UNIVERSIDAD NACIONAL DEL SANTA

FACULTAD DE INGENIERÍA

Escuela Profesional de Ingeniería de Sistemas e Informática

Propuesta de sistema de gestión basado en ISO 27001 para mejorar la seguridad de información en la Municipalidad Provincial del Santa

Tesis para optar el Título Profesional de Ingeniero de Sistemas e Informática

TESISTAS:

- Bach. Cotos López, Adolfo Estróbach
  Cod. ORCID: 0000-0002-2427-3164
- Bach. Chombo Quezada, Elias Mario
  Cod. ORCID: 0009-0009-9567-9231

ASESORA:

- Dra. Briones Pereyra, Lizbeth Dora
  Cod. ORCID: 0000-0003-0626-7227

NUEVO CHIMBOTE – PERÚ

2025

UNIVERSIDAD NACIONAL DEL SANTA

FACULTAD DE INGENIERÍA

Escuela Profesional de Ingeniería de Sistemas e Informática

TÍTULO:

Propuesta de sistema de gestión basado en ISO 27001 para mejorar la seguridad de información en la Municipalidad Provincial del Santa

Tesis para optar el Título Profesional de Ingeniero de Sistemas e Informática

Revisado y Aprobado por la asesora:

Dra. BRIONES PEREYRA, Lizbeth Dora
Cod. ORCID: 0000-0003-0626-7227
Asesora

NUEVO CHIMBOTE – PERÚ

2025

UNIVERSIDAD NACIONAL DEL SANTA

FACULTAD DE INGENIERÍA

Escuela Profesional de Ingeniería de Sistemas e Informática

TÍTULO:

Propuesta de sistema de gestión basado en ISO 27001 para mejorar la seguridad de información en la Municipalidad Provincial del Santa

Tesis para optar el Título Profesional de Ingeniero de Sistemas e Informática

REVISADO Y APROBADO POR EL JURADO EVALUADOR:

Dr. Juan Pablo Sánchez Chávez
Cod. ORCID: 0000-0002-3521-7037
PRESIDENTE

Dr. Hugo Esteban Caselli Gismondi
Cod. ORCID: 0000-0002-2812-6727
SECRETARIO

Dra. Lizbeth Dora. Briones Pereyra
Cod. ORCID: 0000-0003-0626-7227
INTEGRANTE

NUEVO CHIMBOTE – PERÚ
2025

UNS
UNIVERSIDAD NACIONAL DEL SANTA

FACULTAD DE INGENIERÍA
ESCUELA PROFESIONAL INGENIERÍA DE SISTEMAS E INFORMÁTICA

ACTA DE SUSTENTACIÓN INFORME FINAL DE TESIS

A los veintiún días del mes de noviembre del año dos mil veinticinco, siendo las 10:00 am. En el aula S-2 del Pabellón de la Escuela Profesional de Ingeniería Sistema e Informática-FI-UNS, se instaló el Jurado Evaluador designado mediante Resolución 534-2025-UNS-CFI, y de expedito según Resolución Decanal N°827 -2025-UNS-FI integrado por los docentes: DR. JUAN PABLO SANCHEZ CHAVEZ (presidente), DR. HUGO ESTEBAN CASELLI GISMONDI (secretario) y LA DRA. LIZBETH DORA BRIONES PEREYRA (Integrante), para dar inicio a la sustentación de la Tesis intitulada "PROPUESTA DE SISTEMA DE GESTIÓN BASADO EN ISO 27001 PARA MEJORAR LA SEGURIDAD DE INFORMACIÓN EN LA MUNICIPALIDAD PROVINCIAL DEL SANTA", perteneciente a los Bachilleres: CHOMBO QUEZADA ELIAS MARIO, con código de matrícula N° 0200814022 Y al bachiller: COTOS LOPEZ ADOLFO ESTROBACH con código de matricula N°0200914012, quienes fueron asesorado por el Dra. Lizbeth Dora Brior es Pereyra, según T/R. D. N° 685-2021-UNS-FI -UNS-FI

El Jurado Evaluador, después de deliberar sobre aspectos relacionados con el trabajo, contenido y sustentación del mismo, y con las sugerencias pertinentes en concordancia con el Reglamento General de Grados y Títulos, vigente, declaran aprobar:

BACHILLER	PROMEDIO VIGESIMAL	PONDERACIÓN
COTOS LOPEZ ADOLFO ESTROBACH	17	BUENO

Siendo las 11 a m del mismo día, se dio por terminado el acto de sustentación, firmando la presente acta en señal de conformidad.

Nuevo Chimbote, 21 noviembre de 2025

DR. JUAN PABLO SANCHEZ CHAVEZ
PRESIDENTE

DR. HUGO ESTEBAN CASELLI GISMONDI
SECRETARIO

DRA. LIZBETH DORA BRIONES PEREYRA
INTEGRANTE

FACULTAD DE INGENIERÍA
ESCUELA PROFESIONAL INGENIERÍA DE SISTEMAS E INFORMÁTICA

ACTA DE SUSTENTACIÓN INFORME FINAL DE TESIS

A los veintiún días del mes de noviembre del año dos mil veinticinco, siendo las 10:00 am. En el aula S-2 del Pabellón de la Escuela Profesional de Ingeniería Sistema e Informática-FI-UNS, se instaló el Jurado Evaluador designado mediante Resolución 534-2025-UNS-CFI, y de expedito según Resolución Decanal N°827-2025-UNS-FI integrado por los docentes: DR. JUAN PABLO SANCHEZ CHAVEZ (presidente), DR. HUGO ESTEBAN CASELLI GISMONDI (secretario) y LA DRA. LIZBETH DORA BRIONES PEREYRA (Integrante), para dar inicio a la sustentación de la Tesis intitulada "PROPUESTA DE SISTEMA DE GESTIÓN BASADO EN ISO 27001 PARA MEJORAR LA SEGURIDAD DE INFORMACIÓN EN LA MUNICIPALIDAD PROVINCIAL DEL SANTA", perteneciente a los Bachilleres: CHOMBO QUEZADA ELIAS MARIO, con código de matrícula N° 0200814022 Y al bachiller: COTOS LOPEZ ADOLFO ESTROBACH con código de matrícula N°0200914012, quienes fueron asesorado por el Dra. Lizbeth Dora Briones Pereyra, según T/R. D. N° 685-2021-UNS-FI -UNS-FI

El Jurado Evaluador, después de deliberar sobre aspectos relacionados con el trabajo, contenido y sustentación del mismo, y con las sugerencias pertinentes en concordancia con el Reglamento General de Grados y Títulos, vigente, declaran aprobar:

BACHILLER	PROMEDIO VIGESIMAL	PONDERACIÓN
CHOMBO QUEZADA ELIAS MARIO	16	REGULAR

Siendo las 11 a m del mismo día, se dio por terminado el acto de sustentación, firmando la presente acta en señal de conformidad.

Nuevo Chimbote, 21 noviembre de 2025

DR. JUAN PABLO SANCHEZ CHAVEZ
PRESIDENTE

DR. HUGO ESTEBAN CASELLI GISMONDI
SECRETARIO

DRA. LIZBETH DORA BRIONES PEREYRA
INTEGRANTE

turnitin

Recibo digital

Este recibo confirma quesu trabajo ha sido recibido por Turnitin. A continuación podrá ver la información del recibo con respecto a su entrega.

La primera página de tus entregas se muestra abajo.

Autor de la entrega:	ADOLFO ESTROBACH COTOS LOPEZ
Título del ejercicio:	Tesis Acate_Quintana
Título de la entrega:	2025.INFORME_TESIS_FINAL.docx
Nombre del archivo:	2025.INFORME_TESIS_FINAL.docx
Tamaño del archivo:	1.48M
Total páginas:	99
Total de palabras:	17,894
Total de caracteres:	101,031
Fecha de entrega:	26-nov-2025 10:22a. m. (UTC-0500)
Identificador de la entrega:	2828292341

UNIVERSIDAD NACIONAL DEL SANTA

FACULTAD DE INGENIERÍA

UNS

PROPUESTA DE SISTEMA DE GESTIÓN BASADO EN ISO 27001 PARA MEJORAR LA SEGURIDAD DE INFORMACIÓN EN LA MUNICIPALIDAD PROVINCIAL DEL SANTA

2025.INFORME_TESIS_FINAL.docx

INFORME DE ORIGINALIDAD

23%	24%	8%	12%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	hdl.handle.net Fuente de Internet	3%
2	repositorio.uns.edu.pe Fuente de Internet	2%
3	repositorio.unac.edu.pe Fuente de Internet	1%
4	repositorioacademico.upc.edu.pe Fuente de Internet	1%
5	ciencia.lasalle.edu.co Fuente de Internet	1%
6	repository.unad.edu.co Fuente de Internet	1%
7	publicaciones.usanpedro.edu.pe Fuente de Internet	1%
8	repositorio.unsch.edu.pe Fuente de Internet	1%
9	docs.google.com Fuente de Internet	1%

DEDICATORIA

En primer lugar, a Dios, por todas las bendiciones otorgadas en la vida para mí y a mis seres queridos. Así mismo, por la fortaleza e ímpetu de siempre querer crecer como persona y profesional.

A mi familia, que, pese a las adversidades, siempre han estado presente en cada etapa de la vida brindándome la motivación, apoyo y fortaleza para continuar siempre adelante.

Adolfo E. Cotos López

Lo dedico a mi pequeño hijo Jonathan Miguel Chombo Marín, Él es el motivo de mi vida.

A mis estimados padres: Paulina Domitila Quezada Flores en el cielo y Mario Chombo Santiago, por sus palabras alentadoras y su oración constante.

Así también a Katherine Berenice Marín Romero, con mucho cariño en el cielo.

Y, a Yelina Marilyn Sarrin Menacho, mi gran amor, por ser mi apoyo y mi fuerza.

Elías M. Chombo Quezada

AGRADECIMIENTO

Agradecimientos en primer lugar, a Dios, por las bendiciones, dones y fortaleza otorgados en la vida.

A mi familia, que siempre están presente apoyando y motivando frente a todo tipo de situaciones que se presentan en la vida.

En general, a todas las personas que han hecho posible la realización y desarrollo de la presente Tesis.

Adolfo E. Cotos López

Agradezco desde el fondo de mi corazón a Dios Todopoderoso, por la oportunidad de avanzar profesionalmente y por su misericordia cada día, protección y amor. A mi hijo Jonathan, que me da un gran motivo de lucha constante. A mi madre Paulina, a mis abuelos Francisca y Sebastián, ellos en el cielo, a mi padre Mario, por darme esa fuerza. A Katherine por su cariño, y darme un hermoso hijo. A Yelina, por su amor, compañía, apoyo incesante.

Elías M. Chombo Quezada

ÍNDICE

Índice de Tablas

Índice de Figuras

RESUMEN

El presente proyecto de tesis, tiene como objetivo, la propuesta de un sistema de gestión de seguridad basado en la estándar ISO 27001, así bien en el presente proyecto se viene utilizando los contenidos estructurales de la propia norma, como bases conceptuales documentas y un conjunto de indicadores nos permitió lograr conclusiones del impacto de la investigación sobre la seguridad de la información en la Municipalidad Provincial del Santa, cuyo resultado se obtendrá mediante la aplicación de un cuestionario dirigido a los colaboradores de la Gerencia de Tecnologías de información y Comunicación, logrando evaluar la hipótesis de la investigación. Considerando que el análisis de confiabilidad obtenido, el resultado es de 0.927, el cual se considera una confiabilidad muy alta, y que la hipótesis general habiendo obtenido una significancia de ($p < 0.05$), con un valor menor de 0.001, en consecuencia, los resultados muestran la influencia que ha tenido la aplicación de la propuesta sobre la seguridad de la información en la Municipalidad provincial del Santa.

Palabras Clave: Mejora continua, Seguridad, información, Gestión estratégica, Gestión de riesgos

ABSTRACT

The present thesis project aims to propose a security management system based on the ISO 27001 standard, as well as in the present project the structural contents of the standard itself are being used as documented conceptual bases and a set of indicators allowed us to achieve conclusions about the impact of the research on information security in the Provincial Municipality of Santa, whose result will be obtained through the application of a questionnaire directed to the collaborators of the Information and Communication Technologies Management, managing to evaluate the research hypothesis. Considering that the reliability analysis obtained, the result is 0.927, which is considered a very high reliability, and that the general hypothesis having obtained a significance of ($p < 0.05$), with a value less than 0.001, consequently, the results show the influence that the application of the proposal has had on information security in the Provincial Municipality of Santa.

Keywords: Continuous improvement, Security, Information, Strategic management, Risk management

PRESENTACIÓN

Señores miembros del Jurado Evaluador:

En cumplimiento a lo dispuesto en el Reglamento General de Grados y Títulos de la Universidad Nacional del Santa, ponemos a vuestra consideración el presente Proyecto de Tesis intitulado: ***"PROPUESTA DE SISTEMA DE GESTIÓN BASADO EN ISO 27001 PARA MEJORAR LA SEGURIDAD DE INFORMACIÓN EN LA MUNICIPALIDAD PROVINCIAL DEL SANTA"*** *que es, requisito previo para optar el Título Profesional de Ingeniero de Sistemas e Informática.*

La presente Tesis, es gracias a la motivación de crecer profesionalmente, el esfuerzo, la dedicación y aplicación de los conocimientos adquiridos a través de nuestra formación profesional y experiencia laboral, que es la muestra de nuestra capacidad, conocimientos y la iniciativa por la investigación de cada uno de sus egresados inculcados en esta casa superior de estudios.

Por lo expuesto, a ustedes señores miembros del jurado evaluador, teniendo en cuenta las limitaciones propias de este proyecto, dejamos a vuestro criterio y consideración, su revisión con el deseo de que cumpla con los requisitos mínimos para su correspondiente aprobación.

Atentamente,

COTOS LÓPEZ, Adolfo Estróbach

CHOMBO QUEZADA, Elías Mario

INTRODUCCIÓN

En la actualidad el interactuar con cualquier entorno, se genera diversos datos que consecuentemente, pueden transformarse en información, los procesos que se utilicen para ello, tienen un gran impacto en la funcionalidad y eficacia de la información. Así mismo es importante reconocer que la información es uno de los activos más valiosos de todo tipo de organización. El considerar la salvaguarda de la información, mecanismos de seguridad, un apropiado almacenamiento y mecanismos de accesos, así como todo tipo de interacción con la misma, resulta muy importante considerar la normativa de seguridad debida y apropiada.

En ese sentido, la presente investigación comprende desarrollar los acápites relacionados a la seguridad de la información bajo el estándar de ISO 27001, desarrollándolo con el enfoque de mejora continua PHVA, esto nos presente una formulación puntual de la situación ¿De qué manera la propuesta de un sistema de gestión basado en ISO 27001, mejorará la gestión de riesgos y toma de decisiones sobre la seguridad de información en la Municipalidad Provincial del Santa?

Es por ello que se planteó como objetivo general, Diseñar una propuesta de un Sistema de Gestión de Seguridad de la Información basado en ISO 27001, bajo el enfoque de mejora continua PHVA, con el fin de fortalecer la gestión de riesgos y la toma de decisiones relacionadas con la seguridad de la información en la Municipalidad Provincial.

Y mediante los objetivos específicos, Identificar los riesgos de seguridad de la información en la Municipalidad Provincial del Santa, identificando brechas y vulnerabilidades con base en los requisitos de la norma ISO 27001. El Establecer el Tratamiento de riesgos, mediante controles necesarios para abordar las brechas seguridad de la información identificadas en la Municipalidad Provincial del Santa, y el Evaluar el

cumplimiento normativo de las políticas y procedimientos que se ajusten a las políticas y estándares establecidos por la norma ISO 27001 en la Municipalidad Provincial del Santa

Teniendo en cuenta que como hipótesis se presenta, La propuesta de un Sistema de Gestión de Seguridad de la Información basado en ISO 27001, bajo el enfoque de mejora continua PHVA, mejora la seguridad de la información en la Municipalidad Provincial del Santa.

Debido a la apremiante necesidad de la Municipalidad Provincial de Santa de contar con un sistema que salvaguarde su información de muchos riesgos digitales, con lo cual estaría asegurando una atención comunicativa para todos sus usuarios logrando con ellos conectar los derechos de los ciudadanos respecto de la transparencia de la información y los mecanismos de confidencialidad, disponibilidad e integridad de la información con la que debe contar la Municipalidad

La investigación planteada contribuirá a que la Municipalidad Provincial de Santa considere a través de la gerencia de tecnologías de información y comunicación sistema, la alineación de los procesos a un sistema integral de gestión basado en ISO 27001 para mejorar la seguridad de información, con el cual mejorará su gestión de seguridad de la información teniendo en cuenta la confidencialidad, disponibilidad e integridad de la misma

CAPÍTULO I:

INTRODUCCIÓN

1.1. DESCRIPCIÓN DE LA ENTIDAD

1.1.1. Razón Social

Municipalidad Provincial del Santa

1.1.2. Tipo de Entidad

Gobierno Local - Provincial

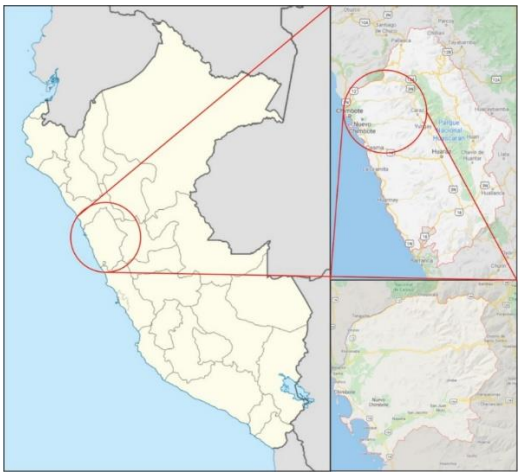
1.1.3. Dirección Legal

Jr. Enrique Palacios N°. 341 – 343, Santa, Chimbote

1.1.4. Datos Generales de la Entidad

Figura 1

Mapas relacionados a la ubicación de la entidad



Nota: El gráfico se compone de diversos niveles de vista del mapa, enfocándolo en la ubicación de la entidad. Elaboración propia

Gerencia de Tecnologías de la Información y Comunicación

Esta gerencia es una entidad encargada de administrar actividades relacionada con la planeación, articulación, orientación, coordinación, despacho y dirección sobre el manejo pertinente de los bienes informáticos, físicos, lógicos y empleo de TIC en la entidad, desarrollando e implementando los sistemas integrados, así también la administración de los sistemas de sistematización, procesamiento electrónico de datos,

organización de redes, soporte informático y aplicaciones para abarcar las necesidades de datos contables, logísticos, laborales, estadísticos y de gestión en general de la comuna provincial.

Entre las principales atribuciones de esta gerencia se encuentran la formulación del Plan Operativo Anual alineándolo al Plan Estratégico de Tecnologías de la Información (PETI), el Plan Estratégico de Gobierno Electrónico (PEGE) así como los diversos documentos de gestión como el Plan Operativo Institucional (POI), el Plan Estratégico Institucional (PEI) y los sistemas de información de la Institución, fortaleciendo la gestión, adquisición, asignación y distribución óptima de Hardware y Software, cumpliendo con los objetivos estratégicos y metas para el periodo; así como, la aplicación efectiva de los planes de contingencia: seguridad e integridad de la información que resguarde la continuidad de la conducción sobre la gestión efectiva de la Entidad.

1.2. PLANTEAMIENTO DEL PROBLEMA

1.3.1. Realidad Problemática

La digitalización de la sociedad moderna ofrece una serie de ventajas que ya están siendo aprovechadas en todos los ámbitos del desarrollo de la vida cotidiana, ya sea como elementos o entidades naturales como como personas jurídicas; en ese sentido, el uso masivo de teléfonos inteligentes, la inteligencia artificial la Big data e incluso el loT, forman parte del uso doméstico y empresarial de la cultura de este época; sin embargo esta nueva tendencia de transformación digital viene acompañada de grandes amenazas que ponen en riesgo la seguridad de la información personal- natural o jurídica comprometiendo tus sistemas; de ahí que, las empresas – principalmente – están en la obligación de tomar las acciones pertinentes en el asunto para velar por la seguridad de

su información dentro de las leyes vigentes de transparencia de la información (Barón, 2020; Rodrguez,2019).

En palabras de Zamora y Ortiz (2021) el mundo global en el que desenvuelven las entidades y organizaciones tanto públicas como privadas, las ha obligado a asumir un enfoque de competitividad donde la información ha conseguido transformarse en una de las herramientas más valiosas de este dimensión de la cultura actual , las organizaciones necesitan saber cómo se mueve el mundo empresarial a su alrededor; de ahí que se vuelve importante empoderarse de la información que por su distinta naturaleza en vasta y que por ello, ha de ser trascendental conocer las fuentes que se manejan actualmente. Ante esta realidad, Martínez y Lara (2014) proponen como requerimientos informativos importante para el ingreso al mundo competitivo de la globalización tanto de la entidad público como privada: permanencia macroeconómica, el acceso y la integración de diversos mercados internacionales o la complejidad de la regulación para el sector empresarial, la infraestructura regional y la competitividad propias de las empresas.

En las entidades públicas actuales, la información constituye un activo indispensable de la administración y una herramienta fundamental para la transparente participación del ciudadano y la respectiva rendición de cuentas. Por su parte, Tafur, J. (2022) indica que acceder a la información por derecho atribuido, la administración pública diáfana y los datos de libre acceso forman cimientos fundamentales donde los gobiernos locales puedan responder debidamente ante los ciudadanos. Sin embargo, debido al acelerado progreso de las tecnologías de la información y comunicación, las instituciones del estado se hallan con vulnerabilidades que van en aumento en lo que concierne a la seguridad de sus activos de información, lo que resulta exigible que adopten enfoques completos sobre gestión de riesgos.

Bajo esta dirección, Altamirano, K. (2021) menciona advirtiendo que hay solamente un porcentaje muy pequeño de entidades públicas que han implementado formalmente la gestión de seguridad de la información donde incluya los principios de confidencialidad, integridad y disponibilidad, lo cual concibe un escenario crítico sobre los datos institucionales. En el contexto de la Municipalidad Provincial del Santa, esta realidad se convierte en carencia de un sistema destinado a la gestión de seguridad de la información que incluya estándares internacionales como lo es la ISO/IEC 27001, lo que conlleva riesgos palpables de filtración, pérdida o manejo de información delicada. Esto no sólo perturba las operaciones en la institución, sino además la confianza que debe tener la ciudadanía y también el cumplimiento obligatorio de las normativas. Frente a esta situación, se plantea la imperiosa necesidad de una propuesta de sistema de gestión que va dirigido a mejorar la seguridad de la información, que conlleva a fortalecer los controles internos, el gobierno tecnológico y la administración de los activos de información.

En el Perú, el problema de seguridad de la información en las entidades públicas, ha pasado por una suerte de normativas que se respaldan en el acceso a la información que como derecho ostentan todos los ciudadanos, en este contexto se emitió la R.M. 004-2016-PCM con la finalidad de obligar la obligatoriedad de la implementación de un Sistema de Gestión de la Seguridad de la Información (SGSI) y la creación del sistema Nacional de Informática (SNI) que suponen la regulación de la gestión de la información en estos organismos; sin embargo, al 2018 solo el 2,4% de la entidades públicas lograron implementar dicho sistema; ya para el año 2020, mediante Decreto de Urgencia 006-2020, se creó el Sistema de Transformación Digital, a través del que se aplicó la Encuesta Nacional de Recursos Informáticos en la Administración Pública (ENRIAP) al 15%

entidades públicas existentes en esta nación, cuyos datos mostraron que solo el 6 % tendría definida su política de seguridad de la información y solo el 6 % habría hecho la clasificación de sus activos informáticos, ambos, requisitos indispensables; además solo el 8 % de los usuarios de los sistemas informáticos del sector público está preparado para reportar algún incidente referente a este aspecto (Altamirano, 2021).

En la Municipalidad provincial del Santa, el sistema de seguridad de información no responde a las normas nacionales e internacionales como la Norma ISO 27001, ordenada por la Resolución Ministerial 004-2016-PCM; esto implica no solo un descuido en su sistema, sino que representa un riesgo que se expresa en clasificación de la información que se debe comunicar, el cumplimiento de los plazos establecidos para poder entregar la información y la garantía de autenticidad de la información.

1.3.2. Características de la realidad específica

Luego de mencionar los principales inconvenientes identificados en el sistema de gestión de información en la Municipalidad Provincial de Santa, se expone el siguiente detalle:

Respecto a la forma de gestionar la información que se realiza en la Municipalidad del Santa, se hace de forma empírica, cada personal realiza el manejo de la información como cree que es mejor y que cree que resguarda la seguridad de la información, cabe mencionar que no existe alguna norma aplicada en tema de información que asegure su confidencialidad, su integridad y su disponibilidad, como saber exactamente qué información es exactamente solo uso restringido (confidencial), que información es completo, necesario e íntegro de acorde a la instancia que lo requiera (integro), no estando en ordenamiento, estructurado y clasificado (disponibilidad)

Respecto del cumplimiento de los plazos establecidos para poder entregar la información la Municipalidad de Santa en sus planes estratégicos y operativos no propone mejoras en la gerencia de tecnología de la información y comunicación relacionadas al Sistema de Gestión de la Seguridad de la Información (SGSI); por lo que no existe un sistema de plazos para la entrega de la información que se publicita que tenga un respaldo normativo.

Respecto de la garantía de autenticidad de la información la Municipalidad de Santa en sus planes estratégicos y operativos no propone mejoras en la gerencia de tecnología de la información y comunicación relacionadas al Sistema de Gestión de la Seguridad de la Información (SGSI); por lo que los mecanismos existentes no son suficientemente validados y contundentes para poder proveer reportes de manera organizada sobre la integridad y autenticidad de la información que se publicita que tenga un respaldo normativo.

1.3.3. Formulación del problema

¿De qué manera la propuesta de un sistema de gestión basado en ISO 27001, mejorará la gestión de riesgos y toma de decisiones sobre la seguridad de información en la Municipalidad Provincial del Santa?

1.3. OBJETIVOS DE LA INVESTIGACIÓN

1.3.1. Objetivo General

Diseñar una propuesta de un Sistema de Gestión de Seguridad de la Información basado en ISO 27001, bajo el enfoque de mejora continua PHVA, con el fin de fortalecer la gestión de riesgos y la toma de decisiones relacionadas con la seguridad de la información en la Municipalidad Provincial.

1.3.2. Objetivos Específicos

Objetivo específico 1. Identificar los riesgos de seguridad de la información en la Municipalidad Provincial del Santa, identificando brechas y vulnerabilidades con base en los requisitos de la norma ISO 27001.

Objetivo específico 2. Establecer el Tratamiento de riesgos, mediante controles necesarios para abordar las brechas seguridad de la información identificadas en la Municipalidad Provincial del Santa

Objetivo específico 3. Evaluar el cumplimiento normativo de las políticas y procedimientos que se ajusten a las políticas y estándares establecidos por la norma ISO 27001 en la Municipalidad Provincial del Santa

1.4. HIPÓTESIS DE LA INVESTIGACIÓN

1.4.1. Hipótesis de la Investigación

La propuesta de un Sistema de Gestión de Seguridad de la Información basado en ISO 27001, bajo el enfoque de mejora continua PHVA, mejora la seguridad de la información en la Municipalidad Provincial del Santa.

1.4.2. Hipótesis Específicas

- Mejora del nivel de identificación de Riesgos

- Aumento de Tratamiento de los Riesgos

- Cumplimiento normativo institucional sobre la seguridad de la información

1.5. JUSTIFICACIÓN E IMPORTANCIA

1.4.1. Justificación Teórica.

El estudio se justifica en fundamento teórico de la documentación sobre los lineamientos de la ISO 27001, como estándar internacional que establece criterios, bases fundamentales y un conjunto amplio de herramientas para la seguridad de la información.

1.4.2. Justificación práctica.

El estudio se justifica en su ámbito práctico, ya que procura la optimización del uso organizado de un sistema de seguridad de información por la gerencia de tecnologías de información y comunicación de la Municipalidad Provincial de Santa, con la finalidad de contribuir al bienestar de toda la comuna de la provincia y la satisfacción de todos sus usuarios.

Dada la necesidad de la Municipalidad Provincial de Santa de contar con un sistema de seguridad de la información administrada por la gerencia de tecnologías de información y comunicación, representa una solución institucional y comunal que mejorará el servicio de comunicación de la Municipalidad con sus operarios y usuarios. Esta mejora disminuirá el manejo de información de cual es confidencial, si es integra o cual información puede estar disponible o no, porque el manejo es de forma empírica, sin respaldo de alguna norma internacional de aseguramiento de calidad, lo cual lo hace que aumente los riesgos al tratarlos.

1.4.3. Justificación metodológica.

Esta investigación se justifica desde su dimensión metodológica en cuanto que propone un programa de sistema de seguridad de información estrictamente validado el cual es una contribución para la comunidad científica en cuanto que constituye un punto de partida para la optimización de estudios científicos relacionados con el uso de las

normas ISO 27001 y la seguridad con el sistema de seguridad de información específicamente con entidades públicas.

1.4.4. Justificación tecnológica.

Debido a la necesidad de la Municipalidad Provincial de Santa para gestionar su información sin el peligro que los riesgos de la era digital podrían representar, este estudio se justifica en la atención a una necesidad tecnológica a partir de la aplicación de las normas ISO 27001 para optimización de uno de los respaldos más importantes de toda entidad del Estado en contraste con los derechos a la transparencia de la información de la comuna.

1.4.5. Justificación social

Debido a la apremiante necesidad de la Municipalidad Provincial de Santa de contar con un sistema que salvaguarde su información de muchos riesgos digitales, con lo cual estaría asegurando una atención comunicativa para todos sus usuarios logrando con ellos conectar los derechos de los ciudadanos respecto de la transparencia de la información y los mecanismos de confidencialidad, disponibilidad e integridad de la información con la que debe contar la Municipalidad.

1.6. IMPORTANCIA DE LA INVESTIGACIÓN

La investigación planteada contribuirá a que la Municipalidad Provincial de Santa considere a través de la gerencia de tecnologías de información y comunicación sistema, la alineación de los procesos a un sistema integral de gestión basado en ISO 27001 para mejorar la seguridad de información, con el cual mejorará su gestión de seguridad de la información teniendo en cuenta la confidencialidad, disponibilidad e integridad de la misma.

CAPÍTULO II:

MARCO TEÓRICO

2.1. ANTECEDENTES DE LA INVESTIGACIÓN

2.1.1. Antecedentes en el ámbito internacional

Saavedra, J. (2021), sustentó mediante una investigación, que con la implementación del SGSI en el caso de estudio dentro de una empresa, alineado al estándar de calidad ISO 27001:2013, se evidencia que cualquier tipo de entidad, pymes u cualquier otra organización que ponga en ejecución estas normas, promueven seguridad en cada uno de los activos de la información y extiende la existencia y valoración de los mismos. Esto, a través del análisis de las amenazas, de los riesgos, las vulnerabilidades y de la aplicación de los procedimientos y/o controles que se pueda garantizar una mayor vida útil a los diversos activos de información, tanto físicos como del ciberespacio, y es a raíz de las estrategias de protección tanto físicos como digitales, basándose en los principios de confidencialidad, integridad, disponibilidad y no repudio de la información.

Campo, L. (2024), concluye que la aplicación del Ciclo PHVA en la Implementación y Mantenimiento del SGSI, en cuanto a la fase de Planificación, pues en esta fase, se debe implementar un plan por memorizado que defina detalladamente los objetivos de seguridad, el alcance del SGSI, así como, los recursos necesarios para su implementación, específicamente, este plan debe incluir un cronograma, un presupuesto aproximado realista y una estrategia de comunicación para asegurar el compromiso de todos los colaboradores y áreas interesadas

Kitsios, F., et al. (2023). realizan un análisis aplicado de la norma ISO/IEC 27001 como parte de un plan corporativo de cumplimiento y describen cómo la adopción ordenada de los controles (anexo A) y la formalización de políticas elevan el nivel de gobernanza de la seguridad de la información. Entre sus hallazgos principales se encuentra que la implementación estructurada de políticas y controles mejora la trazabilidad documental (registros, responsables) y facilita la identificación y tratamiento

de riesgos; además, enfatizan que sin indicadores (KPIs) la revisión por la dirección y la mejora continua quedan subordinadas a prácticas esporádicas. La utilidad para la presente investigación es directa: confirma que un SGSI organizado bajo ISO 27001, con evidencias documentales y métricas, potencia las dimensiones que trabajas (identificación de riesgos, tratamiento y cumplimiento), y provee criterios para diseñar los instrumentos de verificación y las evidencias del ciclo PHVA.

Así bien, se tiene presente que Orellana (2024), concluyó que, la importancia de que, para reducir los riesgos en una entidad, resulta indispensable el implementar una metodología de análisis de riesgo, análisis de brechas, entre otros, lo cual en su investigación se desarrolló bajo la metodología de la ISO/IEC 27001, dado que esta, cuenta con la evaluación y tratamientos de riesgos.

Bono y Tinoco (2024) realiza en su tesis un enfoque mixto con el objetivo de analizar para hacer un diseño de un SGSI, basado en las normativa ISO 27001:2022 y así reguardar usando los tres pilares, la confidencialidad, la integridad y la disponibilidad de información en San Services de R.L. y para ello se han tenido que aplicar encuestas y entrevistas a personas clave del área de TI, para encontrar la situación como se encuentra actualmente en relación a seguridad de la información y lo que requiere la ISO 27001, identificando y evaluando amenazas y riesgos, usando metodología MAGERIT, para que así se pueda lograr con el cumplimiento de la empresa frente a la SGSI, así como definir los riesgos clave y sus respectivas acciones como medidas de solución.

Pillajo, E. (2025) presenta en su tesis los nuevos desafíos que afronta la cooperativa de ahorro y crédito rural sierra norte en su seguridad de la información, como los posibles ataques de malware en la web, parches de seguridad no latentes, uso no adecuado de los equipos informáticos, correos con alta probabilidad de contenido malicioso. Por ello el autor propone implementar políticas de seguridad en el área de TI

tomando la base de la norma ISO/IEC 27001:2022, con enfoque cualitativo, juicio de expertos y metodología MAGERIT, con todo ello se concluyeron que dicha propuesta cumple con la normativa y puede regular los riesgos y vulnerabilidades de la cooperativa, tal así proteger los datos personales tan delicados de sus clientes.

2.1.2. Antecedentes en el ámbito nacional

Cama y Arellano (2024) quienes mostraron una tesis con investigación cuantitativa, en función a la implementación de un sistema de gestión de seguridad de la información (SGSI) basado en la norma ISO/IEC 27001:2022 realizado a favor de la Clínica María del Socorro en Lima, cuyo estudio da inicio evaluando la situación de como se viene dando actualmente la seguridad de la clínica en cuanto a los datos utilizados, en ello se ha hallado riesgos y vulnerabilidades. De este diagnóstico, se pudo diseñar e implementar el SGSI, que contiene, políticas de seguridad, capacitación de personal, controles de seguridad y el ciclo de mejora continua (ciclo Deming), con el apoyo de encuestas y observación con ello se ha logrado mejorar y reconocer el derecho de protección de datos, mayor conciencia en la capacitación del personal, asegurar la calidad de los datos y su tratamiento; y revisar paulatinamente en la efectividad de las medidas de control.

López, J. (2022) aplicó el desarrollo de un SGSI para una empresa constructora, siguiendo los lineamientos de la norma ISO/IEC 27001, con la finalidad de resguardar los activos de información, debido a las constantes amenazas internas y externas, considerando su confiabilidad, integridad y disponibilidad. Esta aplicación se dio en función a 4 fases. Primero, planificar, donde se definen, los objetivos, la política, análisis de los riesgos y la aplicabilidad. Segundo, hacer, donde se da el desarrollo tal cual de la estrategia a utilizar. Tercero, verificar, donde se verifica, se audita las medidas puestas en acción. Cuarto, actuar, donde se toman las medidas de corrección. Con ello, se organizó

de forma más eficiente los eventos y amenazas, los procesos y servicios, así como la reducción de incidentes volviéndolo más rentable.

García (2020), sustentó su tesis donde manifiesta que su objetivo era el de realizar una propuesta, referente de un sistema de gestión de seguridad de la información que se encuentra basado en la Norma ISO 27001 en asistencia a la oficina de tecnologías de información del gobierno Regional de Piura; año 2020, con el fin de reducir notoriamente la pérdida de información, no obstante para tal razón realizó una investigación cuantitativa, no experimental descriptiva en donde se tuvo la participación de una muestra significativa constituida por 23 colaboradores, a los que se les aplicó un cuestionario, cuyos resultados obtenidos fueron que el 91% de los colaboradores no se han encontrado satisfechos y contentos con el sistema de seguridad de la información con la que tiene esta entidad, mientras tanto el pequeño 9%, dicen lo contrario, mencionan que si están satisfechos con el sistema en sí; por cierto la totalidad de los encuestados, mencionaron la necesidad de la implementación de un sistema de seguridad de información con Norma ISO 27001 quedando con ello la salvaguarda de la confidencialidad, la integridad y de la disponibilidad de la información dentro de la oficina de tecnologías de información del referido gobierno regional de Piura.

En consecuencia, se ha consignado la determinación de una propuesta de un sistema de seguridad de la información basado en la norma 27001 dentro de la oficina de tecnologías de información del Gobierno Regional de Piura permite mejorar los procesos propios acerca de la seguridad de información y de la comunicación con la propia entidad.

2.1.3. Antecedentes en el ámbito local

Ibarra, L. (2023) manifestó en su tesis de cómo influye el implementar ISO 27001:2013 referente a la gestión del manejo de información en UGEL Bolognesi ubicado en Ancash. Es una investigación aplicada con diseño experimental, con técnica

la encuesta e instrumento un cuestionario realizando procesos de validación y confiabilidad. Se lograron mejoras significas como en el manejo de información, la disponibilidad, la autenticidad, así como la integridad, la confidencialidad y la trazabilidad, obteniendo cambios en los valores, reduciendo el nivel deficiente, mejorando el nivel regular e incrementando el nivel eficiente.

Bardales, D. (2024), concluye a través de sus resultados, que, en relación a la gestión de la seguridad sobre la conducción de la información, que el 29% de los participantes en la investigación, calificaron la gestión como regular, seguido de un 24% que lo consideraron como eficiente y un 19% quienes lo calificaron como deficiente. Estos resultados de deficiencia, se basa en que la entidad solo realiza de manera ocasional copias de seguridad y gestión de privilegios de usuarios, a pesar de que con poca frecuencia se reportan modificaciones o pérdidas accidentales de datos. Asociado a esto, la falta de un plan de contingencia frente a ciberataques es una debilidad notable

Colonia (2019) indicó en su tesis donde el propósito fue efectuar una propuesta para un sistema de gestión de seguridad de información aplicando la norma ISO 27001 enfocado a Municipio del Distrito de Buenavista Alta, en la Provincia de Casma, 2017, cuyo fin es que fenezca la perdida de información, para esto realizó la investigación usando enfoque cuantitativa, de diseño descriptivo, no experimental, teniendo como participantes en la muestra de 30 servidores a los que se les aplicó la encuesta que sería la técnica y el cuestionario, el instrumento, en la aplicación se obtuvieron que 73.33% de participantes encuestados mencionaron que se encontraban insatisfechos la seguridad de la información actual, por otro lado el 26.67% expreso que estaban muy satisfechos; en referencia a la imperiosa necesidad de implementar un sistema de información que tuviera la norma ISO 27001, todos los empleados dijeron que era sumamente urgente esta implementación.

En cuanto al alcance contiene un sistema de gestión referente a la seguridad de la información con soporte en la norma ISO/IEC 27001, cuyo fin resulta conservar el principio de la confidencialidad, de integridad y el de disponibilidad de información en Municipio Buenavisteño. Como parte concluyente, se estableció que la idea de un sistema de gestión para la seguridad de la información en apego a la norma ISO 27001 para el mencionado Municipio Distrital de Buenavista a permitido la mejora en los mencionados procesos en la seguridad de información y también en el de comunicación.

2.2. ISO 27001

a. La familia ISO 27000 y su conformación

El estándar referente a la ISO de la familia 27000, en específico esta norma ya estructurada es capaz de ser aplicada a múltiples tipos de organizaciones en donde cuente como un activo a la información, y a su vez la esta se utilice como insumo para los objetivos y resultados institucionales.

La serie o familia de la ISO 27000 comprende múltiples sub estándares, a su vez algunos de ellos conllevan detalles específicos, rubros o aplicabilidad, de orientaciones, característica de ser certificables entre otros detalles.

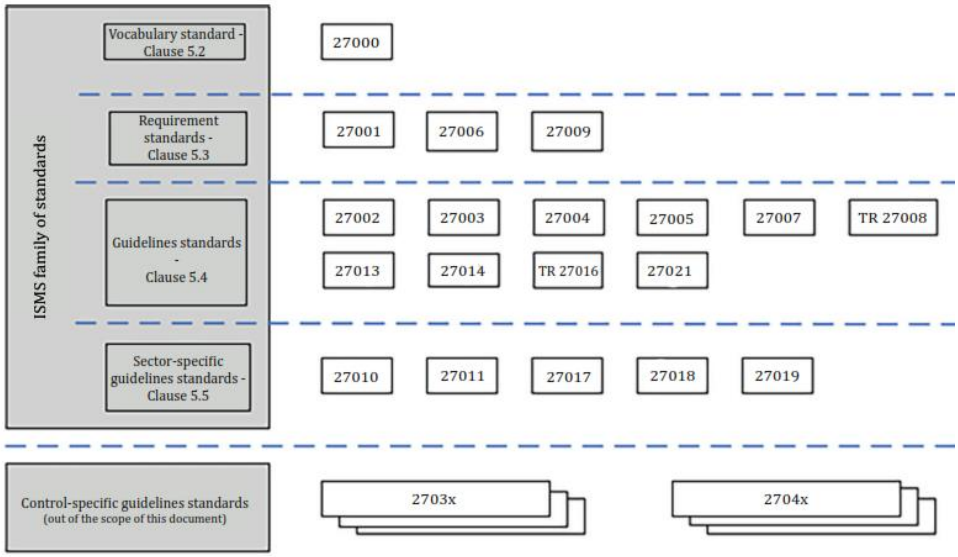
Entiéndase que la ISO/IEC 27000, en específico, comprende lo relacionado al vocabulario estándar para un sistema de Gestión de Seguridad de la Información que por sus siglas en español también conocido como SGSI, o de su expresión internacional en inglés “Information Security Management Systems” como las siglas ISMS.

Para tener en cuenta, este vocabulario a través del tiempo también ha sido reformulado y afinado en sus descripciones y alcances, tal es el caso como se detalla las diversas ediciones del “Tecnología de la información — Técnicas de seguridad —

Sistemas de gestión de la seguridad de la información — Visión general y vocabulario" a continuación:

Figura 2

Esquema de Relaciones de la familia ISO de normas de un SGSI



Nota. Esta figura se representa el esquema General de relaciones de las diversas normas o estándares agrupados de acuerdo a su rol o función dentro de lo concerniente al Sistema de Gestión de Seguridad de la Información Tomado de *ISO/IEC 27000:2018*, por ISO.org, 2018, https://iso.org

b. Estándares que especifican los requisitos

El ISO/IEC 27001, por definición es básicamente, de la norma que establece los diversos requerimientos para poder realizar la implantación de un Sistema de Gestión de Seguridad de la Información de alguna organización.

Según su Alcance, es un documento en el cual se establece los requisitos para la implementación, operación monitoreo, revisión, mantenimiento y las mejoras sobre el Sistema de Gestión de la Seguridad de la Información (SGSI) formal, inmerso en los aspectos concernientes del ámbito de algún riesgo comercial que puede estar expuesta la

organización. Se especifica también los requisitos para la debida implementación de diversos controles de seguridad de la información acorde a las necesidades de las organizaciones de manera individual, ya que este este documento puede ser aplicado en múltiples organizaciones de forma independiente a su tipo, el tamaño o la naturaleza de la misma.

Según su Propósito, se orienta a proporcionar los requisitos normativos para la implementación de los aspectos normativos para el desarrollo y operación SGSI con la inclusión de los objetivos de control, así como de los grupos de controles respectivos que se encuentran en el ISO/IEC 27001, de la edición 2013, Anexo A.

2.3. ANÁLISIS DE ISO 27001 ENFOCADO EN PHVA

Para la implementación del estándar ISO 27001, como marco base para establecer los mecanismos apropiados de un Sistema de Gestión de Seguridad de la información(SGSI), se debe de tener en cuenta que esta estándar cuenta con diversos capítulos, los cuales se alinean con el ciclo de mejora continua (Planificar, Hacer, Verificar, Actuar - PHVA), Así bien a continuación se detalla los capítulos aplicables para el procedimiento de la presente investigación y su posterior segmentación dentro del ciclo de mejora continua.

En el capítulo correspondiente al, Contexto de la Organización: Se procede a centrar al reconocimiento de la entidad, la realidad de su contexto, esto servirá como requisito indispensable de partida para poder considerar el punto de referencia en la aplicación del Sistema de Gestión de Seguridad de la información. (ISO/IEC 27001)

Del capítulo correspondiente al, Liderazgo: Se centra en establecer los requisitos vinculados con el compromiso que debe tener la alta gerencia institucional, con un procedimiento de implementación del SGSI, este capítulo es importante el identificar y

reconocer esta información orientado a una cultura de Seguridad de la Información Organizacional. (ISO/IEC 27001)

En el capítulo correspondiente a la, Planificación: Se realiza posteriormente a los capítulos anteriores, puesto que recoge la información recolectada en cada uno de ellos, para así poder identificar las necesidades y las expectativas de la organización, así como el poder definir los riesgos que se deben tratar conjuntamente con las actividades que se realizan para su mitigación de los mismos.

Del capítulo correspondiente, al Soporte: En este capítulo se orienta en la determinación de los recursos requeridos para la implementación en planificación, considerando también la disponibilidad y el compromiso de la alta gerencia institucional en facilitarlos.

En el Capítulo correspondiente, Operación: En este apartado en donde se aplican las medidas de seguridad de la información que previamente se han definido y establecido acorde al contexto de la organización.

Del capítulo correspondiente a la, Evaluación del desempeño: Se considera los aspectos relacionados a los procesos de evaluación sobre los controles de seguridad de la información que se han aplicado.

En el Capítulo sobre la, Mejora: Se refiere a la actualización continua del sistema de gestión de la seguridad de la información.

Teniendo los detalles de cada uno de los capítulos, y dado la naturaleza de la presente investigación, se procede agrupar los capítulos que conforman el estándar de la ISO/IEC 27001 a poder alinearlos con las fases del ciclo de mejora continua, en ese sentido para la fase de Planificación, estaría constituido por los capítulos de contexto de la organización, Liderazgo, Planificación y Soporte. Así mismo, entendiendo que esta

fase no solo comprendería la recolección de información, sino que también se procede a su análisis, que se realiza mediante la matriz de riesgos.

De igual forma, para el capítulo de Operación, se alinea con la fase de Hacer, lo que conlleva la continuidad de los procesos identificados y su análisis, esto a través de su matriz de análisis respectiva.

De igual forma, para el capítulo de Evaluación de desempeño, se alinea con la fase de Verificar, lo que conlleva la evaluación de los controles implementados y su análisis, esto a través de su matriz de análisis respectiva.

De igual forma, para el capítulo de Mejora, se alinea con la fase de Actuar, lo que conlleva considerar las acciones de mejora continua y su análisis, esto a través de su matriz de análisis respectiva.

Figura 3

Estructura de ISO/IEC 27001 y Ciclo de mejora continua

2.4. MARCO CONCEPTUAL

Activo Informático:

Para Ficco (2019) un activo de información lo define como un bien o como un servicio, es decir puede ser tangible o puede ser intangible, este activo crea, también procesa o acopia la información, consignando un grado determinado de valor en relación a la significancia según la criticidad o la afectación que tiene con los procesos del giro del negocio, dichos procesos están ordenados en función a los objetivos enmarcados por la organización. Por tal razón, estos activos de información necesitan una eficiente y una adecuada defensa, con celo y sustento.

Amenaza:

Una amenaza es cualquier circunstancia o evento que tiene el potencial de causar daño a los activos de información. Puede ser intencional, como un ataque cibernético, o accidental, como un desastre natural. NIST. (2012).

Confidencialidad:

Para Stoneburner (2001), viene a ser la condición necesaria para que la información únicamente sea sabida por personal debidamente autorizado. En el caso que esto faltara, la información podría tener daños muy serios al dueño o que esto se tornara inservible. La intencionalidad de este principio es refrendar de que un solo operario o talvez un grupo autorizado de ellos tengan el acceso pertinente a cierta información dentro de la organización; pues esta, no siempre puede ser sabida por todos o por cualquier personal, más bien por el contrario, viene destinado para cierto grupo de personas, y en muchas de las veces, hacia una sola persona. La confidencialidad debe prevalecer y subsistir, por periodos determinados, tanto en el lugar de acopio, vale decir en cada uno

de los sistemas y dispositivos en los que habita inmerso a la red, así también durante su respectivo procesamiento y el tránsito, hasta finalmente llegar a su destino.

Controles:

Son medidas, prácticas, procedimientos o mecanismos diseñados para proteger los activos de información contra riesgos, amenazas o vulnerabilidades específicas. En ISO/IEC 27001, los controles están especificados en el Anexo A e incluyen medidas técnicas, físicas y administrativas. Calder, A., & Watkins, S. (2015)

Datos:

Se refiere a al recurso intangible pero fundamental para generar la información de todo el sistema en toda organización. Del que siempre es recomendable tener los respaldos debidos.

Directiva:

Es una instrucción formal que establece los procedimientos y prácticas específicas que deben seguirse para cumplir con las políticas organizacionales. En seguridad de la información, las directivas indican cómo implementar controles y gestionar riesgos específicos. Humphreys, E. (2008).

Disponibilidad:

La conceptualización según la Academia de Latinoamérica sobre la seguridad informática (2011) manifiesta de que la disponibilidad viene a ser aquella facultad de estar siempre presente, es decir disponible con el fin de ser procesadas por personal debidamente autorizados. Ello permite que se conserve perfectamente acopiada con el aplicativo, así como el hardware, operando en perfectas condiciones y que sean respetados los diversos formatos para su recuperación pertinente de manera plena. La intención de este principio es meramente resguardar, que la información y que los

diversos sistemas que lo contienen, estén siempre servibles en el tiempo que lo requieran los usuarios que están autorizados con el fin de que lo utilicen. Cuando se refiere a que los sistemas contienen la información, se está enfocando a toda una estructura física y a su tecnología contenida, que van a permitir el acceso, el tráfico y el almacenamiento de información.

Equipos:

Se refiere al hardware, así como las instalaciones que los albergan. El equipamiento que generalmente es utilizado puede ser prontamente reemplazado, e incluso con mayores prestaciones que los existentes, o ser adquirido en un corto plazo en comparación con la de poder contar con personas de alta experiencia y desarrollo relacionado a las líneas de acción especializada de la organización.

Estándar:

Es el conjunto de directrices, requisitos o especificaciones documentadas que son adoptadas y aplicadas de manera consistente para garantizar la calidad, seguridad y eficiencia de productos, servicios o procesos. En el contexto de seguridad de la información, los estándares, como el ISO/IEC 27001, ofrecen un marco reconocido para gestionar riesgos y proteger datos. (International Organization for Standardization, 2013)

Información:

Se define información como un sistema de significados que permite a las personas actuar con certeza frente al conocimiento de una realidad; de esta manera la información se presenta como un mensaje codificado a partir de una determinada situación que permite orientar el comportamiento de las personas de manera individual o colectiva, reduciendo con ello, la incertidumbre del error (Chiavenato, 2006)

Según la INDECOPI (Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual) considera que la información viene a ser un activo que posee valor en la organización y que solicita una defensa conveniente en respuesta a la inquebrantable a las diversas amenazas y las fragilidades. La información acoge varias formas. Podría estar en forma impresa o quizás escrita en un papel, guardada electrónicamente, comunicada por un correo o por un medio vía electrónica, manifestada a través de un video o mediante el habla en dialogo. Cualquiera sea la forma que asuma la información o cual medio en el que se almacene o se comparta, deberá estar propiamente protegida de manera permanente (INDECOPI, 2007)

Integridad:

Instituto Nacional de Estándares y Tecnología (1995), manifiesta que la integridad posee como principal intención, acreditar que la información no se esté transformada, adulterada o falseada en función a su contenido por los agentes que no están autorizados o que se encuentren de forma ilícita; de esta forma se vendría a garantizar la fidelidad y la seguridad de los datos. La integridad posee dos partes:

La integridad de los datos, que indica que los cambios que se produzca en la información por parte de los agentes debidamente acreditados son lo concerniente a: inserciones, también sustituciones o a las eliminaciones que puedan hacerse en el contenido de la información.

Integridad los sistemas, que se orienta al funcionamiento tanto del hardware como del software de manera cabal, sin desperdiciar su total y completa disponibilidad.

Un error en la integridad puede ocurrir por las anomalías que se presenten en el hardware, en el software, por las ocurrencias de virus informáticos y/o las modificaciones hechas por personas que se puedan infiltrar en el sistema.

ISO:

Es la Organización Internacional de Normalización, específicamente, es una organización internacional independiente y no gubernamental que desarrolla y publica estándares internacionales voluntarios. Los estándares de ISO proporcionan especificaciones técnicas para productos, servicios y sistemas, asegurando su calidad, seguridad y eficiencia. (International Organization for Standardization)

Personas:

Lo cual se entiende o se refiere a todos los agentes que interactúan de alguna manera con el sistema de información, sus procesos o alguna característica de influencia, tales como: usuarios, administradores, stakeholders, entre otros. Según la prioridad de lo establece a esta categoría de principal preocupación sobre la protección de las personas por considerase más difíciles de reemplazar en comparación con los equipos o los datos propiamente, la experiencia que tienen en su campo de acción y naturaleza en el desempeño de sus funciones respectivas, lo llevan a la cima de importancia entre estas categorías de activos.

Política:

Es un conjunto de principios o reglas que establece cómo debe gestionarse una organización en un área específica. En seguridad de la información, una política define las directrices para proteger los datos y asegura que las acciones sean consistentes con los objetivos estratégicos de la organización. ISO/IEC. (2013)

Política de seguridad:

Según Gómez y Fernández (2015) las políticas de seguridad vienen a ser la información que se encuentra documentada donde se plasman los objetivos organizacionales, que poseen las principales líneas de acción orientadas a la protección

de la información ante perdidas por confidencialidad, por integridad y por disponibilidad; además esta documentación requiere ser informado a todas las partes interesadas del SGSI.

Riesgo:

Es el efecto de la incertidumbre sobre los objetivos. En seguridad de la información, se define como la combinación de la probabilidad de que ocurra un evento y sus consecuencias negativas sobre la confidencialidad, integridad o disponibilidad de los activos de información. ISO/IEC Risk management. (2013). ISO/IEC 31000:2018

Seguridad:

Por otro lado, Peso y Ramos (2004), asegura que la seguridad llega a ser concretamente la defensa de los activos, los cuales se encuentran frente a acciones o a situaciones que no se esperan, por medio de la creación de controles, lo que deviene conjeturar realmente una transformación y un gran esfuerzo. Todo se lleva a cabo en las organizaciones con el objeto de resguardar los intereses de cada asociado, de cada empleado, de cada cliente, como también de los proveedores y de cada ciudadano afectado según sea el sector.

Seguridad Física:

La seguridad física refiere a los aspectos relacionado con el entorno o ambiente de las instalaciones en donde se encuentra la generación, adquisición, procesamiento, transformación, emisión o transmisión de la información de la organización con base a estos criterios se puede considerar factores combinados como la probabilidad de ocurrencia de uno o más sucesos(riesgo) que afecta sobre una debilidad en los procesos de control(vulnerabilidad) conocida o no y verse afectado según su nivel de daño(amenaza) que pueda causar en el sistema u organización.

La protección de la información que respecta a la seguridad física, Vega (2021) refiere que se subdivide en tres categorías principales y centra su perspectiva en los activos, los cuales son: Personas, Datos, Equipos

Seguridad de información:

Así pues, al teorizar sobre la seguridad de información, se define como la defensa de sus principios, es decir, la confiabilidad, la integridad y el de disponibilidad de información; en otras palabras, corresponde a asegurar que esta información sea viable exclusivamente a personas acreditadas, debiera ser exacta sin algunas modificaciones indeseadas y sea inaccesible a los usuarios de la forma y en el momento que lo necesiten. Además, es posible involucrar más propiedades tal como la autenticidad, el no repudio y la confiabilidad. Esta seguridad de información recubre a la información de una gran gama de amenazas con el propósito de asegurar la continuación del negocio, al reducir los potenciales menoscabos a la organización y extender las posibilidades del regreso de las inversiones y de las oportunidades del negocio a partir de un conjunto propicio de controles, sean estos: de políticas, de prácticas, de procedimientos, referidas de estructuras organizativas y de funciones de software y hardware, atañéndole monitoreo, revisiones y mejoramientos, en donde sea menester (INDECOPI, 2007)

En esta misma línea de razón, Fitzgerald (2007), aporta a esta definición afirmando que la seguridad de información es aquella norma preparatoria y reactiva del hombre, de entidades organizacionales y de sistemas con tecnología que consientan poner a resguardo la información considerando la conservación de su confidencialidad, su autenticidad y su integridad de la propia. Contrastando la diferencia entre la definición de seguridad de información y la seguridad informática, resaltando que este último únicamente se encarga acerca de la seguridad en los ambientes netamente informáticos.

Según Vega (2021) refiere que la seguridad de información involucra cada vez mayores cantidades de aspectos relacionados a nuestra sociedad, como esa parte de la aceptación casi ubicua de la TIC (Tecnología de Información y Comunicación), ya que la mayor parte de las actividades cotidianas las personas se encuentran interactuando con diversos sistemas académicos, comercio, financieros y otros. En un sentido más amplio asevera que la información constituye la protección de nuestros activos, resguardarlos de los atacantes que violentan nuestras redes, de desastres naturales y de condiciones ambientales enemigas.

Sistema de Gestión de Seguridad de la Información (SGSI):

Según Gómez y Fernández (2015), el Sistema de Gestión de Seguridad de la Información (SGSI) lo definen como un grupo que contiene procesos, estos van a permitir el establecimiento, la implementación, mantención y la realización de la mejora continua de la seguridad de la información

Para Peltier et. Al (2005) indica que las políticas de la seguridad de información son elementos ineludibles para garantizar la debida seguridad en cuanto a información: cumpliendo los importantes roles internos y externos.

Vulnerabilidad:

Es una debilidad o deficiencia en un sistema, proceso, o control que puede ser explotada por una amenaza, causando daño a los activos de información. Las vulnerabilidades pueden ser técnicas, como un software desactualizado, o humanas, como errores de procedimiento. NIST. (2012).

CAPÍTULO III:

METODOLOGÍA

3.1. TIPO DE INVESTIGACIÓN

Según su naturaleza es descriptiva, porque se efectuó la recaudación de toda la información mediante el propio diagnóstico de la problemática correspondiente en la seguridad de la información de la Municipalidad Provincial del Santa.

De acuerdo a su fin o Propósito, es Aplicada, dado que, permitió brindar una alternativa de solución, a la problemática planteada en la Gerencia de Tecnologías de la Información y Comunicación de la Municipalidad Provincial del Santa.

3.2. VARIABLES

Variable Independiente: Sistema de Gestión basado en ISO 27001

Variable Dependiente: Seguridad de la información de la Municipalidad Provincial del Santa

3.3. POBLACIÓN Y MUESTRA

Población

Este grupo poblacional se conformará de 13 colaboradores de la gerencia de tecnologías de información y comunicación de La Municipalidad Provincial del Santa.

Muestra

En esta investigación se optará por una muestra censal; la misma que se entiende como aquella muestra donde todas las unidades de estudio de la población de la investigación son consideradas; es decir, este estudio cuenta con una muestra de 13 colaboradores de la gerencia de tecnologías de información y comunicación de La Municipalidad Provincial del Santa.

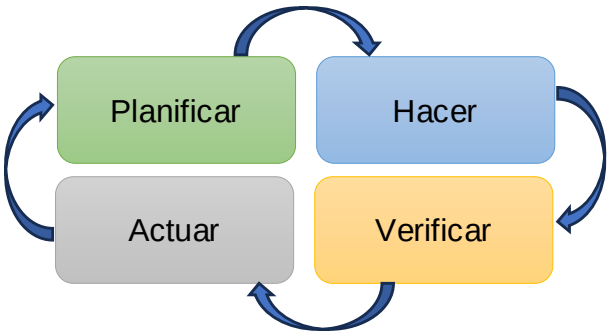
3.4. Marco de trabajo de la ISO 27001

Considerando que la norma ISO 27001 se basa en el ciclo Planificar-Hacer-Verificar-Actuar (PHVA o PDCA), que también es conocido como ciclo de Deming. El

ciclo PHVA puede aplicarse no sólo al sistema de gestión en su conjunto, sino también a cada elemento individual para proporcionar un enfoque continuo en la mejora continua.

Figura 4

Modelo del ciclo de mejora continua



- **Planificación:**

Alcance: Definir claramente el alcance del Sistema de Gestión de Seguridad de la Información (SGSI), es decir, qué áreas y procesos de la organización se incluirán.

Política de seguridad: Establecer una política de seguridad de la información que refleje el compromiso de la alta dirección con la seguridad de la información y sirva como guía para toda la organización.

Análisis del contexto: Identificar los factores internos y externos que pueden afectar a la seguridad de la información, como la cultura organizacional, la legislación aplicable, los riesgos del negocio, etc.

Identificación de partes interesadas: Determinar quiénes son las partes interesadas en la seguridad de la información y cuáles son sus requisitos.

- **Diseño/ Hacer:**

Análisis de riesgos: Evaluar los riesgos a los que está expuesta la información de la organización, identificando las amenazas, vulnerabilidades y posibles impactos.

Selección de controles: Seleccionar los controles de seguridad adecuados para tratar los riesgos identificados, teniendo en cuenta la norma ISO 27001 y las mejores prácticas.

Desarrollo de procedimientos: Crear procedimientos detallados para implementar y gestionar los controles seleccionados.

- **Verificación:**

Auditorías internas: Realizar auditorías internas periódicas para evaluar el cumplimiento del SGSI.

Revisiones por la dirección: Realizar revisiones periódicas por parte de la alta dirección para evaluar el desempeño del SGSI y asegurar su alineación con los objetivos estratégicos de la organización.

- **Tratamiento/Actuar:**

Acciones correctivas: Implementar acciones correctivas para abordar las no conformidades identificadas durante las auditorías y revisiones.

Acciones preventivas: Implementar acciones preventivas para evitar que se produzcan nuevas no conformidades.

Método de Trabajo de la Evaluación

La evaluación de cada característica de activo de la información se procedió a evaluar bajo la Matriz para el cálculo de riesgo, en la cual se está conformada por indicadores de vulnerabilidad en las columnas y nivel de peligro de ocurrencia en las filas.

Tabla 1

Matriz de Riesgos

Probabilidad Muy Alto	Riego Alto	Riego Alto	Riego Muy Alto	Riego Muy Alto
Probabilidad Alto	Riesgo Medio	Riesgo Medio	Riego Alto	Riego Muy Alto
Probabilidad Medio	Riesgo Bajo	Riesgo Medio	Riesgo Medio	Riego Alto
Probabilidad Bajo	Riesgo Bajo	Riesgo Bajo	Riesgo Medio	Riego Alto
	Impacto Bajo	**Impacto Medio**	**Impacto Alto**	**Impacto Muy Alto**

CAPÍTULO IV:

RESULTADOS Y DISCUSIÓN

4.1.RESULTADOS

Desarrollo de Proceso PHVA

Fase 1: Planificación

En la fase de Planificación es la primera etapa del PHVA, donde se identifican y documentan los riesgos relacionados con la seguridad de la información en la Municipalidad Provincial del Santa. Según el estándar ISO 27001, esta fase es fundamental para establecer un marco de referencia que guíe las acciones futuras. Para esto resulta importante analizar la información de esta fase, a través de una matriz de riesgos, de los riesgos potenciales identificados. Algunos de los riesgos más comunes en este contexto son:

Tabla 2

Análisis mediante Matriz de riesgos – Fase 1 Planificación

Impacto Muy Alto (5)			-Ataque de denegación de servicio (DoS)	-Acceso no autorizado a información sensible -Pérdida de datos por fallo en almacenamiento	
Impacto Alto (4)				- Mínima planificación y coordinación - Mínimo compromiso por parte de la Alta Gerencia	- Acceso a información por personal no autorizado
Impacto Medio (3)				-Malware por descargas no supervisadas	
Impacto Bajo (2)					
Impacto Mínimo (1)					
	Probabilidad Mínima (1)	Probabilidad Baja (2)	Probabilidad Media (3)	Probabilidad Alta (4)	Probabilidad Muy Alta (5)

Tabla 3

Detalles de la identificación de Riesgos- Fase 1 Planificación

ID del Riesgo	Descripción del Riesgo	Activo Afectado	Vulnerabilidad	Impacto Potencial	Probabilidad	Impacto	Nivel de Riesgo
R01	Acceso no autorizado a información sensible	Bases de Datos	Controles de acceso insuficientes	Filtración de datos personales	Alta	Muy Alto	Crítico
R02	Pérdida de datos por fallo en almacenamiento	Documentos críticos	Redundancia de almacenamiento baja	Pérdida de documentos clave	Alta	Muy Alto	Crítico
R03	Malware por descargas no supervisadas	Sistemas de TI	Falta de control en descargas	Corrupción de sistemas	Alta	Medio	Alto
R04	Acceso a información por personal no autorizado	Archivos confidenciales	Controles físicos insuficientes	Filtración de información interna	Muy Alta	Alto	Crítico
R05	Ataque de denegación de servicio (DoS)	Servidores web	Ausencia de sistema de detección	Interrupción de servicios	Medio	Muy Alto	Alto
R06	Mínima planificación y coordinación	Gestión de riesgos	Ineficiencia en la gestión de riesgos, pérdida de confianza con los clientes	Limitada perspectiva del giro de negocio	Alto	Alto	Alto
R07	Mínimo compromiso por parte de la Alta Gerencia	Continuidad del Servicio	Ineficiencia falta de compromiso con los	Imposibilidad de Aplicar medidas de prevención y/o protección	Alto	Alto	Alto

Interpretación:

De la tabla anterior presentada, se evidencia los resultados obtenidos de la situación institucional en acorde a las características de Planificación, para hacer frente ello se establece las características de requisitos, necesidades, partes interesadas políticas organizativas, para poder identificar la posibilidad de establecer el SGSI, considerando los siguientes resultados

R01(Riesgo Crítico): Acceso no autorizado a información sensible

Este riesgo es considerado crítico debido a la alta probabilidad de ocurrencia y el impacto elevado en la confidencialidad de los datos de la municipalidad. Frente a ello, los controles desarrollados, se orientan al manejo de un sistema de autenticación robusto, incluyendo de doble factor es crucial para reducir este riesgo y proteger la información sensible.

- Control 1: Implementar un sistema de autenticación y autorización (ISO 27001, 6.4.2) para garantizar que solo los usuarios autorizados accedan a la información sensible.

  Esto se fundamenta en la norma ISO 27001, el acceso no autorizado a la información sensible puede comprometer su confidencialidad e integridad (ISO 27001, 6.4.2).

- Control 2: Realizar auditorías periódicas de los sistemas informáticos para detectar accesos no autorizados (ISO 27001, 9.2.1).

  Se sustenta bajo la norma ISO 27001, que indica que las auditorías periódicas son esenciales para identificar y corregir vulnerabilidades en los sistemas informáticos (ISO 27001, 9.2.1).

R02(Riesgo Crítico): Pérdida de datos por fallo en almacenamiento

El inapropiado almacenamiento, o inapropiada redundancia, de documentos críticos podría provocar una pérdida significativa de información, con impactos

operativos y legales. Para hacer frente a esta situación, se prioriza el contar con un sistema de respaldo diario que almacene automáticamente copias de los archivos en ubicaciones seguras, preferiblemente en servidores externos o en la nube, puede asegurar la recuperación en caso de un fallo en el almacenamiento.

- Control 1: Implementar un sistema de copia de seguridad regular (ISO 27001, 6.3.4) para garantizar que los datos sean recuperables en caso de una falla en el almacenamiento.

  Fundamentación: Según la norma ISO 27001, la pérdida de datos puede comprometer su integridad e inaccesibilidad (ISO 27001, 6.3.4).

- Control 2: Realizar pruebas periódicas del sistema de copia de seguridad (ISO 27001, 9.1.3).

  Fundamentación: Según la norma ISO 27001, las pruebas periódicas son esenciales para garantizar que el sistema de copia de seguridad sea efectivo (ISO 27001, 9.1.3).

R03 (Riesgo Alto): Malware por descargas no supervisadas

El riesgo de malware/virus se considera alto debido a la frecuencia de descargas de archivos, lo que podría comprometer los sistemas y la integridad de los datos. Frente a este escenario, resulta pertinente manejar un sistema de filtro de seguridad y un antivirus actualizado que supervise y limite las descargas no autorizadas. Además, la capacitación del personal en buenas prácticas de seguridad digital puede contribuir a mitigar este riesgo.

- Control 1: Implementar un sistema de control de acceso a Internet (ISO 27001, 6.4.5) para evitar que los usuarios descarguen malware.

  Fundamentación: Según la norma ISO 27001, el malware puede comprometer la seguridad y confidencialidad de los datos (ISO 27001, 6.4.5).

- Control 2: Realizar actualizaciones periódicas del software y antivirus (ISO 27001, 9.2.3).

Fundamentación: Según la norma ISO 27001, las actualizaciones periódicas son esenciales para garantizar que el software y los antivirus estén actualizados y eficaces contra los malware (ISO 27001, 9.2.3).

R04 (Riesgo Crítico): Acceso a información por personal no autorizado

La posibilidad de que el personal no autorizado acceda a archivos confidenciales se clasifica como un riesgo medio. Por ello resulta imprescindible el contar con los controles de seguridad física y capacitar al personal sobre los protocolos de acceso y/o bloqueo para áreas sensibles.

- Control 1: Implementar un sistema de autenticación y autorización (ISO 27001, 6.4.2) para garantizar que solo los usuarios autorizados accedan a la información.

  Fundamentación: Según la norma ISO 27001, el acceso no autorizado a la información puede comprometer su confidencialidad e integridad (ISO 27001, 6.4.2).

- Control 2: Realizar auditorías periódicas de los sistemas informáticos para detectar accesos no autorizados (ISO 27001, 9.2.1).

  Fundamentación: Según la norma ISO 27001, las auditorías periódicas son esenciales para identificar y corregir vulnerabilidades en los sistemas informáticos (ISO 27001, 9.2.1).

R05 (Riesgo Medio): Ataque de denegación de servicio (DoS)

Aunque la probabilidad de un ataque DoS es baja, el impacto en los servicios web de la municipalidad podría ser significativo. Es debido a esto, que resulta necesario contar con firewalls avanzados y sistemas de detección de intrusiones para monitorear y bloquear intentos de ataque, lo cual garantizará la continuidad de los servicios esenciales.

- Control 1: Implementar un sistema de detección de intrusiones (ISO 27001, 6.4.7) para detectar y prevenir ataques DoS.

  Fundamentación: Según la norma ISO 27001, los ataques DoS pueden comprometer la disponibilidad de los sistemas informáticos (ISO 27001, 6.4.7).

- Control 2: Realizar auditorías periódicas de los sistemas informáticos para detectar vulnerabilidades que puedan permitir ataques DoS (ISO 27001, 9.2.1).

  Fundamentación: Según la norma ISO 27001, las auditorías periódicas son esenciales para identificar y corregir vulnerabilidades en los sistemas informáticos (ISO 27001, 9.2.1).

R06: Mínima planificación y coordinación

La planificación de operaciones, cambios, entre otros, es necesaria de manera frecuente y su nivel de impacto es alto dentro de la municipalidad, dado que es indispensable una correcta planificación y establecer los mecanismos apropiados de coordinación, mediante programación de acciones, cambios, producción, establecer apropiada y oportunamente las acciones del personal responsable.

- Control 1: Implementar un sistema de gestión de proyectos (ISO 27001, 6.3.2) para garantizar que se realicen las actividades de planificación y coordinación de manera efectiva.

  Fundamentación: Según la norma ISO 27001, la falta de planificación y coordinación puede comprometer la seguridad y confidencialidad de los datos (ISO 27001, 6.3.2).

- Control 2: Realizar auditorías periódicas de las actividades de planificación y coordinación (ISO 27001, 9.2.1).

  Fundamentación: Según la norma ISO 27001, las auditorías periódicas son esenciales para identificar y corregir vulnerabilidades en los sistemas informáticos (ISO 27001, 9.2.1).

R07: Mínimo compromiso por parte de la Alta Gerencia

El compromiso de la alta gerencia como las partes interesadas tiene que ser permanente y consecuentemente el impacto es crítico, dado que, de ello, se van establecer las políticas organizacionales y organizativas, el compromiso con los cambios y de posibles implementaciones que impacten en el núcleo de la actividad institucional.

- Control 1: Implementar un sistema de gestión de riesgos (ISO 27001, 6.3.1) para garantizar que se identifiquen y gestionen los riesgos asociados con la seguridad y confidencialidad de los datos.

  Fundamentación: Según la norma ISO 27001, el compromiso insuficiente por parte de la Alta Gerencia puede comprometer la seguridad y confidencialidad de los datos (ISO 27001, 6.3.1).

- Control 2: Realizar auditorías periódicas de las actividades de gestión de riesgos (ISO 27001, 9.2.1).

  Fundamentación: Según la norma ISO 27001, las auditorías periódicas son esenciales para identificar y corregir vulnerabilidades en los sistemas informáticos (ISO 27001, 9.2.1).

Fase 2: Hacer

Para esta segunda etapa, se realiza el establecer los controles para mitigar los riesgos, establecidos a través de la planificación y del contexto en el que opera la Municipalidad Provincial del Santa. Algunos de los controles en este contexto son:

Tabla 4

Detalles de la identificación de Controles- Fase 2 Hacer

ID de Control	Descripción del Control	Riesgo Mitigado	Estado de Implementación	Responsable	Frecuencia de Revisión	Métrica de Eficacia
C01	Autenticación de doble factor	Acceso no autorizado	Parcialmente	Administrador de TI	Quincenal/ Mensual	Reducción de intentos de acceso no autorizado
C02	Respaldo diario automático de datos	Pérdida de datos	En proceso	Jefe de Seguridad	Semanal	Disponibilidad de los datos respaldados
C03	Software de antivirus y firewall	Malware y ataques externos	Implementado	Responsable de Redes	Diario	Reducción de incidentes de malware (%)
C04	Restricción de acceso físico a áreas sensibles	Acceso a información confidencial	Implementado	Seguridad Física	Mensual	Disminución de incidentes de acceso no autorizado en áreas restringidas (%)
C05	Sistema de monitoreo de tráfico en la red	Ataques de denegación de servicio	En proceso	Analista de Redes	Diario	Reducción de intentos de ataque de denegación (%)
C06	Capacitación de empleados sobre procedimientos de seguridad	Fuga de información confidencial	En proceso	Administrador de TI	Semestral	Disminución de incidentes de acceso no autorizado a información (%)
C07	Implementar un gestión de riesgos para garantizar que se identifiquen y gestionen los riesgos	Accesos no autorizados y gestión de riesgos.	En proceso	Administrador de TI	Mensual	Nivel de involucramiento en la gestión de la seguridad de información (%)

Interpretación:

De la tabla anterior presentada, se evidencia los resultados obtenidos de la situación institucional en acorde a las características de la fase de "Hacer", para ello se establecer las características de requisitos, partes interesadas, necesidades, entre otros, para poder identificar la posibilidad de implementar el SGSI, considerando los siguientes resultados

Control C01: Autenticación de doble factor

Este control debe ser implementado para mitigar el riesgo de acceso no autorizado a la información. Su revisión quincenal/mensual permite detectar rápidamente cualquier fallo o ineficiencia en su aplicación. La métrica de eficacia proporciona una notable disminución en los intentos de acceso no autorizado, lo que indica que el control es efectivo y se recomienda su monitoreo continuo.

Control C02: Respaldo diario automático de datos

Aún en proceso de implementación, este control es fundamental para asegurar la integridad y disponibilidad de los datos. Una vez completado, permitirá que todos los datos críticos tengan respaldo, garantizando la recuperación en caso de alguna pérdida o fallo. La frecuencia semanal de revisión asegura que los respaldos sean correctos y se mantengan disponibles.

Control C03: Antivirus y firewall

Este control, ya implementado, busca proteger la infraestructura de TI institucional contra malware y ataques externos. La revisión diaria del sistema de antivirus y firewall ha logrado reducir los incidentes de malware, lo cual es un indicador positivo de su eficacia. Este control es fundamental, de constante actualización y revisión para mantener su efectividad.

Control C04: Restricción de acceso físico a áreas sensibles

Este control es una medida clave para proteger la confidencialidad de la información almacenada en ubicaciones específicas dentro de la municipalidad, Gerencia de Tecnología de la Información y Comunicación. La restricción de acceso físico y realizar revisiones mensuales, reduce los incidentes de acceso no autorizado. Este resultado respalda la importancia de mantener estrictas medidas físicas de seguridad en áreas críticas.

Control C05: Sistema de monitoreo de tráfico en la red

Aún en proceso, este control es vital para identificar problemas y mitigar ataques como denegación de servicio (DoS), bucles, caídas de nodos y otras actividades maliciosas en la red. Su implementación, se sugiere un monitoreo diario para detectar y bloquear rápidamente cualquier intento de ataque.

Control C06: Capacitación de empleados sobre procedimientos de seguridad

El contexto de la municipalidad, se identifica como uno de los riesgos la fuga de información, dado que los usuarios tienen acceso a la información, más no se ha establecido plenamente una cultura de procedimientos de seguridad y capacitación para los colaboradores de la entidad, lo que puede llevar a consecuencias contraproducentes para la privacidad y seguridad de la información.

Fase 3: Verificación

La Fase Verificación es la tercera etapa del PHVA, donde se revisa los controles implementados, y plantea las situaciones encontradas observaciones y/o Acciones correctivas en relación con la seguridad de la información de la Municipalidad Provincial del Santa. Algunos de los controles en este contexto son:

Tabla 5

Detalles de verificación de los Controles- Fase 3 Verificación

ID de Control	Descripción del Control de verificación	Estado Actual	Cumple (Sí/No)	Observaciones	Acciones Correctivas
C01	Autenticación de doble factor	Implementado	No	Se mantiene operativo y efectivo en seguridad	Revisión mensual para asegurar funcionamiento óptimo con doble factor.
C02	Respaldo diario automático de datos	Parcialmente	No	Faltan respaldos en ubicaciones críticas	Completar respaldo en todas las áreas
C03	Software antivirus y firewall	Implementado	Sí	Ha reducido incidentes de malware en un 90%	Actualización semanal del software
C04	Restricción de acceso físico	Implementado	Sí	Control eficaz en áreas restringidas	Monitoreo trimestral de acceso
C05	Monitoreo de tráfico en la red	Parcialmente	No	Solo cubre parte de la red; zonas vulnerables detectadas	Expandir cobertura de monitoreo en toda la red
C06	Política alineada a TI	Parcialmente	No	Políticas aplicadas insuficientes	Revisión periódica de las políticas de seguridad

Interpretación:

De la tabla anterior presentada, se evidencia los resultados obtenidos de la situación institucional en acorde a las características de la fase de "Verificar", para ello se establecer las características de requisitos, partes interesadas, necesidades, entre otros, para poder identificar la posibilidad de implementar el SGSI, considerando los siguientes resultados

Control C01: Autenticación de doble factor

Control no aplicado eficientemente, este control no cumple plenamente con los requisitos ya que se encuentra completamente implementado, pero con autenticación simple. Se recomienda incorporar el segundo factor de autenticidad, y mantener la revisión mensual para asegurar que funcione de manera óptima. Su efectividad procura la reducción de intentos de acceso no autorizado respalda su utilidad dentro del SGSI.

Control C02: Respaldo diario automático de datos

Control aplicado insuficiente, este control se encuentra parcialmente implementado, ya que algunos respaldos críticos no están completados en ciertas ubicaciones. Se ha identificado como una prioridad completar el respaldo en todas las áreas críticas para asegurar la integridad de los datos. Se sugiere establecer una revisión semanal hasta completar la implementación total.

Control C03: Antivirus y firewall

Control aplicado completamente, este control cumple con los objetivos de seguridad, y su efectividad ha sido comprobada con una reducción de los incidentes de malware. Sin embargo, es crucial actualizar el software de seguridad semanalmente para mantenerse al día frente a las amenazas emergentes y garantizar una protección continua.

Control C04: Restricción de acceso físico a áreas sensibles

La restricción de acceso físico cumple con los objetivos y se considera eficaz en áreas sensibles. El monitoreo trimestral del control ha mostrado que se reducen los accesos no autorizados. Es recomendable mantener esta frecuencia de revisión para asegurar que la seguridad física esté alineada con los requisitos del SGSI.

Control C05: Sistema de monitoreo de tráfico en la red

Actualmente, el monitoreo de tráfico en la red cubre parcialmente la infraestructura, dejando zonas vulnerables sin protección adecuada. Es necesario expandir el sistema de monitoreo para abarcar toda la red. Esta acción permitirá detectar y mitigar amenazas de manera más efectiva, reduciendo la exposición a posibles ataques.

Control C06: Política alineada a TI

Las políticas aplicadas a las TI en infraestructura y seguridad cumplen parcialmente la necesidad institucional, estas políticas aplicadas son insuficientes, para ello se requiere la revisión periódica de las políticas de seguridad, así como el compromiso alineado a los estándares de seguridad.

Fase 4: Acción

La Fase Acción es la cuarta etapa del PHVA, donde se implementan las acciones necesarias para mejorar la seguridad de la información en la Municipalidad Provincial del Santa. Algunos de los controles en este contexto son:

Tabla 6

Detalles de Acción frente a los Controles- Fase 4 Actuar

ID de Control	Descripción del Control	Desempeño Actual	Meta de Mejora	Acciones de Mejora	Responsable	Fecha de Revisión
C01	Autenticación de doble factor	Cobertura parcial	95% de reducción en accesos no autorizados	Implementar autenticación biométrica complementaria	Responsable de TI	Trimestral
C02	Respaldo diario automático de datos	Cobertura parcial en áreas críticas	Completar 100% de los respaldos en áreas críticas	Automatizar respaldo y ampliar almacenamiento en la nube	Jefe de Seguridad	Mensual
C03	Antivirus y firewall actualizados	Incidentes reducidos en un 90%	Aumento de reducción a 95%	Revisar políticas de actualización y reforzar monitoreo	Administrador de Seguridad	Semestral
C04	Restricción de acceso físico	90% de efectividad	Alcanzar 100% de control de acceso en áreas restringidas	Implementar identificaciones electrónicas y reforzar control de acceso físico	Seguridad Física	Trimestral
C05	Monitoreo de tráfico en la red	Cobertura parcial	Extender a 100% de la red	Ampliar sistema de monitoreo para cubrir red completa	Analista de Redes	Trimestral
C06	Política alineada a TI	Cobertura parcial	Incorporar al 100% las políticas orientadas a estándares de seguridad	Implementar políticas alineadas a estándares de seguridad	Responsable de TI / Alta Gerencia	Trimestral

Interpretación:

De la tabla anterior presentada, se evidencia los resultados obtenidos de la situación institucional en acorde a las características de la fase de "Actuar", para ello se establecer las características de requisitos, partes interesadas, necesidades, entre otros, para poder identificar la posibilidad de implementar el SGSI, considerando los siguientes resultados

Control C01: Autenticación de doble factor

Aunque este control ha reducido los intentos no autorizados, se debe considerar el doble factor, su efectividad puede mejorar con la implementación de autenticación biométrica como una capa adicional de seguridad. Esto permite alcanzar la meta de una reducción del 95% en los accesos no autorizados y reforzará la confidencialidad de los datos sensibles.

Control C02: Respaldo diario automático de datos

Actualmente, la cobertura del respaldo de datos es parcial en áreas críticas. Para asegurar que todos los datos esenciales estén respaldados, se recomienda automatizar el proceso y aumentar el almacenamiento en la nube. Estas acciones permitirán garantizar la disponibilidad del 100% de los datos y facilitarán una recuperación rápida en caso de fallos.

Control C03: Antivirus y firewall

Aunque los incidentes de malware han sido reducidos en un 90%, existe la posibilidad de alcanzar una reducción del 95% mediante políticas de actualización más estrictas y un monitoreo proactivo. Se recomienda realizar revisiones semestrales del software y capacitar al personal en la identificación de amenazas emergentes.

Control C04: Restricción de acceso físico a áreas sensibles

El control de acceso físico es eficaz en un 90%, pero aún hay margen para mejorar hasta alcanzar el 100%. La implementación de identificaciones electrónicas y un refuerzo en los controles de entrada permitirá mayor efectividad en la restricción de acceso a áreas sensibles, protegiendo los activos críticos de la organización.

Control C05: Sistema de monitoreo de tráfico en la red

Se encontró que el monitoreo de la red cubre parcialmente la infraestructura. Se recomienda extender la cobertura a toda la red para detectar de forma temprana posibles amenazas en todos los puntos de acceso. Con este ajuste, se espera mejorar la capacidad de respuesta ante incidentes de seguridad.

Control C06: Política alineada a TI

Las políticas aplicadas a las TI en infraestructura y seguridad cumplen parcialmente la necesidad institucional. Al establecer que las políticas sean adecuadas y apropiadas a la realidad institucional, así mismo, sea alineado a estándares que prevean condiciones de calidad, de garantía en el cumplimiento de métricas y/o parámetros de seguridad.

Resultados de la investigación

Resultados por dimensiones – Dimensión 1

Según la información recolectada y procesada, se tiene los siguientes resultados correspondiente a la Dimensión 1: "Identificación de riesgos"

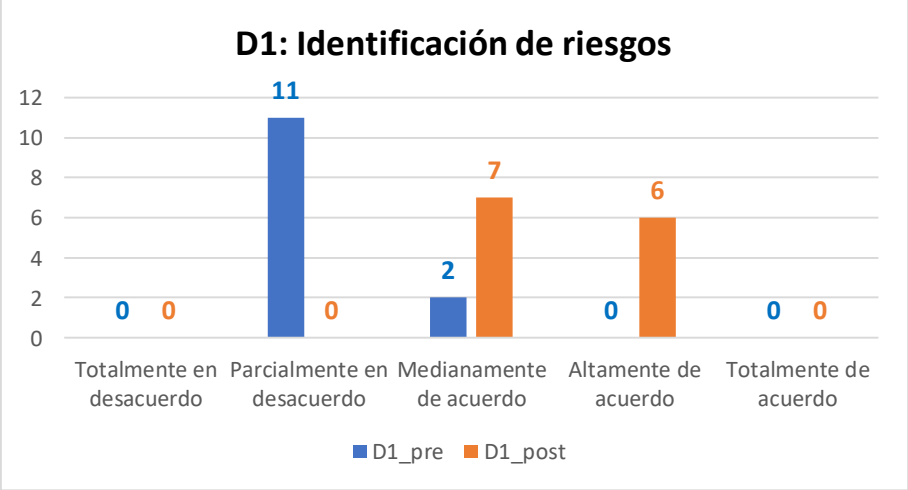
Tabla 7

Resultados de dimensión 1

Criterio	Dimensión 1 – Pre Test	Dimensión 1 – Post Test	Dimensión 1 – Pre Test (%)	Dimensión 1 – Post Test(%)
Totalmente de acuerdo	0	0	0.00%	0.00%
Altamente de acuerdo	0	6	0.00%	46.15%
Medianamente de acuerdo	2	7	15.38%	53.85%
Parcialmente en desacuerdo	11	0	84.62%	0.00%
Totalmente en desacuerdo	0	0	0.00%	0.00%

Figura 5

Gráfico en barras de resultados de dimensión 1



Interpretación:

En cuanto a la identificación de riesgos, la cual pretende conocer el avance que tiene la Municipalidad Provincial del Santa en cuanto a la percepción de la gestión de seguridad de la información, la clasificación de los activos, la identificación de las

amenazas y de las vulnerabilidades, tal así como la existencia de políticas alineadas al estándar de la ISO 27001, lo cual señala en el pre test que la mayoría de respuestas se ubicaron en parcialmente en desacuerdo, con un 84.62%, mientras que solamente el 15.38% indicaron estar en medianamente de acuerdo. Esto muestra que la percepción de la identificación de los riesgos, correspondientemente a su implementación de procesos de gestión referente a la identificación oportuna de los riesgos de seguridad de la información, se encuentra en una etapa inicial.

Por otra parte, en post test se muestra un considerable cambio, al obtener que el 53.85% de los encuestados refieren medianamente de acuerdo, con esto se añade que, un 46.15% lo considera como altamente de acuerdo, con ello se evidencia que existe una mejora en la identificación de riesgos y en el discernimiento de acciones referentes a seguridad de la información ubicadas en la municipalidad.

Resultados por dimensiones – Dimensión 2

Según la información recolectada y procesada, se tiene los siguientes resultados correspondiente a la Dimensión 2: "Tratamiento de riesgos"

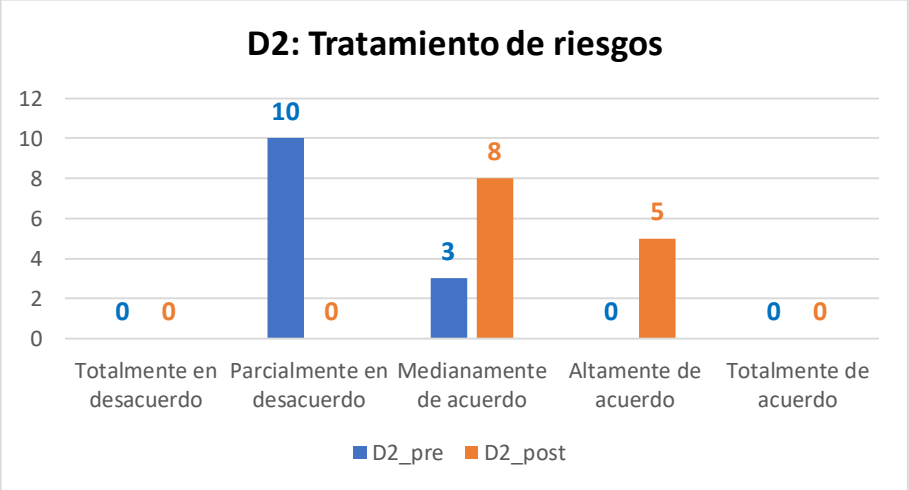
Tabla 8

Resultados de dimensión 2

Criterio	Dimensión 2 – Pre Test	Dimensión 2 – Post Test	Dimensión 2 – Pre Test(%)	Dimensión 2 – Post Test(%)
Totalmente de acuerdo	0	0	0.00%	0.00%
Altamente de acuerdo	0	5	0.00%	38.46%
Medianamente de acuerdo	3	8	23.08%	61.54%
Parcialmente en desacuerdo	10	0	76.92%	0.00%
Totalmente en desacuerdo	0	0	0.00%	0.00%

Figura 6

Gráfico en barras de resultados de dimensión 2



Interpretación:

En cuanto al tratamiento de los riesgos, la cual pretende conocer el avance que tiene la Municipalidad Provincial del Santa en cuanto a las acciones contempladas frente a los riesgos existentes, sobre la gestión de seguridad de la información, que abarcan el acceso físico a los recursos, la implementación de sistemas de respaldos, procedimientos

relacionados a la gestión de los incidentes, entre otros, alineadas al estándar de la ISO 27001, lo cual señala en el pre test que la mayoría imponente de las respuestas se ubicaron en una percepción parcialmente en desacuerdo, con un 76.92%, y que únicamente el 23.08% tienen una se posiciona en medianamente de acuerdo. Esto muestra que la percepción que se tiene, correspondientemente a su implementación apropiada y oportuna del tratamiento de los riesgos de seguridad de la información de la Municipalidad Provincial del Santa, se encuentra en una etapa inicial.

Por otra parte, en post test se evidencia un significativo cambio, al haberse obtenido como resultado que el 61.54% de los encuestados refieren el estar medianamente de acuerdo, y con esto se añade que, un 38.46% lo considera como altamente de acuerdo, lo que posiciona con una media superior, con estos resultados, se evidencia que existe una mejora significativo mejora en la percepción sobre los procedimientos de Tratamiento de riesgos alineados al estándar de ISO 27001 en la Municipalidad Provincial del Santa.

Resultados por dimensiones – Dimensión 3

Según la información recolectada y procesada, se tiene los siguientes resultados correspondiente a la Dimensión 3: "Cumplimiento normativo"

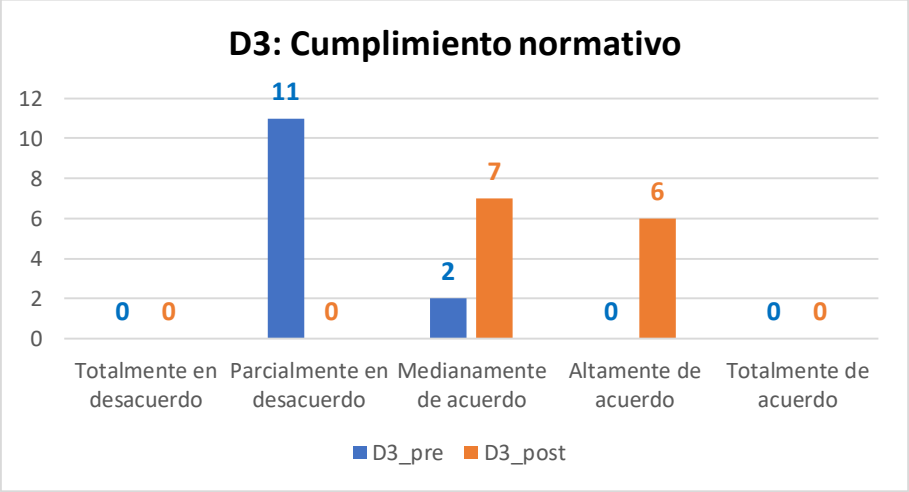
Tabla 9

Resultados de dimensión 3

Criterio	Dimensión 3 – Pre Test	Dimensión 3 – Post Test	Dimensión 3 – Pre Test	Dimensión 3 – Post Test
Totalmente de acuerdo	0	0	0.00%	0.00%
Altamente de acuerdo	0	6	0.00%	46.15%
Medianamente de acuerdo	2	7	15.38%	53.85%
Parcialmente en desacuerdo	11	0	84.62%	0.00%
Totalmente en desacuerdo	0	0	0.00%	0.00%

Figura 7

Gráfico en barras de resultados de dimensión 3



Interpretación:

En cuanto al cumplimiento normativo, la cual pretende identificar y entender el avance que tiene la Municipalidad Provincial del Santa en cuanto a las acciones que abarcan los aspectos regulatorios sobre los activos de la información, procedimientos de respuesta ante incidentes y/o de mejora continua, entre otros, alineadas al estándar de la

ISO 27001, lo cual señala en el pre test que la mayoría imponente de las respuestas se ubicaron en una percepción parcialmente en desacuerdo, con un 84.62%, y que únicamente el 15.38% tienen una se posiciona en medianamente de acuerdo. Esto muestra que la percepción que se tiene, correspondientemente a su implementación apropiada y oportuna del tratamiento de los riesgos de seguridad de la información de la Municipalidad Provincial del Santa, se encuentra en una etapa inicial.

Por otra parte, en post test se evidencia un significativo cambio, al haberse obtenido como resultado que el 53.85% de los encuestados refieren el estar medianamente de acuerdo, y con esto se añade que, un 46.15% lo considera como altamente de acuerdo, lo que posiciona con una media superior, con estos resultados, se evidencia que existe una mejora significativo mejora en la percepción sobre los procedimientos relacionados con el cumplimiento normativo alineados al estándar de ISO 27001 en la Municipalidad Provincial del Santa.

4.2.DISCUSIÓN

Según los resultados de la presente investigación, en cuanto a la dimensión sobre Identificación de Riesgos, en detalle de los resultados obtenidos, se muestra un considerable cambio positivo, al haber obtenido el 53.85% de los encuestados que refieren encontrarse con una percepción de medianamente de acuerdo, así también que, un 46.15% lo considera como altamente de acuerdo, con ello se evidencia la significativa mejora en los registros e identificación de riesgos sobre los activos referente a seguridad de la información ubicadas en la Municipalidad Provincial del Santa.

Esto se, se refuerza con lo concluido por López, J. (2022) quien indica que siguiendo los lineamientos de la norma ISO/IEC 27001, tiene como a la finalidad de resguardar los activos de información, debido a las constantes amenazas internas y externas, se consideró mejoras en la organización y eficiencia en el tratamiento de eventos y amenazas.

De los resultados obtenidos, correspondiente a la dimensión de Tratamiento de los riesgos, se obtuvo como evidencia, un significativo cambio, al haberse obtenido como resultado que el 61.54% de los encuestados refieren el estar medianamente de acuerdo, así como que, un 38.46% lo considera como altamente de acuerdo, lo que evidencia la percepción sobre la media superior, con estos resultados, se evidencia que existe una mejora significativo mejora en la percepción sobre los procedimientos de Tratamiento de riesgos alineados al estándar de ISO 27001 en la Municipalidad Provincial del Santa.

Lo que se refuerza con lo referido por García (2020), la aplicación del estándar ISO 27001, aporta con la salvaguarda de la confidencialidad, la integridad y de la disponibilidad de la información; como de igual forma se refiere dentro del procedimiento de mejora continua.

Con respecto a la tercera dimensión, correspondiente al Cumplimiento normativo, y teniendo en cuenta el haberse obtenido como resultado que el 53.85% de los encuestados refieren el estar medianamente de acuerdo, y con esto se añade que, un 46.15% lo considera como altamente de acuerdo, lo que posiciona con una media superior, con estos resultados, se evidencia que existe una mejora significativo mejora en la percepción sobre los procedimientos relacionados con el cumplimiento normativo alineados al estándar de ISO 27001 en la Municipalidad Provincial del Santa.

Estos hallazgos se relacionan directamente con lo obtenido por Bardales, D. (2024), que el cual resaltó marcadamente que la falta de un plan de contingencia frente a ciberataques es una falencia notable, es por ello que bajo la implementación de la propuesta de seguridad de la información centrada en la ISO 27001, debe tenerse en cuenta fundamentalmente el cumplimiento normativo y el compromiso de la alta gerencia.

CAPÍTULO V:

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

El actual estudio se centró en la recaudación de información teniendo como finalidad el analizar las condiciones actuales de seguridad de la información Evaluación y tratamiento de riesgos e Implementación de controles normativos de seguridad. Considerando la población muestral de los colaboradores o trabajadores de la Gerencia de Tecnologías de la Información y Comunicación de la Municipalidad Provincial del Santa, a través de la aplicación de encuesta con posterior análisis de las respuestas en función de cada uno de los objetivos y dimensiones establecidas en la presente investigación, proporcionando información netamente valiosa para identificar la aplicabilidad de la norma ISO 27001 buscando fortalecer la seguridad de la información en la Municipalidad Provincial del Santa

El diagnóstico del estado actual de la gestión de la seguridad de la información, ha sido imprescindible para la identificación de brechas y vulnerabilidades en la Municipalidad y dar pase a la aplicación de los controles pertinentes y la evaluación de los resultados.

En caso del objetivo general, se concluye que, mediante el conjunto de controles puestos en aplicación bajo el enfoque de mejora continua PHVA, con el fin de fortalecer la gestión de riesgos y la toma de decisiones relacionadas con la seguridad de la información, demostraron tener consistencia y una mejora significativa en la gestión de la seguridad de la información de la Municipalidad Provincial del Santa, esto corroborado a través del análisis de t de Student = -18,620 y una significancia p=0,0000<0,05, se procede a la aceptación de la **hipótesis general** de la investigación y se rechaza a la hipótesis nula.

Se diseñaron los controles de seguridad de la información específicos, según el análisis de la entidad, abordando las brechas identificadas, asegurando que se ajusten a las políticas y estándares establecidos por la norma ISO 27001

Del objetivo específico 1, se concluye que, la aplicación de los controles puestos bajo el enfoque de mejora continua PHVA, en relación del primer objetivo bajo la dimensión de "Identificación de Riesgos", para la toma de decisiones relacionadas con la seguridad de la información, se identificaron los riesgos más resaltantes, tales como: Acceso no autorizado a información sensible, Pérdida de datos por fallo en almacenamiento, Malware por descargas no supervisadas, Acceso a información por personal no autorizado, Ataque de denegación de servicio (DoS), Mínima planificación y coordinación, Mínimo compromiso por parte de la Alta Gerencia. Este análisis demostró tener consistencia y una mejora significativa en la gestión de la seguridad de la información de la Municipalidad Provincial del Santa, esto corroborado a través del análisis de t de Student = -9,859 y una significancia $p=0.0000<0.05$, se procede a la aceptación de la hipótesis específica 1 de la investigación y se rechaza a la hipótesis nula.

Del objetivo específico 2, se concluye que, a aplicación de los controles puestos bajo el enfoque de mejora continua PHVA, en relación del segundo objetivo bajo la dimensión de "Tratamiento de Riesgos", para la toma de decisiones relacionadas con la seguridad de la información, se identificaron los controles aplicables, tales como: Autenticación de doble factor, Respaldo diario automático de datos, Software de antivirus y firewall, Restricción de acceso físico a áreas sensibles, Sistema de monitoreo de tráfico en la red, Capacitación de empleados sobre procedimientos de seguridad, Implementar un gestión de riesgos para garantizar que se identifiquen y gestionen los riesgos. Este análisis demostró tener consistencia y una mejora significativa en la gestión de la seguridad de la información de la Municipalidad Provincial del Santa, esto corroborado

a través del análisis de t de Student = -6,062 y una significancia p=0.0000<0.05, se procede a la aceptación de la hipótesis específica 2 de la investigación y se rechaza a la hipótesis nula.

Del objetivo específico 3, se concluye que, la aplicación de los controles puestos bajo el enfoque de mejora continua PHVA, en la dimensión de "Cumplimiento normativo", para la toma de decisiones relacionadas con la seguridad de la información, información, se identificaron los controles de verificación, tales como: Autenticación de doble factor, Respaldo diario automático de datos, Software antivirus y firewall, Restricción de acceso físico, Monitoreo de tráfico en la red, Política alineada a TI, con sus acciones correctivas respectivas y sus acciones de mejora. Este análisis demostró tener consistencia y una mejora significativa en la gestión de la seguridad de la información de la Municipalidad Provincial del Santa, esto corroborado a través del análisis de t de Student = -10,156 y una significancia p=0.0000<0.05, se procede a la aceptación de la hipótesis específica 3 de la investigación y se rechaza a la hipótesis nula.

La evaluación realizada de cada una de las dimensiones, demuestran efectividad de los controles implementados, y mecanismos de mejora, verificando el nivel de cumplimiento de las políticas y procedimientos establecidos en la propuesta, asegurando que se ajusten a las políticas y estándares establecidos por la norma ISO 27001

RECOMENDACIONES

De acuerdo a la información recogida, así como a la interpretación de la misma, considerando las conclusiones presentadas, se recomienda que la Municipalidad Provincial del Santa implemente un proceso sistemático y estructurado de evaluación continua de la seguridad de la información. Dado que el estudio ha revelado la importancia de aplicar la norma ISO 27001 para fortalecer dicha seguridad, dado que es crucial que se establezca un plan de acción que contemple tanto la identificación de riesgos como el desarrollo de medidas preventivas y correctivas propiamente.

Este proceso debe involucrar activamente, por un lado, a los colaboradores de la Gerencia de Tecnologías de la Información y Comunicación mediante la aplicación periódica de protocolos, encuestas y auditorías internas, por otro lado, a los funcionarios de alto nivel, asegurando así, que se consideren las percepciones y necesidades del personal para mejorar la seguridad de la información. Asimismo, se debe promover la capacitación constante del personal y todos los trabajadores según sus características, en relación con las mejores prácticas en gestión de la seguridad de la información, alineadas con los estándares internacionales de ISO 27001.

En función de la Identificación de Riesgos, dado los significativos resultados obtenidos en la presente investigación, se recomienda el proseguir de manera continua y de forma alineada al estándar ISO 27001, a través de sus lineamientos, que faciliten la adopción de una cultura predominantemente orientado a la seguridad de la información y la gestión de procesos regulados de identificación de riesgo sobre la seguridad.

En función de Tratamiento de Riesgos, dado los significativos resultados obtenidos en la presente investigación, se recomienda el continuar de manera continua y de forma alineada al PHVA y del estándar ISO 27001, a través de sus lineamientos, que faciliten la adopción de una cultura predominantemente orientado a la seguridad de la

información y la gestión de procesos regulados de identificación de riesgo sobre la seguridad.

En función de Cumplimiento normativo, dado los significativos resultados obtenidos en la presente investigación, se recomienda el continuar de manera continua y de forma alineada al estándar ISO 27001, a través de sus lineamientos, que faciliten la adopción de una cultura predominantemente orientado a la seguridad de la información y la gestión de procesos regulados de identificación de riesgo sobre la seguridad, e involucrar activamente a la alta gerencia en establecer esfuerzos coherentes y articulados orientados en el proceso de mejora continua de un SGSI, así como en .los demás colaboradores institucionales que se puedan sensibilizar y comprometer en el cumplimiento de los controles y las normativas relacionadas.

CAPÍTULO VI:

REFERENCIAS BIBLIOGRÁFICAS

BIBLIOGRAFÍA

Academia Latinoamericana De La Seguridad Informática (2011). Unidad 1: Introducción a la Seguridad de Información.

Altamirano, K. (2021). *La seguridad de la información en la administración pública*. Actas del III Congreso Internacional de Ingeniería de Sistemas. págs. 77-95. https://revistas.ulima.edu.pe/index.php/CIIS/article/view/5480

Bardales, D. (2024). Gestión de la seguridad en el manejo de la información y su influencia en la transparencia institucional de la UGEL Requena 2024. [Tesis de grado]. Universidad Nacional de la Amazonía Peruana. https://api-repositorio.unapiquitos.edu.pe/server/api/core/bitstreams/50beaa53-e36f-4b82-8fb0-9a267039737c/content

Barón, D. S. (2020). *Retos en la seguridad de dispositivos para el internet de las cosas (loT)*. [Monografía de Título profesional de Especialista En Seguridad Informática]. Universidad nacional abierta y a distancia. Colombia. https://repository.unad.edu.co/handle/10596/35737?show=full

Bono y Tinoco (2024). Diseño de sistema de gestión de seguridad de la información (SGSI) basado en norma ISO 27001:2022 en empresa san Services S. de R. L. [Tesis de Maestría]. Universidad Tecnológica Centroamericana UNITEC, https://repositorio.unitec.edu/server/api/core/bitstreams/c8d918c9-a695-472a-bee2-ec9f5897e37c/content

Cama y Arellano (2024). Implementación de un sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27001 para la mejora de protección de datos personales en la Clínica María del Socorro. [Tesis de grado]. Universidad Tecnológica del Perú. https://repositorio.utp.edu.pe/handle/20.500.12867/9636

Campo, L. (2024). *Propuesta para la Implementación de la Norma ISO 27001 en el Archivo Central de la Gobernación del Departamento del Magdalena*. [Tesis de Maestría]. Universidad de la Salle. https://ciencia.lasalle.edu.co/server/api/core/bitstreams/2a97f3ed-687a-45da-9e16-2f34d8407bf8/content

Carrasco D.S. (2017). *Metodología de la Investigación Científica: Pauta Metodológicas Para Diseñar y Elaborar el Proyecto de Investigación* (2da ed.). Lima, Perú: San Marcos.

Chiavenato, I. (2006). Introducción a la Teoría General de la Administración. (1ra edición). Editorial McGraw-Hill Interamericana.

Colonia, P.J. (2019). *Propuesta de un sistema de gestión de seguridad de la información con normas ISO 27001 para la Municipalidad Distrital de Buena Vista Alta – Casma; 2017*. Universidad Católica Ángeles de Chimbote.

Díaz, G., Alzórriz, I. Sancristóbal, E. y Castro, M. (2014). Procesos y Herramientas para la Seguridad de Redes. Madrid: UNED.

ESAN Graduate School of Business. (17 de junio 2021) *Cómo identificar a los stakeholders de tu organización*. https://www.esan.edu.pe/conexion-esan/como-identificar-a-los-stakeholders-de-tu-organizacion

Ficco, C. (2019). Los activos intangibles en la normativa contable argentina y en las normas internacionales de información financiera. Contabilidad Y Auditoria, (50).

Fitzgerald, T. (2007). Information Security Governance. En H. Tipton, y M. Krause (Ed.), Information Security Management Handbook (15-34). USA: Auerbach Publications.

García, R.A. (2020). *Propuesta de un sistema de gestión de seguridad de la información basado en la norma ISO 27001 para la oficina de tecnologías de información del gobierno regional Piura; 2020.* Universidad Católica Ángeles de Chimbote.

Gómez F.L. y Fernández, P.P. (2015). Cómo implantar un SGSI según UNE-ISO/IEC 27001:2014 y su aplicación en el Esquema Nacional de Seguridad. (1era Ed) AENOR.

Harris, S. (2004). CISSP Certification: All in One Exam Guide. Emerville California USA: Mc Graw Hill.

Hernández S.R. Fernández C. y Baptista L. (2014). *Metodología de la Investigación* (6ta ed.). Mc Graw Hill.

Ibarra, L. (2023). ISO 27001:2013 para la gestión del manejo de información en la UGEL Bolognesi, Ancash 2023. [Tesis de Maestría]. Universidad Cesar Vallejo

INDECOPI. (2014). Norma Técnica Peruana "NTP-ISO/ IEC 27001:2014. Tecnología de la Información. Técnicas de seguridad. Sistema de gestión de la seguridad de la información. Requisitos. Segunda edición. Lima, Perú.

INDECOPI. (2007). Norma Técnica Peruana "NTP-ISO/ IEC 17799:2007 EDI (ISO 27002:2005). Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información. Segunda edición. Lima, Perú.

Kitsios, F., et al. (2023). La norma ISO/IEC 27001 de gestión de la seguridad de la información: Cómo extraer valor de los datos en el sector de TI. *Sustainability*, *15* (7), 5828. https://doi.org/10.3390/su15075828

López, J. (2022). Implementación del SGSI, basado en la ISO/IEC 27001 para dar tratamiento al riesgo en una empresa constructora. [Tesis de grado]. Universidad San Ignacio de Loyola. https://repositorio.usil.edu.pe/server/api/core/bitstreams/87d8e531-0840-4fcc-a18f-ba851ab40089/content

Martínez, S. Y Lara, P. (2014). *El big data transforma la interpretación de los medios sociales*. Big data y analítica digital (6)23.

National Institute of Standards and Technology. (1995). An Introduction to Computer Security: The NIST Handbook. Special Publication 800-12 Washington USA: National Institute of Standards and Technology (NIST).

Peltier, R. Thomas (2010) Information Security Risk Analysis. Third Edition. Florida: Auerbach.

Periáñez, F. (3 de noviembre de 2016). *Formación Profesional a través de internet - Manual de seguridad informática I*. Obtenido de https://www.fpgenred.es/Seguridad-Informatica-I/clasificacin_de_la_seguridad.html

Peso E. y Ramos, M.A. (2004). El Documento de Seguridad: Análisis técnico y jurídico. Modelo.: Diaz de Santos.

Pillajo, E. (2025). *Implementación de políticas de seguridad de la información en el área de ti con base en la norma ISO/IEC 27001:2022. caso de estudio: cooperativa de ahorro y crédito rural sierra norte*. [Tesis de Maestría]. Universidad Técnica del Norte. https://repositorio.utn.edu.ec/bitstream/123456789/17014/2/PG%202025%20TRABAJO%20DE%20GRADO.pdf

Rodríguez, D.E. (2019). *Los Desafíos del Derecho de las TIC en la Sociedad de la Información en el Siglo XXI: Una Puerta a la Cooperación Internacional*. Universidad Rey Juan Carlos.

Saavedra, J. (2021). Diseño de un plan de gestión de riesgos y vulnerabilidades del caso de estudio de la empresa Qwerty S.A., basados en los estándar NTC-ISO/IEC 27001 Y NTC-ISO/IEC 27032. [Tesis de grado]. Universidad Nacional Abierta y A Distancia - UNAD. https://repository.unad.edu.co/bitstream/handle/10596/36866/jsaavedraag.pdf?sequence=3

Stoneburner, G. NIST (2001). Special Publication 800-33: Underlying Technical. Gaithersburg USA: National Institute of Standards and Technology (NIST)

Tafur, J. (2022) El derecho del acceso a la información, transparencia de la gestión pública y datos abiertos en los gobiernos locales del Perú. https://doi.org/10.51252/rcsi.v2i1.274

Torres, M. (2018). *Diseño de un sistema de gestión de la seguridad de la información (SGSI), basada en la norma ISO/IEC 27001:2013, para el proceso de servicio posventa de un integrador de soluciones en Telecomunicaciones.* Universidad Peruana de Ciencias Aplicadas (UPC).

Vega, E. Seguridad de la información. 3Ciencias. (2021). DOI: https://doi.org/10.17993/tics.2021.4

Zamora, A.I. y Ortiz, M.R. (2021). *Interrelation Between International Competitiveness and Human Development in the Asia-Pacific Region.* (2) 40, Ensayo, Revista económica.

ISO/IEC 27000. (2018). Information technology — Security techniques — Information security management systems — Overview and vocabulary. https://www.iso.org/standard/*73906*.html

CAPÍTULO VII:

ANEXOS

ANEXOS:

Anexo 1: Matriz de consistencia

<table>
<tr><th>Título</th><th>Formulación del problema</th><th>Hipótesis</th><th>Objetivos</th><th>Variable</th><th>Metodología</th></tr>
<tr>
<td rowspan="2">Propuesta de sistema de gestión basado en ISO 27001 para mejorar la seguridad de información en la Municipalidad Provincial del Santa.</td>
<td rowspan="2">General:
¿De qué manera el diseño de una propuesta de un sistema de gestión basado en ISO 27001 podría mejorar la seguridad de información en La Municipalidad Provincial del Santa?</td>
<td rowspan="2">General:
La propuesta de un sistema de gestión basado en ISO 27001, puede mejorar la seguridad de información en La Municipalidad Provincial del Santa.</td>
<td rowspan="2">General:
Diseñar una propuesta de un Sistema de Gestión de Seguridad de la Información basado en ISO 27001, bajo el enfoque de mejora continua PHVA, con el fin de fortalecer la gestión de riesgos y la toma de decisiones relacionadas con la seguridad de la información en la Municipalidad Provincial.

Específicos:
OE 1. Identificar los riesgos de seguridad de la información en la Municipalidad Provincial del Santa, identificando brechas y vulnerabilidades con base en los requisitos de la norma ISO 27001.

OE 2. Establecer el Tratamiento de riesgos, mediante controles necesarios para abordar las brechas seguridad de la información identificadas en la Municipalidad Provincial del Santa

OE 3. Evaluar el cumplimiento normativo de las políticas y procedimientos que se ajusten a las políticas y estándares establecidos por la norma ISO 27001 en la Municipalidad Provincial del Santa</td>
<td>Sistema de Gestión basado en ISO 27001</td>
<td rowspan="2">Método:
Científico
Hipotético - deductivo

Diseño:
experimental
Descriptivo

Población y Muestra
13 colaboradores de la gerencia de tecnologías de información y comunicación de La Municipalidad Provincial del Santa

Técnica de recolección de datos:
Encuesta

Instrumentos de recolección de datos:
Cuestionario
Método de análisis de investigación:
Estadística descriptiva</td>
</tr>
<tr>
<td>Seguridad de la Información</td>
</tr>
</table>

Anexo 2: Instrumento

TITULO: La propuesta de un sistema de gestión basado en ISO 27001, para mejorar la seguridad de información en La Municipalidad Provincial del Santa.

PRESENTACIÓN: El presente instrumento forma parte del actual trabajo de investigación; por lo que se solicita su participación, respondiendo a cada pregunta de manera objetiva y veraz. La información a proporcionar es de carácter confidencial y reservado; y los resultados de la misma serán utilizados solo para efectos académicos y de investigación científica.

INSTRUCCIONES: A continuación, se le presenta un grupo de interrogantes, marque una sola alternativa que estime pertinente con un aspa ("X"), considerando: 1= Totalmente en desacuerdo, 2= Parcialmente en desacuerdo, 3=Medianamente de acuerdo, 4= Altamente de acuerdo, 5= Totalmente de acuerdo

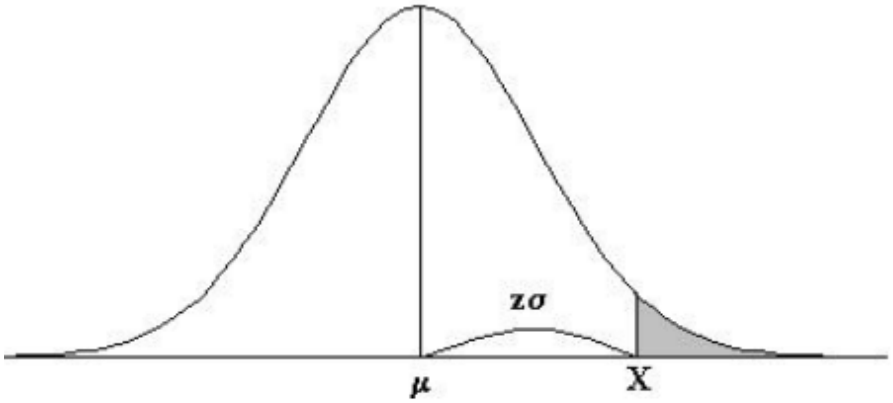
N°	Ítems	1	2	3	4	5
1	¿La Municipalidad Provincial de Santa ha establecido un marco de referencia para la gestión de la seguridad de la información?					
2	¿Los activos de información están clasificados según su nivel de sensibilidad?					
3	¿El análisis de riesgos incluye una identificación de amenazas internas y externas?					
4	¿Se evalúan regularmente las vulnerabilidades de los sistemas de información?					
5	¿Las políticas de seguridad se comunican regularmente a todos los empleados?					
6	¿Existen políticas de seguridad de la información alineadas con ISO 27001?					
7	Según tu percepción. ¿El acceso físico a las áreas de información sensible está restringido y monitoreado?					
8	Se implementan sistemas de respaldo (backup) para garantizar la continuidad del negocio.					
9	Los procedimientos de gestión de incidentes están definidos y son claros para el personal.					
10	¿Se realizan simulacros para evaluar la capacidad de respuesta ante incidentes?					
11	¿Se realiza un monitoreo continuo de los sistemas críticos para detectar anomalías?					
12	¿Se garantiza la disponibilidad de la información en todo momento?					
13	¿Los accesos a los activos de información están restringidos según roles y permisos.?					
14	¿Los procedimientos de respuesta ante incidentes están alineados con las mejores prácticas.?					
15	¿La Municipalidad Provincial de Santa cumple con las regulaciones legales aplicables en seguridad de la información?					

Anexo Nº 03: Tabla distribución T DE ESTUDENT

α / r	0,25	0,2	0,15	0,1	0,05	0,025	0,01	0,005	0,0005
1	1,000	1,376	1,963	3,078	6,314	12,706	31,821	63,656	636,578
2	0,816	1,061	1,386	1,886	2,920	4,303	6,965	9,925	31,600
3	0,765	0,978	1,250	1,638	2,353	3,182	4,541	5,841	12,924
4	0,741	0,941	1,190	1,533	2,132	2,776	3,747	4,604	8,610
5	0,727	0,920	1,156	1,476	2,015	2,571	3,365	4,032	6,869
6	0,718	0,906	1,134	1,440	1,943	2,447	3,143	3,707	5,959
7	0,711	0,896	1,119	1,415	1,895	2,365	2,998	3,499	5,408
8	0,706	0,889	1,108	1,397	1,860	2,306	2,896	3,355	5,041
9	0,703	0,883	1,100	1,383	1,833	2,262	2,821	3,250	4,781
10	0,700	0,879	1,093	1,372	1,812	2,228	2,764	3,169	4,587
11	0,697	0,876	1,088	1,363	1,796	2,201	2,718	3,106	4,437
12	0,695	0,873	1,083	1,356	1,782	2,179	2,681	3,055	4,318
13	0,694	0,870	1,079	1,350	1,771	2,160	2,650	3,012	4,221
14	0,692	0,868	1,076	1,345	1,761	2,145	2,624	2,977	4,140
15	0,691	0,866	1,074	1,341	1,753	2,131	2,602	2,947	4,073
16	0,690	0,865	1,071	1,337	1,746	2,120	2,583	2,921	4,015
17	0,689	0,863	1,069	1,333	1,740	2,110	2,567	2,898	3,965
18	0,688	0,862	1,067	1,330	1,734	2,101	2,552	2,878	3,922
19	0,688	0,861	1,066	1,328	1,729	2,093	2,539	2,861	3,883
20	0,687	0,860	1,064	1,325	1,725	2,086	2,528	2,845	3,850
21	0,686	0,859	1,063	1,323	1,721	2,080	2,518	2,831	3,819
22	0,686	0,858	1,061	1,321	1,717	2,074	2,508	2,819	3,792
23	0,685	0,858	1,060	1,319	1,714	2,069	2,500	2,807	3,768
24	0,685	0,857	1,059	1,318	1,711	2,064	2,492	2,797	3,745
25	0,684	0,856	1,058	1,316	1,708	2,060	2,485	2,787	3,725
26	0,684	0,856	1,058	1,315	1,706	2,056	2,479	2,779	3,707
27	0,684	0,855	1,057	1,314	1,703	2,052	2,473	2,771	3,689
28	0,683	0,855	1,056	1,313	1,701	2,048	2,467	2,763	3,674
29	0,683	0,854	1,055	1,311	1,699	2,045	2,462	2,756	3,660
30	0,683	0,854	1,055	1,310	1,697	2,042	2,457	2,750	3,646
40	0,681	0,851	1,050	1,303	1,684	2,021	2,423	2,704	3,551
60	0,679	0,848	1,045	1,296	1,671	2,000	2,390	2,660	3,460
120	0,677	0,845	1,041	1,289	1,658	1,980	2,358	2,617	3,373
∞	0,674	0,842	1,036	1,282	1,645	1,960	2,326	2,576	3,290

Anexo Nº 04: Tabla de distribución normal

Áreas bajo la curva normal



Ejemplo:

$$Z = \frac{X - \mu}{\sigma}$$

$P\,[Z > 1] = 0.1587$
$P\,[Z > 1.96] = 0.0250$

Desv. normal x	0.00	0.01	0.02	0.03	0.04	0.05	0.06	0.07	0.08	0.09
0.0	0.5000	0.4960	0.4920	0.4880	0.4840	0.4801	0.4761	0.4721	0.4681	0.4641
0.1	0.4602	0.4562	0.4522	0.4483	0.4443	0.4404	0.4364	0.4325	0.4286	0.4247
0.2	0.4207	0.4168	0.4129	0.4090	0.4052	0.4013	0.3974	0.3936	0.3897	0.3859
0.3	0.3821	0.3783	0.3745	0.3707	0.3669	0.3632	0.3594	0.3557	0.3520	0.3483
0.4	0.3446	0.3409	0.3372	0.3336	0.3300	0.3264	0.3228	0.3192	0.3156	0.3121
0.5	0.3085	0.3050	0.3015	0.2981	0.2946	0.2912	0.2877	0.2843	0.2810	0.2776
0.6	0.2743	0.2709	0.2676	0.2643	0.2611	0.2578	0.2546	0.2514	0.2483	0.2451
0.7	0.2420	0.2389	0.2358	0.2327	0.2296	0.2266	0.2236	0.2206	0.2177	0.2148
0.8	0.2119	0.2090	0.2061	0.2033	0.2005	0.1977	0.1949	0.1922	0.1894	0.1867
0.9	0.1841	0.1814	0.1788	0.1762	0.1736	0.1711	0.1685	0.1660	0.1635	0.1611
1.0	0.1587	0.1562	0.1539	0.1515	0.1492	0.1469	0.1446	0.1423	0.1401	0.1379
1.1	0.1357	0.1335	0.1314	0.1292	0.1271	0.1251	0.1230	0.1210	0.1190	0.1170
1.2	0.1151	0.1131	0.1112	0.1093	0.1075	0.1056	0.1038	0.1020	0.1003	0.0985
1.3	0.0968	0.0951	0.0934	0.0918	0.0901	0.0885	0.0869	0.0853	0.0838	0.0823
1.4	0.0808	0.0793	0.0778	0.0764	0.0749	0.0735	0.0721	0.0708	0.0694	0.0681
1.5	0.0668	0.0655	0.0643	0.0630	0.0618	0.0606	0.0594	0.0582	0.0571	0.0559
1.6	0.0548	0.0537	0.0526	0.0516	0.0505	0.0495	0.0485	0.0475	0.0465	0.0455
1.7	0.0446	0.0436	0.0427	0.0418	0.0409	0.0401	0.0392	0.0384	0.0375	0.0367
1.8	0.0359	0.0351	0.0344	0.0336	0.0329	0.0322	0.0314	0.0307	0.0301	0.0294
1.9	0.0287	0.0281	0.0274	0.0268	0.0262	0.0256	0.0250	0.0244	0.0239	0.0233
2.0	0.0228	0.0222	0.0217	0.0212	0.0207	0.0202	0.0197	0.0192	0.0188	0.0183
2.1	0.0179	0.0174	0.0170	0.0166	0.0162	0.0158	0.0154	0.0150	0.0146	0.0143
2.2	0.0139	0.0136	0.0132	0.0129	0.0125	0.0122	0.0119	0.0116	0.0113	0.0110
2.3	0.0107	0.0104	0.0102	0.0099	0.0096	0.0094	0.0091	0.0089	0.0087	0.0084
2.4	0.0082	0.0080	0.0078	0.0075	0.0073	0.0071	0.0069	0.0068	0.0066	0.0064
2.5	0.0062	0.0060	0.0059	0.0057	0.0055	0.0054	0.0052	0.0051	0.0049	0.0048
2.6	0.0047	0.0045	0.0044	0.0043	0.0041	0.0040	0.0039	0.0038	0.0037	0.0036
2.7	0.0035	0.0034	0.0033	0.0032	0.0031	0.0030	0.0029	0.0028	0.0027	0.0026
2.8	0.0026	0.0025	0.0024	0.0023	0.0023	0.0022	0.0021	0.0021	0.0020	0.0019
2.9	0.0019	0.0018	0.0018	0.0017	0.0016	0.0016	0.0015	0.0015	0.0014	0.0014
3.0	0.0013	0.0013	0.0013	0.0012	0.0012	0.0011	0.0011	0.0011	0.0010	0.0010

Anexo Nº 05: Validación y confiabilidad de instrumentos

Validación de instrumentos

La validación de los instrumentos utilizados en el presente trabajo de investigación, han sido validado a través del juico de expertos y mediante el análisis del V. AIKEN, para lo cual se utilizará la siguiente fórmula:

$$V = \frac{S}{(n(c-1))}$$

S = Sumatoria de los valores dados por los jueces al ítem
n = Número de jueces
c = Numero de valores de la escala de valoración

Dado la evaluación de juicios expertos, se precisa que los instrumentos diseñados para la presente investigación, son válidas como se puede evidenciar en el Anexo 3.

Análisis de la Confiabilidad de Instrumentos

La confiablidad con base al análisis de los datos recolectados de las encuestas, con el Alfa de Cronbach a cada uno de los instrumentos aplicados en la presente investigación.

Confiabilidad del Instrumento

Estadísticas de fiabilidad

Alfa de Cronbach	Alfa de Cronbach basada en elementos estandarizados	N de elementos
0,927	0,931	15

Según el análisis de confiabilidad obtenido, el resultado de 0.927 se considera una confiabilidad muy alta, por lo cual se considera que el instrumento aplicado es confiable para la realización de la investigación.

Resultados Total de la confiabilidad del instrumento - SPSS

Estadísticas de total de elemento

	Media de escala si el elemento se ha suprimido	Varianza de escala si el elemento se ha suprimido	Correlación total de elementos corregida	Correlación múltiple al cuadrado	Alfa de Cronbach si el elemento se ha suprimido
IT101	33,31	33,564	0,610	.	0,923
IT102	34,62	31,256	0,800	.	0,917
IT103	35,38	33,923	0,580	.	0,924
IT104	34,46	34,603	0,504	.	0,926
IT105	34,15	29,474	0,751	.	0,921
IT106	34,38	33,923	0,580	.	0,924
IT107	34,15	31,308	0,765	.	0,919
IT108	34,23	32,359	0,808	.	0,918
IT109	34,54	34,103	0,719	.	0,922
IT110	33,69	32,564	0,683	.	0,921
IT111	33,62	33,090	0,529	.	0,926
IT112	34,38	33,923	0,580	.	0,924
IT113	34,31	30,564	0,735	.	0,920
IT114	34,23	32,359	0,808	.	0,918
IT115	34,23	34,192	0,484	.	0,927

Anexo Nº 06: Prueba de Normalidad

Prueba de Normalidad

Según Carrasco Díaz (2017) Método General: Método científico

Resultados de Normalidad del instrumento - SPSS

	Shapiro-Wilk		
	Estadístico	gl	Sig.
Instru1	0,887	13	0,089

Con un valor de significancia de 0.089 es mayor que 0.05, se considera como una distribución normal.

Anexo Nº 07: Validación de Hipótesis

H1: La propuesta de un Sistema de Gestión de Seguridad de la Información basado en ISO 27001, bajo el enfoque de mejora continua PHVA, mejora la seguridad de la información en la Municipalidad Provincial.

H0: La propuesta de un Sistema de Gestión de Seguridad de la Información basado en ISO 27001, bajo el enfoque de mejora continua PHVA, no mejora la seguridad de la información en la Municipalidad Provincial.

Validación

Dado que la distribución de los datos, muestran normalidad, por lo tanto, se procede a realizar la prueba de muestras paramétricas, T de Student, lo que muestra como resultado

Resultados de Validación de Hipótesis General - SPSS

Prueba de muestras emparejadas

		Diferencias emparejadas					t	gl	Sig. (bilateral)
		Media	Desv. Desviación	Desv. Error promedio	95% de intervalo de confianza de la diferencia Inferior	Superior			
Par 1	PRE_T - POST_T	-19,385	3,754	1,041	-21,653	-17,116	-18,620	12	0,000

En relación a los resultados obtenidos del análisis estadístico, la diferencia entre los resultados de los datos de la pre y post pruebas obtenidas ($p < 0.05$), la significancia es menor de 0.001, en consecuencia, se acepta la hipótesis alternativa y se rechaza la hipótesis nula.

Validación de Hipótesis Específicas

Hipótesis Específica 1- Mejora del nivel de identificación de Riesgos Dimensión 1

Resultados de Validación de Hipótesis Específica 1 - SPSS

Prueba de muestras emparejadas

		Diferencias emparejadas					t	gl	Sig. (bilateral)
					95% de intervalo de confianza de la diferencia				
		Media	Desv. Desviación	Desv. Error promedio	Inferior	Superior			
Par 1	D1_pre - D1_post	-1,385	0,506	,140	-1,691	-1,079	-9,859	12	0,000

En relación a los resultados obtenidos del análisis estadístico de la tabla anterior, la diferencia entre los resultados de los datos de la pre y post pruebas obtenidas ($p < 0.05$), la significancia menor de 0.001, en consecuencia, se acepta la hipótesis especifica 1 y se rechaza la hipótesis nula

Hipótesis Específica 2- Aumento de Tratamiento de los Riesgos institucional sobre la seguridad de la información

Resultados de Validación de Hipótesis Específica 2 - SPSS

Prueba de muestras emparejadas

		Diferencias emparejadas					t	gl	Sig. (bilateral)
					95% de intervalo de confianza de la diferencia				
		Media	Desv. Desviación	Desv. Error promedio	Inferior	Superior			
Par 1	D2_pre - D2_post	-1,077	0,641	,178	-1,464	-,690	-6,062	12	0,000

En relación a los resultados obtenidos del análisis estadístico de la tabla anterior, la diferencia entre los resultados de los datos de la pre y post pruebas obtenidas ($p < 0.05$), la significancia menor de 0.001, en consecuencia, se acepta la hipótesis especifica 2 y se rechaza la hipótesis nula

Hipótesis Específica 3 - Cumplimiento normativo institucional sobre la seguridad de la información

Resultados de Validación de Hipótesis Específica 3 - SPSS

Prueba de muestras emparejadas

		Diferencias emparejadas					t	gl	Sig. (bilateral)
					95% de intervalo de confianza de la diferencia				
		Media	Desv. Desviación	Desv. Error promedio	Inferior	Superior			
Par 1	D3_pre - D3_post	-1,462	0,519	,144	-1,775	-1,148	-10,156	12	0,000

En relación a los resultados obtenidos del análisis estadístico de la tabla anterior, la diferencia entre los resultados de los datos de la pre y post pruebas obtenidas ($p < 0.05$), la significancia menor de 0.001, en consecuencia, se acepta la hipótesis especifica 3 y se rechaza la hipótesis nul