad de información en la Unidad de TIC´s. Esta selección, que se puede evidenciar en la Tabla1 y en el Anexo7, es un paso clave para alcanzar la meta de fortalecer la seguridad de la información conforme a los objetivos del trabajo de integración curricular, asegurando que las prácticas de seguridad estén alineadas con estándares internacionales y fomentando una cultura de seguridad robusta dentro del departamento.

1.3. Marco situacional

1.3.1. Evolución histórica de la seguridad de la información

La seguridad de la información ha experimentado una notable transformación desde que se centró en proteger datos militares y de inteligencia durante la Guerra Fría. Originalmente, la seguridad estaba orientada a resguardar documentos físicos. No obstante, con la aparición de la computación y el internet, la seguridad de la información se extendió para incluir la protección de datos digitales (López y López, 2023)

- **Antes de la era de Internet:** Previo a la expansión de Internet, la seguridad de la información se concentraba en medidas físicas y administrativas para proteger documentos impresos y otros soportes físicos. Técnicas como la clasificación de documentos, el control de acceso físico y la destrucción segura eran habituales.
- **Aparición de Internet:** Con el surgimiento de Internet en los años noventa, la seguridad de la información empezó a enfrentar retos únicos de la era digital. La necesidad de proteger la información transmitida a través de redes abiertas llevó al desarrollo de tecnologías como el cifrado y la autenticación electrónica.

- **Era de la información y el auge de las amenazas cibernéticas:** Conforme avanzaba la tecnología, también lo hacían las amenazas. Virus informáticos, malware y ataques de piratas informáticos se volvieron más sofisticados.

Esto propició un enfoque más integrado y estratégico hacia la seguridad de la información, con la creación de políticas exhaustivas y la implementación de soluciones de seguridad multinivel, incluyendo el desarrollo de normativas internacionales como la ISO 27001.

- **Era de la conformidad y la gobernanza de datos:** Recientemente, el enfoque de la seguridad de la información ha evolucionado hacia la gobernanza de datos y la conformidad normativa.

La proliferación de leyes de protección de datos, como el RGPD en Europa, ha obligado a las organizaciones a no solo proteger los datos, sino también a demostrar esfuerzos de conformidad con las regulaciones vigentes.

- **Impacto en las entidades gubernamentales:** Para entidades como el GAD Municipal de Cantón Paute, esta evolución enfatiza la importancia crítica de adoptar un enfoque proactivo y regulado hacia la seguridad de la información.

Es esencial que las instituciones públicas garanticen la protección de los datos personales de los ciudadanos, gestionan los riesgos de seguridad y cumplan con las expectativas de transparencia y responsabilidad.

1.3.2. Derecho a la protección de los datos personales

El derecho a la protección de datos personales, reconocido en los artículos 11 y 66 de la Constitución, se ha establecido como un derecho fundamental en la era digital. Este derecho asegura que los individuos tengan control sobre cómo se recogen, utilizan y comparten sus datos personales, promoviendo la transparencia y la adherencia a la ley en su manejo.

En el ámbito legal, definido por el artículo 2 del Código Orgánico General de Procesos, los datos personales incluyen cualquier información que pueda ser usada para identificar a una persona, ya sea directa o indirectamente. Las entidades que procesan estos datos deben adherirse a principios de protección estrictos como la minimización de datos, la limitación del almacenamiento, y la implementación de controles de seguridad avanzados para prevenir accesos no autorizados y filtraciones de información (Ministerio de Telecomunicaciones, 2018).

Además, las regulaciones en los artículos 4 y 7 del mismo código establecen derechos específicos para los ciudadanos respecto a sus datos personales, incluyendo el derecho a acceder a su información, solicitar rectificaciones o incluso pedir la eliminación de sus datos bajo ciertas circunstancias. Estos derechos facilitan a los individuos la capacidad de mantener una influencia significativa sobre su información personal, permitiéndoles gestionar su privacidad de manera efectiva en un entorno cada vez más digitalizado (Ministerio de Telecomunicaciones, 2018).

1.3.3. Norma ISO 27001

La norma ISO 27001 es un estándar internacional diseñado para gestionar la seguridad de la información, enfocándose en mantener la confidencialidad e integridad de los datos dentro de una organización (Barba, 2023). La implementación de esta norma implica identificar y gestionar los riesgos, además de aplicar los controles de seguridad pertinentes, que pueden incluir políticas, procedimientos y soluciones técnicas específicas. La certificación ISO 27001 refleja la responsabilidad de la institución con la seguridad de información, lo que genera confianza entre clientes y socios comerciales (Rodriguez, et al., 2020).

1.3.3.1. Funcionamiento de la norma

La norma ISO 27001 se centra en la identificación y prevención de posibles amenazas que puedan afectar la integridad de la información. Su enfoque principal, se basa en la gestión

de riesgos: se investiga la ubicación y naturaleza de los riesgos, seguido por un tratamiento sistemático de los mismos (Al Hadad y Maulana, 2023). Esto implica un proceso exhaustivo de análisis y acción para salvaguardar la información de manera efectiva.

1.3.3.2. Beneficios de la norma 27001

Los beneficios fundamentales que la norma ISO 27001 brinda a una organización incluyen:

- **Cumplimiento de requisitos legales:** La implementación de la norma ISO 27001 ayuda a las empresas a cumplir con las regulaciones y leyes relacionadas con la seguridad de la información. Esto es crucial en un entorno gubernamental donde la protección de los datos y la privacidad se han vuelto cada vez más importantes y están sujetos a estrictos requisitos legales.
- **Obtención de una ventaja competitiva:** La certificación ISO 27001 puede diferenciarlo de sus competidores, demuestra el compromiso de la organización con la seguridad de la información y puede ser un factor decisivo para los habitantes que buscan que sus gobernantes (GAD Municipal) sean confiables y seguros (Eskaluspita, 2020).
- **Reducción de costos:** La implementación de una planificación adecuada ayuda a reducir los costos relacionados con incidentes de seguridad, como violaciones de datos o pérdida de información. Además, al mejorar la eficiencia y la efectividad de los procesos relacionados con la seguridad de la información, la institución puede lograr ahorros a largo plazo.
- **Mejora en la organización empresarial:** Fomenta una cultura de seguridad dentro de la organización al establecer procesos y controles claros para proteger la información. Esto conduce a una mayor organización y coherencia en la forma en que se gestionan y protegen los activos de información, lo que a su vez contribuye a una mejor gestión general (Eskaluspita, 2020).

1.3.4. Análisis FODA

El análisis FODA es un componente clave de la planificación estratégica, ya que permite identificar las amenazas a través de las oportunidades, lo que facilita la toma de decisiones en una Institución gubernamental (Barragán y González, 2020).

Este enfoque puede ser utilizado en una amplia variedad de contextos, tanto para individuos como para instituciones en proceso de análisis. Permite identificar las posiciones, oportunidades, debilidades y amenazas, lo que facilita el diagnóstico y se convierte en una herramienta valiosa. Los pasos a seguir para llevar a cabo un análisis FODA se pueden resumir de la siguiente manera (Vega, et al., 2022):

- Identificar las oportunidades externas clave que afectan a la organización.
- Identificar las amenazas externas clave que enfrenta la organización.
- Enumerar las principales fortalezas internas de la organización.
- Identificar las debilidades internas principales de la organización.
- Identificar las estrategias FO al combinar las fortalezas con oportunidades.
- Determinar las estrategias DO fusionando las debilidades con las oportunidades.
- Determinar las estrategias FA fusionando las fortalezas con las amenazas.
- Determinar las estrategias DA fusionando las debilidades con las amenazas.

1.3.5. Plan de acción

El plan de acción es una herramienta administrativa clave que consiste en un conjunto de acciones priorizadas destinadas a alcanzar un objetivo específico. Esta herramienta representa la fase operativa del plan estratégico, donde se implementan las estrategias previamente definidas para lograr los objetivos establecidos (Tognoli, et al., 2020). En el contexto de la seguridad de la información, el plan de acción detalla las medidas necesarias para la protección de riesgos y vulnerabilidades, asegurando así la integridad y confidencialidad de los datos.

1.4. Marco contextual

1.4.1. Seguridad de la información en la unidad de TIC's

En el contexto actual, las TI son fundamentales para las instituciones gubernamentales, especialmente en la protección de la información y la gestión adecuada de los datos. El GAD Municipal del Cantón Paute busca convertirse en una "ciudad" tecnológica y segura, lo que plantea desafíos en la seguridad de la información y la gestión de riesgos. Este trabajo de integración curricular se enfoca en elaborar un plan estratégico para fortalecer la seguridad de la información en la Unidad de TIC´s, siguiendo las tendencias y estándares internacionales en seguridad de la información. La seguridad de la información es una preocupación creciente en el ámbito gubernamental, dado el aumento de los ataques y amenazas cibernéticas.

En este sentido, el diseño de un PESI para la Unidad de TIC´s no solo es necesario para proteger la integridad, confidencialidad y disponibilidad de la información, sino también para garantizar la eficiencia en la prestación de servicios públicos. Este enfoque está alineado con las metas institucionales de convertir a Paute en un cantón tecnológicamente avanzado y seguro.

La importancia de este trabajo radica en su impacto directo en la comunidad de Paute. Al fortalecer la seguridad de la información en la Unidad de TIC´s, se contribuirá a la protección de los datos de los ciudadanos, garantizando un servicio público eficiente y seguro. Además, al seguir estándares internacionales en seguridad de la información, el GAD Municipal del Cantón Paute estará en una posición favorable para enfrentar los desafíos tecnológicos futuros y mantener la confianza de sus ciudadanos.

MARCO METODOLÓGICO

CAPÍTULO II

Capítulo II: Metodología del proceso de investigación

1.1. Enfoque de la investigación

El enfoque de la investigación adoptado para este trabajo fue cualitativo, siguiendo las definiciones y directrices establecidas por Hernández y Mendoza (2020). Este enfoque se caracterizó por la búsqueda de una comprensión profunda y detallada de los fenómenos observados, permitiendo explorar las experiencias y percepciones de los involucrados en la gestión de la seguridad de la información dentro de la Unidad de TIC´s del GAD Municipal del Cantón Paute.

La investigación cualitativa se centró en el análisis interpretativo de la realidad social, lo que permitió abordar las complejidades y particularidades del contexto específico del cantón Paute. A través de este enfoque, se buscó captar la riqueza y diversidad de opiniones, actitudes y comportamientos relacionados con la seguridad de la información en la Unidad de TIC's. García y Sánchez (2020) destacan que la investigación cualitativa se orienta hacia la comprensión de los significados y las interacciones sociales, lo cual fue fundamental para identificar las necesidades, riesgos y vulnerabilidades específicos de esta entidad gubernamental.

También, esta se enfocó en entender los fenómenos a través de la visión de los participantes, analizando en profundidad sus experiencias, percepciones y motivaciones (Piña, 2023). Además, este enfoque facilitó la recolección de datos mediante la técnica de las entrevistas, proporcionando una visión holística y contextualizada de los problemas y desafíos que enfrenta la Unidad de TIC's del GAD Municipal de Paute.

La elección del enfoque cualitativo se justificó por la necesidad de comprender en profundidad cómo se gestiona la seguridad de la información, así como por la importancia de captar las percepciones y experiencias de los funcionarios y responsables de TI. Esta

comprensión permitió identificar las áreas críticas y elaborar un plan estratégico que respondiera de manera efectiva a las particularidades del contexto local.

1.2. Alcance de la investigación

El alcance de la investigación adoptado para el trabajo de integración curricular es exploratorio y descriptivo. Este enfoque es adecuado porque se busca entender y describir detalladamente la situación actual de la seguridad de la información en la Unidad de TIC's.

Exploratorio porque permite identificar y descubrir aspectos clave sobre las prácticas, percepciones y desafíos que enfrenta la Unidad de TIC's en su gestión de la seguridad de la información. Al no haber suficiente información previa específica sobre este contexto, la investigación exploratoria ayuda a establecer una base sólida para futuros estudios más detallados.

El enfoque exploratorio se emplea para obtener una visión general del problema de investigación (Amaíz & Flores, 2021)

Por otro lado, el enfoque descriptivo complementa la exploración al proporcionar una descripción clara y precisa de los fenómenos observados. Mediante el uso de entrevistas y encuestas cualitativas, se recolectaron datos que permitieron describir cómo se gestionan actualmente los riesgos y vulnerabilidades en la seguridad de la información.

El enfoque descriptivo permite detallar y caracterizar un fenómeno o población específica, ofreciendo una imagen clara y precisa del objeto de estudio (Valle, Manrique, & Revilla, 2022).

El alcance de la investigación fue descriptivo, alineándose con la definición propuesta por Hernández y Mendoza (2020). Este tipo de investigación se centró en especificar las propiedades, características y perfiles de las personas, eventos, comunidades o cualquier otro fenómeno que se someta a análisis. En el caso de la Unidad de TIC´s del GAD Municipal del

Cantón Paute, la investigación descriptiva permitió delinear claramente la situación actual de la seguridad de la información en su Unidad de TIC's.

La elección de un alcance descriptivo se justificó por la necesidad de proporcionar una visión detallada y precisa de los elementos y procesos involucrados en la gestión de la seguridad de la información. Se buscó documentar el estado actual, identificar las prácticas vigentes, y señalar las fortalezas y debilidades existentes.

Este enfoque permitió obtener una comprensión exhaustiva y objetiva de cómo se manejaban los riesgos y vulnerabilidades, así como de las medidas de seguridad implementadas. A través de la investigación descriptiva, se recolectaron datos cualitativos que facilitaron la elaboración de un panorama integral de la seguridad de la información en la institución.

Este tipo de investigación no solo se enfocó en describir el estado de las prácticas de seguridad, sino también en proporcionar una base sólida sobre la cual se pudieran desarrollar estrategias futuras (Valle, et al., 2022). Al detallar los elementos específicos y las circunstancias particulares de la Unidad de TIC´s del GAD Municipal de Paute, la investigación ofreció una imagen clara y completa que fue esencial para la formulación de recomendaciones y planes de acción concretos.

1.3. Delimitación de la investigación

La investigación se centró en especificar claramente los límites y alcances del estudio, asegurando que el análisis se mantuviera enfocado y manejable. Esta investigación se circunscribió al ámbito del GAD Municipal del Cantón Paute, específicamente a su Unidad de TIC's. Se buscó fortalecer la seguridad de la información dentro de este contexto particular, excluyendo otros departamentos y entidades municipales.

El periodo temporal considerado abarcó desde febrero 2024 hasta julio del año 2024. Este lapso permitió obtener datos relevantes y actualizados, reflejando tanto la situación previa

a la implementación de nuevas políticas como los cambios introducidos durante el proceso de reestructuración de la Unidad de TIC's. La elección de este periodo se basó en la necesidad de capturar una visión completa y dinámica de la evolución de la seguridad de la información.

En términos geográficos, la investigación se limitó al cantón Paute, ubicado en la provincia de Azuay, Ecuador. Esta delimitación geográfica fue crucial para contextualizar los hallazgos y recomendaciones, tomando en cuenta las características específicas y necesidades locales. Al enfocar el estudio en esta área, se garantizó que las estrategias desarrolladas fueran directamente aplicables y relevantes para el entorno de la Unidad de TIC’s.

Así mismo, la investigación también se restringió a la evaluación y diseño de estrategias basadas en un estándar internacional de seguridad de la información, como ISO 27001. Este enfoque permitió asegurar que las recomendaciones estuvieran alineadas con las mejores prácticas internacionales, proporcionando un plan estratégico robusto y reconocido para fortalecer la seguridad de la información.

Finalmente, la investigación se delimitó a la evaluación de prácticas, políticas y tecnologías actualmente implementadas en la Unidad de TIC's, excluyendo áreas como la formación y capacitación del personal fuera del ámbito de TI. Esta delimitación ayudó a mantener un enfoque claro y específico, facilitando un análisis detallado y la formulación de estrategias directamente aplicables a las necesidades de la unidad en cuestión.

1.4. Población

Para el presente estudio, se definió como población a los integrantes de la Unidad de TIC's del GAD Municipal del Cantón Paute, conformado por dos personas. La elección de esta población fue fundamental para obtener información precisa y detallada sobre la gestión de la seguridad de la información en esta unidad específica.

Al centrarse en los dos miembros de la Unidad de TIC's, se garantizó una comprensión profunda y directa de las prácticas actuales, desafíos y necesidades en materia de seguridad de la información.

1.5. Muestra

Debido al reducido tamaño de la población, no fue necesario realizar un muestreo, ya que se pudo acceder a todos los integrantes sin restricción. La población, compuesta por los dos miembros de la Unidad de TIC's del GAD Municipal del Cantón Paute, como se evidencia en la Tabla2, se convirtió directamente en la muestra para este estudio.

Tabla 2

Distribución de la muestra

Cargo	Cantidad
Jefe de la Unidad de TIC´s	1
Desarrollador	1
Total	2

Nota. Esta tabla muestra la distribución de la muestra de estudio.

1.6. Métodos empleados

1.6.1. Encuesta

Los métodos empleados en esta investigación se centraron en una encuesta cualitativa, una técnica fundamental que, según Hernández y Mendoza (2020) la investigación cualitativa es una herramienta de investigación que utiliza preguntas abiertas para comprender las opiniones, experiencias, narrativas o historias de los encuestados.

Este tipo de encuesta es útil para generar información en una conversación, identificando temas iniciales o preguntas que se explorarán más adelante en la encuesta. La encuesta cualitativa requiere opiniones, puntos de vista, sugerencias y otros tipos de

respuestas que no son tan fáciles de categorizar y contar como números que permita obtener datos valiosos.

La encuesta realizada incluyó un total de 59 preguntas abiertas, que se evidencia en el Anexo5, diseñadas para explorar diversas variables críticas para la seguridad de la información. Estas preguntas abiertas permitieron a los entrevistados proporcionar respuestas amplias y detalladas, ofreciendo una comprensión profunda de sus percepciones y experiencias.

Una de las variables abordadas fue el entendimiento básico de la seguridad de la información y las normativas relacionadas. A través de las preguntas, se descubrió que, aunque los integrantes de la unidad tenían un conocimiento general de la seguridad de la información, carecían de un entendimiento profundo sobre la norma ISO 27001 y la ley de protección de datos. Esta falta de conocimiento representaba un área de mejora crítica para la unidad.

Otro aspecto importante fue la actualización de licencias y la evaluación de riesgos. Las entrevistas revelaron que existían problemas significativos en la actualización regular de licencias y en la implementación de evaluaciones de riesgos sistemáticas. Aunque se aplicaban algunas políticas de seguridad, como el uso de un firewall y medidas de protección en la nube, estas no eran suficientes para garantizar una seguridad robusta y actualizada.

Las preguntas también exploraron variables relacionadas con los usuarios, incluyendo prácticas de autentificación y autorización. Se examinó cómo se gestionaban los accesos y permisos dentro de la unidad, identificando posibles vulnerabilidades y áreas donde se necesitaban mejoras en los procedimientos de control de acceso.

La administración de sistemas y equipos informáticos fue otra área clave investigada. Se evaluaron los procesos de mantenimiento y gestión de los sistemas, así como el estado de los equipos informáticos utilizados. Las entrevistas destacaron la necesidad de una

administración más proactiva y regular para asegurar el funcionamiento eficiente y seguro de los sistemas.

Los activos fijos y el estado físico actual de la Unidad de TIC's también fueron examinados. Las respuestas proporcionaron información valiosa sobre la infraestructura existente, identificando debilidades en el mantenimiento y la actualización de los activos físicos que podrían comprometer la seguridad de la información.

1.6.2. Entrevista

Para Hernández y Mendoza (2020), es un proceso de comunicación o interacción orientado a obtener información relevante sobre el tema de estudio a través de preguntas formuladas por el entrevistador al entrevistado, que se evidencian en el Anexo4.

Este método permitió recopilar datos detallados y específicos sobre la situación de la seguridad de la información en la Unidad de TIC's del GAD Municipal del Cantón Paute. Las entrevistas realizadas incluyeron un total de 7 preguntas abiertas, diseñadas para explorar diversas variables críticas para la seguridad de la información, adicional se realizaron acuerdos con el personal que se evidencian en el Anexo1 y el Anexo2.

1.7. Análisis de datos

El análisis de datos en esta investigación se estructuró meticulosamente para asegurar una interpretación precisa y significativa de la información recopilada. Inicialmente, se realizó la tabulación de los datos obtenidos a través de las entrevistas, lo que permitió organizar y resumir las respuestas de manera sistemática. La tabulación facilitó la identificación de patrones y tendencias, proporcionando una visión general de las percepciones y experiencias de los integrantes de la Unidad de TIC's del GAD Municipal del Cantón Paute.

Posteriormente, se llevó a cabo la codificación de la información cualitativa. Este proceso implicó categorizar y etiquetar las respuestas en temas y subtemas específicos, lo que

ayudó a descomponer la información en unidades manejables. La codificación permitió una comprensión más detallada y profunda de los datos, destacando aspectos clave como el entendimiento de la seguridad de la información, las prácticas de actualización de licencias, la evaluación de riesgos, y las políticas de seguridad implementadas. Este enfoque sistemático facilitó el análisis de las variables críticas y reveló áreas de mejora y fortalezas dentro de la unidad.

Para complementar este análisis, se utilizó la matriz FODA (Fortalezas, Oportunidades, Debilidades y Amenazas). Esta herramienta estratégica permitió evaluar tanto los factores internos como externos que afectan la seguridad de la información en la Unidad de TIC's. Las fortalezas identificadas incluyeron la aplicación de políticas de seguridad como el uso de firewalls y medidas en la nube, mientras que las debilidades señalaron la falta de conocimiento sobre la norma ISO 27001 y la ley de protección de datos, así como problemas en la actualización de licencias y la evaluación de riesgos.

Las oportunidades destacadas en el análisis FODA incluyeron la posibilidad de mejorar la capacitación del personal y la implementación de estándares internacionales de seguridad, como la ISO 27001. Las amenazas se relacionaron con la creciente complejidad de las amenazas informáticas y la falta de recursos adecuados para enfrentar estos desafíos de manera efectiva.

ANÁLISIS E INTERPRETACIÓN DE LOS RESULTADOS

CAPÍTULO III

Capítulo III: Análisis e interpretación de resultados de la investigación

2.1. Descripción de los resultados

2.1.1. Fase 1: Visión

Actualmente, con el avance constante de las TIC, las instituciones públicas tienen que adaptarse a los cambios para mejorar la utilidad de los servicios prestados a los ciudadanos, como por ejemplo la introducción de páginas web o plataformas digitales que les permitan hacer lo correcto en el cumplimiento de las obligaciones como ciudadano y con el fin de brindar servicios de calidad con estándares internacionales.

Cabe mencionar que, considerando los resultados obtenidos, mediante las entrevistas y encuestas realizadas al jefe de la Unidad de TIC´s y al desarrollador de la Unidad de TIC´s, se logró verificar varios aspectos muy importantes relacionados con la gestión de la seguridad de la información. Los aspectos de seguridad críticos encontrados: la falta de organización y carencia de buenas prácticas, evidenciándose la mala organización en la sala de servidores, gestión de claves se realizan anualmente, inexistencia de procesos de seguridad adecuados, falta de auditorías informáticas, dependencia de sistemas de proveedores externos, falta de personal, presupuestos limitados, equipos informáticos en mal estado.

Además, este proceso también incluye nuevas tecnologías estrechamente relacionadas con oportunidades que parten de la implementación de estándares internacionales, capacitación continua del personal, inversión en infraestructura, desarrollo de un plan estratégico, auditorias regulares.

Por otro lado, frente a amenazas se denoto que en el departamento en los últimos tiempos persiste incremento de ataques cibernéticos evolución de amenazas constantes, falta

de recursos, incumplimiento a los reglamentos regulatorios, amenazas internas y falta de capacitación continua.

2.1.2. Fase 2: Situación actual - Análisis de la población

2.1.2.1. Entrevistas.

Esta técnica ayudó a recopilar información importante y es utilizada principalmente frente al jefe y desarrollador de la Unidad de TIC's. Para obtener más información, se aplicó este instrumento en diferentes fechas y horas en las que no había contaminación de ningún tipo en cuanto a la dimensión ambiental (es decir, se intentó minimizar que las partes no respondieran de la misma manera)

Fecha de la entrevista 1: 15/03/2024

Entrevistado: Jefe de la Unidad de TIC 's

- **¿En qué norma o estándar basan sus procesos y controles?**

  Actualmente no hemos adoptado ninguna norma.

- **¿Mejoras que se han realizado en esta administración en cuanto a la seguridad de la información?**

  En cuanto a las mejoras se han realizado monitoreos esporádicos (antes no se realizaban), y en cuanto a los equipos se han corregido las fallas técnicas que han surgido eventualmente.

- **¿Existe algún plan estratégico?**

  Actualmente no existe ningún plan estratégico

- **¿Como es la seguridad de la información para la Unidad de TIC´s del GAD Municipal?**

La verdad no es tan buena, puesto que aún estamos en proceso de adecuación de las nuevas tecnologías, pero el presupuesto limitado no permite darle la adecuada inversión en la seguridad de la información por los elevados costos.

- **¿Cuáles son las herramientas tecnológicas manejadas que sustentan la seguridad de la información?**

  No se manejan herramientas especializadas en la seguridad de la información, solo se adaptaron las actividades a usar tecnologías donde las mismas eran manuales y ahora se puede realizar de manera más fácil y ágil.

- **¿Falencias encontradas hasta el momento en el uso de las TIC´s frente a la seguridad de la información?**

  En la actualidad, no manejamos procesos estandarizados, no se le da la importancia necesaria a la seguridad de la información, falta de presupuesto para equipos tecnológicos y dependemos de externos.

- **¿Beneficios encontrados hasta el momento en el uso de las TIC's frente a la seguridad de la información?**

  Ahorro de tiempo, dinero y seguridad de los datos o actividades manejadas.

Fecha de la entrevista 2: 17/05/2024

Entrevistado:

  - Desarrollador de la Unidad de TIC´s

- **¿En qué norma o estándar basan sus procesos y controles?**

  No manejamos los procesos de forma estandarizada

- **¿Mejoras que se han realizado en esta administración en cuanto a la seguridad de la información?**

  Se comenzaron a realizar monitoreos cada cierto tiempo.

- **¿Existe algún plan de estratégico?**

  Actualmente la unidad no tiene ningún plan.

- **¿Cómo es la seguridad de la información para la Unidad de TIC´s?**

Debería mejorarse, puesto que no le damos aun la importancia necesaria a la seguridad de la información.

- **¿Cuáles son las herramientas tecnológicas manejadas que sustentan la seguridad de la información?**

  Solo tenemos un firewall y dependemos de proveedores externos

- **¿Falencias encontradas hasta el momento en el uso de los TIC´s frente a la seguridad de la información?**

  Desorganización en el data center, equipos en mal estado, falta de personal adecuado para las diferentes necesidades de la unidad de TIC´s

- **¿Beneficios encontrados hasta el momento en el uso de las TIC´s frente a la seguridad de la información?**

  Nos permite salvaguardar la información y reaccionar de forma ante problemáticas o amenazas externas.

2.1.2.2. Encuesta.

Con la finalidad de evaluar el estado actual de la seguridad de la información en la Unidad de TIC´s, se realizó una encuesta cualitativa al personal de la Unidad de TIC´s del Gad

municipal. Puesto que esta herramienta, fue diseñada con preguntas abiertas, permitió a los encuestados brindar respuestas personales y únicas. Este tipo de datos es muy valioso para la investigación dado que proporciona un rico contexto de conocimiento, experiencia y profundidad que normalmente no se encuentran en los datos numéricos.

La encuesta fue ejecutada al jefe y al desarrollador de la Unidad de TIC 's, que brindaron información importante desde varios ángulos de las cuales se deriva el tema de interés, lo cual permitió tener un conocimiento más profundo del tema de investigación en curso. Por lo tanto, en comparación con los datos proporcionados, el encuestado manifestó las siguientes opiniones, visibles en la Tabla3, Tabla4, Tabla5, Tabla6, Tabla7, Tabla8, Tabla9, las cuales se explican sin ningún cambio ni manipulación de información:

1. **A modo general**

Tabla 3

Resultados de la encuesta, variable: modo general.

Cargo	Cantidad
Jefe de la Unidad de TIC's	**1**
1. ¿Cuál es su nivel de conocimiento sobre la seguridad de información?	Lo que respecta a la seguridad de Tic, poseo un conocimiento normal sobre dicho tema.
2. ¿Qué conocimientos posee sobre las normas que regulan la seguridad de la información?	En cuanto a la norma de seguridad de Tic, mi nivel de conocimiento es regular.
3. ¿Cuál es su nivel de comprensión respecto a la norma ISO 27001?	Poseo un conocimiento limitado sobre la norma ISO 27001.
4. ¿Cuánta información sabe acerca de la ley de protección de los datos?	Tengo un conocimiento limitado con la legislación de protección de los datos.
5. ¿Qué equipos de cómputo tienen las licencias actualizadas?	No, las licencias de los equipos de cómputo no están vigentes.
6. ¿Qué nivel de seguridad cumplen los mecanismos de acceso al sistema?	La seguridad para el acceso al sistema se considera de nivel intermedio
7. ¿Está toda la información necesaria para los usuarios autorizados plenamente accesible?	Toda la información para los usuarios del sistema es única.
8. ¿Se evidencia algún tipo de filtración de información fuera del departamento?	No se detecta la filtración de información, incluidos los activos informáticos.

9. ¿Los procedimientos actuales cuentan con una documentación exhaustiva y siempre disponible?	Los procedimientos están documentados y siempre accesibles.
10. ¿Se aplican actualmente políticas de seguridad para administrar las informaciones ser así, ¿Cuáles son?	Si mediante Firewall y seguridad de disco en la nube.
11. ¿Se realiza una gestión de riesgos en cuenta a la seguridad de la información?	Actualmente no se está llevando a cabo una evaluación de riesgos en base a la seguridad de información.

Nota. La tabla muestra las opiniones del entrevistado. Fuente: Elaborado por los autores.

2. **Usuarios**

Tabla 4

Resultados de la encuesta, variable: usuarios.

Cargo	**Cantidad**
Jefe de la Unidad de TIC's	**1**
1. ¿Hay una persona designada exclusivamente para la creación de cuentas de usuario?	Si solo es una persona que tiene la responsabilidad de crear cuentas de usuario.
2. ¿Se mantiene un registro de los usuarios que han sido creados?	No se conserva un registro completo de todos los usuarios creados.
3. ¿Se realiza el bloqueo de las cuentas de usuario durante las vacaciones o cuando un empleado deja la empresa?	Las cuentas de usuario de los empleados en vacaciones no son bloqueadas, pero se realiza un seguimiento para bloquear las cuentas de los empleados que dejan la empresa.
4. ¿Es necesario solicitar permiso para crear cuentas de usuario?	Se requiere obtener permiso previo para crear nuevas cuentas de usuario.
5. ¿Las contraseñas tienen fecha de caducidad?	Se establece un período de tiempo después del cual las contraseñas creadas expiran.
6. ¿Se establecen responsabilidades a los usuarios en cuanto al uso adecuado de los recursos?	Se asignan responsabilidades a los usuarios en cuanto al uso apropiado de los recursos.
7. ¿Se implementa algún control para prevenir el acceso no autorizado a los equipos y sistemas de la empresa?	Actualmente se cuenta con un control para evitar el acceso no autorizado a los sistemas y equipos de la empresa.

Nota. La tabla muestra las opiniones del entrevistado. Fuente: Elaborado por los autores.

3. **Autenticación**

Tabla 5

Resultados de la encuesta, variable: autenticación.

Cargo	Cantidad
Jefe de la Unidad de TIC's	**1**
1. ¿Se utiliza una contraseña genérica para los nuevos usuarios?	Al crear una cuenta en un sistema determinado, se asigna una contraseña genérica para el primer ingreso del usuario
2. ¿Está especificado el tamaño y la complejidad de la contraseña?	La contraseña se define según la preferencia del usuario.
3. ¿El usuario se bloquea después de ingresar una contraseña incorrecta?	Después de tres intentos fallidos, la cuenta del usuario se bloquea.
4. ¿Los usuarios pueden acceder al sistema desde cualquier dispositivo?	En algunos casos los usuarios complementan su trabajo desde otro lugar que no sea la empresa
5. ¿Es posible acceder al sistema desde otro dispositivo si el usuario ya está conectado?	Se permite el acceso desde múltiples dispositivos simultáneamente.

Nota. La tabla muestra las opiniones del entrevistado. Fuente: Elaborado por los autores.

4. **Autorización**

Tabla 6

Resultados de la encuesta, variable: autorización.

Cargo	Cantidad
Jefe de la Unidad de TIC's	**1**
1. ¿Los usuarios tienen permiso para actualizar o alterar la base de datos?	Los usuarios no poseen ningún permiso para hacer ninguna modificación, consulta o modificación en la base de datos.
2. ¿Están claramente definidos los permisos para cada usuario?	Si se tiene definido el control sobre los permisos para cada usuario.
3. ¿Se requiere autorización para cambiar el usuario o la contraseña?	El usuario es responsable de realizar sus propios cambios.
4. ¿Está permitido el acceso a sitios web no institucionales?	El acceso está controlado por Lista de Control de Acceso.
5. ¿Está permitido el acceso a sitios web no institucionales?	Si porque no existe ninguna política de la institución que prohíba eso.

Nota. La tabla muestra las opiniones del entrevistado. Fuente: Elaborado por los autores.

5. **Administración de sistemas**

Tabla 7

Resultados de la encuesta, variable: administración de sistemas.

Cargo	Cantidad
Jefe de la Unidad de TIC's	**1**
1. ¿El administrador puede realizar cambios en la Base de Datos (BDD)?	Si, solo y únicamente el administrador puede manejarla base de datos.
2. ¿Las sesiones de todos los usuarios están en estado activo durante los periodos de inactividad?	No, las sesiones están configuradas para expirar después de un periodo de inactividad.
3. ¿Existen controles de acceso a los Backups para el Administrador de Base de Datos?	No se tiene personal exclusivo solo para el manejo en el área de Base de Datos.
4. ¿Los usuarios pueden extraer información mediante dispositivos externos?	Por el momento no contamos con un sistema de bloqueo contra dispositivos extraíbles.
5. ¿Existe un algún tipo de seguimiento de todas las personas autorizadas para realizar los respaldos del sistema de Gad?	Si, está documentado las personas responsables de realizar los respaldos.
6. ¿Han realizado en la unidad de TIC´s simulacros para enfrentar la caída de los sistemas de información y comunicación? Si es así, ¿cómo se han realizado? Si no, ¿por qué?	No se ha realizado ningún simulacro.
7. ¿Se monitorean los sistemas de información que gestionan?	Los sistemas internos son controlados al igual que los externos que gestión la información si monitorean y controlan el sistema (ODOO, SIGAME, SAGA).

Nota. La tabla muestra las opiniones del entrevistado. Fuente: Elaborado por los autores.

6. Equipos informáticos

Tabla 8

Resultados de la encuesta, variable: equipos informáticos.

Cargo	Cantidad
Jefe de la Unidad de TIC's	**1**
1. ¿Los equipos cuentan con suficiente memoria para ejecutar los programas y aplicaciones necesarias de manera eficiente?	Siempre antes de otorgar un equipo se hace un análisis para realizar la compra.
2. ¿Todos los procedimientos relacionados con los equipos están documentados?	Si, tenemos los procedimientos para el resguardo de los activos fijos.
3. ¿Se lleva a cabo un mantenimiento periódico de los equipos?	Sí, aunque no existe un cronograma fijo para mantenimiento de equipos.
4. ¿Los usuarios tienen permiso para abrir o destapar los equipos de cómputo asignados?	Se les comunica a los usuarios que poseen los equipos propios de GAD, solo el personal técnico autorizado puede abrir los equipos.

Nota. La tabla muestra las opiniones del entrevistado. Fuente: Elaborado por los autores.

7. Activos fijos

Tabla 9

Resultados de la encuesta, variable: activos fijos.

Cargo	Cantidad
Jefe de la Unidad de TIC's	**1**
1. ¿Los registros de activos fijos contienen la información y detalles necesarios?	Sí, se intenta incluir toda la información relevante para una mejor identificación de los activos.
2. ¿Qué políticas o reglas se aplican para la autorización de retiro, destrucción, adquisición o venta de activos fijos?	No están las políticas o procesos bien definidos.
3. ¿Se realiza periódicamente un inventario físico o digital de los activos fijos para verificar su existencia y estado?	Si algunas veces se realiza.
4. ¿Las personas responsables de los activos fijos están comprometidas reportar cualquier cambio o daño que suceda con el software?	Sí, durante las entregas se les informa que deben reportar cualquier defecto o daño a la Unidad de TIC 's para su reposición.
5. ¿La venta de activos fijos del departamento de la Unidad de TIC 's requiere autorización previa de los directivos?	Siempre la Gerencia General debe aprobar o autorizar la baja de activos.
6. ¿Se dispone de información sistematizada y actualizada del inventario de activos fijos de la empresa?	No se cuenta con personal encargado para realizar esta tarea, pero si se lo realiza cada cierto tiempo.
7. ¿El inventario está segmentado por áreas?	Sí, está por áreas para un mejor control.
8. ¿Se ha realizado procesos específicos para los registros de resguardo de activos de altas, bajas y la toma física de todos los inventarios?	Existen procesos para el manejo de activos, pero no para las bajas y la toma física de todos los inventarios.
9. ¿Se tiene una base de datos o algún programa que estén los inventarios de los activos fijos?	Actualmente no, eso por el momento se controla en una hoja de cálculo.
10. ¿Se mantiene un registro actualizado de los ingresos de activos de los proveedores?	No existe un control interno específico; se depende de la contabilidad.
11. ¿Existe el personal capacitado para controlar los activos fijos?	Si existe un personal capacitado para controlar los activos.
12. ¿Es necesario implantar un proceso adecuado para el control de los activos fijos?	Sí, es esencial tener un control adecuado de cada activo fijo.

Nota. La tabla muestra las opiniones del entrevistado. Fuente: Elaborado por los autores.

2.2. Análisis de los Resultados

2.2.1. Entrevistas

Las entrevistas realizadas revelan importantes carencias en la gestión de la seguridad de la información dentro de la Unidad de TIC's del GAD Municipal del Cantón Paute. Tanto el Jefe de la Unidad como el Desarrollador destacaron la ausencia de normas o estándares que guíen los procesos y controles, lo que implica una falta de estandarización y de un marco sólido que garantice la protección de la información. Este problema es agravado por la inexistencia de un plan estratégico, lo cual refleja una dirección poco clara y esfuerzos dispersos en la implementación de medidas de seguridad.

Además, los recursos tecnológicos actuales son limitados y no especializados en seguridad de la información, lo que obliga a la unidad a depender de proveedores externos. Este hecho, junto con la desorganización en el data center y la falta de personal especializado, indica que la infraestructura y el personal actual no están preparados para manejar de manera efectiva las amenazas a la seguridad de la información. Estos problemas estructurales dificultan la capacidad de la Unidad para salvaguardar los datos y reaccionar ante incidentes de seguridad.

En conclusión, las respuestas obtenidas subrayan la urgencia de implementar un plan estratégico integral, alineado con estándares internacionales como la ISO 27001. A pesar de algunos esfuerzos recientes, las deficiencias identificadas ponen en riesgo la integridad, confidencialidad y disponibilidad de la información crítica manejada por la Unidad de TIC's. La adopción de un enfoque más estructurado y la inversión en herramientas y personal especializado son esenciales para fortalecer la seguridad de la información en la institución.

2.2.2. Encuestas

Las respuestas obtenidas de la encuesta cualitativa aplicada al personal de la Unidad de TIC's del GAD Municipal de Paute revelan una serie de desafíos críticos en la gestión de la seguridad de la información. Uno de los aspectos más preocupantes es la falta de estandarización en los procesos, lo cual es fundamental para garantizar la consistencia y la eficacia en la protección de la información. La encuesta muestra que, aunque se han implementado algunos controles, estos no siguen un marco normativo reconocido, como la ISO 27001, lo que limita su efectividad y aumenta la vulnerabilidad frente a posibles amenazas.

El conocimiento limitado del personal sobre normas y estándares de seguridad de la información también contribuye a esta deficiencia, lo que evidencia una necesidad urgente de capacitación y concientización en esta área. Por otro lado, la administración de usuarios y la gestión de activos fijos también presentan problemas significativos. El control sobre las cuentas de usuario no es exhaustivo, lo que podría llevar a accesos no autorizados y poner en riesgo la información crítica. Asimismo, la gestión de activos fijos carece de políticas claras y procedimientos bien definidos para la baja, retiro o destrucción de estos, lo que podría derivar en pérdidas financieras y en la exposición innecesaria de datos sensibles. Aunque existen procedimientos documentados para algunos aspectos, como el mantenimiento de equipos, la falta de un cronograma fijo y de personal exclusivamente dedicado a estas tareas revela una administración reactiva más que preventiva.

Finalmente, el análisis también destaca la insuficiencia de prácticas de monitoreo y mantenimiento de los sistemas de TI, lo que podría comprometer la disponibilidad y confiabilidad de los servicios prestados por la unidad. No se realizan simulacros de caída de sistemas, lo que sugiere una falta de preparación ante posibles incidentes, y el mantenimiento

de los equipos, aunque se realiza, no sigue un plan estructurado, lo que puede conducir a fallas imprevistas.

Estas observaciones subrayan la necesidad de un plan estratégico robusto que aborde estas carencias y fortalezca las capacidades de la Unidad de TIC's, alineando sus prácticas con los estándares internacionales de seguridad de la información para garantizar una operación más segura y eficiente.

2.3. Discusión

En el contexto actual de evolución constante de las tecnologías de la información y la comunicación (TIC), las autoridades públicas deben adaptarse a estos cambios para cumplir con las misiones y objetivos establecidos. Los resultados de esta investigación subrayan la importancia de implementar buenas prácticas en la gestión de la seguridad de la información, con el fin de asegurar la continuidad de los servicios y mitigar los riesgos a los que están expuestos. La introducción de estas prácticas permite no solo identificar áreas de mejora y control, sino también tomar acciones correctivas de manera oportuna y efectiva, alineándose con lo planteado por Muñoz (2022), quien destaca la necesidad de leyes, regulaciones y estándares para respaldar una base confiable en la toma de decisiones dentro de las organizaciones.

Los resultados reflejan cómo las TIC se convierten en herramientas clave para el desarrollo integral, especialmente en la optimización de servicios a la ciudadanía. La decisión de adquirir nuevos equipos para mejorar la seguridad de la información y prever posibles vulnerabilidades demuestra el enfoque en mejorar la comunicación entre los municipios y la sociedad, tal como lo menciona Guaman (2022). Las TIC, al estar estrechamente vinculadas con la seguridad de la información, mejoran los procesos internos de las instituciones públicas y permiten a los ciudadanos un mejor acceso a servicios y programas.

Es evidente que la gestión empírica o basada en la experiencia previa no garantiza la seguridad de la información, especialmente en un entorno como el de la Unidad de TIC's, donde el volumen de datos manejados es considerablemente alto. Los resultados de esta investigación destacan la necesidad de monitorear la seguridad, gestionar adecuadamente los respaldos y utilizar las TIC como un recurso clave para garantizar una gestión de seguridad eficiente. La importancia de la administración en la seguridad de la información, resaltada por Pino (2022), se refleja en la capacidad de la administración pública para innovar, mejorar resultados y, en última instancia, crear valor público y mejorar la calidad de vida de los ciudadanos.

Finalmente, se concluye que un plan estratégico de seguridad de la información no solo mitiga los riesgos críticos, sino que también fomenta un sentido de pertenencia y compromiso entre el personal involucrado, permitiendo su participación activa en las diferentes etapas del desarrollo de dicho plan, tal como se detalla en el Anexo 9, para abordar los riesgos identificados en los procesos, infraestructura y sistemas de la Unidad de TIC's.

CONCLUSIONES

El trabajo de integración curricular comenzó con una revisión exhaustiva de estudios académicos y conceptos fundamentales sobre seguridad de la información. Este análisis teórico no solo destacó la importancia creciente de proteger los datos sensibles en un entorno digitalizado, sino que también sirvió como base sólida para comprender mejor los desafíos que enfrenta la Unidad de TIC's del GAD Municipal del Cantón Paute. Al utilizar la norma ISO 27001 como guía, se establecieron principios clave para mitigar los riesgos y fortalecer la seguridad de la información de manera eficaz y eficiente.

La identificación detallada de la situación actual de la seguridad de la información en la Unidad de TIC's reveló varios riesgos críticos y deficiencias, como la ausencia de políticas de seguridad adecuadas y recursos insuficientes. Este diagnóstico inicial permitió establecer un marco de referencia claro para abordar las debilidades existentes y resaltar la urgencia de implementar medidas de seguridad más rigurosas. La falta de procesos estructurados y el bajo nivel de importancia otorgado a la seguridad de la información subrayan la necesidad de priorizar este aspecto dentro de la organización.

Con base en el diagnóstico realizado, se diseñó un plan estratégico de seguridad de la información que incorpora la identificación, evaluación, y priorización de los riesgos, así como estrategias de mitigación efectivas. Este plan se fundamenta en la norma ISO 27001 e incluye acciones específicas como el establecimiento de políticas formales, la capacitación continua del personal, y la mejora de la infraestructura tecnológica. Estas medidas están destinadas a fortalecer significativamente la postura de seguridad de la Unidad de TIC's y asegurar la continuidad operativa de sus servicios.

Finalmente, el plan estratégico fue evaluado por expertos en seguridad de la información, incluido el jefe de la Unidad de TIC's. Los expertos validaron la pertinencia y efectividad del plan, destacando su alineación con las mejores prácticas de la norma ISO 27001 y su potencial para mejorar la seguridad de la información. Las recomendaciones recibidas enfatizan la importancia de seguir optimizando ciertas áreas del plan para maximizar su impacto y garantizar su adaptabilidad a futuros cambios tecnológicos y de amenazas, asegurando así una postura de seguridad proactiva y resiliente.

RECOMENDACIONES

Basado en las evaluaciones de los expertos, es esencial que el PESI continúe desarrollándose y adaptándose a las nuevas amenazas y avances tecnológicos. Los expertos han subrayado la importancia de establecer un programa continuo de capacitación para el personal, asegurando que todos los miembros de la Unidad de TIC's estén actualizados sobre las mejores prácticas en seguridad de la información. Esto incluye no solo la capacitación técnica, sino también el fortalecimiento de la cultura organizacional hacia una mayor concienciación de la seguridad.

Además, se recomienda que el PESI se someta a revisiones periódicas y ajustes en función de las evaluaciones de riesgos emergentes y cambios en el entorno operativo del GAD Municipal del Cantón Paute. La incorporación de nuevas tecnologías, como la inteligencia artificial para la detección de amenazas, y el uso de análisis de datos avanzados para monitorear la seguridad, pueden ofrecer ventajas significativas en la protección de los datos. También es crucial establecer un sistema de retroalimentación robusto para captar las experiencias y sugerencias del personal y expertos, lo que facilitará la mejora continua del plan y su alineación con las necesidades reales de la organización.

REFERENCIAS

Acosta, Á., Padilla, P., & Rojas, Y. (2023). Análisis de las metodologías PETI para las instituciones públicas del Ecuador. *Estudios de la gestión*(14), 25-51. doi:https://doi.org/10.32719/25506641.2023.14.2

Al Hadad, R., & Maulana, H. (2023). A Comprehensive Review of COBIT and ISO 27001: Approaches to Auditing Credit Bureau Automation System (CBAS) at PT XYZ. *IEEE*, 1-8. doi:10.1109/ICSPIS59665.2023.10402713

Amaíz , A., & Flores, M. (2021). Estudio exploratorio-descriptivo sobre las actitudes de los odontólogos costarricenses hacia la aplicación interdisciplinaria de los principios psicológicos en la consulta bucodental. *Revista Odontología Vital, 1*(34), 7-20. Recuperado el 2024, de https://www.scielo.sa.cr/scielo.php?pid=S1659-07752021000100007&script=sci_arttext

Arévalo, F., Ordoñez, I., Peñaherrera, M., & Suárez, V. (2020). Importancia de la seguridad de los sistemas de información frente el abuso, error y hurto de información. *Revista cientifica Dominio de las ciencias, 6*, 835-846. doi:dx.doi.org/10.23857/dc.v6i2.1197

Barba, J. (2023). Fortalecimiento de la ciberseguridad en una PYME mediante la aplicación de controles de la norma ISO 27001:2013. *Repositorio Digital Universidad Casa Grande*. Recuperado el 2024, de http://dspace.casagrande.edu.ec:8080/bitstream/ucasagrande/3964/1/Tesis4056BARf.pdf

Barragán, J., & González, E. (2020). Análisis FODA como elemento de la planeación estratégica. *Revista Daena: International Journal of Good Conscience, 15*(1). Recuperado el 2024, de https://openurl.ebsco.com/EPDB%3Agcd%3A12%3A3822012/detailv2?sid=ebsco%3Aplink%3Ascholar&id=ebsco%3Agcd%3A144462790&crl=c

Briceño, E. (2021). *SEGURIDAD DE LA INFORMACIÓN.* España: Área de Innovación y Desarrollo,S.L. doi:https://doi.org/10.17993/tics.2021.4

Bustamante, S., Valles, M., Cuellar, I., & Lévano, D. (2021). Políticas basadas en la ISO 27001:2013 y su influencia en la gestión de seguridad de la información en municipalidades de Perú. *Enfoque UTE, 12*(2), 69-79. doi:https://doi.org/10.29019/enfoqueute.743

Cabrera, N. (2023). Disponibilidad, aceptación y uso de TIC como mecanismos de coordinación asistencial y los factores que influyen en dos servicios públicos de salud en México y Colombia durante la pandemia COVID-19. *Instituto de Ciencias de la Salud Región Xalapa*. Recuperado el 2024

Cáceres, M. (2022). *Municipio aún identifica los intentos de acceso a su sistema informático.* Obtenido de El Comercio: https://www.elcomercio.com/actualidad/quito/municipio-quito-identifica-intentos-sistema.html

Cano, G. (2018). Las TICs en las empresas: evolución de la tecnología y cambio estructural en las organizaciones. *4*(1). Portoviejo, Ecuador. Recuperado el 2024

Cañón, E. (2020). Elaboración del plan estratégico de tecnologías de la información y las comunicaciones –peti para la alcaldía municipal de chía. *Repositorio Universidad de Cundinamarca*. Recuperado el 2024, de https://repositorio.ucundinamarca.edu.co/handle/20.500.12558/2900

Casanova, M., & Calderón, C. (2020). Modelo para la gestión de infraestructuras de tecnologías de la información. *23*(48), págs. 31-53. doi:10.22430/22565337.1449

Castaño, P. (2020). Modelo de gobierno de SI/TI en empresas líquidas y altamente especializadas.

Castillo, J., & Zavala, B. (2019). CIBERSEGURIDAD Y VIGILANCIA TECNOLÓGICA: UN RETO PARA LA PROTECCIÓN DE DATOS PERSONALES EN LOS ARCHIVOS. *Revista Academica de investigacion TLATEMOANI*. Recuperado el 2024, de https://www.eumed.net/rev/tlatemoani/31/ciberseguridad.pdf

Cedeño , F., & Towsend, J. (2021). *Evaluación de la inversión en tic como factor de competitividad de las empresas Pymes del Cantón Guayaquil*. Recuperado el 2024, de Revista Universidad y Sociedad: http://scielo.sld.cu/scielo.php?pid=S2218-36202021000200452&script=sci_arttext

Chadwick, G. (1978). *A systems view of planning : towards a theory of the urban and regional planning process* (2 ed.). (G. Chadwick, Ed.) doi:https://doi.org/10.1016/B978-0-08-020625-7.50009-6.

Chapin, E., & Cuenca, J. (2021). Planificación estratégica de tecnologías de la información en industria cartonera orense. *Polo del Conocimiento: Revista científica - profesional, 6*(9), 1749-1773. Recuperado el 2024, de https://dialnet.unirioja.es/servlet/articulo?codigo=8094559

Comunicación Social RPDMQ. (2022). *Iniciamos con el proceso de Implementación de las Normas ISO 9001:2015 y 27001:2013*. Obtenido de Registro de la Propiedad del Distrito Metropolitano de Quito: https://registrodelapropiedadquito.gob.ec/prensa-rdp/33-2022/68-iniciamos-con-el-proceso-de-implementaci%C3%B3n-de-las-normas-iso-9001-2015-y-27001-2013.html

De La Cruz, G., Méndez , R., & Mendoza , A. (2023). Seguridad de la información en el comercio electrónico basado en ISO 27001 : Una revisión sistemática. *Innovación y software, 4*(1). doi:10.48168/innosoft.s11.a79

Delgado, B., Bravo, W., & Pinzón, L. (2022). La planificación estratégica como herramienta clave para el desarrollo de las microempresas. *Revista Publicando, 9*(34), 96-107. doi:doir.org/10.51528/rp.vol9.id2323

Dubois, P. (2023). Seguridad de la información: un desafío de múltiples dimensiones. *Cirion Technologies*. Obtenido de Cirion Technologies: https://blog.ciriontechnologies.com/es/seguridad-informacion-desafio-multiples-dimensiones/

Erbes, A., & Roitter, S. (2020). Estrategia Tecnológica y Organización del Trabajo: Especificidades de la Industria Manufacturera Argentina. *Revista de Economía y Estadística, 58*(1), 81-111. doi:https://doi.org/10.55444/2451.7321.2020.v58.n1.31868

Escofet, A. (2020). Aprendizaje-servicio y tecnologías digitales: ¿una relación posible? *RIED. Revista Iberoamericana de Educacion a Distancia, 23*(1), 169-182. doi:doi.org/10.5944/ried.23.1.244680

Eskaluspita, A. (2020). ISO 27001:2013 for Laboratory Management Information System at School of Applied Science Telkom University. (I. Publishing, Ed.) *IOP Conference Series: Materials Science and Engineering, 879*(1). doi:10.1088/1757-899X/879/1/012074

Fernández, G., & Carrera, B. (2019). Auditoría informática mediante la aplicación de la metodología cobit, para el control operativo de los procesos informáticos en la empresa Nexus Technologies. *DSpace de Uniandes*. Recuperado el 2024, de https://dspace.uniandes.edu.ec/handle/123456789/9890

Franciskovic, J., Hamann, A., & Miralles, F. (2020). LAS TIC, UNA OPORTUNIDAD DE PARTICIPACIÓN CIUDADANA EN LOS GOBIERNOS SUBNACIONALES. *Revista republicana, 29*, 21-46. doi:10.21017/rev.repub.2020.v29.a85

Galante, O., & Marí, M. (2020). Jorge Sabato y el Pensamiento Latinoamericano en Ciencia, Tecnología, Desarrollo y Dependencia. *Repositorio de ESOCITE, 3*(5). doi:ISSN 26183188

García, F. (2020). La sociedad del conocimiento y sus implicaciones en la formación universitaria docente. *Politicas, universidad e innovacion: retos y perspectivas*, 133-155.

García, J., & Sánchez, P. (2020). Diseño teórico de la investigación: instrucciones metodológicas para el desarrollo de propuestas y proyectos de investigación científica. *Información tecnológica, 31*(6), 159-170. doi:http://dx.doi.org/10.4067/S0718-07642020000600159

Gómez, Á. (2022). Auditoría de seguridad informática. *ediciones de la U*. Recuperado el 2024, de https://books.google.com.ec/books?hl=es&lr=&id=No5dEAAAQBAJ&oi=fnd&pg=PA33&dq=G%C3%B3mez,+%C3%81.+(2022).+Auditor%C3%ADa+de+seguridad+inform%C3%A1tica.+Ediciones+de+la+U.&ots=RgwM1xRzm3&sig=Qd4PgFt7kOAv_i76KdHpp8Ph5Jw&redir_esc=y#v=onepage&q=G%C3%B3mez%2C

González, J., & Rodríguez, M. (2019). Manual práctico de planeación estratégica. *Ediciones Díaz de Santos*. Recuperado el 2024, de https://books.google.com.ec/books?hl=en&lr=&id=kGzWDwAAQBAJ&oi=fnd&pg=PR9&dq=Gonz%C3%A1lez+Mill%C3%A1n,+J.+J.,+%26+Rodr%C3%ADguez+D%C3%ADaz,+M.+T.+(2019).+Manual+pr%C3%A1ctico+de+planeaci%C3%B3n+estrat%C3%A9gica.+Ediciones+D%C3%ADaz+de+Santos.+Obtenido+de

Groš, S. (2021). A Critical View on CIS Controls. *2021 16th International Conference on Telecommunications (ConTEL)*, 122-128. doi:10.23919/ConTEL52528.2021.9495982

Guaman, I. (2022). Propuesta de plan estrategico de tecnologias de informacion-peti para mejorar la gestion de ti del gad municipal de Cañar. (U. C. Cañar, Ed.) *Repositorio de la*

Universidad Católica de Cuenca. Obtenido de https://dspace.ucacue.edu.ec/items/6d7a1421-bd24-43df-8eae-325e33218ae1

Guevara, H., Huarachi, L., Lozano, G., & Vértiz, J. (2021). Gestión del cambio en organizaciones educativas pospandemia. *Revista Venezolana de Gerencia, 26*(93), 178-191. Recuperado el 2024, de https://www.redalyc.org/journal/290/29066223012/29066223012.pdf

Gutiérrez, J., Borré, J., Hernández, L., & Vega, F. (2021). Planificación estratégica situacional: Un proceso metódico-práctico. *Revista Venezolana de Gerencia: RVG, 26*(94), 762-783. Recuperado el 2024, de https://dialnet.unirioja.es/servlet/articulo?codigo=8890456

Hernández-Sampieri, R., & Mendoza, C. (2020). *Metodología de la investigación: las rutas cuantitativa, cualitativa y mixta.* McGraw-Hill Interamericana.

ISO/IEC. (2022). *ISO/IEC 27001:2022*. Obtenido de ISO: https://www.iso.org/es/contents/data/standard/08/28/82875.html#:~:text=La%20certificaci%C3%B3n%20ISO%2FIEC%2027001%20es%20una%20forma%20de%20demostrar,de%20forma%20segura%20y%20protegida.

Kurii, Y., & Opirskyy, I. (2022). Analysis and Comparison of the NIST SP 800-53. *CEUR Workshop*. Recuperado el 2024, de https://ceur-ws.org/Vol-3288/paper3.pdf

López, S. (2019). *La breve historia de la ciberseguridad*. Obtenido de Sofistic cybersecurity: https://www.sofistic.com/blog-ciberseguridad/la-breve-historia-de-la-ciberseguridad/

Lucas, J. (2023). Planificar la Implementación del Sistema de Gestión de Seguridad de la Información Basado en la Norma ISO/IEC 27001:2013 para la Integridad, Confidencialidad y Disponibilidad de su Información en la Empresa Automatisoft S.A.C. *Repositorio Dspace*. Obtenido de https://repositorio.upci.edu.pe/bitstream/handle/upci/843/Tesis%20Final%20Presentado%20-%20Lucas%20Asencio%20Jesus%20Lorenzo.pdf?sequence=1&isAllowed=y

Martínez, J., Palacios, G., & Juárez, L. (2020). Análisis de validez de constructo del instrumento: “Enfoque Directivo en la Gestión para Resultados en la Sociedad del Conocimiento”. *RETOS. Revista de Ciencias de la Administración y Economía, 10*(19), 153-165. doi:https://doi.org/10.17163/ret.n19.2020.09

Mera , C., Vera, D., Mendoza , J., Briones, J., Mendoza, H., & Mendoza, K. (2021). GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN EN INSTITUCIONES PÚBLICAS. *EIDEC, 1*. doi:doi.org/10.34893/tng4-8488

Ministerio del Trabajo. (2021). PLAN ESTRATÉGICO INSTITUCIONAL. Ecuador.

Moreira, M., & Adell, J. (2021). Tecnologías Digitales y Cambio Educativo. Una Aproximación Crítica. *REICE. Revista Iberoamericana sobre Calidad, Eficacia y Cambio en Educación, 19*(4), 83-96. doi:doi.org/10.15366/reice2021.19.4.005

Morocho, M. (2023). *PAUTE APUNTA A SER UNA CIUDAD TECNOLÓGICA Y SEGURA* . Obtenido de Municipio de Paute: https://www.paute.gob.ec/destacada/paute-apunta-a-ser-una-ciudad-tecnologica-y-segura/

Municipio de Paute. (2020). *Ogranigrama de la institucion*. Obtenido de Alcaldia de Paute: https://www.paute.gob.ec/mdocs-posts/literal_a1-organigrama_de_la_institucion-1-2/

Municipio de Paute. (2024). Obtenido de Municipio de Paute: https://www.paute.gob.ec/

Muñiz, L., Tomalá, R., & Alvarado, J. (2022). La Planificación Estratégica y su Aporte al Desarrollo Empresarial de las Mipymes en Manabí. *Dominio de las Ciencias, 8*(1). doi:https://doi.org/10.23857/dc.v8i1.2577

Muñoz, P. (2021). *Modelos de seguridad para prevenir riesgos de ataques Informáticos: Una revisión sistemática.* Obtenido de Repositorio Institucional de la Universidad Politécnica Salesiana: https://dspace.ups.edu.ec/handle/123456789/20932

Muñoz, R. (2022). *Evaluación del plan de mantenimiento preventivo y correctivo de las estaciones de trabajo informático del GAD municipal.* Obtenido de http://dspace.utb.edu.ec/handle/49000/12570

Pazmiño, C., Serrano, A., & González, M. (2020). Las Tics como herramienta para la gestión de riesgos. *RECIMUNDO, 4*. doi:https://doi.org/10.26820/recimundo/4.(1).esp.marzo.2020.173-181

Pino, M. (2022). *Plan estratégico institucional para el mejoramiento de la gestión del GAD Parroquial Rural El Altar, cantón Penipe, periodo 2021-2025.* Obtenido de http://dspace.espoch.edu.ec/handle/123456789/18317

Piña, L. (2023). El enfoque cualitativo: Una alternativa compleja dentro del mundo de la investigación. *Revista Arbitrada Interdisciplinaria Koinonía, 8*(15), 1-3. doi:10.35381/r.k.v8i15.2440

Reina, E. (2021). Modelo de un Plan Estratégico Green IT y BPM para minimizar el impacto ambiental en la educación superior. *Revista Digital Novasinergia, 4*(1), 136-150. doi:https://doi.org/10.37135/ns.01.07.08.

Rodriguez, L., Cruzado, C., Mejía, C., & Alarcón, M. (2020). Aplicación de ISO 27001 y su influencia en la seguridad de la información de una empresa privada peruana. *Propositos y Representaciones, 8*(3). doi: http://dx.doi.org/10.20511/pyr2020.v8n3.786

Rodriguez, X. (2022). Los 8 pasos de Kotter para liderar el cambio. *WILLACHIKUY, 2*(1), 26-29. doi:https://doi.org/10.46363/willachikuy.v2i1.7

Romero, M., Figueroa, G., Vera, D., Álava, J., Parrales, G., Álava, C., . . . Castillo, M. (2018). Introducción a la seguridad informática y el análisis de vulnerabilidades. *3ciencias*. doi:http://dx.doi.org/10.17993/IngyTec.2018.46

Rueda, K., & Rodríguez, L. (2020). Estrategia tecnológica para nivelar los presaberes matemáticos en la educación superior. *Editorial Universitat Politècnica de València*, 357-365. doi:10.4995/INRED2020.2020.11979

Ruiz, F. (2024). Diseño de un sistema de gestión de seguridad de la información al proceso de tic en la organización ortopédica alca plus s.a.s. *Repositorio Universidad Nacional Abierta y a Distancia UNAD*. Recuperado el 2024, de https://repository.unad.edu.co/handle/10596/61633

Saavedra, C., Figueroa, C., & Sánchez, P. (2021). Acercamiento teórico al concepto de tecnología desde la educación en tecnología. *Fundación Dialnet, 10*(5), 110-120. Obtenido de https://dialnet.unirioja.es/servlet/articulo?codigo=8116432

Sánchez, A., & Hidalgo, W. (2023). Evaluación de riesgos para un sistema de gestión de seguridad de la información en base a la Norma ISO/IEC 27001 aplicado a un proveedor de servicios de internet. *Repositorio Universidad Técnica de Ambato*. Obtenido de https://repositorio.uta.edu.ec/handle/123456789/39448

Solarte, F., Enriquez, E., & Del Carmen, M. (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. *Revista Tecnológica - ESPOL, 28*(5), 492-507. Recuperado el 2024, de https://rte.espol.edu.ec/index.php/tecnologica/article/view/456

Ticona, H. (2021). USO DE LA NORMA ISO 27001 Y SU INFLUENCIA EN LA SEGURIDAD DE INFORMACIÓN DE LA EMPRESA ICO EL AÑO 2021. *Repositorio de la Universidad Privada del Norte*. Recuperado el 2024, de Repositorio de la Universidad Privada del Norte: https://repositorio.upn.edu.pe/handle/11537/28162

Tognoli, J., Fideleff, V., & Naser, A. (2020). Gestión de planes de acción locales de gobierno abierto: herramientas para la cocreación, el seguimiento y la evaluación. *Repositorio Digital BETA CEPAL*. Recuperado el 2024, de https://repositorio.cepal.org/entities/publication/ab64c05f-65dd-4e01-b7ad-c9760120ad06

UdeCataluña. (2024). *Los desafíos y las tendencias de la ciberseguridad y la seguridad de la información en el 2024: ¿estás preparado?* Obtenido de Udecataluña: https://www.ucatalunya.edu.co/blog/los-desafios-y-las-tendencias-de-la-ciberseguridad-y-la-seguridad-de-la-informacion-en-el-2024-estas-preparado

Valle, A., Manrique, L., & Revilla, D. (2022). La Investigación descriptiva con enfoque cualitativo en educación. *Pontificia Universidad Católica del Perú. Facultad de Educación*. Recuperado el 2024, de https://repositorio.pucp.edu.pe/index/handle/123456789/184559

Vázquez, G., Jiménez, I., & Juárez, L. (2022). Clasificación de Estrategias de Gestión del Conocimiento para impulsar la innovación educativa en Instituciones de Educación Superior. *GECONTEC: Revista Internacional de Gestión del Conocimiento y la Tecnología, 10*(1), 18-35. doi:https://doi.org/10.5281/zenodo.6785484

Vega, V., Leyva, M., & Sánchez, B. (2022). Análisis FODA-PAJ: Una alternativa esencial para realizar el estudio de la empresa avícola Matanzas. *Universidad y Sociedad, 14*, 34-46.

Villalba, C., Sánchez, M., Zambrano, C., & López, S. (2021). Modelo de calidad para el mejoramiento de la eficiencia en las instituciones públicas del Ecuador. *Ciencia Digital, 5*(1), 15-29. doi:10.33262/cienciadigital.v5i1.1516

Zuñiga, F. (2021). Relación entre la Planificación Estratégica y Gestión del Conocimiento. *Horizontes Revista de Investigación en Ciencias de la Educación, 5*(21), 336-342. doi:https://doi.org/10.33996/revistahorizontes.v5i21.308

ANEXOS

ANEXO 1

Acuerdos Realizados con el personal de la Unidad de TIC´s

Fecha: 15/03/2024
Lugar: Unidad de TIC´s del GAD Municipal del Cantón Paute
Asistentes:

- Ana Paulina Cabrera Bravo
- Nain Alexander Valladares Sierra (Virtual)

Entrevistas Realizadas

Fecha	Entrevistado	Cargo	Entrevistador/es	Hora de inicio	Hora de Fin
15/03/2024	Ing. Pablo Guillermo	Jefe de la Unidad de TIC´s	Paulina Cabrera Nain Valladares	13:00	16:00
15/03/2024	Anónimo	Desarrollador Unidad de TIC's	Paulina Cabrera Nain Valladares	14:00	16:00

Acuerdos de Privacidad
Durante la reunión con el Equipo de la Unidad de TIC's, se acordó lo siguiente:

- **Confidencialidad de la Información:** La información recopilada durante las entrevistas no será compartida de manera precisa o detallada fuera del ámbito del trabajo de integración curricular. Se respetará la privacidad de los datos proporcionados por los entrevistados.
- **Uso de la Información:** La información obtenida puede ser utilizada para el trabajo de integración curricular, incluyendo la elaboración del FODA y la redacción de un resumen general de las entrevistas realizadas.
- **Entrevistados Anónimos:** Se acordó que algunos entrevistados prefieren no revelar sus credenciales debido a la naturaleza pública de la entidad. En tales casos, solo se mencionará el cargo del entrevistado sin detallar información personal.

Resumen de Entrevista

1. **Ing. Pablo Guillermo**:

- **Cargo**: jefe de la Unidad de TIC´s
- **Años de Experiencia:** 8 años
- **Fecha**: 15/03/2024
- **Hora de Inicio:** 13:00
- **Hora de Fin:** 16:00
- **Resumen**: Durante la entrevista, se discutieron aspectos críticos relacionados con la gestión de la seguridad de la información en la Unidad de TIC´s. Se destacó la necesidad de mejorar los procesos de identificación de riesgos y vulnerabilidades, así como la importancia de contar con un plan estratégico claro para abordar estos desafíos. El Ing. Pablo Guillermo subrayó la urgencia de implementar medidas más robustas para garantizar la integridad, confidencialidad y disponibilidad de los datos.

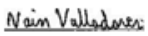
2. **Desarrollador Unidad de TIC's**:

- **Cargo:** Desarrollador Unidad de TIC's
- **Fecha:** 15/03/2024
- **Resumen:** En esta entrevista, se identificaron varias debilidades en la infraestructura actual de TI y la falta de un sistema formalizado para la gestión de la seguridad de la información. El entrevistado prefirió mantener su anonimato, pero señaló problemas recurrentes con la disponibilidad de los sistemas y la ausencia de políticas estandarizadas que fortalezcan la seguridad de los datos manejados por la unidad.

Firmantes:

Ing. Pablo Guillermo

Paulina Cabrera



Nain Valladares

Elaborado por: Ana Paulina Cabrera Bravo – Nain Alexander Valladares Sierra
Fecha de Elaboración: 15/03/2024

Fecha: 17/05/2024
Lugar: Unidad de TIC´s del GAD Municipal del Cantón Paute
Asistentes:

- Ana Paulina Cabrera Bravo
- Nain Alexander Valladares Sierra (Virtual)

Entrevistas Realizadas

Fecha	Entrevistado	Cargo	Entrevistador/es	Hora de inicio	Hora de Fin
17/05/2024	Ing. Pablo Guillermo	Jefe de la Unidad de TIC´s	Paulina Cabrera Nain Valladares	13:00	15:00

Acuerdos de Privacidad

Durante la reunión con el Equipo de la Unidad de TIC's, se acordó lo siguiente:

- **Confidencialidad de la Información:** La información recopilada durante las entrevistas no será compartida de manera precisa o detallada fuera del ámbito del trabajo de integración curricular. Se respetará la privacidad de los datos proporcionados por los entrevistados.
- **Uso de la Información:** La información obtenida puede ser utilizada para el trabajo de integración curricular, incluyendo la elaboración del FODA y la redacción de un resumen general de las entrevistas realizadas.
- **Entrevistados Anónimos:** Se acordó que algunos entrevistados prefieren no revelar sus credenciales debido a la naturaleza pública de la entidad. En tales casos, solo se mencionará el cargo del entrevistado sin detallar información personal.

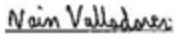
Resumen de Entrevista

- **Ing. Pablo Guillermo**:
  - **Cargo**: jefe de la Unidad de TIC´s
  - **Años de Experiencia:** 8 años
  - **Fecha**: 15/03/2024
  - **Hora de Inicio:** 13:00
  - **Hora de Fin:** 16:00
  - **Resumen**: La entrevista con el Ing. Pablo Guillermo permitió profundizar en las necesidades estratégicas de la Unidad de TIC's en cuanto a la seguridad de la información. Se confirmó la importancia de desarrollar un plan estratégico enfocado en mejorar la identificación de riesgos y vulnerabilidades, priorizando la implementación de medidas preventivas y correctivas que aseguren la protección de los datos y sistemas críticos.

Firmantes:

Ing. Pablo Guillermo

Paulina Cabrera



Nain Valladares

Elaborado por: Ana Paulina Cabrera Bravo – Nain Alexander Valladares Sierra
Fecha de Elaboración: 17/05/2024

ANEXO 2

Acta de Compromiso de Miembros del Equipo

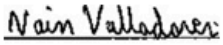
ACTA DE COMPROMISO DE LOS MIEMBROS DEL EQUIPO

Samborondon,22 de enero del 2024

Nain Valladares y Paulina Cabrera acordaron realizar su trabajo de integración curricular en conjunto. Los miembros del equipo se comprometieron a trabajar en el diseño de un plan estratégico para la seguridad de la información de la Unidad de TIC's de la institución. Sus responsabilidades incluyen el análisis de riesgos y vulnerabilidades, la recolección y análisis de datos, la redacción del informe final y la preparación para la defensa de la tesis. Se usará un estándar internacional de la seguridad de la Información como base para el diseño del plan estratégico, aplicando técnicas de análisis de riesgos y manteniendo una comunicación constante con la Unidad de TIC's. El cronograma abarca desde la planificación en enero hasta la redacción final.

Los miembros del equipo también se comprometen a tratar todos los datos recopilados con la confidencialidad, utilizando la información exclusivamente para el propósito del trabajo de integración curricular. Se garantizará la privacidad de los entrevistados conforme a los acuerdos establecidos. Además, se realizarán revisiones periódicas del progreso del trabajo y ajustes necesarios para asegurar el cumplimiento de los objetivos. Este documento formaliza el compromiso de Nain Valladares y Paulina Cabrera para cumplir con las responsabilidades descritas y garantizar el éxito del proyecto.

Firmantes:



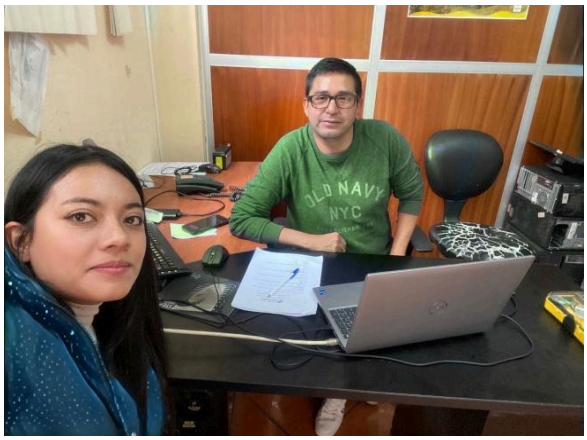
Nain valladares

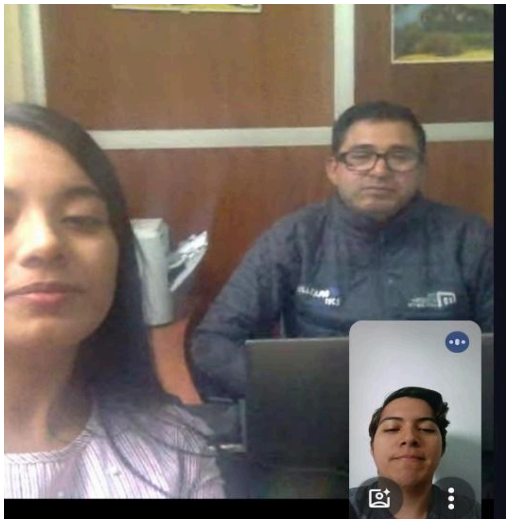
Paulina Cabrera

ANEXO 3

Evidencia de Reuniones

Se denota en las imágenes las dos reuniones pertinentes efectuadas a fin de establecer las pautas de la investigación que sustentaran este trabajo de integración curricular y en segunda instancia se denota la entrevista efectuada a cada una de las partes. Las mismas se hicieron en tiempos y localizaciones diferentes para que existiera mayor seguridad en las respuestas proporcionadas por la muestra.





ANEXO 4

Preguntas realizadas al personal de la Unidad de TIC´s en las entrevistas

Fecha entrevista 1: 15/03/2024

- **Entrevistados:**
    - Jefe de la Unidad de TIC ‘s

Fecha entrevista 2: 17/05/2024

- **Entrevistados:**
    - Desarrollador de la Unidad de TIC ‘s

Cuerpo de la entrevista

- ¿En qué norma o estándar basan sus procesos y controles?
- ¿Mejoras que se han realizado en esta administración en cuanto a la seguridad de la información?
- ¿Existe algún plan estratégico?
- ¿Como es la seguridad de la información para la Unidad de TIC´s del GAD Municipal?
- ¿Cuáles son las herramientas tecnológicas manejadas que sustentan la seguridad de la información?
- ¿Falencias encontradas hasta el momento en el uso de las TIC´s frente a la seguridad de la información?
- ¿Beneficios encontrados hasta el momento en el uso de las TIC’s frente a la seguridad de la información?

ANEXO 5

Preguntas de la encuesta cualitativa realizada al personal de la Unidad de TIC´s

Cuerpo de la encuesta

Perspectivas directas sobre aspectos relacionados con la seguridad de la información.

1. ¿Cuál es su nivel de conocimiento sobre la seguridad de información?
2. ¿Qué conocimientos posee sobre las normas que regulan la seguridad de la información?
3. ¿Cuál es su nivel de comprensión respecto a la norma ISO 27001?
4. ¿Cuánta información sabe acerca de la ley de protección de los datos?
5. ¿Qué equipos de cómputo tienen las licencias actualizadas?

Usuarios

1. ¿Hay una persona designada exclusivamente para la creación de cuentas de usuario?
2. ¿Se mantiene un registro de los usuarios que han sido creados?
3. ¿Se realiza el bloqueo de las cuentas de usuario durante las vacaciones o cuando un empleado deja la empresa?
4. ¿Es necesario solicitar permiso para crear cuentas de usuario?
5. ¿Las contraseñas tienen fecha de caducidad?
6. ¿Se establecen responsabilidades a los usuarios en cuanto al uso adecuado de los recursos?
7. ¿Se implementa algún control para prevenir el acceso no autorizado a los equipos y sistemas de la empresa?

Autenticación

1. ¿Se utiliza una contraseña genérica para los nuevos usuarios?
2. ¿Está especificado el tamaño y la complejidad de la contraseña?
3. ¿El usuario se bloquea después de ingresar una contraseña incorrecta?
4. ¿Los usuarios pueden acceder al sistema desde cualquier dispositivo?

5. ¿Es posible acceder al sistema desde otro dispositivo si el usuario ya está conectado?

Autorización

1. ¿Los usuarios tienen permiso para actualizar o alterar la base de datos?

2. ¿Están claramente definidos los permisos para cada usuario?

3. ¿Se requiere autorización para cambiar el usuario o la contraseña?

4. ¿Está permitido el acceso a sitios web no institucionales?

5. ¿Está permitido el acceso a sitios web no institucionales?

Administración de sistemas

1. ¿El administrador puede realizar cambios en la Base de Datos (BDD)?

2. ¿Las sesiones de todos los usuarios están en estado activo durante los periodos de inactividad?

3. ¿Existen controles de acceso a los Backups para el Administrador de Base de Datos?

4. ¿Los usuarios pueden extraer información mediante dispositivos externos?

5. ¿Existe un algún tipo de seguimiento de todas las personas autorizadas para realizar los respaldos del sistema de Gad?

6. ¿Han realizado en la unidad de TIC´s simulacros para enfrentar la caída de los sistemas de información y comunicación? Si es así, ¿cómo se han realizado? Si no, ¿por qué?

7. ¿Se monitorean los sistemas de información que gestionan?

Equipos informáticos

1. ¿Los equipos cuentan con suficiente memoria para ejecutar los programas y aplicaciones necesarias de manera eficiente?

2. ¿Todos los procedimientos relacionados con los equipos están documentados?

3. ¿Se lleva a cabo un mantenimiento periódico de los equipos?

4. ¿Los usuarios tienen permiso para abrir o destapar los equipos de cómputo asignados?

Activos fijos

1. ¿Los registros de activos fijos contienen la información y detalles necesarios?

2. ¿Qué políticas o reglas se aplican para la autorización de retiro, destrucción, adquisición o venta de activos fijos?

3. ¿Se realiza periódicamente un inventario físico o digital de los activos fijos para verificar su existencia y estado?

4. ¿Las personas responsables de los activos fijos están comprometidas reportar cualquier cambio o daño que suceda con el software?

5. ¿La venta de activos fijos del departamento de la Unidad de TIC ‘s requiere autorización previa de los directivos?

6. ¿Se dispone de información sistematizada y actualizada del inventario de activos fijos de la empresa?

7. ¿El inventario está segmentado por áreas?

8. ¿Se ha realizado procesos específicos para los registros de resguardo de activos de altas, bajas y la toma física de todos los inventarios?

9. ¿Se tiene una base de datos o algún programa que estén los inventarios de los activos fijos?

10. ¿Se mantiene un registro actualizado de los ingresos de activos de los proveedores?

11. ¿Existe el personal capacitado para controlar los activos fijos?

12. ¿Es necesario implantar un proceso adecuado para el control de los activos fijos?

A través de la encuesta se denoto en primera instancia las falencias actuales previstas en el departamento en temas de seguridad de la información, la cual permitió identificar la situación actual de la Unidad de TIC´s del GAD Municipal del Cantón Paute.

ANEXO 6

Fotografías para evidencia del estado actual de la Unidad de TIC´s

- **Sala de servidores - estado actual**



Se evidencia a través de las fotos anteriores el estado de la sala de servidores. Lo cual deja ver el mal estado en que se encuentra la misma, pues se denoto desorden y equipos en deterioro. Esto es una de las principales debilidades evidenciadas en el departamento.

ANEXO 7

Cuadros comparativos

Criterio	NIST SP 800-53	CIS Controls	ISO 27001
Enfoque	Protección y gestión de la seguridad de información	Guía práctica para la implementación de seguridad de TI	Protección integral de la información mediante buenas prácticas
Aplicabilidad	Recomendaciones y controles para la seguridad de información en sistemas federales	Prioriza las mejores prácticas de seguridad cibernética en 18 controles críticos	Aplicación de buenas prácticas y recursos para la seguridad de información
Fortalezas	Conjunto exhaustivo de controles, enfoque en gestión de riesgos	Facilidad de implementación, enfoque práctico y eficiente	Cumplimiento normativo y mejora continua de seguridad.
Limitaciones	Puede ser complejo y burocrático, más adecuado para organizaciones grandes	Menos formal, puede no cubrir todas las necesidades de organizaciones grandes	Recursos y compromiso a largo plazo para implementación y mantenimiento de buenas prácticas
Idoneidad para Paute	Medio, adecuado para entidades que requieren alto nivel de detalle en controles de seguridad	Medio, proporciona controles prácticos fáciles de implementar	Alto, ideal para protección integral y gestión continua de la seguridad de información

Nota. Elaboración basada en la comparación de normativas de seguridad de información. Elaborado por los Autores.

ANEXO 8

Fichas de evaluación por expertos

Ficha evaluación de experto 1:

FICHA EVALUACION DE EXPERTOS

NOMBRE COMPLETO	GALO CHRISTIAN ULLOA SANCHEZ		
INSTITUCION DONDE EJERCE	PATIOSEO.COM		
AUTORES DEL INSTRUMENTO	Ana Paulina Cabrera Bravo Nain Alexander Valladares Sierra		
TEMA	Plan Estratégico de seguridad de la información para la Unidad de TIC´s del GAD Municipal 2024-2025.		
FECHA	Dia: 29	Mes: JULIO	Año: 2024

Perfil del experto

Ing. Christian G. Ulloa Sanchez en **Computer Systems Programming (Desarrollo de Sistemas Informáticos)** tengo 23 años de experiencia laboral en el área de **Desarrollo de Software**, tengo certificaciones en **Programación (Javascript, NodeJS, Java, C++, C#), Google Certified Trainer, Business Data Mining)** poseo un amplio conocimiento en el área de **desarrollo de software**, adicional poseo gran conocimiento en estándares de seguridad de la información, en especial sobre la ISO 27001.

Aspectos a evaluar

Indicadores	Contenido	1	2	3	4	5
Funcionalidad	Aborda y satisface los objetivos definidos				X	
Organización	La estructura es clara y lógica, facilitando su comprensión y aplicación por el personal de la Unidad de TIC´s.				X	
Suficiencia	Incluye las estrategias necesarias y un plan detallado para abordar los riesgos críticos identificados.				X	
Consistencia	Está respaldado por una base teórica sólida y referencias a la ISO 27001, asegurando coherencia en su aplicación.					X
Aplicabilidad	Los procedimientos propuestos son prácticos y pueden ser implementados efectivamente por el personal.					X
Evaluación y mejora	Incluye mecanismos de evaluación continua y mejora basada en los resultados obtenidos.				X	
Cumplimiento normativo	Asegura el cumplimiento de las normativas y regulaciones aplicables en el ámbito de la seguridad de la información.					X

Opinión sobre el PESI

En general, el contenido del Plan Estratégico de Seguridad de la Información proporciona una sólida base para mejorar la postura de seguridad del departamento de TI. Los autores han demostrado un buen entendimiento del marco de trabajo ISO 27001 y han realizado una evaluación de riesgos exhaustiva. Sin embargo, hay algunas áreas donde el plan podría fortalecerse aún más.

Christian Ulloa

Ing. Christian Ulloa

Ficha evaluación de experto 2:

FICHA EVALUACION DE EXPERTOS

NOMBRE COMPLETO	Marlon Teófilo Briceño Jiménez		
INSTITUCION DONDE EJERCE	Policía Nacional		
AUTORES DEL INSTRUMENTO	Ana Paulina Cabrera Bravo Nain Alexander Valladares Sierra		
TEMA	Plan Estratégico de seguridad de la información para la Unidad de TIC´s del GAD Municipal 2024-2025.		
FECHA	Dia:29	Mes: Julio	Año:2024

Perfil del experto

Ing. Marlon Teófilo Briceño Jiménez tengo 9 años de experiencia laboral en la Policía Nacional, en la cual he desempeñado un papel importante como analista de sistemas, poseo una certificación certiprof en la norma ISO 27001 y poseo un amplio conocimiento en el área de la seguridad de la información.

Aspectos a evaluar

Indicadores	Contenido	1	2	3	4	5
Funcionalidad	Aborda y satisface los objetivos definidos					X
Organización	La estructura es clara y lógica, facilitando su comprensión y aplicación por el personal de la Unidad de TIC´s.					X
Suficiencia	Incluye las estrategias necesarias y un plan detallado para abordar los riesgos críticos identificados.					X
Consistencia	Está respaldado por una base teórica sólida y referencias a la ISO 27001, asegurando coherencia en su aplicación.				X	
Aplicabilidad	Los procedimientos propuestos son prácticos y pueden ser implementados efectivamente por el personal.					X
Evaluación y mejora	Incluye mecanismos de evaluación continua y mejora basada en los resultados obtenidos.					X
Cumplimiento normativo	Asegura el cumplimiento de las normativas y regulaciones aplicables en el ámbito de la seguridad de la información.					X

Opinión sobre el PESI

El PESI muestra un enfoque exhaustivo y alineado con las buenas prácticas de la norma ISO 27001. Destaca por su coherencia, viabilidad y aplicabilidad práctica, asegurando una gestión efectiva de los riesgos. Además, incluye mecanismos de evaluación y mejora continua, garantizando su adaptación a las necesidades cambiantes del entorno de seguridad de la información.

Ing. Marlon Briceño

Ficha de evaluación realizada por el jefe de la Unidad de TIC´s:

FICHA EVALUACION DE EXPERTOS

NOMBRE COMPLETO	Pablo Rigoberto Guillermo Anguisaca		
INSTITUCION DONDE EJERCE	GAD Municipal del Cantón Paute		
AUTORES DEL INSTRUMENTO	Ana Paulina Cabrera Bravo, Nain Alexander Valladares Sierra		
TEMA	Plan Estratégico de seguridad de la información para la Unidad de TIC´s del GAD Municipal 2024-2025.		
FECHA	Dia: 31	Mes: 07	Año: 2024

Perfil del experto

Ingeniero en Sistemas, tengo 15 años de experiencia laboral en el área de Sistemas, tengo certificaciones en seguridad de la información, poseo un amplio conocimiento en el área de la seguridad de la información.

Aspectos a evaluar

Indicadores	Contenido	1	2	3	4	5
Funcionalidad	Aborda y satisface los objetivos definidos					x
Organización	La estructura es clara y lógica, facilitando su comprensión y aplicación por el personal de la Unidad de TIC´s.				x	
Suficiencia	Incluye las estrategias necesarias y un plan detallado para abordar los riesgos críticos identificados.					x
Consistencia	Está respaldado por una base teórica sólida y referencias a la ISO 27001, asegurando coherencia en su aplicación.					x
Aplicabilidad	Los procedimientos propuestos son prácticos y pueden ser implementados efectivamente por el personal.				x	
Evaluación y mejora	Incluye mecanismos de evaluación continua y mejora basada en los resultados obtenidos.					x
Cumplimiento normativo	Asegura el cumplimiento de las normativas y regulaciones aplicables en el ámbito de la seguridad de la información.					x

Opinión sobre el PESI
El PESI muestra un enfoque exhaustivo y alineado con las buenas practicas de la norma ISO 27011.

Firmado electrónicamente por:
PABLO RIGOBERTO GUILLERMO ANGUISACA

Nombre del experto

Análisis de las fichas evaluadas por expertos

Luego de la evaluación por parte de varios expertos e incluso del principal interesado que es el jefe de la Unidad de TIC´s, se pudo destacar de manera positiva el enfoque y la exhaustividad del PESI propuesto para la Unidad de TIC's. El Ing. Pablo Rigoberto Guillermo Anguisaca, con una amplia experiencia en seguridad de la información, subraya que el plan está bien alineado con las mejores prácticas de la norma ISO 27001, destacando su viabilidad y aplicabilidad dentro del contexto organizacional del GAD.

Igualmente, el Ing. Marlon Teófilo Briceño Jiménez enfatiza que el PESI presenta una estructura coherente que facilita su implementación práctica y resalta su enfoque adaptativo a los constantes cambios en el entorno de la seguridad de la información, haciendo hincapié en la importancia de contar con mecanismos continuos de evaluación y mejora.

Por otro lado, el Ing. Christian Ulloa Sánchez, quien también es el jefe de la Unidad de TIC's, proporciona una perspectiva interna, destacando que el PESI no solo cumple con los requisitos normativos, sino que también ofrece una base sólida para fortalecer la seguridad de la información en el departamento.

Sin embargo, señala que hay ciertas áreas que podrían mejorar aún más para maximizar la eficacia del plan, sugiriendo que se podrían optimizar algunas estrategias de mitigación para hacerlas más robustas. En conjunto, las evaluaciones reflejan una aceptación positiva del PESI, validando su relevancia y adecuación para enfrentar los desafíos de seguridad de la información en la Unidad de TIC's, y proporcionan valiosos comentarios para su futura implementación y mejora.

ANEXO 9

Plan estratégico de la seguridad de la información para la Unidad de TIC´s del GAD Municipal del Cantón Paute

Plan Estratégico de seguridad de la información para la Unidad de TIC´s del GAD Municipal 2024-2025.

Plan Estratégico de seguridad de la información para la Unidad de TIC´s del GAD Municipal 2024-2025.

Realizado por: Ana Paulina Cabrera Bravo

Nain Alexander Valladares Sierra

1. Introducción

La seguridad de la información es un componente esencial para el éxito y la continuidad de las operaciones de cualquier organización, incluida la Unidad de TIC´s del GAD Municipal del Cantón Paute. En un entorno donde la información se considera un activo estratégico, protegerla contra amenazas y vulnerabilidades es crucial para garantizar su integridad, confidencialidad y disponibilidad. La implementación de un Plan Estratégico de Seguridad de la Información (PESI) es fundamental para establecer una base en los procesos que permita identificar, mitigar y priorizar los riesgos y vulnerabilidades.

Actualmente, la Unidad de TIC´s de la Municipalidad del Cantón Paute enfrenta desafíos significativos en la administración de sus sistemas de información, especialmente en lo que respecta a la protección de datos sensibles, la gestión de riesgos y vulnerabilidades tecnológicas. La falta de estrategias, planificaciones o procesos estandarizados en el área de seguridad de la información deja al departamento vulnerable ante posibles amenazas a corto y mediano plazo de forma exponencial.

Este PESI tiene como objetivo principal proporcionar estrategias para identificar amenazas, valorar riesgos y priorizarlas según el grado de riesgo, de esta forma lograr fortalecer la seguridad de la información en la Unidad de TIC´s.

El desarrollo de este PESI se basa en las buenas prácticas de la norma internacional ISO/IEC 27001:2022, que ofrece un marco de trabajo reconocido mundialmente para la gestión de la seguridad de la información. La adopción de esta norma permitirá a la Unidad de TIC´s mitigar las posibles amenazas que puedan suscitarse en el futuro a corto plazo.

Por último, este plan estratégico no solo se enfoca en la protección de la información, sino también en la mejora continua de los procesos. El compromiso del departamento en la revisión y actualización periódica del PESI garantizarán que la Unidad de TIC´s de la Municipalidad del Cantón Paute pueda adaptarse a los cambios tecnológicos y de amenazas, manteniendo siempre un alto nivel de seguridad y resiliencia frente a posibles incidentes de seguridad de la información.

2. Objetivo general

- Definir una estrategia de seguridad de la información para la Unidad de TIC´s del GAD Municipal del Cantón Paute con el fin de identificar, valorar y priorizar los riesgos para fortalecer la seguridad de la información basándose en la norma ISO 27001:2013.

3. Objetivos específicos

- Analizar los riesgos relacionados con la seguridad de la información.
- Definir estrategias de mitigación de riesgos y mejora de la seguridad de la información.
- Elaborar un plan de implementación y costos.

4. Alcance del PESI

El Plan Estratégico de Seguridad de la Información (PESI) para la Unidad de TIC´s del GAD Municipal del Cantón Paute se centrará en la evaluación exhaustiva y

mitigación de los riesgos y vulnerabilidades que afectan la seguridad de la información dentro de esta unidad. Este plan abarca todos los sistemas, procesos y activos de información gestionados por la Unidad de TIC´s, con el objetivo de fortalecer la integridad, confidencialidad y disponibilidad de la información.

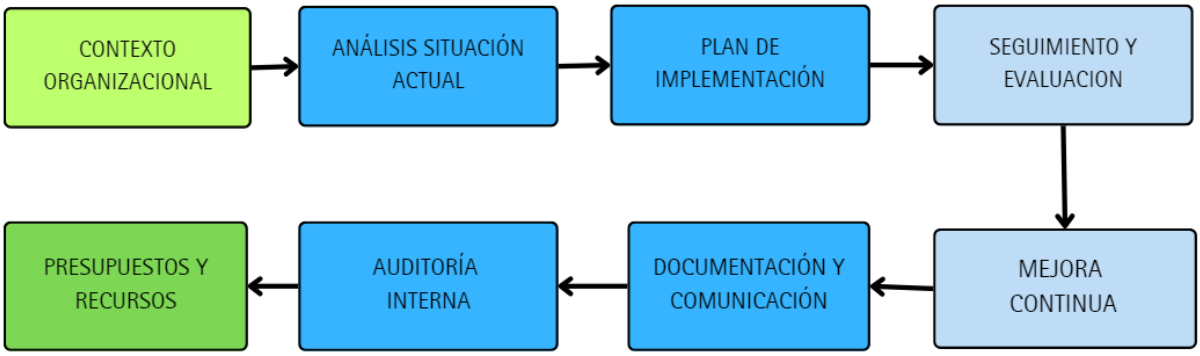
El PESI definirá estrategias basadas en las mejores prácticas de la norma ISO 27001:2013, las cuales se orientarán a mitigar los riesgos identificados y mejorar la protección de los datos. Estas estrategias incluirán la implementación de controles de seguridad específicos y la creación de políticas y procedimientos de seguridad detallados.

Además, se desarrollará un plan de implementación que incluirá una planificación de las actividades y un presupuesto estimado de costos, garantizando que las estrategias de seguridad se ejecuten de manera organizada y efectiva.

5. Metodología

Se utilizo la siguiente metodología para la elaboración del PESI, la cual se visualiza en el siguiente grafico:

Figura 1.*Metodología del PESI*



Nota. La imagen muestra las fases del PESI. Elaborado por los Autores.

6. Contexto organizacional

Esta fase es el inicio de la elaboración del PESI, en la cual se describe a la institución con la finalidad de que los objetivos planteados en el PESI se alineen con los objetivos estratégicos tales como la misión y visión del GAD Municipal del Cantón Paute. A continuación, se presenta una descripción detallada de la organización y su estructura:

6.1 Descripción de la institución

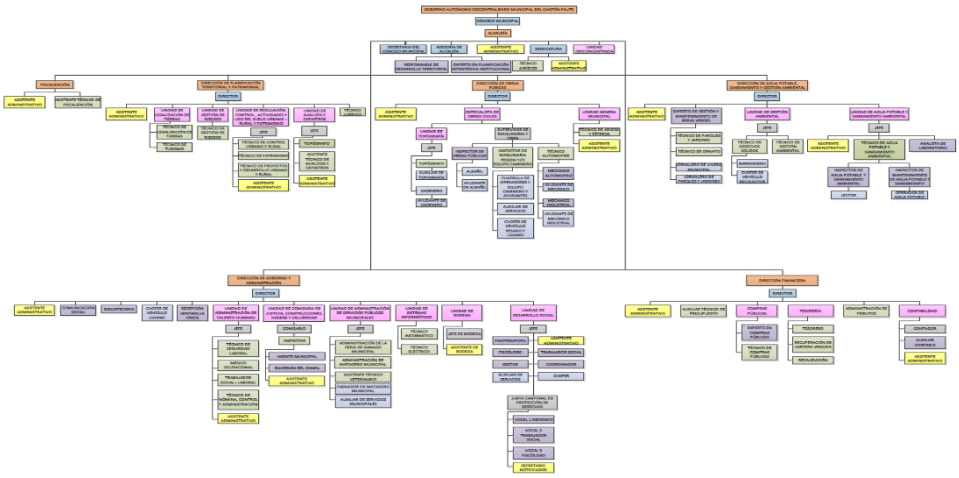
El GAD Municipal del Cantón Paute es una entidad gubernamental local responsable de la administración y gestión de los recursos y servicios municipales del cantón Paute. Su misión es promover el desarrollo integral del cantón mediante la implementación de políticas públicas que mejoren la calidad de vida de sus habitantes, fomentando el crecimiento sostenible y la participación ciudadana.

- **Misión**: Proveer servicios públicos eficientes y de calidad, promoviendo el desarrollo sostenible y el bienestar de la comunidad del cantón Paute.
- **Visión**: Ser un referente de excelencia en la gestión municipal, reconocido por su transparencia, eficiencia y compromiso con el desarrollo integral y sostenible del cantón Paute.

6.2 Estructura de la organización

El organigrama del GAD Municipal del Cantón Paute está diseñado para asegurar una gestión eficiente y coordinada de todas sus áreas. La Unidad de TIC´s juega un papel crucial en el soporte técnico y la gestión de la infraestructura tecnológica de la institución.

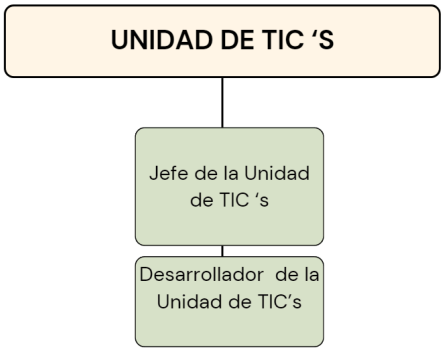
Figura 2.*Organigrama del Unidad de TIC'S del GAD-Paute*



Nota. La imagen muestra el organigrama que constituye la Unidad de TIC'S del GAD de Paute.

Fuente: Elaborado por los autores.

Figura 3.*Organigrama de la unidad de TIC´S*



Nota. La imagen muestra el organigrama que constituye la Unidad de TIC´s. Fuente: Elaborado por los autores.

Dichos organigramas representan la estructura organizativa del GAD Municipal del Cantón Paute. Proporcionando una representación visual de la jerarquía y relaciones dentro de la institución municipal y de la Unidad de TIC´s. Permitiendo una comprensión clara de la distribución de responsabilidades, niveles de autoridad y funciones dentro de cada área, lo que facilita la coordinación, la comunicación y la toma de decisiones eficiente.

6.3 Descripción de responsabilidades del personal de la Unidad de TIC´s

Jefe de la Unidad de TIC´s:

- Supervisa, coordina, planifica y controla actividades administrativas y técnicas.

- Supervisa las redes internas y externas de las autoridades municipales.
- Coordina la actualización y el mantenimiento de los sistemas.
- Verifica los soportes de información y bases de datos.
- Supervisa el desarrollo, mantenimiento y control del hardware y software.
- Comunicación con proveedores e intermediarios.
- Gestiona y planifica el presupuesto asignado por el GAD a la Unidad.

Desarrollador de la Unidad de TIC´s:

- Planifica, coordina, monitorea y controla actividades técnicas y administrativas.
- Opera redes internas y externas de las autoridades municipales.
- Controla y coordina la actualización y mantenimiento de los sistemas.
- Supervisa las copias de seguridad de la información y bases de datos.
- Desarrolla, mantiene y monitorea los equipos y sistemas tecnológicos.
- Realiza otras funciones asignadas por el jefe relacionados con su entorno.

6.4 Equipos y sistemas tecnológicos de la Unidad de TIC´s

La infraestructura tecnológica de la Unidad de TIC's incluye una variedad de equipos y sistemas que son esenciales para el funcionamiento y la seguridad de la

información. A continuación, se detallan los equipos y software manejados por la entidad:

Tabla 10.*Equipos con los que cuenta la institución.*

ID	Tipo	Nombre	Proceso
TICS-00019	SERVIDOR	SIGAME SERVIDOR VIRTUAL	TIC
TICS-00184	ROUTER	TPLINK INFORMATICA	TIC
TICS-00130	SWITH	SWITCH 5 PUERTOS	TIC
TICS-00196	MY CLOUD	NAS WDMYCLOUD1	TIC
TICS-00181	NVR	NVR CAMARAS GAD	TIC
TICS-00204	SERVIDOR	SERVIDOR ODOO VIRTUAL	TIC
TICS-00018	SERVIDOR	SAGA SERVIDOR VIRTUAL	TIC
TICS-00112	SWITCH	SWITCH CISCO SF-100-24	TIC
TICS-00020	SERVIDOR	ACTIVE DIRECTORY SERVIDOR VIRTUAL	TIC
TICS-00041	LAPTOP	HP PORTATIL PROBOOK	TIC
TICS-00052	LAPTOP	TIL DELL PRECISION 3571 15,6" I7-12800H 16G	TIC
TICS-00054	PC-ESCRITORIO	COMPUTADOR ADIT@	TIC
TICS-00023	IMPRESORA	EPSON WORKFORCE PRO WF-6590	TIC

Nota. La tabla muestra los equipos que conforman la institución. Fuente: Elaborada por los autores basada en información brindada por el personal de la Unidad de TIC´s.

Tabla 11.*Softwares manejados por la entidad.*

Área	Nombre	Proceso
TIC	MVWARE	TIC
TIC	PUTTY	TIC
TIC	ACTIVE DIRECTORY	TIC
TIC	CPANEL	TIC
TIC	WINBOX	TIC

TIC	NAVITCAD	TIC
TIC	IVMS-4200	TIC
TIC	CCLNEER	TIC
TIC	REVO	TIC
TIC	WICRESET	
ÁREAS VARIAS	ANYDESK	TIC
ÁREAS VARIAS	FIREFOX	TIC
ÁREAS VARIAS	MICROSOFT EDGE	TIC
ÁREAS VARIAS	ANTIVIRUS	TIC
ÁREAS VARIAS	ODOO	TIC
ÁREAS VARIAS	SAGA	TIC
ÁREAS VARIAS	SIGAME	TIC
ÁREAS VARIAS	FIRNAEC	TIC
ÁREAS VARIAS	AUTOCAD	TIC
ÁREAS VARIAS	MICROSOFT OFFICE	TIC
ÁREAS VARIAS	ZOOM	TIC
ÁREAS VARIAS	ADOBE READER	TIC
ÁREAS VARIAS	WINRAR	TIC
ÁREAS VARIAS	ADOBE PHOTOSHOP	TIC
Fuente obtenida de Autores		

Nota. La tabla muestra los softwares que conforman la Unidad de TIC'S del GAD-Paute.

Fuente: Elaborada por los autores basada en información brindada por el personal de la Unidad de TIC´s.

7. Análisis de la situación actual de la Unidad de TIC´s

7.1 Análisis DOFA – situación actual

Se realizó un análisis FODA (Fortalezas, Oportunidades, Debilidades y Amenazas) con el objetivo de examinar de manera integral los aspectos y evidencias, visibles en los Anexo3 y Anexo6, en el más relevantes de la Unidad de TIC. Este proceso nos permitió identificar y evaluar tanto los puntos fuertes y oportunidades que pueden

aprovecharse para el crecimiento y desarrollo de la Unidad, como las áreas de mejora y posibles desafíos que deben abordarse.

En base a las encuestas cualitativas y entrevistas, se elaboró el FODA que destaca la necesidad urgente de fortalecer la seguridad de la información. A pesar de contar con medidas como el acceso restringido a la información y copias de seguridad diarias, la Unidad de TIC enfrenta debilidades críticas como la falta de procesos de seguridad de información adecuados y la ausencia de auditorías informáticas regulares.

Además, la dependencia de proveedores externos y la falta de un plan estratégico aumentan significativamente los riesgos de seguridad. Las oportunidades identificadas, como la implementación de estándares internacionales y la inversión en infraestructura de TI, son vitales para contrarrestar amenazas como el incremento de ataques cibernéticos y la evolución constante de nuevas amenazas.

La realización de auditorías regulares y la capacitación continua del personal son esenciales para crear un entorno seguro y resiliente. Este análisis permite dirigir los esfuerzos a priorizar la seguridad de la información, enfocándonos en la identificación de riesgos y vulnerabilidades, estableciendo una base sólida para el diseño de un plan estratégico adecuado. Dicha prioridad es compartida con el jefe de la Unidad de TIC´s, puesto que les beneficiará para sentar una base en futuros proyectos tecnológicos del departamento.

- **Fortalezas**

Tabla 12. *Fortalezas identificadas.*

Fortalezas	
F 1	Acceso restringido de la información mediante firewall y seguridad del disco en la nube para personal ajeno
F 2	Realizan copias de seguridad diarias (Backups c/día)
F 3	Establecen políticas de claves exclusivas laborales
F 4	Identificación proactiva de riesgos y vulnerabilidades
F 5	Revisión periódica de sistemas informáticos (cobranzas, rubros de compras, financiero, etc)
F 6	Existe documentación y estatus de procesos establecidos

Nota. La tabla muestra el FODA aplicado. Fuente: Elaborado por los autores.

- **Debilidades**

Tabla 13. *Debilidades identificadas.*

Debilidades	
D1	Sala de servidores en mal estado: desorden y equipos en deterioro
D2	Cambio de claves anual
D3	Falta de procesos de seguridad de información adecuados
D4	Anotación de claves personales en notas físicas
D5	Falta de auditorías informáticas
D6	Dependencia de proveedores para sistemas informáticos
D7	Caídas frecuentes del sistema informático Externo
D8	Ausencia de una estrategia o plan estratégico en TI
D9	Presupuesto inadecuado: falta de inversión en TI
D10	Insuficiencia de personal adecuado para cubrir todas las funciones del departamento
D11	Falta de un plan de acción para la seguridad de la información
D12	NO dispone de generador eléctrico, afectando la disponibilidad del Data center
D13	Redes IP no encriptadas
D14	Equipos informáticos en mal estado
D15	Ausencia d políticas estandarizadas

D16	Falta de capacitación en seguridad de la información
D17	Uso parcial de licencias de software originales
D18	Acceso físico al área de servidores sin protección adecuada
D19	Falta de un servidor alterno, afectando la continuidad operativa

Nota. La tabla muestra el FODA aplicado. Fuente: Elaborado por los autores.

- **Oportunidad**

Tabla 14.*Oportunidades identificadas.*

Oportunidades	
O1	Implementación de estándares internacionales
O2	Capacitación continua del personal
O3	Inversión en infraestructura de TI
O4	Adopción de nuevas tecnologías
O5	Desarrollo de un plan estratégico de Seguridad de la información
O6	Obtención de funcionamiento adicional
O7	Auditorias regulares
O8	Colaboración con otros municipios

Nota. La tabla muestra el FODA aplicado. Fuente: Elaborado por los autores.

- **Amenazas**

Tabla 15. *Amenazas identificadas.*

Amenazas	
A1	Incremento de ataques cibernéticos
A2	Evolución constante de amenazas
A3	Dependencia de proveedores externos
A4	Falta de recursos financieros
A5	Desastres naturales y fallo de infraestructura
A6	Cumplimiento regulatorio
A7	Amenazas internas
A8	Falta de capacitación continua

Nota. La tabla muestra el FODA aplicado. Fuente: Elaborado por los autores.

7.2 Identificación de riesgos

Para la identificación de riesgos en la Unidad de TIC's del GAD Municipal del Cantón Paute, se utilizarán varias técnicas y herramientas para garantizar una identificación exhaustiva y precisa de todos los posibles riesgos. Este proceso incluyo entrevistas y encuestas con el personal clave y revisiones documentales. Estos métodos permiten recopilar información valiosa y detallada sobre los riesgos a los que está expuesta la unidad de TIC´s.

7.2.1 Metodología de Evaluación de Riesgos

La evaluación de riesgos en el contexto de la ISO 27001 implica un proceso sistemático que incluye la identificación, análisis y evaluación de riesgos asociados con la pérdida de confidencialidad, integridad y disponibilidad de la información. Para llevar a cabo esta evaluación, se seguirán los siguientes pasos:

Establecer Criterios de Riesgo:

Criterios de Impacto:

- **Alto**: La pérdida o el compromiso de la información tiene consecuencias graves para la organización, tales como pérdidas financieras significativas, daños a la reputación o incumplimiento de regulaciones.
- **Medio**: La pérdida o el compromiso de la información tiene consecuencias moderadas, incluyendo interrupciones en los procesos de negocio y afectaciones temporales a la reputación.
- **Bajo**: La pérdida o el compromiso de la información tiene un impacto menor, con consecuencias limitadas y fácilmente manejables.

Criterios de Probabilidad:

- **Alta**: Existe una alta probabilidad de que el riesgo ocurra debido a la frecuencia de la amenaza o la existencia de vulnerabilidades significativas.
- **Media**: La probabilidad de que el riesgo ocurra es moderada, y aunque las amenazas son presentes, las vulnerabilidades son parcialmente controladas.
- **Baja**: La probabilidad de que el riesgo ocurra es baja, ya que existen controles efectivos y la frecuencia de la amenaza es limitada.

7.2.2 Identificación de activos y evaluación de vulnerabilidades

Para realizar una identificación exhaustiva de los activos y sus vulnerabilidades, se utilizarán las tablas presentadas anteriormente sobre equipos y software.

Dichas tablas mencionadas son la **tabla 10** y **tabla 11.**

7.2.2.1 Identificación de Amenazas

Las amenazas son eventos potenciales que pueden explotar las vulnerabilidades y causar daños a los activos de información. A continuación, se enumeran algunas amenazas comunes:

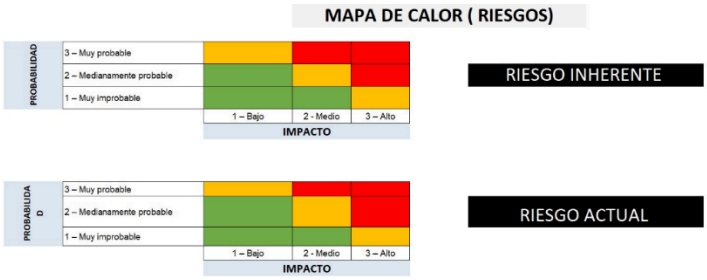
- **Amenazas Internas**:
  - Errores humanos (configuración incorrecta de sistemas, eliminación accidental de datos).
  - Fallos del sistema (hardware defectuoso, software desactualizado).
  - Accesos no autorizados por parte del personal interno.
- **Amenazas Externas**:
  - Ciberataques (malware, ransomware, phishing).
  - Desastres naturales (incendios, inundaciones).

- Fallos de infraestructura (cortes de energía, fallos en el suministro de internet).

7.2.2.2 Análisis de Riesgos

El análisis de riesgos implica combinar la probabilidad y el impacto de las amenazas para evaluar el nivel de riesgo. Utilizando una matriz de riesgo, se puede visualizar y categorizar. La finalidad de dicha matriz es proporcionar una base sólida para la gestión de riesgos inherentes y actuales, permitiendo una toma de decisiones informada y la implementación de controles efectivos para minimizar el impacto de las amenazas en los activos de información (IT Governance, 2022).

Figura 4.*Mapa de calor de riesgos ISO 27001:2022*



Nota. La figura muestra el mapa de calor que define los niveles de clasificación de los riesgos inherente y actuales que se encontraron para el plan. Fuente: Elaborado por los autores

Descripción de los Colores en el Mapa de Calor de Riesgos

Verde

- **Probabilidad**: Muy improbable (1)
- **Impacto**: Bajo (1), Medio (2)
- **Descripción**: Los riesgos en esta área son considerados de bajo impacto y muy baja probabilidad. Estos riesgos son los menos críticos y requieren una mínima atención y monitoreo.

Amarillo

- **Probabilidad**: Medianamente probable (2)
- **Impacto**: Bajo (1), Medio (2)
- **Descripción**: Los riesgos en esta área son de probabilidad e impacto moderado. Deben ser gestionados para asegurar que no escalen y se conviertan en problemas más serios.

Rojo

- **Probabilidad**: Medianamente probable (2), Muy probable (3)
- I**mpacto**: Medio (2), Alto (3)
- **Descripción**: Los riesgos en esta área son críticos debido a su alta probabilidad y/o alto impacto. Requieren atención inmediata y acciones de mitigación robustas.

Aplicación del Mapa de Calor

- **Riesgo Inherente:** Representa el nivel de riesgo antes de implementar cualquier control. Aquí es donde inicialmente se mapea el riesgo sin considerar medidas de mitigación.

- **Riesgo Actual:** Representa el nivel de riesgo después de implementar los controles detectados. Este es el riesgo residual que queda después de las acciones de mitigación.

Figura 5.*Matriz de riesgo de activos ISO 27001:2022*

MATRIZ DE RIESGOS DE ACTIVOS

IDENTIFICACIÓN DE RIESGO						RIESGO INHERENTE												RIESGO ACTUAL			
						EVALUACIÓN DE RIESGOS															
						Valoración del Impacto															
						Confidencialidad		Integridad		Disponibilidad		Impacto CID (C+I+D)/3	PROBABILIDAD		Cálculo de Evaluación Riesgo	Cálculo de Evaluación Riesgo	Nivel de Riesgo	Tipo de Control	Controles detectados	Nivel de Efectividad Controles	Nivel de Riesgo con el Control Implementado
ID RIESGO	Activo	Tipo Activo	Amenaza	Vulnerabilidad	Descripción Riesgo																
RTI-001+A7: S7	Sala de servidores	ormación Fí	Fallas en el hardware	Falta de entrenamiento en seguridad de la información	Fallas en el hardware debido a falta de entrenamiento en seguridad de la información sobre el activo sala de servidores	2	MEDIO	3	ALTO	3	ALTO	2	3	MUY PROBABLE	6	ALTO	ALTO	PREVENTIVO	Monitoreo y alerta	ALTA	MEDIO
RTI-002	Cambio de claves anual	Software	Ataque Informático	Falta de políticas / normas / procedimientos / estándares	Ataque Informático debido a falta de políticas / normas / procedimientos / estándares sobre el activo cambio de claves anual	3	ALTO	1	BAJO	3	ALTO	2	3	MUY PROBABLE	6	ALTO	ALTO	PREVENTIVO	Monitoreo y alerta	MUY BAJA	ALTO
RTI-003	Procesos de seguridad de informacion	Servicio	Ataque Informático	Falta de entrenamiento en seguridad de la información	Ataque Informático debido a falta de entrenamiento en seguridad de la información sobre el activo procesos de seguridad de informacion	2	MEDIO	2	MEDIO	2	MEDIO	2	2	MEDIANAMENTE PROBABLE	4	MEDIO	MEDIO	PREVENTIVO	Monitoreo y alerta	MUY BAJA	MEDIO
RTI-004	Claves personales	Persona	Divulgación de información	Debilidad en las contraseñas	Divulgación de información debido a debilidad en las contraseñas sobre el activo claves personales	3	ALTO	3	ALTO	3	ALTO	3	3	MUY PROBABLE	9	ALTO	ALTO	PREVENTIVO	Monitoreo y alerta	MUY BAJA	ALTO
RTI-005	Auditorias informaticas	Servicio	Fuga, robo o perdida de información	Falta de generación y monitoreo de registros de auditoria	Fuga, robo o perdida de información debido a falta de generación y monitoreo de registros de auditoria sobre el activo auditorias informaticas	3	ALTO	2	MEDIO	3	ALTO	2	2	MEDIANAMENTE PROBABLE	4	MEDIO	MEDIO	PREVENTIVO	Politicas y Procedimeinto	MUY BAJA	MEDIO
RTI-006	Proveedores sistemas infromaticos	Software	Fallas en el servicio	Falta de controles en el intercambio de información	Fallas en el servicio debido a falta de controles en el intercambio de información sobre el activo proveedores sistemas infromaticos	3	ALTO	3	ALTO	2	MEDIO	2	2	MEDIANAMENTE PROBABLE	4	MEDIO	MEDIO	PREVENTIVO	Politicas y Procedimeinto	MUY BAJA	MEDIO
RTI-007	Fallo sistema infromatico externo	Software	Fallas en el dispositivo	Falta de políticas / normas / procedimientos / estándares	Fallas en el dispositivo debido a falta de políticas / normas / procedimientos / estándares sobre el activo fallo sistema infromatico externo	2	MEDIO	3	ALTO	3	ALTO	2	2	MEDIANAMENTE PROBABLE	4	MEDIO	MEDIO	PREVENTIVO	Politicas y Procedimeinto	MUY BAJA	MEDIO
RTI-008	Plan estrategico de TI	Software	Ataque Informático	Falta de entrenamiento en seguridad de la información	Ataque Informático debido a falta de entrenamiento en seguridad de la información sobre el activo plan estrategico de ti	3	ALTO	2	MEDIO	3	ALTO	2	2	MEDIANAMENTE PROBABLE	4	MEDIO	MEDIO	PREVENTIVO	Monitoreo y alerta	MUY BAJA	MEDIO

RTI-009	Presupuesto inadecuado	Persona	Ocurrencia o reincidencia de incidentes	Falta de políticas / normas / procedimientos / estándares	Ocurrencia o reincidencia de incidentes debido a falta de políticas / normas / procedimientos / estándares sobre el activo presupuesto inadecuado	3	ALTO	2	MEDIO	3	ALTO	2	2	MEDIANAMENTE PROBABLE	4	MEDIO	MEDIO	PREVENTIVO	Monitoreo y alerta	MUY BAJA	MEDIO
RTI-0010	Insuficiencia de personal	Persona	Ocurrencia o reincidencia de incidentes	Falta de gestión de vulnerabilidades	Ocurrencia o reincidencia de incidentes debido a falta de gestión de vulnerabilidades sobre el activo insuficiencia de personal	3	ALTO	2	MEDIO	3	ALTO	2	2	MEDIANAMENTE PROBABLE	4	MEDIO	MEDIO	PREVENTIVO	Acceso de control	MUY BAJA	MEDIO
RTI-0011	Plan de accion de seguridad de informacion	Software	Ataque Informático	Falta de gestión de vulnerabilidades	Ataque Informático debido a falta de gestión de vulnerabilidades sobre el activo plan de accion de seguridad de informacion	3	ALTO	3	ALTO	3	ALTO	3	3	MUY PROBABLE	9	ALTO	ALTO	PREVENTIVO	Acceso de control	MUY BAJA	ALTO
RTI-0012	Generador electrico	Información Electrónica	Fallas en el servicio	Concentración de funciones	Fallas en el servicio debido a concentración de funciones sobre el activo generador electrico	3	ALTO	3	ALTO	3	ALTO	3	2	MEDIANAMENTE PROBABLE	6	ALTO	ALTO	PREVENTIVO	Monitoreo y alerta	MUY BAJA	ALTO
RTI-0013	Redes ip no encriptadas	Red	Ataque Informático	Falta de gestión de incidentes de seguridad	Ataque Informático debido a falta de gestión de incidentes de seguridad sobre el activo redes ip no encriptadas	3	ALTO	3	ALTO	2	MEDIO	2	1	MUY IMPROBABLE	2	BAJO	BAJO	PREVENTIVO	Politicas y Procedimeinto	MUY BAJA	BAJO
RTI-0014	Equipos informaticos mal estado	Hardware	Fallas en el servicio	Falta de gestión de vulnerabilidades	Fallas en el servicio debido a falta de gestión de vulnerabilidades sobre el activo equipos informaticos mal estado	3	ALTO	2	MEDIO	2	MEDIO	2	3	MUY PROBABLE	6	ALTO	ALTO	PREVENTIVO	Politicas y Procedimeinto	MUY BAJA	ALTO
RTI-0015	Falta de capacitacion continua	Persona	Errores de mantenimiento / actualización de programas (software)	Falta de políticas / normas / procedimientos / estándares	Errores de mantenimiento / actualización de programas (software) debido a falta de políticas / normas / procedimientos / estándares sobre el activo falta de capacitacion continua	3	ALTO	2	MEDIO	3	ALTO	2	2	MEDIANAMENTE PROBABLE	4	MEDIO	MEDIO	PREVENTIVO	Politicas y Procedimeinto	MUY BAJA	MEDIO
RTI-0016	Ausencia politicas estandarizadas	Servicio	Ataque Informático	Falta de políticas / normas / procedimientos / estándares	Ataque Informático debido a falta de políticas / normas / procedimientos / estándares sobre el activo ausencia politicas estandarizadas	3	ALTO	2	MEDIO	3	ALTO	2	3	MUY PROBABLE	6	ALTO	ALTO	PREVENTIVO	Monitoreo y alerta	MUY BAJA	ALTO
RTI-0017	Uso parcial icencias de sofware originales	Software	Fuga, robo o perdida de información	Falta de monitoreo de privilegios	Fuga, robo o perdida de información debido a falta de monitoreo de privilegios sobre el activo uso parcial icencias de sofware originales	2	MEDIO	2	MEDIO	3	ALTO	2	2	MEDIANAMENTE PROBABLE	4	MEDIO	MEDIO	PREVENTIVO	Politicas y Procedimeinto	MUY BAJA	MEDIO
RTI-0018	Acceso fisico area de servidores sin proteccion adecuada	Persona	Ocurrencia o reincidencia de incidentes	Falta de políticas / normas / procedimientos / estándares	Ocurrencia o reincidencia de incidentes debido a falta de políticas / normas / procedimientos / estándares sobre el activo acceso fisico area de servidores sin proteccion adecuada	3	ALTO	2	MEDIO	2	MEDIO	2	3	MUY PROBABLE	6	ALTO	ALTO	PREVENTIVO	Monitoreo y alerta	MUY BAJA	ALTO
RTI-0019	Falta de un servidor alterno	Información Fisica	Fallas en el dispositivo	Falta de gestión de vulnerabilidades	Fallas en el dispositivo debido a falta de gestión de vulnerabilidades sobre el activo falta de un servidor alterno	3	ALTO	2	MEDIO	2	MEDIO	2	3	MUY PROBABLE	6	ALTO	ALTO	PREVENTIVO	Monitoreo y alerta	MUY BAJA	ALTO
RTI-0020	Incrementos de ataques ciberneticos	Base de Datos	Ataque Informático	Falta de monitoreo de privilegios	Ataque Informático debido a falta de monitoreo de privilegios sobre el activo incrementos de	3	ALTO	2	MEDIO	2	MEDIO	2	3	MUY PROBABLE	6	ALTO	ALTO	PREVENTIVO	Monitoreo y alerta	MUY BAJA	ALTO
RTI-0021	Evolucion constante de amenazas	Servicio	Alteración, Eliminación, Pérdida o Robo de los dispositivos	Manipulación de los equipos	Alteración, Eliminación, Pérdida o Robo de los dispositivos debido a manipulación de los equipos sobre el activo evolucion constante de amenazas	3	ALTO	2	MEDIO	2	MEDIO	2	2	MEDIANAMENTE PROBABLE	4	MEDIO	MEDIO	PREVENTIVO	Politicas y Procedimeinto	MUY BAJA	MEDIO
RTI-0022	Desastres naturales	Servicio	Condiciones inadecuadas de temperatura o humedad	Falta de monitoreo de las condiciones ambientales	Condiciones inadecuadas de temperatura o humedad debido a falta de monitoreo de las condiciones ambientales sobre el activo desastres naturales	3	ALTO	2	MEDIO	2	MEDIO	2	3	MUY PROBABLE	6	ALTO	ALTO	PREVENTIVO	Monitoreo y alerta	MUY BAJA	ALTO
RTI-0023	Cumplimiento regulatori	Servicio	Ataque Informático	Falta de controles sobre la gestión del cambio	Ataque Informático debido a falta de controles sobre la gestión del cambio sobre el activo cumplimiento regulatorio	3	ALTO	2	MEDIO	3	ALTO	2	1	MUY IMPROBABLE	2	BAJO	BAJO	CORRECTIVO	Acceso de control	MUY BAJA	BAJO

Nota. La tabla muestra los factores de riesgo y vulnerabilidades que se encontraron para el PESI. Fuente: Elaborado por los investigadores.

7.2.2.3 Priorización de Riesgos

La evaluación de riesgos implica determinar la gravedad de cada riesgo identificado en la matriz, considerando tanto la probabilidad de que ocurra como su impacto en la organización. Este proceso ayuda a enfocar los recursos y esfuerzos en los riesgos más críticos para la seguridad de la información.

Criterios de Evaluación:

- **Probabilidad:** La frecuencia con la que se espera que ocurra el riesgo.
- **Impacto:** La gravedad de las consecuencias si el riesgo llega a materializarse.

Estos criterios se combinan en una escala de evaluación que categoriza los riesgos en niveles bajo, medio y alto.

Proceso de Evaluación:

- Asignar un valor a la probabilidad de cada riesgo (bajo, medio, alto).
- Asignar un valor al impacto de cada riesgo (bajo, medio, alto).
- Utilizar la matriz de riesgos para determinar el nivel de riesgo combinando probabilidad e impacto.

Priorización de Riesgos

La priorización de riesgos consiste en clasificar los riesgos evaluados según su nivel de criticidad. Esta clasificación ayuda a decidir el orden en que los riesgos deben ser abordados y mitigados.

- **Criterios de Priorización:**
    - **Nivel de Riesgo:** Riesgos clasificados como altos serán priorizados sobre los de nivel medio y bajo.
    - **Impacto en la Continuidad del Negocio:** Riesgos que amenacen la continuidad operativa del GAD Municipal del Cantón Paute serán priorizados.
- **Proceso de Priorización:**
    - Clasificar los riesgos evaluados de acuerdo con los criterios mencionados.
    - Generar una lista priorizada de riesgos que guiará la implementación de controles y medidas de mitigación.

La tabla de priorización de riesgos refleja una clasificación basada en la gravedad y la probabilidad de cada riesgo identificado. Los riesgos se ordenan de mayor a menor prioridad según el impacto que tendrían en la seguridad de la información y la operatividad del departamento de TIC's. Esta priorización es fundamental para asegurar que los recursos y esfuerzos se dirijan hacia los riesgos que presentan una amenaza más significativa. A continuación, se interpretan algunos de los riesgos más críticos:

Tabla 16. *Priorización de riesgos del PESI*

Tipo de riesgo	Nivel de Riesgo	Impacto	Prioridad
Sala de servidores en mal estado: desorden y equipos en deterioro	Alto	Alto	**1**
Falta de procesos de seguridad de información adecuados	Alto	Alto	**2**
Falta de un plan de acción para la seguridad de la información	Alto	Alto	**3**

Ausencia de políticas estandarizadas	Alto	Alto	**4**
No dispone de generador eléctrico, afecta disponibilidad del Data center	Alto	Alto	**5**
Presupuesto inadecuado: falta de inversión en TI	Alto	Alto	**6**
Equipos informáticos mal estado	Alto	Alto	**7**
Ausencia de una estrategia o plan estratégico en TI	Alto	Alto	**8**
Presupuesto inadecuado	Medio	Medio	**9**
Insuficiente personal	Medio	Medio	**10**
Falta de capacitación continua	Medio	Medio	**11**

Nota: La tabla muestra los riesgos prioritarios identificados de la matriz de riesgo de activos basado. Fuente: Elaborado por los investigadores.

7.2.2.4 Evaluación y tratamiento de riesgos

Evaluación de los riesgos prioritarios

Esta evaluación cubre los riesgos más críticos y sus estrategias de mitigación basadas en las mejores prácticas de la norma ISO 27001 (ISO/IEC, 2022).

1. Sala de servidores en mal estado: desorden y equipos en deterioro

- **Causa raíz:** La falta de mantenimiento regular y la ausencia de un plan estructurado para la renovación de equipos han llevado al deterioro físico y funcional de la sala de servidores.
- **Consecuencia:** La falta de mantenimiento y orden en la sala de servidores puede resultar en la interrupción de servicios críticos, pérdida de datos, y mayor vulnerabilidad a fallos de hardware.
- **Medidas actuales:** Monitoreo esporádico sin un plan de mantenimiento estructurado.
- **Estrategia de mitigación:** Implementar un plan de mantenimiento preventivo y correctivo (ISO/IEC 27001:2022, Control A.11.2.4), organizar la sala de servidores y renovar los equipos obsoletos. Adicionalmente, considerar la implementación de controles de acceso físico (ISO/IEC 27001:2022, Control A.11.1.1).

2. Falta de procesos de seguridad de información adecuados

- **Causa raíz:** La inexistencia de políticas y procedimientos formales para la gestión de la seguridad de la información.
- **Consecuencia:** La ausencia de procesos de seguridad puede llevar a la exposición de información sensible, aumento de la vulnerabilidad a ataques y brechas de seguridad.
- **Medidas actuales:** Procesos ad-hoc sin formalización.
- **Estrategia de mitigación:** Desarrollar e implementar políticas y procedimientos de seguridad de la información, incluyendo la gestión de acceso, cifrado de datos y auditorías regulares. Las buenas prácticas de la ISO 27001 recomiendan establecer un marco de control claro y estructurado para garantizar la protección de la información (ISO/IEC 27001:2022, Control A.5.1.1).

3. Falta de un plan de acción para la seguridad de la información

- **Causa raíz:** La carencia de un enfoque estratégico y sistemático para abordar la seguridad de la información.

- **Consecuencia:** La falta de un plan puede resultar en una respuesta inadecuada a incidentes de seguridad, incrementando el tiempo de recuperación y la exposición a riesgos.
- **Medidas actuales:** Reacciones reactivas a incidentes de seguridad.
- **Estrategia de mitigación:** Desarrollar un plan de acción detallado para la seguridad de la información que incluya procedimientos de respuesta a incidentes, planes de contingencia y recuperación ante desastres. Estas prácticas están alineadas con los controles recomendados por la ISO 27001 para asegurar la resiliencia operativa (ISO/IEC 27001:2022, Control A.16.1.5).

3. Ausencia de políticas estandarizadas

- **Causa raíz:** La falta de un marco de trabajo estandarizado para la creación y mantenimiento de políticas de seguridad.
- **Consecuencia:** La inexistencia de políticas estandarizadas puede llevar a la inconsistencia en la aplicación de medidas de seguridad, incrementando la vulnerabilidad a ataques.
- **Medidas actuales:** Políticas inconsistentes y no estandarizadas.
- **Estrategia de mitigación:** Desarrollar y formalizar políticas de seguridad estandarizadas basadas en las mejores prácticas de ISO 27001, asegurando su revisión y actualización periódica. Dicha norma destaca la importancia de contar con políticas coherentes y actualizadas para mantener un entorno seguro (ISO/IEC 27001:2022, Control A.5.1.1).

4. No dispone de generador eléctrico, afectando la disponibilidad del Data Center

- **Causa raíz:** La falta de inversión en infraestructura de respaldo energético.
- **Consecuencia:** La ausencia de un generador eléctrico puede provocar la interrupción total de los servicios en caso de fallos eléctricos, afectando la disponibilidad del Data Center.
- **Medidas actuales:** Dependencia total del suministro eléctrico externo.
- **Estrategia de mitigación:** Adquirir e instalar un generador eléctrico de respaldo para garantizar la continuidad operativa del Data Center durante cortes de energía. La norma

ISO 27001 subraya la necesidad de contar con medidas de continuidad del negocio para mantener la disponibilidad de los servicios críticos (ISO/IEC 27001:2022, Control A.17.2.1).

5. **Presupuesto inadecuado: falta de inversión en TI**

- **Causa raíz:** La asignación insuficiente de recursos financieros para el área de TI.
- **Consecuencia:** La falta de inversión en TI puede resultar en infraestructura obsoleta, personal insuficiente y limitaciones para implementar mejoras necesarias.
- **Medidas actuales:** Prioridades de presupuesto orientadas a otras áreas.
- **Estrategia de mitigación:** Presentar un caso de negocio sólido a la dirección para aumentar el presupuesto de TI, destacando la importancia de la seguridad de la información para la operación continua y la protección de datos. La ISO 27001 recomienda la asignación adecuada de recursos para garantizar una gestión efectiva de la seguridad de la información (ISO/IEC 27001:2022, Control A.6.1.2).

6. **Incremento de ataques cibernéticos**

- **Causa raíz:** La evolución constante de las técnicas de ataque y el aumento en la sofisticación de los cibercriminales.
- **Consecuencia:** La mayor frecuencia de ataques cibernéticos puede comprometer la seguridad de la información, resultando en pérdida de datos y daños a la reputación.
- **Medidas actuales:** Protección básica con firewall y antivirus.
- **Estrategia de mitigación:** Implementar un sistema de detección y respuesta a incidentes (IDS/IPS), realizar auditorías de seguridad periódicas y capacitar al personal en ciberseguridad. Estas medidas están alineadas con los controles de la ISO 27001 para proteger contra amenazas externas (ISO/IEC 27001:2022, Control A.12.4.1).

7.3 Plan de implementación

Esta fase del PESI detallará las acciones necesarias para poner en práctica las estrategias de mitigación identificadas en la evaluación de riesgos. El plan de implementación

incluirá la definición de responsabilidades, la asignación de recursos y la elaboración de un cronograma.

El objetivo es asegurar que cada medida de mitigación sea ejecutada de manera efectiva y oportuna, alineándose con los objetivos estratégicos del PESI y siguiendo las mejores prácticas de la norma ISO 27001.

7.3.1 Definición de responsabilidades

Para cada acción de mitigación, se asignarán responsabilidades específicas a los miembros del equipo de la Unidad de TIC's. Esto incluye identificar quién será responsable de supervisar y ejecutar cada acción, así como definir los roles de apoyo necesarios.

Acción: Implementar un plan de mantenimiento preventivo y correctivo para la sala de servidores.

- **Responsable**: Jefe de la unidad de TIC's
- **Apoyo**: Desarrollador de la unidad de TIC's

Acción: Desarrollar e implementar políticas y procedimientos de seguridad de la información.

- **Responsable:** Jefe de la Unidad de TIC's
- **Apoyo:** Equipo de seguridad de la información

Acción: Desarrollar un plan de acción detallado para la seguridad de la información.

- **Responsable:** Jefe de la Unidad de TIC's
- **Apoyo:** Desarrollador de la Unidad de TIC's

Acción: Adquirir e instalar un generador eléctrico de respaldo.

- **Responsable:** Jefe de la Unidad de TIC's
- **Apoyo:** Equipo de seguridad de la información

Acción: Presentar un caso de negocio para aumentar el presupuesto de TI.

- **Responsable:** Jefe de la Unidad de TIC's
- **Apoyo:** Equipo de seguridad de la información

Acción: Implementar un sistema de detección y respuesta a incidentes (IDS/IPS).

- **Responsable:** Jefe de la Unidad de TIC's
- **Apoyo:** Equipo de seguridad de la información

7.3.2 Asignación de recursos

Cada acción de mitigación requerirá una asignación adecuada de recursos para su ejecución. Esto incluye tanto recursos financieros como humanos.

Acción: Implementar un plan de mantenimiento preventivo y correctivo para la sala de servidores.

- **Recursos financieros:** Presupuesto para renovación de equipos y mantenimiento.
- **Recursos humanos:** Personal técnico para realizar el mantenimiento.

Acción: Desarrollar e implementar políticas y procedimientos de seguridad de la información.

- **Recursos financieros:** Presupuesto para consultoría en seguridad de la información.

- **Recursos humanos:** Personal de seguridad de la información y consultores externos.

Acción: Adquirir e instalar un generador eléctrico de respaldo

- **Recursos financieros:** Presupuesto para la compra e instalación del generador.
- **Recursos humanos:** Personal técnico para la instalación y mantenimiento.

Acción: Presentar un caso de negocio para aumentar el presupuesto de TI.

- **Recursos financieros:** Presupuesto para la elaboración del caso de negocio.
- **Recursos humanos:** Personal del equipo financiero y de la Unidad de TIC's.

Acción: Implementar un sistema de detección y respuesta a incidentes (IDS/IPS).

- **Recursos financieros:** Presupuesto para la adquisición e implementación del sistema IDS/IPS.
- **Recursos humanos:** Personal de seguridad de la información y soporte técnico.

7.3.3 Etapas de implementación

Acción: Implementar un plan de mantenimiento preventivo y correctivo para la sala de servidores.

- **Etapas**:
    - **Evaluación inicial:** Inspección completa de la sala de servidores para identificar necesidades de mantenimiento.
    - **Desarrollo del plan:** Creación de un calendario de mantenimiento preventivo y correctivo.
    - **Ejecución**: Realización de tareas de mantenimiento según el plan.

- **Revisión**: Evaluación periódica del estado de los servidores y ajustes al plan de mantenimiento.

Acción: Desarrollar e implementar políticas y procedimientos de seguridad de la información.

- **Etapas**:
  - **Revisión de políticas existentes:** Evaluación de las políticas actuales y sus deficiencias.
  - **Desarrollo de nuevas políticas:** Creación de políticas y procedimientos basados en ISO 27001.
  - **Implementación:** Comunicación y aplicación de las nuevas políticas.
  - **Monitoreo:** Seguimiento y auditoría de la implementación y efectividad de las políticas.

Acción: Desarrollar un plan de acción detallado para la seguridad de la información.

- **Etapas**:
  - **Análisis de necesidades:** Identificación de áreas críticas que requieren un plan de acción.
  - **Desarrollo del plan:** Creación de un plan de acción que incluya procedimientos de respuesta a incidentes y planes de contingencia.
  - **Implementación:** Ejecución del plan y capacitación del personal.
  - **Revisión:** Evaluación y actualización periódica del plan de acción.

Acción: Adquirir e instalar un generador eléctrico de respaldo.

- **Etapas**:
    - **Evaluación de necesidades:** Identificación de los requisitos energéticos del Data Center.
    - **Adquisición:** Compra del generador adecuado.
    - **Instalación:** Configuración y prueba del generador.
    - **Mantenimiento:** Establecimiento de un plan de mantenimiento regular para el generador.

Acción: Presentar un caso de negocio para aumentar el presupuesto de TI.

- **Etapas**:
    - **Recolección de datos:** Identificación de necesidades y beneficios de un mayor presupuesto.
    - **Desarrollo del caso:** Creación de un documento que resuma la importancia de la inversión en TI.
    - **Presentación:** Exposición del caso de negocio a la dirección.
    - **Revisión:** Ajuste y refinamiento del caso según el feedback recibido.

Acción: Implementar un sistema de detección y respuesta a incidentes (IDS/IPS).

- **Etapas**:

- **Evaluación de necesidades:** Identificación de los requisitos de seguridad para el sistema IDS/IPS.
- **Adquisición**: Compra e instalación del sistema IDS/IPS.
- **Configuración**: Configuración inicial y prueba del sistema.
- **Monitoreo**: Monitoreo continuo y ajuste del sistema según sea necesario.

Esta fase del PESI permite asegurar que las estrategias de mitigación se realicen de manera estructurada y efectiva, alineándose con las mejores prácticas de la norma ISO 27001. Este enfoque sistemático es crucial para fortalecer la seguridad de la información en la Unidad de TIC's del GAD Municipal del Cantón Paute.

7.4 Seguimiento y evaluación

Para asegurar la correcta implementación del plan, se establecerán mecanismos de seguimiento y control, tal como lo señala la norma (ISO/IEC, 2022) .

Esta fase tiene la finalidad de:

- **Garantizar la eficacia de las medidas implementadas:** Asegura que las estrategias de mitigación estén funcionando como se espera.
- **Identificar áreas de mejora:** Detecta debilidades o deficiencias para acciones correctivas.
- **Asegurar la conformidad:** Verificar que las políticas y procedimientos cumplan con la ISO 27001.
- **Adaptación continua:** Ajusta las estrategias en respuesta a nuevos riesgos o cambios tecnológicos.

Actividades

- **Monitoreo continuo:**

  Control A.12.4.1: Implementar sistemas de monitoreo continuo para detectar eventos de seguridad. Utilizar herramientas automatizadas para alertas en tiempo real sobre anomalías o brechas.

- **Auditorías internas:**

  Control A.18.2.2: Realizar auditorías internas periódicas para revisar la conformidad con políticas y procedimientos, y la efectividad de los controles de seguridad. Documentar hallazgos y recomendaciones.

- **Revisiones periódicas:**

  Control A.18.1.1: Programar revisiones del PESI trimestralmente y anualmente para evaluar su relevancia y efectividad. Revisar y actualizar el análisis de riesgos según cambios en el entorno o nuevas amenazas.

- **Informes de incidentes:**

  Control A.16.1.2: Establecer procedimientos para la notificación, documentación y análisis de incidentes de seguridad. Utilizar los informes para identificar patrones y ajustar estrategias de mitigación.

- **Evaluación de la capacitación:**

  Control A.7.2.2: Evaluar periódicamente la efectividad de las capacitaciones en seguridad de la información. Asegurar que el personal esté actualizado sobre mejores prácticas y nuevos riesgos.

- **Indicadores de desempeño:**

  Control A.18.2.3: Definir y monitorear indicadores clave de desempeño (KPIs) para evaluar el éxito de las estrategias de mitigación, tales como: medir la cantidad de

incidentes reportados, tiempo de respuesta a incidentes, conformidad con las politicas establecidas, cumplimiento de políticas, y participación en capacitaciones.

Esta fase asegura que el PESI se mantenga dinámico y adaptable, respondiendo efectivamente a nuevos desafíos y mejorando continuamente la postura de seguridad de la Unidad de TIC's del GAD Municipal del Cantón Paute.

7.5 Mejora continua

Esta fase de mejora continua garantiza que el PESI no sea un documento estático, sino un marco dinámico que evoluciona para enfrentar nuevas amenazas y aprovechar nuevas oportunidades en el ámbito de la seguridad de la información. Esto asegura que la Unidad de TIC's del GAD Municipal del Cantón Paute mantenga un alto nivel de seguridad y resiliencia frente a las amenazas en constante cambio.

Esta fase tiene la finalidad de:

- **Mantener la relevancia del PESI:** Asegurar que el PESI se adapte a los cambios en el entorno de TI y en las amenazas de seguridad.
- **Optimizar los controles de seguridad:** Mejorar continuamente los controles de seguridad basados en la retroalimentación y los resultados de las evaluaciones.
- **Fomentar una cultura de seguridad:** Promover una mentalidad de mejora continua y responsabilidad en todos los niveles de la organización.

Actividades

- **Revisión y actualización del PESI:**

  Control A.12.1.2: Establecer un calendario para revisar y actualizar el PESI, asegurando que refleje los cambios en la infraestructura de TI, las regulaciones y las

mejores prácticas. Incorporar los resultados de auditorías internas y externas en las revisiones.

Por ejemplo, si durante una auditoría se detecta una nueva vulnerabilidad, el PESI debe ser ajustado para incluir medidas que mitiguen este nuevo riesgo.

- **Implementación de cambios basados en incidentes:**

  Control A.16.1.6: Analizar los incidentes de seguridad y las vulnerabilidades detectadas para identificar las áreas que necesitan mejoras. Actualizar las políticas, procedimientos y controles en base a estas lecciones aprendidas.

  Por ejemplo, si se detecta que un incidente fue causado por una contraseña débil, se pueden implementar políticas más estrictas de gestión de contraseñas.

- **Incorporación de nuevas tecnologías:**

  Control A.12.1.3: Evaluar e integrar nuevas tecnologías y soluciones de seguridad que puedan ofrecer mejor protección y eficiencia. Realizar pruebas piloto y análisis de impacto antes de la implementación completa.

  Un ejemplo podría ser la implementación de un sistema de detección y respuesta a incidentes (IDS/IPS) para mejorar la detección de amenazas.

- **Capacitación y concienciación continua:**

  Control A.7.2.2: Desarrollar programas de capacitación continua para todos los empleados, enfocándose en nuevas amenazas y técnicas de seguridad. Realizar evaluaciones periódicas de la efectividad de la capacitación y ajustar los programas según sea necesario.

  Por ejemplo, se pueden realizar talleres semestrales sobre las últimas tendencias en ciberseguridad y técnicas de phishing.

- **Evaluación de la eficacia de los controles**

Control A.18.2.3: Monitorear y evaluar continuamente la eficacia de los controles de seguridad implementados. Utilizar KPIs y otros métricos para medir el desempeño y realizar ajustes según sea necesario.

Por ejemplo, monitorear la cantidad de incidentes de seguridad antes y después de la implementación de un nuevo control de seguridad para evaluar su efectividad.

- **Retroalimentación de los stakeholders:**

  Control A.6.1.4: Recoger retroalimentación regularmente de los diferentes stakeholders, incluyendo empleados, directivos, y proveedores, para identificar áreas de mejora y asegurar que el PESI esté alineado con las necesidades y expectativas de la organización.

  Un ejemplo es realizar encuestas trimestrales a los empleados sobre su percepción de la seguridad de la información y utilizar sus respuestas para ajustar las políticas de seguridad.

7.6 Documentación y comunicación

7.6.1 Documentación

Es fundamental mantener una documentación detallada de todas las actividades relacionadas con la seguridad de la información. Esta documentación debe ser accesible y actualizada para garantizar que todos los miembros del equipo tengan acceso a la información necesaria para cumplir con sus responsabilidades. La documentación debe incluir:

- **Políticas y procedimientos de seguridad de la información:**
  - **Contenido**: Detalles sobre las políticas de seguridad, procedimientos, roles y responsabilidades.
  - **Actualización**: Revisión y actualización periódica para reflejar los cambios en el entorno de seguridad y la infraestructura de TI.
  - **Referencia ISO:** ISO: ISO/IEC 27001:2022, Control A.5.1.1. (ISO/IEC, 2022)

- **Registros de incidentes de seguridad:**
    - Contenido: Información detallada sobre los incidentes de seguridad, análisis de causas raíces, acciones correctivas y preventivas.
    - Actualización: Registros actualizados inmediatamente después de la identificación y resolución de cada incidente.
    - Referencia ISO: ISO/IEC 27001:2022, Control A.16.1.2. (ISO/IEC, 2022)
- **Informes de auditoría y evaluación:**
    - **Contenido:** Resultados de auditorías internas y externas, evaluaciones de riesgos y revisiones de cumplimiento.
    - **Actualización:** Documentación actualizada tras cada auditoría o evaluación.
    - **Referencia ISO:** ISO/IEC 27001:2022, Control A.18.2.2. (ISO/IEC, 2022)
- **Planes de continuidad del negocio y recuperación ante desastres:**
    - **Contenido:** Estrategias de continuidad y recuperación, roles y responsabilidades, y procedimientos de activación.
    - **Actualización:** Revisión periódica y pruebas de los planes.
    - **Referencia ISO:** ISO/IEC 27001:2022, Control A.17.1.1. (ISO/IEC, 2022)

7.6.2 Comunicación

La comunicación efectiva es esencial para asegurar que todos los stakeholders estén informados sobre las políticas, procedimientos y cambios en la seguridad de la información. La estrategia de comunicación debe incluir:

- **Comunicación interna:**
    - **Métodos**: Boletines internos, reuniones regulares, y plataformas de colaboración digital.

  - **Frecuencia**: Regular y continua para mantener a todos los empleados informados.
  - **Referencia ISO:** ISO/IEC 27001:2022, Control A.7.2.2. (ISO/IEC, 2022)
- **Comunicación externa:**
  - **Métodos**: Comunicados de prensa, informes públicos, y actualizaciones en la página web oficial del GAD Municipal.
  - **Frecuencia**: Según sea necesario, especialmente tras incidentes de seguridad o actualizaciones importantes.
  - **Referencia ISO:** ISO/IEC 27001:2022, Control A.6.1.4. (ISO/IEC, 2022)

7.6.3 Formación y concienciación

La fase de formación y concienciación es crucial para asegurar que todo el personal esté debidamente informado y capacitado en las políticas y procedimientos de seguridad de la información específicos de su área. Esta fase debe alinearse con las buenas prácticas de la norma ISO 27001 para garantizar que todos los empleados comprendan la importancia de la seguridad de la información y sepan cómo actuar en caso de incidentes de seguridad.

Esta fase tiene la finalidad de:

- Capacitar al personal de la Unidad de TIC's en las políticas y procedimientos de seguridad de la información.
- Sensibilizar a los empleados sobre las amenazas y vulnerabilidades comunes en el ámbito de las TIC.
- Fomentar una cultura de seguridad dentro de la Unidad de TIC's.

Plan de Formación y Concienciación

- **Desarrollo de materiales de capacitación:**

- **Contenido:** Manuales, guías rápidas, videos explicativos y presentaciones específicas para la Unidad de TIC's.
- **Frecuencia:** Actualización anual o cuando se introduzcan nuevas políticas o tecnologías.
- **Referencia ISO:** ISO/IEC 27001:2022, Control A.7.2.2.

- **Sesiones de capacitación:**
  - **Métodos:** Talleres presenciales, seminarios web y cursos en línea adaptados a las necesidades del personal de TIC's.
  - **Frecuencia:** Mínimo una vez al año y sesiones adicionales según las necesidades identificadas.
  - **Referencia ISO:** ISO/IEC 27001:2022, Control A.7.2.2.
- **Campañas de sensibilización:**
  - **Contenido:** Boletines informativos, posters, correos electrónicos y mensajes en intranet dirigidos a la Unidad de TIC's.
  - **Frecuencia:** Continuamente a lo largo del año.
  - **Referencia ISO:** ISO/IEC 27001:2022, Control A.7.2.2.
- **Evaluación de la eficacia de la formación:**
  - **Métodos:** Encuestas de satisfacción, pruebas de conocimiento y análisis de incidentes de seguridad.
  - **Frecuencia:** Después de cada sesión de capacitación y anualmente.
  - **Referencia ISO:** ISO/IEC 27001:2022, Control A.18.2.2.

7.8 Auditoría interna

La auditoría interna es fundamental para evaluar la eficacia del PESI y asegurar su cumplimiento con los estándares ISO 27001. Esta fase implica la revisión sistemática de las políticas, procedimientos y controles de seguridad implementados.

Esta fase tiene la finalidad de:

- Evaluar la conformidad del PESI con los requisitos de la norma ISO 27001.
- Identificar áreas de mejora y no conformidades.
- Recomendar acciones correctivas y preventivas.

Actividades

- **Planificación de la Auditoría:**
    - **Contenido:** Desarrollar un plan de auditoría anual que cubra todas las áreas críticas de la seguridad de la información.
    - **Frecuencia:** Anualmente.
    - **Referencia ISO:** ISO/IEC 27001:2022, Control A.18.2.1.
- **Ejecución de la Auditoría:**
    - **Métodos:** Realizar auditorías internas mediante la revisión de documentos, entrevistas con el personal y pruebas de los controles de seguridad.
    - **Frecuencia:** Según el plan de auditoría.
    - **Referencia ISO:** ISO/IEC 27001:2022, Control A.18.2.2.
- **Informe de Auditoría:**
    - **Contenido:** Documentar los hallazgos de la auditoría, incluyendo las conformidades y no conformidades, y las recomendaciones para mejoras.
    - **Frecuencia:** Después de cada auditoría.
    - **Referencia ISO:** ISO/IEC 27001:2022, Control A.18.2.3.
- **Acciones Correctivas y Preventivas:**
    - **Métodos:** Desarrollar e implementar planes de acción para corregir las no conformidades y prevenir su recurrencia.
    - **Frecuencia:** Continuamente.
    - **Referencia ISO:** ISO/IEC 27001:2022, Control A.18.2.4.

7.9 Presupuesto y recursos

Esta fase del PESI estima los costos y asigna los recursos necesarios para implementar las estrategias de mitigación identificadas en las evaluaciones de riesgos. La siguiente estimación de costos se basaron en los precios variables que se ofrecen en el mercado ecuatoriano y del exterior en algunos casos, dichos precios son respaldados por el jefe de la Unidad de TIC´s.

Costos aproximados

- **Implementar un plan de mantenimiento preventivo y correctivo (Control A.11.2.4)**
    - **Costo de renovación de equipos:**

      Servidor: USD 2,000 - 4,000 cada uno.

      Componentes de red (switches, routers): USD 500 - 1,500.

      UPS (Uninterruptible Power Supply): USD 300 - 1,000.
    - **Costo de mantenimiento regular:**

      Contrato de mantenimiento anual: USD 1,000 - 3,000.

      Personal técnico: USD 800 - 1,200 mensuales.
- **Desarrollar e implementar políticas y procedimientos de seguridad de la información (Control A.5.1.1)**
    - **Costo de consultoría para desarrollo de políticas**

      Consultoría externa: USD 2,000 - 5,000
    - **Costo de software de gestión de políticas**

      Herramientas de software: USD 500 - 2,000
- **Desarrollar un plan de acción detallado para la seguridad de la información (Control A.16.1.5)**
    - **Costo de desarrollo de plan de acción:**

Consultoría para desarrollo de plan: USD 1,500 - 3,000.

- **Costo de simulacros y formación:**

  Simulacros de incidentes: USD 500 - 1,000 por evento.

  Formación del personal: USD 200 - 500 por sesión.

- **Adquirir e instalar un generador eléctrico de respaldo (Control A.17.2.1)**
  - **Costo de generador eléctrico:**

    Generador de capacidad media: USD 5,000 - 10,000.

  - **Costo de instalación:**

    Instalación profesional: USD 1,000 - 2,000.

- **Presentar un caso de negocio para aumentar el presupuesto de TI (Control A.6.1.2)**
  - **Costo de preparación del caso de negocio:**

    Consultoría para desarrollo de caso de negocio: USD 1,000 - 2,000.

- **Implementar un sistema de detección y respuesta a incidentes (IDS/IPS) (Control A.12.4.1)**
  - **Costo de IDS/IPS**

    Sistema de detección: USD 2,000 - 5,000.

    Costo de integración y configuración: USD 1,000 - 3,000.

  - **Costo de auditorías de seguridad:**

    Auditoría externa: USD 2,000 - 4,000 anuales.

  - **Costo de formación en ciberseguridad:**

    Cursos y certificaciones: USD 300 - 1,000 por curso.

Resumen de costos estimados

- Renovación de equipos y mantenimiento: USD 5,000 - 10,000
- Desarrollo de políticas y procedimientos: USD 2,500 - 7,000

- Desarrollo de plan de acción y formación: USD 2,000 - 5,500
- Generador eléctrico de respaldo: USD 6,000 - 12,000
- Presentación de caso de negocio: USD 1,000 - 2,000
- Sistema de detección y respuesta a incidentes: USD 4,000 - 12,000
- Total estimado: USD 20,500 - 48,500

7. Conclusión final

El PESI para la Unidad de TIC's del GAD Municipal del Cantón Paute está diseñado para proporcionar una estructura sólida y adaptable para la gestión de la seguridad de la información. Siguiendo las mejores prácticas de la norma ISO 27001, este plan asegura que todos los riesgos sean identificados, evaluados y mitigados de manera efectiva, garantizando la protección de los activos de información y la continuidad operativa de la unidad de TIC´s.