UNIVERSIDAD NACIONAL

SANTIAGO ANTÚNEZ DE MAYOLO

FACULTAD DE CIENCIAS

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

"MODELO DE SEGURIDAD DE LA INFORMACIÓN PARA MEJORAR LA GESTIÓN INFORMÁTICA EN LA MUNICIPALIDAD PROVINCIAL DE YUNGAY, 2022"

TESIS

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO DE SISTEMAS E INFORMÁTICA

PRESENTADO POR:

Bachiller: MENDEZ PASION, Michael Wilfredo

ASESOR:

Ing. MEDINA RAFAILE, ESTEBAN JULIO

HUARAZ - PERU

2022

Nº Registro: T178

DEDICATORIA

A Dios, por darme la oportunidad de llegar hasta este punto y por haberme dado salud para poder lograr mis objetivos, por la fuerza y la fe para culminar este proyecto importante en mi vida, además de su infinita bondad y amor.

A mis padres, por ser el pilar fundamental en todo, por la paciencia, confianza, apoyo incondicional y por demostrarme cada día que la vida está llena de retos y que no hay mejor satisfacción en el mundo que poder cumplirlos con el apoyo de la familia. A mis hermanos, por su amor y por impulsarme cada día las ganas de ser mejor como persona y como profesional.

Al asesor de Tesis porque hasta el final de este proyecto nos ayudaron a ser minucioso en cada detalle, así como también en la vida profesional.

Finalmente, a los docentes, que son la fuente de conocimientos, los cuales marcaron cada etapa en mi vida universitaria, quienes me ayudaron en asesorías y dudas presentadas en la elaboración de este proyecto.

Michael Wilfredo MÉNDEZ PASIÓN

AGRADECIMIENTO

En primer lugar, a Dios, por ofréceme día a día el privilegio de vivir, disfrutar de las cosas sencillas de ella y aprovechar nuevas oportunidades que se me presente a lo largo del camino.

A mis padres, que siempre me han dado su apoyo incondicional y su amor, a quien le debo la vida, por todo su trabajo, empeño y dedicación para brindarme una formación académica, humanista y sobre todo espiritual y a mis hermanos por demostrarme que siempre hay tiempo para cumplir las tareas y metas de la vida. A ellos les debo todo mi agradecimiento.

A mi alma mater, UNIVERSIDAD NACIONAL SANTIAGO ANTÚNEZ DE MAYOLO, por ser quien me acogió y me dio la oportunidad de seguir la formación académica y profesional.

Al asesor de tesis, Ing. MEDINA RAFAILE ESTEBAN JULIO, por su esfuerzo, empeño, dedicación e impulso brindado, pues hasta el final confió en que esta tesis sería un proyecto por el que valdría la pena esperar y apostar, así como también el tiempo y paciencia dedicados para elaborar un excelente trabajo.

PRESENTACIÓN

Señores miembros del Jurado:

Cumpliendo con las disposiciones del Reglamento de Grados y Títulos de la Escuela Profesional de Ingeniería de Sistemas e Informática, de la Facultad de Ciencias de la Universidad Nacional Santiago Antúnez de Mayolo, presentamos ante su ilustrado criterio la tesis, que lleva por título "MODELO DE SEGURIDAD DE LA INFORMACIÓN PARA MEJORAR LA GESTIÓN INFORMÁTICA EN LA MUNICIPALIDAD PROVINCIAL DE YUNGAY, 2022 ".

La Unidad de Estadística y Sistemas es uno de los órganos de apoyo que cumple un papel importante en la Municipalidad Provincial de Yungay, ya que esta área tiene bajo su control el archivo, mantenimiento y almacenamiento de equipos e información en general, luego de realizar la investigación se pudo apreciar que la información que se maneja está expuesta a riesgos y amenazas. Es aquí donde empezamos a hablar de seguridad de la información, ya que ésta nos ayuda a resguardar y proteger la información manteniendo su confidencialidad, disponibilidad e integridad de la misma, todos estos criterios son importantes porque nos ayudaran a identificar los controles que se deben aplicar. Por otro lado, esta área tiene implicancia en algunos procesos de las demás gerencias de la Municipalidad Provincial de Yungay.

Además, siendo este requisito obligatorio para obtener el Título Profesional de Ingeniero de Sistemas e Informática.

El autor

HOJA DE VISTO BUENO

Ing. **Arias Lazarte Elizabeth Gladys**

Presidente

CIP N° 43138

Ing. **Miguel Ángel Silva Zapata**

Secretario

CIP N° 96195

Ing. **Medina Rafaile Esteban Julio**

Vocal

CIP N° 88145

RESUMEN

El presente trabajo de investigación titulado "Modelo de seguridad de la información para mejorar la gestión informática en la Municipalidad Provincial de Yungay" se ha realizado con la finalidad de mejorar la gestión tecnológica en los aspectos de seguridad informática (hardware, software, operaciones y servicios), que forma parte a su vez de la seguridad de la información.

Entre los objetivos específicos planteados para esta tesis se tuvo: gestionar de manera segura todos los activos de la Municipalidad, controlar los accesos a los recursos informáticos de la Municipalidad, definir políticas de cifrado, establecer la seguridad física y ambiental en toda la Municipalidad, establecer la seguridad en las operaciones del negocio, establecer la seguridad en las telecomunicaciones y definir medidas adecuadas para la adquisición, desarrollo y mantenimiento de los sistemas de información.

El diseño de la investigación ha sido Experimental, aplicativo debido que la recolección de datos se realizó en su momento. El esquema del diseño de investigación fue descriptivo simple.

La metodología utilizada para el desarrollo de la presente tesis se basa en el uso de los controles de seguridad a nivel operativo de la norma internacional ISO 27002:2013, los cuales corresponden a un modelo de seguridad de la información propiamente dicho.

Los controles de seguridad seleccionados fueron: gestión de activos, control de accesos, cifrado, seguridad física y ambiental, seguridad en las operaciones, seguridad en las telecomunicaciones y adquisición, desarrollo y mantenimiento de los sistemas de información.

En cuanto a los logros obtenidos, éstos se encuentran plasmados en las conclusiones de la presente tesis, donde cada uno de ellos permite observar, medir y cuantificar el cumplimiento de los objetivos planteados al inicio de la presente investigación.

Palabras Clave: Seguridad de la Información, Seguridad Informática, Controles de Seguridad, Gestión Informática.

ABSTRACT

This research work entitled "Information security model to improve computer management in the Provincial Municipality of Yungay" has been carried out with the purpose of improving technological management in aspects of computer security (hardware, software, operations and services), which in turn forms part of information security.

Among the specific objectives set for this thesis were: to securely manage all the Municipality's assets, control access to the Municipality's computer resources, define encryption policies, establish physical and environmental security throughout the Municipality, establish security in business operations, establish security in telecommunications and define adequate measures for the acquisition, development and maintenance of information systems.

The design of the research has been Non-Experimental, Transversal because the data collection will be carried out in a single moment. The research design scheme was simple descriptive.

The methodology used for the development of this thesis is based on the use of security controls at the operational level of the international standard ISO 27002:2013, which correspond to an information security model itself.

The security controls selected were: asset management, access control, encryption, physical and environmental security, security in operations, security in telecommunications, and acquisition, development, and maintenance of information systems.

Regarding the achievements, these are reflected in the conclusions of this thesis, where each of them allows to observe, measure and quantify the fulfillment of the objectives set at the beginning of this investigation.

Keywords: Information Security, Computer Security, Security Controls, Computer Management.

INDICE

INDICE DE LAS TABLAS

I. INTRODUCCIÓN

1.1. Formulación del problema

1.1.1. Problema general

¿DE QUÉ MANERA EL MODELO DE SEGURIDAD DE LA INFORMACIÓN MEJORARA LA GESTIÓN INFORMÁTICA EN LA MUNICIPALIDAD PROVINCIAL DE YUNGAY, 2022?

1.1.2. Problemas específicos

a) ¿De qué manera se puede determinar el Modelo actual de la seguridad de la información de la Municipalidad Provincial de Yungay?

b) ¿De qué manera se evaluarán los Modelos de Seguridad de la Información existentes en el mercado informático orientado a la gestión segura y efectiva de los procesos ediles de un municipio?

c) ¿Cómo se diseñará el nuevo Modelo de Seguridad de la Información en la Gestión informática de la Municipalidad provincial de Yungay?

1.2. Objetivos de la investigación:

1.2.1. Objetivo general

Mejorar la gestión informática de la Municipalidad Provincial de Yungay a través de la aplicación de un modelo de seguridad de la información.

1.2.2. Objetivos específicos

- Determinar el modelo de seguridad de la información actual en la municipalidad Provincial de Yungay en todos sus dominios y controles de seguridad.
- Evaluar los modelos de seguridad de la información existentes en el mercado informático orientado a la gestión segura y efectiva de los procesos ediles de un municipio.
- Diseñar el modelo de gestión de seguridad de la información que permita reducir el nivel de incidencias en los recursos informáticos en la Municipalidad Provincial de Yungay.
- Medir los niveles de seguridad que proporciona el modelo en la Municipalidad Provincial De Yungay.

1.3. Justificación de la investigación

1.3.1. Justificación Social

Se justifica socialmente ya que dentro del desarrollo de un Modelo de Seguridad de la Información; la identificación, el análisis y tratamiento de riesgos es uno de los temas centrales y críticos, por lo tanto, buscamos concientizar a la población profesional que laborar en la Municipalidad Provincial de Yungay acerca de tecnologías de la información de la importancia de tener un MSI para poder Identificar, analizar y evaluar los riesgos a los cuales están expuestos los activos identificados, por lo tanto puedan brindar un servicio eficiente a la población, y que la población se sienta segura y satisfecha al momento de realizar cualquier tipo de trámite.

1.3.2. Justificación Tecnológica

Tecnológicamente el presente proyecto es factible puesto que con el pasar de los años han ido mejorando los equipos necesarios para el proyecto y además se cuenta con dichos recursos, ya que además contamos con el conocimiento de la protección de la información ya sea en formato digital o físico. El correcto uso de la TI nos permite brindar una mejor seguridad a los usuarios, permitiendo que la información llegue de manera oportuna y segura.

Pero aun así hay deficiencias pendientes a corregir y mejorar, lo cual a futuro traerá beneficios para dicha institución.

1.3.3. Justificación Legal

Decreto Supremo Nº029-2021-PCM, que aprueba el Reglamento del Decreto Legislativo N°1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, y establece disposiciones sobre las condiciones, requisitos y uso de las tecnologías y medios electrónicos en el procedimiento administrativo.

Además, que el Artículo 96. Modelo de Seguridad Digital, componente y que en enmarca y hace énfasis al Sistemas de Gestión de Seguridad de la Información.

En consecuencia, al realizar el modelo de la seguridad de información, estaríamos contribuyendo al cumplimiento de los objetivos de esta ley y el decreto.

II. MARCO TEÓRICO

2.1. Antecedentes de la investigación

2.1.1. Antecedentes Internacionales

a) Estrada-Esponda, R. D., Unás-Gómez, J. L., & Flórez-Rincón, O. E. (2021). Prácticas de seguridad de la información en tiempos de pandemia. Caso Universidad del Valle, sede Tuluá. Revista Logos Ciencia & Tecnología, 13(3), 98-110.Resumen:

La pandemia generada por el COVID-19 implicó estrategias de confinamiento masivo como respuesta pública de emergencia en el marco de derecho de policía para combatir el nivel de contagios. Adicionalmente, dicha situación coyuntural implicó cambiar las distintas formas de interacción social (virtual) en torno a temas como la educación, la atención en salud y el empleo. De manera directamente proporcional, la delincuencia aprovechó la situación virtual para intensificar delitos electrónicos como el phishing, las fake news y en general actividades como inyección de malware. El propósito de la investigación fue identificar las prácticas de seguridad de la información en una comunidad universitaria por medio de una encuesta, bajo un enfoque de investigación mixto que consideró entre otras variables la pandemia como precursora de nuevos hábitos de higiene digital. Entre los resultados más representativos se destaca que tanto los profesores como estudiantes tienen un aceptable conocimiento sobre seguridad de la información, pese a no recibir capacitación significativa por entidades gubernamentales. Finalmente, se concluye que los esfuerzos institucionales para combatir ese tipo de delitos no han sido suficientes y por tanto se está en mora de generar estrategias de sensibilización para promover una mejor higiene digital.

b) Guerra, Neira, Diaz, & Patiño(2021), Desarrollo de un sistema de gestión para la seguridad de la información basado en metodología de identificación y análisis de riesgo en bibliotecas universitarias, Universidad de la costa, Barranquilla - Colombia,2021.Resumen

La presente investigación tiene como objeto de estudio aplicar un sistema de gestión de la información basado en la metodología de identificación y análisis de riesgos para los procesos de bibliotecas universitarias. Se adapta la norma ISO/IEC 27001:2013 aplicando la metodología MARGERIT en una biblioteca universitaria. Los resultados obtenidos de los cálculos de riesgos intrínseco y efectivo demuestran la presencia de salvaguardas y la evaluación de los impactos. Se establece el porcentaje de afectación en cada riesgo por proceso de calidad, se identifica la medida correctiva, y se incorporan formatos de registros. Se concluye que la incorporación de los formatos propuestos para desarrollar el control y auditorías a los indicadores de calidad permite la optimización del sistema de gestión de la seguridad de la información (SGSI) para los procesos de la biblioteca universitaria.

c) D. L. Carvajal, A. Cardona2, F. J. Valencia (2019), Una propuesta de gestión de la seguridad de la información aplicado a una entidad pública colombiana, Universidad Autónoma de Manizales, Manizales, Colombia,2019. Resumen

La información es considerada actualmente uno de los recursos más importantes en las organizaciones, no solo como insumo fundamental de los procesos, sino como recurso que adecuadamente gestionado permite delimitar estrategias organizacionales, lo que no ha sido ajeno en el sector público, en especial en lo que tiene que ver con su protección. El presente artículo tiene como objetivo presentar un caso de aplicación de la gestión de seguridad de la información en una entidad pública, utilizando para ello, previa revisión de la literatura, cuatro de los estándares internacionales de seguridad de la información (ISO/IEC 27001:2013, ISO/IEC 27002:2013, ISO/IEC

27003:2010 e ISO/IEC 27005:2008) y su contextualización en Colombia, a partir de las directrices establecidas por el Ministerio de Tecnologías de Información. Se obtuvo como resultado el desarrollo de una metodología ajustada a las necesidades de la entidad pública con parámetros e indicadores de gestión del riesgo y controles pertinentes para disminuir la incertidumbre en la gestión de la información. El aporte realizado por el presente trabajo está relacionado con la integración de estándares internacionales de seguridad de la información y su contextualización en un ámbito gubernamental, dando respuesta a requerimientos regulatorios y permitiendo una vez finalizada la implementación, contar con un desarrollo metodológico pertinente que le permite a la organización pública desarrollar de forma continuada los procesos de gestión de seguridad de la información.

2.1.2. Antecedentes Nacionales

a) Bustamante S., Coral Miguel, Rodríguez Immer, Rodríguez Lévano, Políticas basadas en la ISO 27001:2013 y su influencia en la gestión de seguridad de la información en municipalidades de Perú, Universidad Peruana Unión, Tarapoto, Perú, 2021.Resumen

La gestión de seguridad de la información dentro de una organización debe ser un proceso bien definido, ya que implica un enorme esfuerzo tanto de usuarios, jefes de área y demás servidores para conocer cómo responder ante eventos sospechosos y cómo gestionar vulnerabilidades identificadas. El objetivo de esta investigación fue mejorar la gestión de seguridad de la información en una municipalidad distrital peruana, mediante la implantación de un modelo de políticas basado en la ISO 27001:2013. Para ello, se hizo una investigación preexperimental con una muestra de 30 trabajadores a quienes se les aplicó un cuestionario para medir el grado de satisfacción con el modelo implantado. En promedio, más del 90 % de los encuestados reconoció mejoras en la municipalidad, lo que marca una gran diferencia entre el pre y postest, de 49 % a 96 %. Se

concluye que el modelo de políticas de seguridad basado en tres pilares fundamentales: confidencialidad, integridad y disponibilidad mejoró la gestión de seguridad de la información, garantizando un adecuado resguardo de los datos.

b) Rodriguez Baca, Cruzado Puente de la Vega, Mejía Corredor, & Alarcón Diaz(2020), Aplicación de ISO 27001 y su influencia en la seguridad de la información de una empresa privada peruana, Universidad César Vallejo, Lima, Perú,2020.Resumen

El avance de la tecnología en el mundo provoca, entre otros aspectos, el manejo de importante información la misma que puede considerarse como fundamental para los intereses estratégicos de las empresas. La investigación tuvo como objetivo el analizar la influencia de la aplicación del ISO 27001 en la seguridad de la información de una empresa privada de Lima (Perú). A partir de la aplicación de una metodología cuantitativa, se empleó un estudio pre experimental en el que se determinó la influencia de la aplicación del ISO 27001.Para ello se consideró a una muestra de 30 colaboradores de la empresa. La conclusión cuantitativa muestra que si existe una influencia de la aplicación del ISO en la seguridad de la información y en las dimensiones confidencialidad, integridad y disponibilidad.

c. Rojas & Clemente, Seguridad en los datos e implantación de la NTP-ISO/IEC 27001:2014 en la Sub Gerencia de Gestión de Base de Datos del RENIEC,Universidad Cesar Vallejo, Lima, Peru,2019.Resumen

El presente proyecto de investigación lleva por título "Seguridad en los Datos e Implantación de la NTP-ISO/IEC 27001:2014 en la Sub Gerencia de Gestión de Base de Datos del RENIEC", que tiene como objetivo implantar la Norma Técnica Peruana ISO/IEC 27001:2014 para mejorar la seguridad de los datos en la Base de Datos de la Sub Gerencia de Gestión de Base de Datos del RENIEC. Los sistemas tecnológicos que dan soporte a los procesos claves del RENIEC, generan grandes volúmenes de información, los que crecen

constantemente a consecuencia de las operaciones diarias. Asumir, tratar y procesar la información creciente supone un gran reto, en la gestión de los datos, demarcando mucho más en la seguridad, puesto que siendo un activo clave que respalda la información de más de 38 millones de personas (mayores y menores), debe ser protegida, es por eso que la implantación de controles alineados a la NTP ISO/IEC 27001:2014 en la Sub Gerencia de Gestión de Base de datos, permite gestionar la Confidencialidad, Integridad y Disponibilidad implementando mejores políticas en base a la Misión, Visión y Objetivos de la Organización. Este proyecto de investigación tiene un enfoque Cuantitativo, tipo Aplicada Experimental, diseño Pre-experimental, y un análisis de Pre-test y Post-test. Lo que intenta demostrar este proyecto de investigación, es cuanto contribuye la implantación de la NTP ISO/IEC 27001:2014 en la gestión de la Confidencialidad, de la Integridad y de la Disponibilidad de la base de datos del RENIEC. Las reuniones con las unidades orgánicas y con los especialistas de la Sub Gerencia de Gestión de Base de Datos, dieron como resultado la selección de los controles de la norma técnica necesarios para garantizar la seguridad de los datos, generar los indicadores y los documentos normativos, con la proyección de una posterior certificación en la ISO/IEC 27001:2013.

2.2. Bases teóricas

2.2.1. Sistema de gestión de seguridad de la información.

Este concepto, también nombrado SGSI, o ISMS ("*Information Security Management System*") nace como respuesta a la necesidad de las empresas de proteger la información, que es crítica para sus operaciones, tanto del acceso por personas no autorizadas como de daños producidos por las consecuencias de la materialización de los riesgos a los cuales esta se encuentra expuesta. Se encuentra muy relacionado con el plan de continuidad de negocios que se encarga de definir las acciones a seguir en caso un evento produzca una interrupción en las operaciones normales de la compañía.

A grandes rasgos el SGSI contiene la identificación de los activos de información que deban ser protegidos, el motivo por el que se deban proteger – es decir, la criticidad que éstos representan para la organización – los riesgos y amenazas ante los que se encuentran expuestos y los controles que se apliquen para asegurar la preservación de dichos activos. Al ser de vital importancia para las operaciones de la organización, se define también como "la parte del sistema de gestión global, basada en una orientación a riesgo de negocio, para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información" (ALEXANDER, 2007).

Al requerir una identificación de los objetivos que se deban proteger, así como de todas las amenazas a las cuales se encuentran expuestos y los controles que deban implementarse, la implementación de un SGSI se realiza utilizando los resultados que se obtengan del Análisis de Riesgos. (ALEXANDER, 2007)

i. **SEGURIDAD INFORMÁTICA:**

La seguridad informática es una disciplina que se encarga de proteger la integridad y la privacidad de la información almacenada en un sistema informático. De todas formas, no existe ninguna técnica que permita asegurar la inviolabilidad de un sistema. Un sistema informático puede ser protegido desde un punto de vista lógico (con el desarrollo de software) o físico (vinculado al mantenimiento eléctrico, por ejemplo). Por otra parte, las amenazas pueden proceder desde programas dañinos que se instalan en la computadora del usuario (como un virus) o llegar por vía remota (los delincuentes que se conectan a Internet e ingresan a distintos sistemas). (Pérez Porto y Merino, 2008)

ii. **SEGURIDAD DE LA INFORMACIÓN**

Se denomina así al conjunto de políticas, estándares y controles que se implementan en la organización con la

finalidad de asegurar la preservación de las siguientes propiedades de la información:

- **Confidencialidad:** Protección de la información confidencial del acceso o divulgación por parte de entidades – personas jurídicas o naturales – no autorizadas al mismo, tanto por parte del originario de la información como por parte de la entidad que maneja la misma.
- **Integridad:** Protección de la información frente a la modificación o eliminación sin la autorización o accesos necesarios. De esta forma se garantiza que la información sea la correcta en todo momento.
- **Disponibilidad:** La información se encuentra accesible en todo momento, bajo demanda de todo usuario que se encuentre autorizado a poder acceder a la misma.
- **Autenticación:** Mediante esta propiedad, se permite identificar a la persona o personas que han generado la información que se está verificando, permite una validación en la autoría de la información por parte de un usuario específico.
- **No repudio:** Permite que la información sea validada a través de algún mecanismo que compruebe su integridad y contenido, declarándola como genuina.

La Seguridad de la Información es la disciplina que se encarga de garantizar la confidencialidad, integridad y disponibilidad de la información. Para alcanzar el objetivo se apoya en la Seguridad Informática (que estaría gobernada por las directrices de la Seguridad de la Información), es decir, a pesar de ser disciplinas diferentes, la una no puede "ir" sin la otra. De modo que la Seguridad de la Información será la encargada de "regular" y establecer las pautas a seguir para la protección de la información.

Pues bien, ahora que sabemos la diferencia entre seguridad informática y seguridad de la información podemos saber lo

que es un Sistema de Gestión de la Seguridad de la Información. Conocemos por Sistema de Gestión de Seguridad de la Información o SGSI, a las directrices, procedimientos y controles de seguridad que se utilizan para gestionar la información.

De una manera más estricta, un Sistema de Gestión de Seguridad de la Información es aquella parte del sistema general de gestión de una organización que comprende de lo siguiente para implantar la gestión de la seguridad de la información.

- La política.
- La estructura organizativa.
- Los procedimientos.
- Los procesos
- Los recursos necesarios.

Con un sistema de gestión de seguridad de la información nos aseguraremos de cubrir todos los aspectos de seguridad tomando medidas encaminadas a reducir paulatinamente los riesgos a los que la organización se enfrente.

Como cualquier sistema de gestión, el SGSI debe ayudar a conseguir los objetivos de la organización, no convertirse en un impedimento para ello. Por tanto, definiremos un Sistema de Gestión de Seguridad de la información (SGSI) como la manera en la que una organización conoce los riesgos a los que está sometida su información y los gestiona mediante una sistemática definida, documentada y conocida por todos, que se revisa y mejora constantemente.

Estas propiedades son las mínimas que un SGSI debe proteger para asegurar la información de la organización. (CNB - INDECOPI, 2008) (ISACA, 2012).

iii. ACTIVO DE INFORMACIÓN

Se denomina activo a aquello que tiene algún valor para la organización y por tanto debe protegerse. De manera que un activo de información es aquel elemento que contiene o manipula información.

Activos de información son ficheros y bases de datos, contratos y acuerdos, documentación del sistema, manuales de los usuarios, material de formación, aplicaciones, software del sistema, equipos informáticos, equipo de comunicaciones, servicios informáticos y de comunicaciones, utilidades generales como por ejemplo calefacción, iluminación, energía y aire acondicionado y las personas, que son al fin y al cabo las que en última instancia generan, transmiten y destruyen información, es decir dentro de un organización se han de considerar todos los tipos de activos de información.

"El activo es algo a lo que una organización directamente le asigna un Valor y, por lo tanto, la organización debe proteger." El ISO 17799:2005 clasifica los activos de información en las categorías siguientes:

- Activos de información (datos, manuales de usuario, etc.).

- Activos de software (aplicación, software de sistemas, etc.).

- Activos físicos (computadoras, medios magnéticos, etc.).

- Personal (clientes, personal).

- Imagen de la compañía y reputación.

- Servicios (comunicaciones, etc.).

2.2.2. Metodología Del Desarrollo Del Proyecto Normatividad Y Modelos

i. FAMILIA DE NORMAS ISO/IEC 27000

La Organización Internacional para la Estandarización ISO por sus siglas en inglés se encarga de publicar estándares sobre diferentes temas que tienen una gran importancia en diferentes aspectos relacionados con el comercio, fabricación, etc. Siguiendo el constante crecimiento que ha tenido el desarrollo del campo de las Tecnologías de Información, dicho ente ha emitido varios estándares que regulan el ciclo de DEMING del software, estándares de calidad, sistemas de información y seguridad de la información.

Correspondiente a este último grupo, se realizó la publicación de la familia de normas de la serie 27000, enfocadas directamente a la estandarización de los aspectos relacionados con la gestión de la seguridad de la información en las empresas y organizaciones que requieran contar con sistemas de gestión para este fin. A continuación, se detallan las principales normas pertenecientes a esta serie, algunas de las cuales servirán de soporte para realizar los procesos requeridos para completar el presente proyecto.

- ISO 27001:2013, *Information security management systems Requirements*

Especifica los requisitos a cumplir para poder establecer el Sistema de Gestión de Seguridad de la Información.

- ISO 27002:2013, *Code of practice for information security controls*

Presenta una guía de recomendaciones y buenas prácticas a seguir en la gestión de seguridad de la información.

- ISO 27003:2010, *Information security management system implementation guidance*, Establece una guía de implementación para las normas de

la serie.

- ISO 27005:2009, *Information security risk management* Centrada en presentar una metodología para el análisis de riesgos.

- ISO 27799:2008, *Health informatics – Information security management in health using* ISO/IEC 27002 s una guía que extiende los conceptos y

aspectos presentados en ISO 27002 aplicándolos al contexto específico de las entidades de salud.

Dado el alcance del presente proyecto, se utilizarán las normas ISO 27001 como soporte de la implementación de lo indicado por la Norma Técnica Peruana 27001, la cual se detalla en la siguiente sección ISO 27005 como herramienta para cubrir el análisis de riesgos necesario para establecer el SGSI e ISO 27799 dada su especificación de conceptos en el contexto sobre el cual se desarrollará el proyecto. (ORMELLA, 2013) (ISO 27001, 2013) (ISO 27002, 2013)

(ISO 27799, 2008).

ii. NORMA TÉCNICA PERUANA NTP ISO/IEC 27001

Es una norma elaborada por el Comité Técnico Permanente de Codificación e Intercambio Electrónico de Datos, publicada en el año 2009 y establecida como de uso obligatorio mediante la Resolución Ministerial N° 129-2012PCM el año 2012, se encuentra alineada al estándar ISO/IEC 27001 - estándar internacional publicado en el año 2005 que provee un modelo a seguir para el establecimiento y mantenimiento de un SGSI. El objetivo principal de esta norma es establecer los requisitos que se deben cumplir para la implementación del SGSI utilizando un enfoque a procesos, lo cual requiere que se tenga disponible la mayor cantidad de documentación respecto a los mismos.

La norma utiliza la metodología Plan-Do-Check-Act, también llamado ciclo de Deming para definir las fases de vida y mejora continua del SGSI a través de un seguimiento de este que asegura el mantenimiento de los controles y los cambios necesarios para poder mitigar los posibles nuevos riesgos que aparezcan luego de la implementación del sistema. A continuación, se presenta un diagrama que detalla las etapas de esta metodología.

El diseño del SGSI siguiendo las fases del ciclo de Deming comprende las siguientes etapas:

- Establecimiento

Se dan las recomendaciones a seguir para establecer el alcance que tendrá el sistema sobre la organización sobre la que se está trabajando. A continuación,

se realiza un análisis de identificación de activos de información en conjunto con los riesgos y amenazas a los que se encuentran expuestos, además de realizar la valoración tanto de los activos como de los riesgos asociados y los posibles controles que podrían implementarse para mitigar los mismos.

- Implementación

En esta fase se implementan las políticas y planes de mitigación que se requieren para poder tratar el riesgo identificado en el alcance del sistema. Como parte de esta etapa se detallan las acciones específicas que se deben realizar como parte del plan de mitigación.

- Monitoreo y revisión

El establecimiento de políticas que rijan los procesos desde el punto de vista de la seguridad de los activos de información que los mismos utilizan, requiere que se establezcan también métricas y procedimientos con los cuales se pueda evaluar su eficiencia y determinar si es necesario realizar algún cambio para mejorar su desempeño, el cual es el objetivo principal de esta etapa.

- Mantenimiento y mejora continua. Luego de realizar las evaluaciones de desempeño del SGSI en la etapa anterior, se puede identificar cambios que son necesarios para reajustar el alcance o mejorar su eficacia en el control de riesgos.

Esto, sumado a que el SGSI es una entidad que continua vigente a lo largo del tiempo de vida de la organización, hace que el mantenimiento de este sea una tarea crítica como parte de su ciclo de DEMING.

Recientemente, mediante la Resolución Ministerial N°129-2012/PCM (PRESIDENCIA DEL CONSEJO DE MINISTROS, 2012), fue aprobado el uso obligatorio de esta norma para todas las entidades que pertenezcan al Sistema Nacional de Informática entre ellas el Ministerio de Salud y todas sus dependencias – siguiendo el cronograma de implementación incremental determinado por la Oficina Nacional de Gobierno Electrónico e Informática, el cual determina las fases y duración del desarrollo de estas.

Para el presente proyecto de fin de carrera, además de seguir los requisitos establecidos por la presente norma. Debido a su carácter de obligatoriedad, está

estrechamente relacionada con la problemática que ataca este proyecto y representa uno de los documentos más importantes a seguir durante el desarrollo del Sistema de Gestión de Seguridad de la Información. 2008 (CNB - INDECOPI, 2008) (ISO27001, 2013) (ALEXANDER, 2007).

27001:2008 (CNB - INDECOPI, 2008)

iii. LA NORMA ISO 27002

La ISO 27002 es una guía de buenas prácticas de seguridad de la información que presenta una extensa serie de controles de seguridad. Es la única norma que no sólo cubre la problemática de la seguridad de las tecnologías de información, sino que hace una aproximación holística a la seguridad de la información corporativa, abarcando todas las funcionalidades de una organización en cuanto a la seguridad de la información que maneja. La norma considera también los riesgos organizacionales, operacionales y físicos de una empresa, con todo lo que esto implica. (AltoSec Blog).

Desde el 1 de julio de 2007, la ISO 27002 es el nuevo nombre de ISO 17799:2005. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable, sólo hace recomendaciones sobre el uso de 133 controles de seguridad diferentes aplicados en 11 áreas de control o dominios.

La ISO 27002, también nos hace mención de ciertas cláusulas entre ellas la Evaluación y Tratamiento del Riesgo, la cual es punto clave para el desarrollo de este proyecto, ya que nos proporciona indicaciones sobre cómo evaluar y tratar los riesgos de seguridad de la información. Este punto se desarrollará teniendo en cuenta la realidad problemática expuesta con anterioridad. Esta cláusula considera dos puntos muy importantes para poder establecer objetivos de control en una organización:

Los objetivos de control contemplados en la Norma son:

- Política de Seguridad: Documento de política de seguridad y su gestión.

- Aspectos Organizativos de la Seguridad de la Información: Organización interna; organización externa.

- Gestión de Activos: Responsabilidad sobre los activos; clasificación de la información.

- Seguridad Ligada a los Recursos Humanos: Anterior al empleo; durante el empleo; finalización o cambio de empleo.

- Seguridad Física del Entorno: Áreas seguras; seguridad de los equipos.

- Gestión de Comunicaciones y Operaciones: procedimientos y responsabilidades de operación; gestión de servicios de terceras partes; planificación y aceptación del sistema; protección contra software malicioso; backup; gestión de seguridad de redes; utilización de soportes de información; intercambio de información y software; servicios de comercio electrónico; monitorización.

- Control Accesos: Requisitos de negocio para el control de accesos; gestión de acceso de usuario; responsabilidades del usuario; control de acceso en red; control de acceso al sistema operativo; control de acceso a las aplicaciones e informaciones; informática y conexión móvil.

- Adquisición, desarrollo y mantenimiento de sistemas de información: Requisitos de seguridad de los sistemas de información; procesamiento correcto en aplicaciones; controles criptográficos; seguridad de los ficheros del sistema; seguridad en los procesos de desarrollo y soporte; gestión de vulnerabilidades técnicas. - Gestión de incidentes en la Seguridad de la Información:

Comunicación de eventos y puntos débiles de seguridad de la información; gestión de incidentes y mejoras de seguridad de la información.

- Gestión Continuidad de negocio: Aspectos de la seguridad de la información en la gestión de continuidad del negocio.

- Cumplimiento legal: Con los requisitos legales; políticas de seguridad y estándares de conformidad y conformidad técnica; consideraciones sobre la auditoría de sistemas de información.

iv. EVALUANDO LOS RIESGOS DE SEGURIDAD:

Las evaluaciones del riesgo debieran identificar, cuantificar y priorizar los riesgos en comparación con el criterio para la aceptación del riesgo y los objetivos relevantes para la organización. Los resultados debieran guiar y determinar la acción de gestión apropiada y las prioridades para manejar los riesgos de la seguridad de la información y para implementar los controles seleccionados para protegerse contra estos riesgos. Es posible que el proceso de evaluación de riesgos y la selección de controles se deba realizar un número de veces para abarcar las diferentes partes de la organización o sistemas de información individuales.

La evaluación del riesgo debiera incluir el enfoque sistemático de calcular la magnitud de los riesgos (análisis del riesgo) y el proceso de comparar los riesgos estimados con un criterio de riesgo para determinar la importancia de los riesgos (evaluación del riesgo).

Las evaluaciones del riesgo también se debieran realizar periódicamente para tratar los cambios en sus requerimientos de seguridad y en la situación del riesgo; por ejemplo, en los activos, amenazas, vulnerabilidades, impactos, evaluación del riesgo, y cuando ocurren cambios significativos. Estas evaluaciones del riesgo se debieran realizar de una manera metódica capaz de producir resultados comparables y reproducibles.

La evaluación del riesgo de seguridad de la información debiera tener un alcance claramente definido para ser efectiva y debiera incluir las relaciones con las evaluaciones del riesgo en otras áreas, si fuese apropiado. El alcance de la evaluación del riesgo puede ser la organización en su conjunto, partes de la organización, un sistema de información individual, componentes específicos del sistema o servicios donde esto es practicable, realista y útil. Los ejemplos de las tecnologías de evaluación del riesgo se discuten en ISO/IEC TR 13335-3 (Lineamientos para la Gestión de la Seguridad TI: Técnicas para la Gestión de la Seguridad de Tecnologías de Información)

v. TRATAMIENTO DE LOS RIESGOS DE SEGURIDAD:

Antes de considerar el tratamiento del riesgo, la organización debiera decidir el criterio para determinar si se pueden aceptar los riesgos, o no. Los riesgos pueden ser aceptados si, por ejemplo, se ha evaluado que el riesgo es bajo o

que el costo del tratamiento no es efectivo en costo para la organización. Estas decisiones debieran ser registradas. Para cada uno de los riesgos definidos después de una evaluación del riesgo se necesita tomar una decisión de tratamiento del riesgo. Las opciones posibles para el tratamiento del riesgo incluyen:

a) Aplicar los controles apropiados para reducir los riesgos;

b) Aceptar los riesgos consciente y objetivamente, siempre que cumplan claramente con la política y el criterio de aceptación de la organización de la organización.

c) Evitar los riesgos no permitiendo acciones que podrían causar que el riesgo ocurra.

d) Transferir los riesgos asociados a otros grupos; por ejemplo, aseguradores o proveedores.

e) Para aquellos riesgos donde la decisión del tratamiento del riesgo ha sido aplicar los controles apropiados, estos controles debieran ser seleccionados e implementados para satisfacer los requerimientos identificados por la evaluación del riesgo. Los controles debieran asegurar que se reduzcan los riesgos a un nivel aceptable tomando en cuenta:

f) Los requerimientos y restricciones de la legislación y las regulaciones nacionales e internacionales.

g) Objetivos organizacionales.

h) Requerimientos y restricciones operacionales.

i) Costo de implementación y operación en relación a los riesgos que se están reduciendo, y manteniéndolo proporcional a los requerimientos y restricciones de la organización;

j) La necesidad de equilibrar la inversión en implementación y operación de los controles con el daño probable resultado de fallas en la seguridad.

Los controles se pueden seleccionar a partir de este estándar o de otros conjuntos de controles, o se pueden diseñar controles nuevos para cumplir con

necesidades específicas de la organización. Es necesario reconocer que algunos controles pueden no ser aplicables a todo sistema de información o medio ambiente, y podría no ser practicable en todas las organizaciones.

Se debieran considerar los controles de seguridad de la información en los sistemas y la especificación de los requerimientos de proyectos, así como la etapa de diseño.

El no hacerlo puede resultar en costos adicionales y soluciones menos efectivas, y tal vez, en el peor de los casos, la incapacidad de lograr la seguridad adecuada.

Se debiera tener en mente que ningún conjunto de controles puede lograr la seguridad completa, y que se debiera implementar una acción de gestión adicional para monitorear, evaluar y mejorar la eficiencia y efectividad de los controles de seguridad para apoyar los objetivos de la organización.

2.3. Definición de términos

- **Activo:** Algo que tenga valor para lo organización. Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos (ISO 27001, 2021).
- **Amenaza:** Causa potencial de un incidente que puede causar daños a un sistema de información o a una organización. Causa potencial de un incidente no deseado que puede resultar en daño al sistema u organización. (ISO 27000, 2005).
- **Confidencialidad:** Propiedad o característica consistente en que la información ni se pone a disposición ni se revela a individuos, entidades o procesos no autorizados. (ISO 27000, 2005)
- **Control:** Herramienta de la gestión del riesgo, incluido: políticas, pautas, estructuras organizacionales, que pueden ser de naturaleza administrativa, técnica, gerencial o legal. (ISO 27002, 2020)

- **Disponibilidad:** Aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados (ISO 27001, 2021)
- **Enunciado de aplicabilidad:** Enunciado documentado que describe los objetivos de control y los controles que son relevantes y aplicables al SGSI de la organización. (ISO 27001, 2021)
- **Integridad:** Propiedad o característica consistente en que el activo no ha sido alterado de manera no autorizada. (ISO 27000, 2005)
- **Impacto**[1]: Consecuencia que sobre un activo tiene la materialización de una amenaza.
- **Incidente de seguridad de información:** Es indicado por una o varias series de eventos inesperados y no deseados que tienen una gran probabilidad de comprometer las operaciones de negocios y de amenazar la seguridad de información. (ISO, 2004).
- **Investigación:** Está determinada por la averiguación de datos o la búsqueda de soluciones para ciertos inconvenientes. (ISO 27000, 2005)
- **ISO**: Organización de Estandarización Internacional. (ISO 27000, 2005)
- **MPY:** Municipalidad Provincial de Yungay.
- **Norma:** Regla o conjunto de reglas que hay que seguir para llevar a cabo una acción, porque está establecido o ha sido ordenado de ese modo. (ISO 27000, 2005)
- **PDCA:** Ciclo de Deming conocido como círculo PDCA que es (planificar-hacer-verificar-actuar) también conocido como espiral de mejora continua.
- **Riesgo:** Es un problema potencial que puede ocurrir dentro de una organización (ISO 27000, 2005).
- **Salvaguarda:** Procedimiento o mecanismo tecnológico que reduce el riesgo (ISO 27000, 2005).
- **Seguridad de la información**: Confianza en que los sistemas de información están libres y exentos de todo peligro o daño inaceptables. Preservación de la confidencialidad, integridad y disponibilidad de la información, así mismo, otras propiedades como la autenticidad, no

[1] 3 ISO 27000, Glosario de Términos, Impacto, http://www.iso27000.es/glosario.html (Consultada el 15 de febrero de 2016).

rechazo, contabilidad y confiabilidad también pueden ser consideradas (ISO 27000, 2005).

- **MSI:** Modelo de Seguridad de la Información. Es una herramienta de gestión.
- **Vulnerabilidad:** Defecto o debilidad en el diseño, implementación u operación de un sistema que habilita o facilita la materialización de una amenaza. Propiedades intrínsecas de que algo se produzca como resultado de una sensibilidad a una fuente de riesgo que puede conducir a un suceso con una consecuencia[2].

2.4. Hipótesis

2.4.1. Hipótesis general

EL MODELO DE SEGURIDAD DE LA INFORMACIÓN MEJORA LA GESTIÓN INFORMÁTICA EN LA MUNICIPALIDAD PROVINCIAL DE YUNGAY, 2022.

2.4.2. Hipótesis especificas

- ✓ Determinar el modelo de seguridad de la información actual en la municipalidad Provincial de Yungay en todos sus dominios y controles de seguridad.
- ✓ Evaluar los modelos de seguridad de la información existentes en el mercado informático orientado a la gestión segura y efectiva de los procesos ediles de un municipio.
- ✓ Se diseño el modelo de seguridad de la información orientándolo a la mejora de la gestión informática para la Provincial de Yungay.

2.5. Variables

2.5.1. Variable Independiente

- SEGURIDAD DE LA INFORMACIÓN

2.5.2. Variable dependiente

- GESTIÓN INFORMÁTICA

[2] 3 ISO 27000, Glosario de Términos, Impacto, http://www.iso27000.es/glosario.html (Consultada el 15 de febrero de 2016).

2.5.3. Operacionalización de variables

Tabla 1

Operacionalización de variables

VARIABLES	TIPO DE VARIABLE	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL	DIMENSIÓN	METODOLOGIA
SEGURIDAD DE LA INFORMACIÓN	INDEPENDIENTE	Conjunto de políticas, estándares y controles que se implementan en la organización con la finalidad de asegurar la preservación de la información.	Gestión en la implementación de controles de seguridad de la información en la entidad.	Gestión de seguridad	Tipo: Aplicada Diseño: Pre Experimental Enfoque de la investigación: contrastación - descriptiva Técnica: Encuesta, entrevista Instrumento: Cuestionario
GESTIÓN INFORMÁTICA	DEPENDIENTE	Es todo aquello que las entidades consideran importante o de alta validez para la misma ya que puede contener importante información.	Gestión de recursos para conservar la confidencialidad, integridad y disponibilidad de la información .	Recursos Tecnológicos	

Fuente: Elaboración propia

III. METODOLOGÍA

3.1. Tipo de estudio

a. De acuerdo a la orientación

La presente investigación es de tipo aplicada, porque se buscó la aplicación o utilización de los conocimientos que hemos adquirido durante el desarrollo y se empleó conocimientos relacionados con este instrumento teórico y metodológico, la cual está basada en el desarrollo de un modelo de seguridad de la información para mejorar la gestión de información de la Municipalidad Provincia de Yungay.

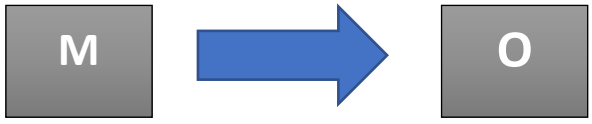
b. De acuerdo a la técnica de contrastación

Es descriptiva ya que, se basó en la observación directa de la situación actual de la Municipalidad Provincial de Yungay y se obtuvo datos en relación a las necesidades, problemas u oportunidades de mejora que constituyen el punto de partida para el presente proyecto de investigación, el investigador se esforzó por especificarlos tal como lo identifica; es decir sin alterarlos o modificarlos.

3.2. El diseño de investigación

Diseño general:

- Descriptivo, considerando el tipo y nivel de la investigación, el diseño de la investigación es descriptivo porque se analizó la realidad problemática y se logró comprender de forma íntegra el presente, de una sola casilla y se grafica de la siguiente manera:



Dónde:

M = Muestra,

O = Observación

- Bibliográfico, se realizó a través de la información documentada, las cuales fueron el punto de partida para el desarrollo del siguiente proyecto de investigación.

Diseño metodológico:

Para el proyecto se usó un diseño metodológico que nos brinda el "Ciclo de Deming" de Edwards Deming, la cual tiene una mejor afinidad con el tema del presente proyecto. De acuerdo a Edwards Deming, es también conocido como círculo PDCA esto es: Planificar, Hacer, Verificar y Actuar, es una estrategia de mejora continua de la calidad en cuatro pasos, basada en un concepto ideado por Walter A. Shewhart. Es muy utilizado por los sistemas de gestión de la calidad (SGC) y los sistemas de seguridad de la información (SSI).

En la siguiente investigación, se han utilizado la metodología de Investigación del autor Roberto Hernández Sampieri, relacionando con el ciclo de Deming, basándonos en la estructura del informe de tesis del reglamento de grados y títulos de la escuela académico profesional de ingeniería de sistemas e informática, y en el reglamento del PGT-ISI 2014.

Esperamos que este documento de aplicabilidad sirva como punto de partida para su futura ampliación e implementación debidamente autorizada por la alta gerencia de la Municipalidad Distrital de Independencia, con la finalidad de proteger los activos de información del Subgerencia de Informática y Telecomunicaciones de la Municipalidad distrital de independencia.

3.3. Descripción de la unidad de análisis, población y muestra (cuantitativo).

a. Población

La población en la cual se aplicó los instrumentos de recolección de datos es el personal que labora en las oficinas de la Municipalidad Provincial de Yungay, para realizar el estudio piloto en los procesos involucrados con el personal administrativo. El cual lo podemos observar en la Tabla N° 2.

Tabla 2

Población Total

Usuarios internos	Cantidad
Gerentes	7
Jefes de área	18
Total	25

Fuente: Elaboración propia

b. Muestra:

Para calcular el tamaño de la muestra utilizamos el muestreo probabilístico, muestreo aleatorio simple cuya fórmula es:

$$n = \frac{NZ^2pq}{Ne^2 + Z^2pq}$$

Donde:

n = El tamaño de la muestra.

N = Tamaño de la población.

p= Población de la población con la característica deseada (éxito).

q=Proporción de la población sin la característica deseada (fracaso).

Z = Valor obtenido mediante niveles de confianza. Es un valor constante que, si no se tiene su valor, se lo toma en relación al 95% de confianza equivale a 1,96 (como en nuestro caso).

e = Límite aceptable de error muestral que, generalmente cuando no se tiene su valor, suele utilizarse un valor que varía entre el 1% (0,01) y 9% (0,09), en este caso usaremos el 5% (0.05). Aplicando la fórmula, se obtuvo que la muestra es de 25 trabajadores administrativos dentro de la municipalidad.

c. Unidad de análisis

Personal administrativo que labora en la Municipalidad Provincial de Yungay, que hacen uso de los servicios e información que se maneja dentro de ellos, El objetivo de contar con la información de este personal es analizar la situación actual de la gestión de información y

presentar la declaración de aplicabilidad del modelo de seguridad de la información en la Municipalidad Provincial de Yungay.

3.4. Técnicas de instrumentos de recolección de datos.

➢ **Instrumentos de recolección de datos**

Tabla 3

Instrumentos de recolección

TÉCNICA	INSTRUMENTOS
Observación	Visión, observación
Entrevista	Preguntas
Encuestas	Cuestionario
documentos	Fuentes de Datos: Libros, Informes, Páginas de Internet, etc.

Fuente: Elaboración propia

➢ **Técnicas de procesamiento de información**

La presente investigación utilizó las siguientes técnicas de recopilación y procesamiento de información:

- Encuestas dirigidas al personal que labora, procesadas en Microsoft Excel 2021, lo cual nos permitirá obtener un consolidado de los resultados, así como gráficos para su interpretación.

- Análisis de las entrevistas realizadas (guía de entrevistas), así como también de los documentos, libros y guías (digital e impreso) que se estén empleando para la realización de este proyecto.

- Análisis de las observaciones realizadas durante la recopilación de información.

En base a estas técnicas de procesamiento de información, se establece la situación actual de la entidad y las necesidades a ser resueltas en base al problema planteado.

3.5. Técnicas de análisis y prueba de hipótesis (estudio cuantitativo).

PROCEDIMIENTO

Para el desarrollo de la tesis se utilizará una propuesta metodológica basada en la aplicación de los controles de seguridad de la norma ISO 27002:2013, que corresponden a un Modelo de Seguridad de la Información para la parte de la gestión informática, la cual consta de siete etapas como sigue:

- Etapa I - Gestión de Activos
- Etapa II - Control de Accesos
- Etapa III - Cifrado
- Etapa IV - Seguridad Física y Ambiental
- Etapa V - Seguridad en las Operaciones
- Etapa VI - Seguridad en las Telecomunicaciones
- Etapa VII - Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información

IV. RESULTADOS DE LA INVESTIGACIÓN

4.1. Descripción del trabajo de campo

4.1.1. Etapa I - Gestión de Activos

4.1.1.1. Responsabilidad sobre los Activos

4.1.1.1.1. Inventario de activos (Visualizar en el Anexo G)

En la Municipalidad se puede identificar los siguientes activos:

- Recursos de software: software de aplicaciones, sistemas operativos, herramientas de desarrollo y publicación de contenidos, utilitarios, etc.

- Activos físicos: equipamiento informático, equipos de comunicaciones, medios magnéticos, mobiliario, lugares de emplazamiento, etc.

- Servicios: servicios informáticos y de comunicaciones, utilitarios generales, soporte.

Se pudo evidenciar que cuenta con una política en la cual se exige inventariar los activos. Los activos se encuentran debidamente documentados, mediante un procedimiento formal. Se identifica, confecciona y mantiene un inventario de activos mostrando los propietarios de los activos y los detalles relevantes como ubicación, Nº de serie, Nº de versión, estado de desarrollo / pruebas / producción, etc.

Recursos de información de bases de datos y archivos, documentación de sistemas, manuales de usuario, material de capacitación, procedimientos operativos o de soporte, etc. Se pudo evidenciar que cuenta con una política en la cual se exige inventariar los activos. Los activos se encuentran debidamente documentados, mediante un procedimiento formal. Se identifica, confecciona y mantiene un inventario de activos mostrando los propietarios de los activos y los detalles relevantes como ubicación, Nº de serie, Nº de versión, estado de desarrollo / pruebas / producción, etc.

4.1.1.1.2. Propiedad de los activos

Se pudo evidenciar controles sobre la propiedad de los activos. Existe la documentación correspondiente respecto a las responsabilidades de los propietarios (control de la producción, desarrollo, mantenimiento, uso y seguridad de los activos) y la identificación de éstos. Así mismo se realiza una actualización periódica de los activos y sus propietarios cada seis meses.

4.1.1.1.3. Uso aceptable de los activos

Se pudo constatar que existen regulaciones para el uso adecuado de la información y los activos asociados a recursos de tratamiento de la información.

Se identifica, documenta e implanta convenios con el personal interno y cláusulas en los contratos con terceros sobre el uso aceptable de los activos.

4.1.1.1.4 Devolución de activos

En la Municipalidad, existe una política formalizada de devolución de activos en la cual todos los empleados y usuarios de terceras partes devuelven los activos que estuvieron en su posesión / responsabilidad una vez finalizada el acuerdo, contrato de prestación de servicios o actividades relacionadas con su contrato de empleo en todas las áreas de la Municipalidad Provincial de Yungay

4.1.1.2 Clasificación de la Información

4.1.1.2.1. Directrices de clasificación

Actualmente la Municipalidad Provincial de Yungay tiene directrices de clasificación de la información, se utiliza un esquema de clasificación de la información en relación a su valor, requisitos legales, sensibilidad y criticidad para la Municipalidad; definiendo el conjunto adecuado de niveles de protección y la necesidad de medidas especiales para su tratamiento.

4.1.1.2.2. Etiquetado y manipulado de la información

Se constató que se realiza el etiquetado y manipulado de la información correctos. Etiquetando la información y los soportes para que el personal sepa cómo manipularlos. Para ello, se establece un conjunto apropiado de procedimientos para el etiquetado y tratamiento de la información, de acuerdo a un esquema de clasificación de los activos de información, definiendo el conjunto adecuado de niveles de protección.

4.1.1.2.3. Manipulación de Activos

Se evidenció que existen procedimientos o manuales en forma de documento impreso, de cómo usar los activos en la UES, más no en las demás áreas de la Municipalidad Provincial de Yungay. Se recomienda establecer y revisar los procedimientos de manipulación de activos, acorde con el esquema de clasificación de activos adoptado por la organización, basado en la norma ISO/IEC 27002.

4.1.1.3. Manejo de los Soportes de Almacenamiento

4.1.1.3.1. Gestión de soportes extraíbles

En la Municipalidad Provincial de Yungay, el personal de la Unidad de Estadística y Sistemas tiene prohibido el uso de soportes extraíbles; el resto de áreas no realiza la gestión de soportes extraíbles. Se recomienda el establecimiento de procedimientos formales para proteger los documentos, medios informáticos, datos de entrada o salida y documentación del sistema contra la divulgación, modificación, retirada o destrucción de activos no autorizadas a nivel de la y acorde con el esquema de clasificación de activos que se adopta en la Municipalidad.

4.1.1.3.2. Eliminación de soportes medios

Se evidenció que en la Municipalidad Provincial de Yungay (fuera de la UES donde no se permite el uso de soportes de medios) no se realiza la eliminación segura de soportes de medios.

Se recomienda llevar a cabo procedimientos formales para la eliminación segura y sin riesgo de los soportes de medios cuando ya no son requerido para así evitar la divulgación, modificación, retirada o destrucción de activos no autorizada.

4.1.1.3.3. Soportes físicos en tránsito

Sin considerar la UES, donde no se permite el uso de soportes de medios, se constató que en las demás áreas Municipalidad Provincial de Yungay no hay procedimientos formales para el transporte de medios que contienen información, contra acceso no autorizado, mal uso o corrupción fuera de los límites físicos de la Municipalidad Provincial.

Se recomienda asegurar los soportes y la información en tránsito no solo físico sino electrónico (a través de las redes) y cifrar todos los datos sensibles o valiosos antes de ser transportados.

4.1.2. Etapa II - Control de Accesos

4.1.2.1. Requisitos de negocio para el Control de Accesos

4.2.1.1.1. Política de control de accesos

- Toda aplicación a utilizar debe contar con un usuario y una clave de acceso asignada al personal que labora en la Municipalidad Provincial de Yungay.
- Cada personal debe tener un determinado perfil para según eso darle acceso a solo funcionalidades que lo competen.
- Está terminantemente prohibido hacer uso de usuarios que no le corresponde bajo la responsabilidad del que lo brinda.
- Cerrar sesión una vez que este deje de trabajar en el los aplicativos de la Municipalidad Provincial de Yungay con la finalidad de que otros usuarios no usen su sesión.

4.1.2.1.2. Control de acceso a las redes y servicios asociados

- El administrador de red es el encargado de brindar los privilegios correspondientes al personal y a los equipos que usaran tales como impresoras fotocopiadoras, etc.
- Estadísticas de cortafuegos, tales como porcentaje de paquetes o sesiones salientes que han sido bloqueadas (por ejemplo: intentos de acceso a páginas web prohibidas; número de ataques potenciales de hacking repelidos, clasificados en insignificantes / preocupantes /críticos).

4.1.2.2 Gestión de Acceso de Usuario

4.1.2.2.1. Gestión de altas/bajas en el registro de usuarios

- El administrador de los aplicativos asigna cada personal un usuario y una contraseña.
- Cada personal una vez que este deja de laborar en la municipalidad se le da de baja su usuario temporalmente por si este en algún momento puede regresar a laborar como también puede servir para una auditoria posterior.
- El usuario se da de baja definitivamente si este fallece o ya no volverá a trabajar definitivamente en la Municipalidad.

4.1.2.2.2. Gestión de los derechos de acceso asignados a usuarios

- El personal tiene que autorizar para que el especialista ingrese a su pc remotamente para darle soporte.
- Todo personal, dependiendo de su perfil profesional, puede ingresar remotamente a una PC para darle soporte esto.
- Queda terminantemente prohibido copiar información o borrar la información de personal que accede a su pc remotamente.

4.1.2.2.3. Gestión de los derechos de acceso con privilegios especiales

- Se revisa los derechos de acceso de los usuarios a intervalos de tiempo regulares (se recomienda cada seis meses) y después de cualquier cambio como promoción, degradación o término del empleo.
- Los derechos de acceso de los usuarios son revisados y reasignados cuando se traslade desde un empleo a otro dentro de la misma organización.
- Se revisa más frecuentemente (se recomienda cada tres meses) las autorizaciones de derechos de acceso con privilegios especiales.
- Se comprueba las asignaciones de privilegios a intervalos de tiempo regulares para asegurar que no se han obtenido privilegios no autorizados.
- Los cambios en las cuentas privilegiadas deben ser registradas para una revisión periódica.

4.1.2.2.4. Gestión de información confidencial de autenticación de usuarios

Mediante la autenticación se verifica si dicha persona es la que está accediendo a los aplicativos o a información que le compete sea la persona asignada.

4.1.2.2.5. Revisión de los derechos de acceso de los usuarios

Cada cierto periodo de tiempo un encargado del área de UES revisa si verdaderamente los usuarios tienen los permisos que se les asignó. Se verifica cuando este es cambiado de cargo, área o cuando este tiene vacaciones o licencia.

4.1.2.2.6. Retirada o adaptación de los derechos de acceso

El administrador es el encargado de retirar los derechos de acceso para todos los empleados, contratistas o usuarios de terceros a la información y a las instalaciones del procesamiento de información a la finalización del empleo, contrato o acuerdo, o ser revisados en caso de cambio.

4.1.2.3. Responsabilidades del Usuario

4.1.2.3.1. Uso de información confidencial para la autenticación

La contraseña es de uso exclusivo del personal de la Municipalidad Provincial de Yungay. Se recomienda establecer una regla en la cual cada cierto tiempo el personal cambie la contraseña y cesar la sesión una vez finalizado su trabajo para que este no sea utilizado por personal que no le pertenece.

4.1.2.4. Control de Acceso a Sistemas y Aplicaciones

4.1.2.4.1. Restricción del acceso a la información

Acceso solo a personal autorizado y, según el cargo que este tenga debe tener un determinado nivel de acceso a las aplicaciones.

4.1.2.4.2. Procedimientos seguros de inicio de sesión

Se controla los inicios de sesión mediante un algoritmo de encriptación de contraseñas, con este mecanismo de autenticación, ni el desarrollador sabe cuál es la contraseña del personal y así se controla el diseño de las pantallas de inicio de sesión.

4.1.2.4.3. Gestión de contraseñas de usuario

- El personal que labora en la municipalidad tiene la facilidad de cambiar su contraseña en el momento que lo desee.
- Si en caso este fuera olvidada el administrador del aplicativo puede resetear y el usuario tendrá que ingresar una contraseña nueva.
- Todo usuario debe tener una contraseña compuesta por letras números y caracteres especiales.

4.1.2.4.4. Uso de herramientas de administración de sistemas

Se usa la herramienta llamada Webmin, el cual ayuda a la configuración de sistemas accesible vía web, con él se pueden configurar aspectos internos de muchos sistemas operativos, como usuarios, cuotas de espacio, servicios, archivos de configuración, apagado del equipo, etc. Gracias a este software es que se puede trabajar remotamente.

4.1.2.4.5. Control de acceso al código fuente de los programas

Cada analista de sistemas, coordinador etc. tiene un usuario y contraseña al servidor de versiones el cual accede y puede guardar las versiones de las fuentes de los aplicativos.

4.1.3. Etapa III - Cifrado

4.1.3.1. Controles Criptográficos

4.1.3.1.1. Política de uso de los controles criptográficos

La Municipalidad Provincial de Yungay debería desarrollar e implementar una política de uso de las medidas criptográficas para proteger para la protección de claves de acceso a sistemas, datos y servicios, para la transmisión de información clasificada y/o para el resguardo de aquella información relevante en atención a los resultados de la evaluación de riesgos realizada por la Municipalidad.

Actualmente no cuenta con dicha política. El desarrollo de una política de controles criptográficos debe considerar lo siguiente:

- Un enfoque de gestión del uso de las medidas criptográficas, incluyendo los principios generales en base a los cuales se debería proteger la información Municipalidad Provincial de Yungay.
- Basados en la evaluación de riesgos, el nivel requerido de protección debe ser identificado tomando en cuenta el tipo, fuerza y calidad del algoritmo cifrado requerido.
- El uso de cifrado para la protección de información sensible transportada en medios o dispositivos móviles o removibles y en las líneas de comunicación.
- Un enfoque de gestión de claves, incluyendo métodos para tratar la recuperación de la información cifrada en caso de pérdida, divulgación o daño de las claves.
- Los roles y responsabilidades de cada cual que es responsable de la implementación de la política y la gestión de claves, incluyendo la generación de claves.
- Los estándares a ser adoptados para una efectiva implementación a través de la Municipalidad (que solución es utilizada para cada proceso del negocio).
- Las normas para utilizar información cifrada en controles que confíen en la inspección de contenido (como la detección de virus).

Los controles criptográficos pueden ser utilizados para alcanzar diferentes objetivos de seguridad, por ejemplo:

- Confidencialidad: utilizando cifrado de información para proteger información sensible o crítica, así sea transmitida o almacenada.

- Integridad/autenticidad: utilizando firmas digitales o códigos de autentificación de mensajes para proteger la autenticidad e integridad de la información crítica o sensible que es almacenada o transmitida.
- No repudio: utilizando técnicas criptográficas para obtener prueba de ocurrencia o no ocurrencia de un evento o acción.

4.1.3.1.2. Gestión de claves

El sistema de gestión de claves se debería basar en un conjunto acordado de normas, procedimientos y métodos seguros para:

- Generar claves para distintos sistemas criptográficos y distintas aplicaciones.
- Distribuir claves a los usuarios previstos, incluyendo la forma de activar y recibir las claves.
- Almacenar claves, incluyendo la forma de obtención de acceso a las claves por los usuarios.
- Cambiar o actualizar claves, incluyendo reglas para saber cuándo y cómo debería hacerse en atención a la seguridad requerida y los avances en técnicas de descifrado.
- Tratar las claves comprometidas (afectadas).
- Revocar claves, incluyendo la forma de desactivarlas o retirarlas, por ejemplo, cuando tienen problemas o el usuario deja la organización (en cuyo caso las claves también se archivan).
- Recuperar claves que se han perdido o corrompido como parte de la gestión de continuidad del negocio, por ejemplo, para recuperar la información cifrada.
- Archivar claves, por ejemplo, para información archivada o de respaldo.
- Destruir claves.

- Hacer seguimiento y auditorias de las actividades relacionadas con la gestión de las claves. Para reducir la probabilidad de comprometer las claves, se deberían definir fechas de activación y desactivación para que sólo puedan utilizarse durante un periodo limitado. Este debería depender de las circunstancias del uso de las medidas de control criptográficas y del riesgo percibido.

4.1.4 Etapa IV - Seguridad Física y Ambiental

4.1.4.1. Áreas Seguras

4.1.4.1.1. Perímetro de seguridad física

Los perímetros de seguridad (como paredes, tarjetas de control de entrada a puertas o un puesto manual de recepción) deberían utilizarse para proteger las áreas que contengan información y recursos para su procesamiento. Lista de chequeo para implementación de políticas.

a) Verifique y documente de que material están constituidas las áreas de trabajo.

Se verificó en la Municipalidad que las paredes son de cemento hasta la oficina de Informática, sin embargo, tiene una puerta de seguridad.

b) Documente si existe algún control de ingreso de personal.

Se pudo verificar que a la Municipalidad Distrital el ingreso al centro de cómputo es restringido, no dispone de una cámara de seguridad para verificar el personal que va a entrar.

c) Documente si existen escaleras de emergencia

Si existe escalera de emergencia para cualquier sismo

d) Documente si existen alarmas de seguridad

Actualmente no se dispone de alarma de seguridad.

4.1.4.1.2. Controles físicos de entrada

Las áreas de seguridad deberían estar protegidas por controles de entrada adecuados que garanticen el acceso únicamente al personal autorizado. Lista de chequeo para implementación de políticas:

a) Verificar si hay restricciones al área de caja

Actualmente para el ingreso al área de caja solo existe la puerta del área que no siempre permanece con seguro.

b) Verificar si hay restricción centro de computo

La puerta del centro de cómputo se encuentra asegurada con su respectiva llave.

c) Cada visitante que se dirija a todas las áreas debe estar identificado.

Referente al área de caja el ingreso está prohibido a personal no autorizado. Para el ingreso al centro de cómputo solo ingresa el encargado de esa área y aparte está aislada del área administrativa.

d) Revisar los movimientos de ingreso y salida

Personal de sistemas se encarga de entregar las tarjetas de ingreso y asignar los permisos.

4.1.4.1.3. Seguridad de oficinas, despachos y recursos

Se debería diseñar y aplicar un sistema de seguridad física a las oficinas, salas e instalaciones de la organización.

Lista de chequeo para implementación de políticas:

a) Existe políticas de seguridad

No se encontró manuales de seguridad física.

b) Detallar claramente todos los lugares que se encuentran con restricciones de acceso

Actualmente, el ingreso del área de dirección únicamente se encuentra un guardia de seguridad.

4.1.4.1.4. Protección contra las amenazas externas y ambientales

Se debería diseñar y aplicar una protección física contra desastres naturales, ataques maliciosos o accidentes.

Lista de chequeo para implementación de políticas:

a) Se cuenta con un sistema central de incendios

Actualmente no se encuentra un sistema central de incendios.

b) Se han desarrollado simulacros de evacuación con el personal

No se realizan simulacros de evacuación, no se cuenta con un área específica que se encargue de realizar esto.

4.1.4.1.5. El trabajo en áreas seguras

Se deberían diseñar y aplicar procedimientos para el desarrollo de trabajos

y actividades en áreas seguras.

Lista de chequeo para implementación de políticas:

a) Verifique si existen directorios públicos que especifican la ubicación de

lugares restringidos.

No existe información publicada que revele lugares restringidos.

b) Documente que existan cámaras y monitores constantes dentro de áreas seguras.

Actualmente no se encuentran instaladas ninguna cámara de seguridad en ninguna área de la Municipalidad Provincial.

c) Verifique si existe política de toma de foto y grabaciones

No existen políticas referentes a toma de fotos o grabaciones en los

manuales internos.

4.1.4.1.6. Áreas de acceso público, carga y descarga

Se deberían controlar puntos de acceso a la organización como las áreas de entrega y carga/descarga (entre otros) para evitar el ingreso de personas no autorizadas a las dependencias aislando estos puntos, en la medida de lo posible, de las instalaciones de procesamiento de información.

Lista de chequeo para implementación de políticas:

a) Hacer un tour cada piso para ver si hay acceso para algo adicional, alguna puerta abierta donde esta alguna computadora apagada.

El acceso al área de depósito o almacén, está habilitado solo para el encargado de dicha área; al momento de descargar suministros estos serán ubicados en la puerta principal, y el encargado de almacén lo llevara hasta al área que corresponde.

4.1.4.2. Seguridad de los Equipos

4.1.4.2.1. Emplazamiento y protección de equipos

Actualmente todos los equipos de la Municipalidad se encuentran protegidos en sus respectivas áreas con una ventilación adecuada para evitar que se sobrecalienten y con seguridad del cableado para evitar que exista alguna ruptura.

4.1.4.2.2. Instalaciones de suministro

La Municipalidad Provincia cuenta con un generador de energía para mantener los servicios en línea el tiempo que dure el corte de fluido eléctrico que se puede originar en forma imprevista.

4.1.4.2.3. Seguridad del cableado

Para la protección del cableado de los equipos se han detectado las siguientes medidas:

a) Utiliza cableado empotrado para evitar daños en su estructura.

b) El cableado pasa por el techo de las instalaciones para las conexiones a computadores.

c) Evita interferencia entre los cables de comunicaciones y energía.

4.1.4.2.4. Mantenimiento de los equipos

Para prevenir errores en los sistemas lógicos como físicos de las instalaciones el encargado de TI realiza un mantenimiento cíclico y preventivo (limpieza, revisión, ajustes) acorde al uso del equipo.

4.1.4.2.5. Salida de activos fuera de las dependencias de la empresa

Al momento de recibir una solicitud de las áreas, para el traslado de un equipo informático fuera de la Municipalidad Provincial, el compromiso de TI,

es el siguiente:

a) Verificará el estado de los equipos tecnológicos a ser entregados a las áreas, a través de un Formulario de Activos (Equipos), aprobado por el Jefe de Informática, para comprobar su salida y recepción en buen estado.

b) Se deberá otorgar a los activos que serán utilizados fuera de la Municipalidad no sea mayor de tres (3) días.

c) El usuario deberá reportar cualquier inconveniente que suceda con los activos que estén fuera de la Municipalidad Provincial.

d) Debe realizar un reporte dentro de las 24 horas que se haya sucedido

algún inconveniente con el activo o reportando el estado del activo.

4.1.4.2.6. Seguridad de los equipos y activos fuera de las instalaciones

Se debería aplicar seguridad a los equipos que se encuentran fuera de los locales de la organización

considerando los diversos riesgos a los que están expuestos.

Lista de chequeo para implementación de políticas

a) Indagar con el jefe de Sistemas de la Municipalidad Provincial, ¿Para que indique si existen seguros de equipos al momento de trasladarlos de un lugar otro?

b) No existen seguros de traslados de equipos. Además, los equipos solo se trasladan cuando se quiere realizar algún servicio técnico.

c) Documentar las políticas y controles físicos para laptops.

d) Actualmente la Municipalidad Provincial solo registra en un libro de Excel los datos de los equipos que existen en la Municipalidad Provincial. Solo realiza ese registro mas no cumple con una política de documentar las laptops.

e) Consultar si se realizan respaldos de la información de los discos de las computadoras portátiles.

f) Actualmente no se realizan respaldos de la información de los discos, se sugiere implantar una política para que el personal que utilice un computador portátil realice respaldos antes de emprender vacaciones.

g) Consultar si se realizan encriptación de los discos de las computadoras portátiles

h) No se realizan encriptación de los discos.

Detalle los códigos de los procedimientos revisados. Reunión con el jefe de Sistemas. Detalle los códigos de los procedimientos revisados. Los discos duros de las computadoras portátiles no son encriptación por cualquier

software de encriptación.

4.1.4.2.7. Reutilización o retirada segura de dispositivos de almacenamiento

Se deberían verificar todos los equipos que contengan medios de almacenamiento para garantizar que cualquier tipo de datos sensibles y software con licencia se hayan extraído o se hayan sobrescrito de manera segura antes de su eliminación o reutilización.

Si este dispositivo lo "extraemos directamente del PC" podríamos dañarlo, perder los datos contenidos en él y en caso extremo, dañar el puerto USB

del equipo, por tanto, siempre antes de retirar una unidad externa conectada por USB a nuestro equipo debemos detenerla, utilizando para ello, por ejemplo, la "extracción segura de dispositivos de almacenamiento masivo USB".

Muchas veces los usuarios de las computadoras de la Municipalidad Provincial no se toman el tiempo para poder realizar una reutilización o retirada segura de dispositivos de almacenamiento simplemente retiran el dispositivo de la computadora, siendo esto una mala práctica.

4.1.4.2.8. Equipo informático de usuario desatendido

Los usuarios deberían asegurar que los equipos informáticos desatendidos estén debidamente protegidos.

Lista de chequeo para implementación de políticas:

a) Verificar si existen políticas o procedimientos que detallan la protección de sus equipos en su ausencia (Protector de pantalla con clave, desconectarse de las aplicaciones, etc.).

   No se cuentan con políticas de dominio de inactivación.

   Se debe incluir una política de que todos los equipos al finalizar el día deben de estar apagados o cuando no sea utilizados.

4.1.4.2.9. Política de puesto de trabajo despejado y bloqueo de pantalla

Se debería adoptar una política de puesto de trabajo despejado para documentación en papel y para medios de almacenamiento extraíbles y una

política de monitores sin información para las instalaciones de procesamiento de información.

4.1.5. Etapa V - Seguridad en las Operaciones

4.1.5.1. Responsabilidades y Procedimientos de Operación

4.1.5.1.1. Documentación de procedimientos de operación

La Municipalidad Provincial de Yungay está en proceso de documentación de los aplicativos con la finalidad de facilitar a los demás trabajadores en cuanto a los procesos propios de los sistemas.

Se recomienda la documentación de los procedimientos operativos y dejar a disposición de todos los usuarios que los necesiten.

4.1.5.1.2. Gestión de cambios

En la Municipalidad Provincial de Yungay no hay un control total de los cambios que afectan a la seguridad de la información en la organización.

4.1.5.1.3. Gestión de capacidades

La Municipalidad Provincial de Yungay realiza un monitoreo y ajuste del uso de los recursos, como los servidores, junto a proyecciones necesarias de requisitos de capacidad en el futuro con el objetivo de garantizar el rendimiento adecuado en los sistemas.

4.1.5.1.4. Separación de entornos de desarrollo, prueba y producción

El área de TI que es la encargada y responsable de los sistemas que se usan en todo el consorcio y tiene bien marcado los sistemas que son de desarrollo, prueba y de producción el cual se tiene acceso según el perfil y módulos encargados.

Además, existe la documentación de los controles que se tiene para pases de producción.

4.1.5.2. Protección contra Código Malicioso

4.1.5.2.1. Controles contra el código malicioso

La Municipalidad Provincial de Yungay cuenta con antivirus originales actualizados en las computadoras, Deep freezer en los laboratorios, VMware Workstation o para evitar la propagación de infección de virus mediante memoria o dispositivos externos.

4.1.5.3. Copias de Seguridad

4.1.5.3.1. Copias de seguridad de la información

Actualmente, la Municipalidad Provincial de Yungay cuenta con un plan de respaldo de copias de seguridad de forma automática y de forma diaria todo esto perfectamente establecido mediante un plan desarrollado.

Dichas copias son almacenadas en un servidor de copias en diferentes puntos por si estos sufran algún accidente operacional o natural. Se aplican técnicas de cifrado a copias de seguridad y archivos.

4.1.5.4. Registro de Actividad y Supervisión

4.1.5.4.1. Registro y gestión de eventos de actividad

La Municipalidad Provincial de Yungay recientemente ha implementado un log de actividades de manera interna con la finalidad de dar seguimiento a los posibles errores del sistema, actividad del usuario, excepciones y eventos de seguridad de la información y poder subsanarlos por TI.

Se realiza periódicamente la producción, mantenimiento y revisión de estos registros de actividad.

4.1.5.4.2. Protección de los registros de información

Se realiza la protección contra posibles alteraciones y accesos no autorizados a través de actividades de

seguimiento de comportamiento irregular y el envío de alertas a los responsables de operación.

4.1.5.4.3. Registros de actividad del administrador y operador del sistema

Se realiza el registro de las actividades del administrador y del operador del sistema, tanto su hora de inicio de sesión como las acciones que realizan.

Además de la protección de estos registros, como se menciona en el apartado anterior, así como la revisión regular de éstos.

4.1.5.4.4. Sincronización de relojes

Actualmente, existe sincronización de los relojes dentro del dominio Municipalidad Provincial de Yungay, de todos los sistemas de procesamiento de información pertinentes en relación a una fuente de sincronización única de referencia.

4.1.5.5. Control del Software en Explotación

4.1.5.5.1. Instalación del software en sistemas en producción

En la Municipalidad Provincial de Yungay, se implementan procedimientos para controlar la instalación de software en sistemas operacionales mediante una herramienta que permite realizar la gestión de inventario, de cambio y distribución de paquetes de software con el fin de garantizar la integridad de los sistemas operacionales.

4.1.5.6. Gestión de la Vulnerabilidad Técnica

4.1.5.6.1. Gestión de las vulnerabilidades técnicas

Se realizan periódicamente pruebas de seguridad para vulnerabilidades técnicas y test de intrusión para detección de intrusos tanto en infraestructura, software y base de datos para evaluar el grado de exposición de la Municipalidad y tomar las medidas necesarias para abordar los riesgos asociados.

Se clasifican los errores por niveles los cuales en un primer nivel es atendido por el personal Help Desk y si estos son más complejos pasan a un nivel 2 que son analizados por un personal de TI según sea el caso reportado.

4.1.5.6.2. Restricciones en la instalación de software

Actualmente, la Municipalidad Provincial de Yungay, sólo utiliza una herramienta Time Freeze como medida de seguridad para evitar cambios no permitidos en sus sistemas; lo que se considera insuficiente.

Con el fin de evitar la explotación de vulnerabilidades técnicas en los sistemas se recomienda lo siguiente:

- Implementar reglas que rijan la instalación de software por parte de personal autorizado y en atención a los términos y condiciones que surjan de la licencia de uso, además de procedimientos formales que garanticen su cumplimiento, y respetando la división de funciones.
- Efectuar un análisis de riesgos previo a los cambios en atención al posible impacto por situaciones adversas.
- Aplicar los cambios de manera escalonada empezando por los sistemas menos críticos y aplicar medidas de copias de seguridad y puntos de restauración
- Actualizar la documentación para cada cambio implementado, tanto de los manuales de usuario como de la documentación operativa.
- Informar a las áreas antes de la implementación de un cambio que pueda afectar sus operaciones y realizar pruebas de aceptación del nuevo estado para los usuarios finales.
- Realizar actualización de versiones oportunamente para evitar quedar fuera de soporte por el fabricante.

4.1.5.7. Consideraciones de las Auditorías de los Sistemas de Información

4.1.5.7.1. Controles de auditoría de los sistemas de información

Con el fin de minimizar el impacto de actividades de auditoría en los sistemas operacionales se hacen las siguientes recomendaciones:

- Acordar los requerimientos de auditoría con las áreas correspondientes.
- Limitar las verificaciones hechas por los auditores, como permisos de "sólo lectura" en software y aislar y contrarrestar los efectos de modificaciones realizadas al finalizar la auditoría como la revocación de los privilegios otorgados.
- Identificar claramente los recursos para llevar a cabo las verificaciones y puestos a disposición de los auditores.
- Documentar todos los procedimientos de auditoría, requerimientos y responsabilidades.

4.1.6. Etapa VI - Seguridad en las Telecomunicaciones

4.1.6.1. Gestión de la Seguridad en las Redes

4.1.6.1.1. Controles de Red

Control:

Se debería mantener y controlar adecuadamente las redes para protegerlas de amenazas y mantener la seguridad en los sistemas y aplicaciones que utilizan las redes, incluyendo la información en tránsito.

Se puede encontrar información adicional sobre seguridad de redes en ISO/IEC 18028, Tecnología de Información. Técnicas de seguridad. Seguridad de la red de tecnología de la información.

a) Existe una segregación de responsabilidad en el departamento de Sistemas

Se verificó el manual de responsabilidades, actividades y servicios y se pudo verificar que existe

segregación de funciones en las responsabilidades del personal.

b) Indagar con el jefe de Sistemas y consultar que controles especiales se tiene para que los datos transmitidos a través de la LAN y WAN, estén protegidos su confidencialidad e integridad, por ejemplo, uso de criptografía.

Para prevenir cualquier situación de riesgo, existen medidas de seguridad dentro de la red de la Municipalidad.

4.1.6.1.2. Mecanismos de seguridad asociados a servicios en red

Control

Las características de seguridad, niveles de servicio y los requisitos de gestión de todos los servicios de red deben ser identificadas e incluidos en cualquier acuerdo de servicios sean provistos dentro o fuera de la organización.

Lista de chequeo para implantación de políticas.

a) Obtenga el contrato de Enlaces y extraiga las cláusulas que indiquen los compromisos acordados para gestionar de forma segura la red (Integridad, disponibilidad y confidencialidad).

No se pudo obtener el contrato debido a que son documentos que no están autorizados a entregar a cualquier persona.

4.1.6.1.3. Segregación de redes

Control:

Se debería segregar los grupos de usuarios, servicios y sistemas de información en las redes

Actualmente la Municipalidad no tiene a todos sus grupos de usuario, servicios y sistema de información en las redes separados o excluidos. Por el mismo hecho de que, son 25 empleados, de los cuales sólo 08 tienen

un rol importante en la Municipalidad; así mismo, intercambian información.

4.1.6.2. Intercambio de Información con Partes Externas

4.1.6.2.1. Políticas y procedimientos de intercambio de información

Deberían existir políticas, procedimientos y controles formales de transferencia para proteger la información que viaja a través del uso de todo
tipo de instalaciones de comunicación.

Lista de chequeo para implantación de políticas:

a) Investigar en los manuales internos que políticas de seguridad especifican intercambio de información.

Actualmente en la Municipalidad Provincial no existen políticas al intercambio de información.

b) Intercambio de información electrónica En la Municipalidad Provincial las transmisiones se hacen acercándose al banco.

c) En caso que se intercambie información sensitiva por correo electrónico, este también debe de estar encriptada.

Actualmente esa información no es encriptada, no se ve la necesidad por el momento de encriptar la información de correo electrónico porque no es enviada información confidencial.

4.1.6.2.2. Acuerdos de intercambio

Los acuerdos deberían abordar la transferencia segura de información comercial entre la organización y las partes externas.

a) Analice si existe una política que especifique que deberá existir un acuerdo de confidencialidad y buen uso de los recursos de procesamiento de la información, antes de otorgar acceso a un externo.

Actualmente la Municipalidad Provincial no cuenta con esta política, no se cuenta con convenios de confidencialidad.

4.1.6.2.3. Mensajería electrónica

Se debería proteger adecuadamente la información referida en la mensajería electrónica implementando alguna de estas herramientas:

- ALBALIA: Herramienta gratuita y genera firmas codificadas según el formato PKCS#7 o CMS (Cryptographic Message Syntax).
- ELEFILE: Sistema de intercambio cifrado de información adjunta a emails de forma gratuita de extremo a extremo y sin instalaciones de software en los extremos. Sólo es necesaria el alta gratuita del emisor del mensaje (no es necesaria la del receptor).
- FOCA: Herramienta para por la extracción de metadatos en documentos públicos antes de proceder a su envío. La herramienta permite adicionalmente la realización de procesos de fingerprinting e information gathering en trabajos de auditoría web. La versión Free realiza búsqueda de servidores, dominios, URLs y documentos publicados, así como el descubrimiento de versiones de software en servidores y clientes.
- KRIPTOPOLIS: Plataforma Wiki de Kriptópolis con una recopilación de herramientas de cifrado para programas de mensajería instantánea.
- Metashield Protector: La fuga de la información por medio de canales ocultos como son los metadatos y la información oculta en los documentos requiere que se comprueben todos los documentos antes de ser entregados a los clientes. Módulo para IIS 7 capaz de eliminar los metadatos

de los documentos ofimáticos. De este modo con solo instalar este módulo todos los documentos accesibles públicamente a través de un portal no contendrán metadatos. MetaShield protector puede limpiar documentos de Microsoft Office de la versión 97 a la 2007, OpenOffice, Portable Document Format (pdf), wpd y jpg.

4.1.6.2.4. Acuerdos de confidencialidad y secreto

Se deberían identificar, revisar y documentar de manera regular los requisitos para los acuerdos de confidencialidad y no divulgación que reflejan las necesidades de la organización para la protección de información.

4.1.7. Etapa VII - Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información

4.1.7.1. Requisitos de Seguridad de los Sistemas de Información

4.1.7.1.1. Análisis y especificación de los requisitos de seguridad

Control:

Los enunciados de requisitos de los requisitos de negocios para sistemas nuevos o mejoras a sistemas existentes deberían especificar los requisitos de control.

Lista de chequeo para implantación de políticas:

a) Detallar si existen políticas de la adquisición o desarrollo de software según las necesidades de la Municipalidad Provincial.

Las políticas de la adquisición o desarrollo de software en la Municipalidad Provincial no existen.

Se tienen como buena práctica de seguridad que sólo el personal del área de sistemas pueda realizar la adquisición de algún software. En caso de que el personal docente o administrativo requiera algún

aplicativo, éste se canaliza por medio del jefe de Informática.

b) Documentar si existen políticas de pruebas antes de la adquisición o desarrollo de un software. En la Municipalidad Provincial no se cuenta con segregación de las redes, como, por ejemplo: red de desarrollo y pruebas. Sólo se tiene la red de producción. Al momento del desarrollo de un aplicativo en el área de Sistemas, las pruebas son realizadas en máquinas virtuales.

c) Verificar que se cuente con estándares para el desarrollo de software no se cuenta con estándares para el desarrollo de software.

d) Documentar la existencia de los controles que deberán incluir para la seguridad de la información en los aplicativos de la Municipalidad.

Los controles que deberían incluir en todas las aplicaciones de la Municipalidad para la seguridad informática serían:

- Único inicio de sesión.
- Perfiles de usuario.
- Para acceso a las B/D serán a través de interfases aplicativas.
- El token o inicio de sesión.
- Identificación única de la sesión del usuario.

4.1.7.1.2. Seguridad de las comunicaciones en servicios accesibles por redes públicas

No se cuenta con seguridad de las comunicaciones en servicios accesibles por redes públicas, puesto que todo se maneja localmente en la Municipalidad.

4.1.7.1.3. Protección de las transacciones por redes telemáticas.

No se cuenta con una protección de las transacciones por redes telemáticas, puesto que no existe un centro de datos propiamente en la Municipalidad.

4.2. Presentación resultado y prueba de hipótesis

Sustentación de Variables

a. Variable Independiente

Sea la variable "Modelo de Seguridad de la Información", plan basado en la Norma Internacional ISO 27002:2013, del cual se aplican sus dominios y controles respectivos.

b. Variable Dependiente

Sea la variable "Gestión Informática de la Municipalidad Provincial de Yungay", que consiste en el conjunto de operaciones (administrativas) que se realizan en la Municipalidad.

Verificación de Variables

a. Medición de los Indicadores antes de la Influencia del Modelo de Seguridad de la Información

- **Indicador 1: Percepción de la Confidencialidad de la Información**

- Métrica:

Calificativo de la percepción la confidencialidad de la información con respecto a la realización actual de sus operaciones (administrativas).

- Procedimiento Actual:

Uno de los problemas principales de la Municipalidad era la confidencialidad de la información con respecto al control del acceso a la información trayendo como consecuencia la inseguridad en la

realización de sus operaciones (administrativas), esto por el sistema actual que opera y, la falta de seguridad informática.

- Dirigido a:

Personal (jefes y gerentes) de la Municipalidad Provincial de Yungay.

- Resultado de la Encuesta:

1. ¿La confidencialidad de la información actual con respecto a las operaciones (administrativas) que se realizan en la Municipalidad Distrital se da adecuadamente?

Tabla 4

Indicador Confidencialidad de la información

Ítem	Población
Si	1
No	24
Total	25

Fuente: Elaboración propia

- Interpretación:

Como muestra los resultados en el cuadro anterior, el personal empleado de la Municipalidad Provincial de Yungay percibe que con el sistema actual existen inconvenientes en la confidencialidad de la información para realizar sus operaciones (administrativas), pues consideran que la seguridad de la información no está implementada adecuadamente.

- **Indicador 2: Percepción de la Integridad de la Información**

- Métrica:

Calificativo de la percepción la integridad de la información con respecto a la realización actual de sus operaciones (administrativas).

- Procedimiento Actual:

Uno de los problemas principales de la Municipalidad era la integridad de la información con respecto a la exactitud y completitud de la información trayendo como consecuencia la inseguridad en la realización de sus operaciones (administrativas), esto por el sistema actual que opera y, la falta de seguridad.

- Dirigido a:

Personal (jefes y gerentes) de la Municipalidad Provincial de Yungay.

- Resultado de la Encuesta:

2. ¿La integridad de la información actual con respecto a las operaciones (administrativas) que se realizan en la Municipalidad Provincial de Yungay se da adecuadamente?

Tabla 5

Indicador Integridad de la información

Ítem	Población
Si	08
No	17
Total	25

Fuente: Elaboración propia

- Interpretación:

Como muestra los resultados en el cuadro anterior, el personal empleado de la Municipalidad Provincial de Yungay percibe que con el sistema actual existen inconvenientes en la integridad de la información para realizar sus operaciones (administrativas), pues consideran que la seguridad de la información no está implementada adecuadamente.

- **Indicador 3: Percepción de la Disponibilidad de la Información**

- Métrica:

Calificativo de la percepción la disponibilidad de la información con respecto a la realización actual de sus operaciones (administrativas).

- Procedimiento Actual:

Uno de los problemas principales de la Municipalidad Provincial era la disponibilidad de la información con respecto a la disposición de la información trayendo como consecuencia la inseguridad en la realización de sus operaciones (administrativas), esto por el sistema actual que opera y la falta de seguridad informática.

- Dirigido a:

Personal (jefes y gerentes) de la Municipalidad Provincial de Yungay.

- Resultado de la Encuesta:

3. ¿La disponibilidad de la información actual con respecto a las operaciones (administrativas) que se realizan en la Municipalidad Provincial de Yungay se da adecuadamente?

Tabla 6

Indicador Integridad de la información

Ítem	Población
Si	10
No	15
Total	25

Fuente: Elaboración propia

- Interpretación:

Como muestra los resultados en el cuadro anterior, el personal empleado de la Municipalidad Provincial de Yungay percibe que con el sistema actual existen inconvenientes en la disponibilidad de la información para realizar sus operaciones (administrativas), pues consideran que la seguridad de la información no está implementada adecuadamente.

b. Medición de los Indicadores después de la Influencia del Modelo de Seguridad de la Información

- **Indicador 1: Percepción de la Confidencialidad de la Información**

- Métrica:

Calificativo de la percepción la confidencialidad de la información con respecto a la realización actual de sus operaciones (administrativas).

- Procedimiento Actual:

Se formula la implantación de un Modelo de Seguridad de la Información que permitirá realizar un adecuado control de acceso a la información.

- Dirigido a:

Personal Empleado de la Municipalidad Provincial de Yungay.

- Resultado de la Encuesta:

1. ¿La confidencialidad de la información actual con respecto a las operaciones (administrativas) que se realizan en la Municipalidad Provincial de Yungay se da adecuadamente?

Tabla 7

Indicador Integridad de la información

ítem	Población
Si	20
No	05
Total	25

Fuente: Elaboración propia

- Interpretación:

Como muestra los resultados en el cuadro anterior, el personal empleado de la Municipalidad Provincial de Yungay percibe que con

el sistema actual (Modelo de Seguridad de la Información) existe una adecuada confidencialidad de la información para realizar sus operaciones (administrativas), pues consideran que la seguridad de la información está implementada adecuadamente.

- **Indicador 2: Percepción de la Integridad de la Información**

- Métrica:

Calificativo de la percepción la integridad de la información con respecto a la realización actual de sus operaciones (administrativas).

- Procedimiento Actual:

Se formula la implantación de un Modelo de Seguridad de la Información que permitirá realizar una adecuada exactitud y completitud de la información.

- Dirigido a:

Personal (jefes y gerentes) Empleado de la Municipalidad Provincial.

- Resultado de la Encuesta:

2. ¿La integridad de la información actual con respecto a las operaciones (administrativas) que se realizan en la Municipalidad Provincial de Yungay se da adecuadamente?

Tabla 8

Indicador Integridad de la información

ítem	población
Si	18
No	07
Total	25

Fuente: Elaboración propia

- Interpretación:

Como muestra los resultados en el cuadro anterior, el personal empleado de la Municipalidad Provincial de Yungay percibe que con el sistema actual (Modelo de Seguridad de la Información) existe una adecuada integridad de la información para realizar sus operaciones (administrativas), pues consideran que la seguridad de la información está implementada adecuadamente.

- **Indicador 3: Percepción de la Disponibilidad de la Información**

- Métrica:

Calificativo de la percepción la disponibilidad de la información con respecto a la realización actual de sus operaciones (administrativas).

- Procedimiento Actual:

Se formula la implantación de un Modelo de Seguridad de la Información que permitirá realizar una adecuada disposición de la información.

- Dirigido a:

Personal Empleado (gerentes y jefes) de la Municipalidad Provincial de Yungay.

- Resultado de la Encuesta:

3. ¿La disponibilidad de la información actual con respecto a las operaciones (administrativas) que se realizan en la Municipalidad Provincial de Yungay se da adecuadamente?

Tabla 9

Indicador de disponibilidad de la información

ítem	Población
Si	22
No	03
Total	25

Fuente: Elaboración propia

- Interpretación:

Como muestra los resultados en el cuadro anterior, el personal empleado de la Municipalidad Provincial de Yungay percibe que con el sistema actual (Modelo de Seguridad de la Información) existe una adecuada disponibilidad de la información para realizar sus operaciones (administrativas), pues consideran que la seguridad de la información está implementada adecuadamente.

4.3. Discusión de resultados

Sean la Hipótesis:

H0: "La implantación de un modelo de seguridad de la información basado en la norma ISO 27002 no permite la mejora de la gestión informática de la Municipalidad Provincial de Yungay".

H1: "La implantación de un modelo de seguridad informática basado en la norma ISO 27002 permite la mejora de la gestión informática de la Municipalidad Provincial de Yungay".

Para demostrar que la hipótesis H1 es aceptada y que la hipótesis H0 es rechazada, se procederá a realizar un conjunto de cálculos estadísticos:

Tabla 10

Análisis de los Indicadores de Contrastación

N°	Indicador	%Aceptación actual	%Aceptación con estimulo	d	D - d	$(D-d)^2$
1	Percepción la confidencialidad de la información	0.04	0.8	-0.76	0.21	0.045
2	Percepción de la integridad de la información	0.32	0.72	-0.4	0.15	0.021
3	Percepción de la Disponibilidad de la	0.4	0.88	-0.48	0.067	0.004

Información			
	∑	**-1.64**	**0.071**

Fuente: Elaboración propia

Contrastación de Hipótesis

Para realizar la contrastación de la hipótesis, realizaremos un conjunto de cálculos estadísticos:

a. Valores:

N: Número de indicadores = 3

M_1: Antes del estimulo

M_2: Después del estimulo

D: Diferencia (M_1- M_2)

D^2: Varianza (M_1- M_2)

$$DP = \frac{\sum D_j}{\text{n}}$$

$$d = \frac{-1.64}{3}$$

$$d = 0.547$$

b. Desviación Estándar (ő):

$$S^2 = \sqrt[2]{\frac{\sum(D-d)^2}{\text{n}-1}}$$

$$S^2 = \sqrt[2]{\frac{0.071}{3-1}}$$

c. Hipótesis Estadística:

H_0: El sistema actual es mejor que el Propuesto (solución basada en la implantación de un Modelo de Seguridad de la Información)

$$H_0: M_1 >= M_2 \rightarrow M_1 - M_2 >= 0$$

H_1: El sistema propuesto (solución basada en la implantación de un Modelo de Seguridad de la Información) es mejor que el Actual

$$H_1: M_1 < M_2 \rightarrow M_1 - M_2 < 0$$

d. Nivel del Significancia:

$$O = 0.025$$

e. Estadístico de Prueba:

Se utilizará el valor critico de "t" Student usado para muestras menores a 30 (Valor N < 30).

f. Criterios de Decisión:

Este punto se halla el valor de "t" de tabla al ubicar la intersección de grados de libertad con el nivel de confianza.

Donde:

$$t\ (1\text{-}a)\ (n\text{-}1)$$

Grados de libertad (n-1) = 3 -1 = 2

Nivel de Confianza (1-a) = 1 - 0.025 = 0.975

Luego: "t" de tabla es entonces igual a -4.303

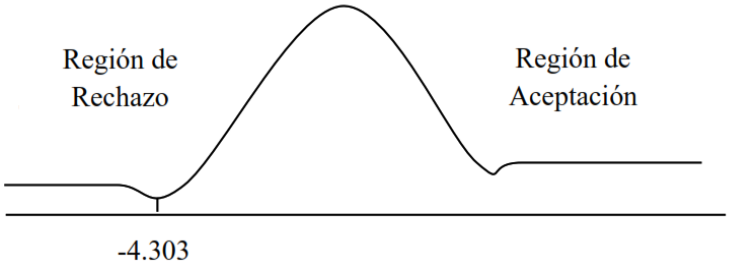


Figura N° - Criterios de decisión

Fuente: Elaboración propia

g. Cálculo de "t":

$$t = \frac{-0.547}{\frac{0189}{\sqrt{3}}}$$

$$t = -5.009$$

$$t_1 - 5.009 < t_0 - 4.303$$

h. Conclusiones:

Como "t_1" calculando es menor que "t_0" de la tabla de Student, entonces se acepta H_1 y se rechaza H_0.

Hay evidencias que la solución propuesta (aplicación del Modelo de Seguridad de la Información) es mejor que la solución actual con un nivel de significación del 2.5 % y, por lo tanto, es una alternativa de solución adecuada para el problema planteado.

Este proyecto abarcó lo que es el Sistema de la Seguridad de la Información para mejorar la gestión informática de la municipalidad provincial de Yungay, por ser una de las dependencias con activos de información importantes para la institución, es por ello que al presentar alguna falla en cualquier momento puede ocasionar problemas e inconvenientes en el desarrollo normal de los procesos. A pesar de ello se ha observado que hasta el momento no se ha puesto mayor esfuerzo en lo que respecta a la seguridad de la información.

En el desarrollo del presente proyecto se han observado estudios e información sobre el tema en cuestión, incluso dentro de nuestro ámbito Nacional, los autores Bustamante S., Coral Miguel, Rodríguez Immer, Rodríguez Lévano, median la tesis Políticas basadas en la ISO 27001:2013 y su influencia en la gestión de seguridad de la información en municipalidades de Perú, Universidad Peruana Unión, Tarapoto, Perú, 2021. Para lo cual los autores realizan el diagnóstico y diseño de un Sistema de Gestión de Seguridad de Información aplicado a una Empresa Constructora según el estándar internacional ISO/IEC 27001:2013 la cual no es certificada debido a que ahora se cuenta con la actualización al estándar internacional ISO/IEC 27001:2013, estas investigaciones se realizaron antes del

cambio contractual por lo que fueron a grandes rasgos puesto que su aplicación de todo o en parte se está imponiendo de manera necesaria y obligatoria para las instituciones públicas ya que generalmente no cuentan con este tipo de políticas de seguridad ni mucho menos cuentan con un documento de aplicabilidad por lo cual están a la deriva. En base a nuestros antecedentes vemos que a pesar de que nos encontramos en una etapa donde la información es importante, poco o nada se hace para salvaguardarlo y protegerla de los riesgos y amenazas a los que se ven expuestos diariamente ya que varios estudios confirman lo dicho.

V. CONCLUSIONES

- ✓ Se controló los accesos a los recursos informáticos de la Municipalidad para aumentar la disponibilidad de la información.
- ✓ Se definió políticas de cifrado para aumentar la integridad de la información.
- ✓ Se estableció la seguridad física y ambiental en toda la Municipalidad para aumentar la integridad de la información.
- ✓ Se estableció la seguridad en las operaciones del negocio para aumentar confidencialidad de la información.
- ✓ Se estableció la seguridad en las telecomunicaciones para aumentar la confidencialidad de la información.
- ✓ Se definió medidas adecuadas para la adquisición, desarrollo y mantenimiento de los sistemas de información para aumentar la disponibilidad de la información.

VI. RECOMENDACIONES

- Se recomienda realizar campañas de concientización a todo el personal de la Municipalidad sobre la importancia de la seguridad informática.
- Por motivos de fuerza mayor como el cambio de sus autoridades principales como son lo gerentes y jefes de diferentes áreas no se pudo concluir con la implementación que se venia haciéndolo con ciertos estándares, es por ello que se recomienda a la nueva gestión que tome conciencia al momento de hacer cada cambio de funcionario, para que no se ventile la información confidencial.
- Se recomienda que se establezca de forma clara las políticas de seguridad de la información complementarias al presente plan; publicando y manteniendo éstas.
- El personal empleado de la Municipalidad debe manifestar su apoyo y compromiso; todo con la finalidad de la aplicación con éxito del presente modelo de seguridad de la información.
- Una vez implantadas los controles de seguridad propuestas por el presente plan, se recomienda su revisión y su actualización regular por cambios significativos sucedidos, para garantizar su eficacia y eficiencia (efectividad).

VII. REFERENCIAS BIBLIOGRÁFICAS

Bustamante García, S., Valles Coral, M., Cuellar Rodríguez, I., & Lévano Rodríguez, D. (2021). *Políticas basadas en la ISO 27001:2013 y su influencia en la gestión de seguridad de la información en municipalidades de Perú.* Tarapoto: Universidad Peruana Unión.

Estrada Esponda , R., Unás-Gómez, J., & Flórez Rincón , O. (2021). Prácticas de seguridad de la información en tiempos de pandemia. Caso Universidad del Valle, sede Tuluá . *Logos Ciencia & Tecnología*, 98-110.

Aguilar Inquel, J. L. (2019). Propuesta de un modelo de gestión de seguridad de la información para la Cooperativa Santo Domingo de Guzmán Agencia Sicuani basado en el marco de referencia de Cobit 5. *Escuela Profesional de Ingeniería de Sistemas*.

ALEXANDER, A. G. (2007). *Diseño de un sistema de gestión de seguridad de información: Optica ISO 27001:2005.* Alfaomega Colombiana.

D. L. Carvajal, A. C. (2019). Una propuesta de gestión de la seguridad de la información aplicado a una entidad pública colombiana. *Entre Ciencia e Ingeniería*, 68-79.

Guerra, E., Neira, H., Diaz, J., & Patiño, J. (2021). Desarrollo de un sistema de gestión para la seguridad de la información basado en metodología de identificación y análisis de riesgo en bibliotecas universitarias. *Información tecnológica*, 145-156.

ISO. (10 de 2004). *ISO/CEI TR 18044:2004*. ISO/CEI TR 18044:2004: https://www.iso.org/standard/35396.html

ISO 27000. (2005). *ISO27000.ES*. ISO27000.ES: https://www.iso27000.es/iso27000.html

ISO 27001. (2021). *AENOR*. AENOR: https://www.aenor.com/certificacion/tecnologias-de-la-informacion/seguridad-informacion

ISO 27002. (2020). *PLATAFORMA TECNOLÓGICA PARA LA GESTIÓN DE LA EXCELENCIA*. PLATAFORMA TECNOLÓGICA PARA LA GESTIÓN DE LA EXCELENCIA: https://www.isotools.org/2019/06/11/iso-27002-la-importancia-de-las-buenas-practicas-en-los-sistemas-de-seguridad-de-la-informacion/

Pérez Porto, J., & Merino, M. (2008). *Definición.de.* Definciion.de: https://definicion.de/seguridad-informatica/

Rodriguez Baca, L., Cruzado Puente de la Vega, C., Mejía Corredor, C., & Alarcón Diaz, M. (2020). Aplicación de ISO 27001 y su influencia en la seguridad de la información de una empresa privada peruana. *Propósitos y Representaciones*.

Rojas, J., & Clemente, M. (2019). *Seguridad en los datos e implantación de la NTP-ISO/IEC 27001:2014 en la Sub Gerencia de Gestión de Base de Datos del RENIEC.* Lima: Respositorio de la Universidad Cesar Vallejo.

VIII. ANEXOS:

ANEXO A - MODELO DE ENTREVISTA APLICADO AL PERSONAL DIRECTIVO DE LA MUNICIPALIDAD PROVINCIAL DE YUNGAY

El objetivo de la presente entrevista es conocer las circunstancias en las que se labora en la que se gestiona la seguridad informática en el Municipalidad Provincial de Yungay.

1. ¿Cómo define Ud. la seguridad informática con respecto a las operaciones académica y administrativa que realiza en la Municipalidad Provincial de Yungay?

_____

_____

2. ¿Cuáles cree Ud. que son las fortalezas y debilidades que tiene la gestión | de la Municipalidad Provincial de Yungay?

_____

_____

3. ¿Cree Ud. que aprovecha de la mejor manera las oportunidades que le brinda el entorno? Sí/No, ¿Por qué?

_____

_____

4. ¿Cree Ud. que enfrenta de la mejor manera las amenazas que se presentan en el entorno? Sí/No, Por qué?

_____

_____

5. ¿Cree usted que la implantación de un Modelo de Seguridad de la Información contribuiría al mejoramiento de la Gestión Informática Municipalidad Provincial de Yungay? Sí/No, ¿Por qué?

_____

_____

ANEXO B - MODELO DE ENCUESTA DE PERCEPCIÓN APLICADO AL PERSONAL OPERARIO DE LA MUNICIPALIDAD PROVINCIAL DE YUNGAY

El objetivo de la presente encuesta es conocer la percepción del personal operario que labora en la Municipalidad Provincial de Yungay con respecto a la implantación de un Modelo de Seguridad de la Información.

1. ¿La confidencialidad de la información actual con respecto a las operaciones (administrativas) que se realizan en la Municipalidad Provincial de Yungay se da adecuadamente?

Sí ☐ No ☐

2. ¿La integridad de la información con respecto a las operaciones (administrativas) que se realizan en Municipalidad Provincial de Yungay se da adecuadamente?

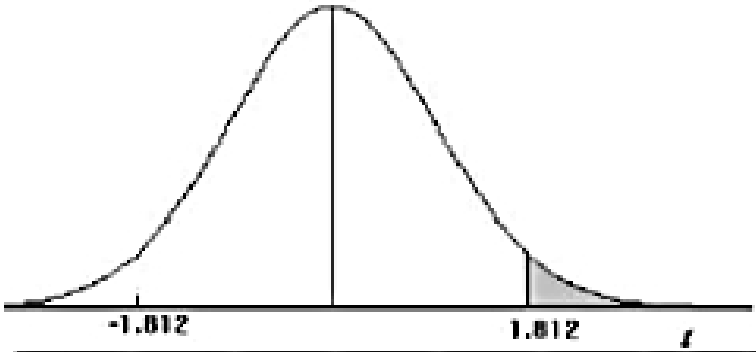
v
Sí ☐ No ☐

3. ¿La disponibilidad de la información con respecto a las operaciones (administrativas) que se realizan en la Municipalidad Provincial de Yungay se da adecuadamente?

Sí ☐ No ☐

ANEXO C - DISTRIBUCIÓN DE "T" STUDENT

Puntos de porcentaje de la distribución t



Ejemplo

Para $\phi = 10$ grados de libertad:

$P[t > 1.812] = 0.0$
$P[t < -1.812] = 0.0$

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 D – CARTA DE AUTORIZACIÓN PARA REALIZAR LA INVESTIGACION EN LA MUNICIPALIDAD PROVINCIAL DE YUNGAY

MUNICIPALIDAD PROVINCIAL DE YUNGAY
GERENCIA DE ADMINISTRACION Y FINANZAS

"AÑO DEL FORTALECIMIENTO DE LA SOBERANÍA NACIONAL"

Yungay, 05 de setiembre de 2022

CARTA Nº 030-2022-MPY/GAF/06.40

ESTIMADO SEÑOR:
MENDEZ PASIÓN MICHAEL WILFREDO
Pampac Bajo S/N

YUNGAY. -

ASUNTO : COMUNICO AUTORIZACIÓN PARA REALIZAR TESIS

REF. : EXPEDIENTE ADMINISTRATIVO Nº 00007123-2022

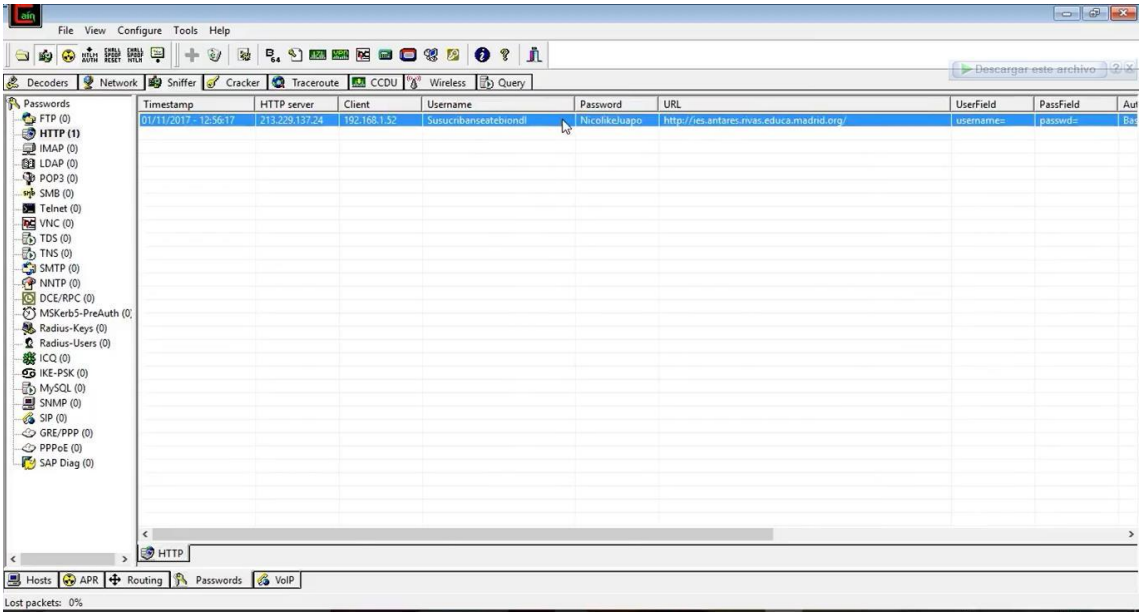
Por intermedio de la presente me dirijo a Ud., con la finalidad de comunicarle que, esta Institución otorga la Autorización a su representada para poder realizar TESIS con respecto al "MODELO DE SEGURIDAD DE LA INFORMACIÓN PARA MEJORAR LA GESTIÓN INFORMATICA" dentro de esta entidad Pública, concerniente a entrevistas y encuestas con el personal seleccionado previamente, para recojo de información.

Aprovecho la oportunidad para expresarle las muestras de mi especial consideración y estima personal.

Atentamente;

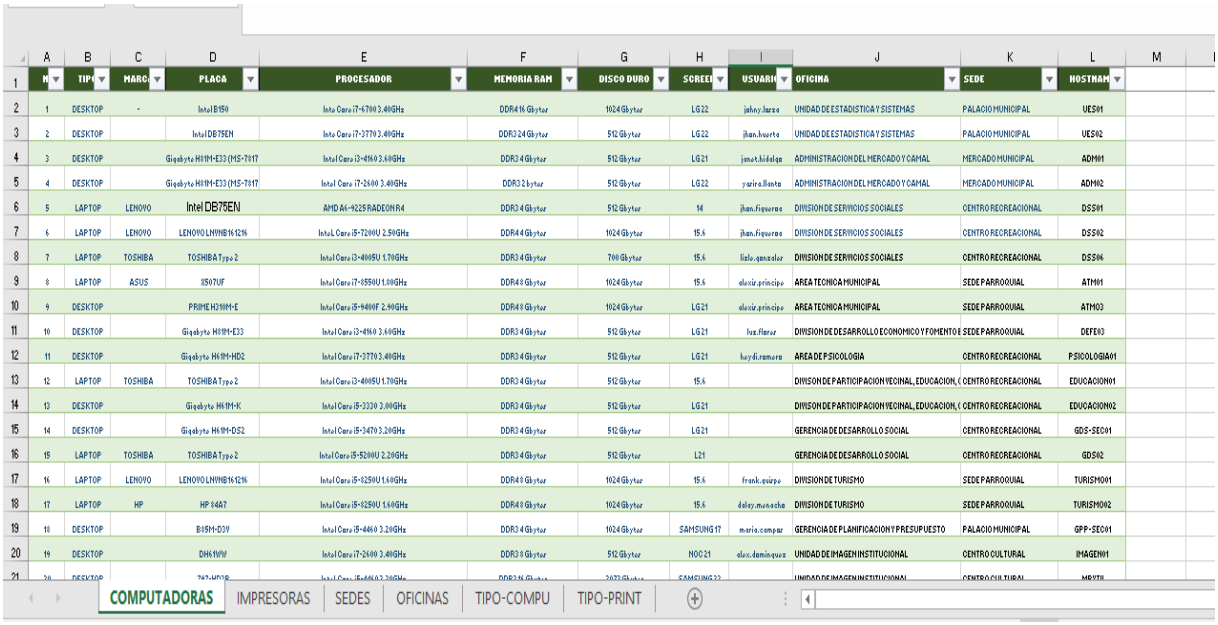
Lic. Hecki A. Rivera Prieto
GERENTE DE ADMINISTRACION Y FINANZAS

ANEXO E – PRUEBAS DE VULNERABILIDADES DE USUARIO CONTRASEÑAS CON EL CAIN Y ABEL ANTES QUE SE COMPRE LA LICENCIA DEL SOPHOS



ANEXO F – INSTALACION DE LAS CAMARAS DE SEGURIDAD EN LAS ENTRADAS DE CADA SEDE DE LA MUNICIPALIDAD PROVINCIAL DE YUNGAY

ANEXO G – HOJA DE REGISTRO DE LOS BIENES INFORMATICOS



	A	B	C	D	E	F	G	H	I	J	K	L	M
1	N	TIPO	MARCA	PLACA	PROCESADOR	MEMORIA RAM	DISCO DURO	SCREEN	USUARIO	OFICINA	SEDE	HOSTNAME	
2	1	DESKTOP	-	Intel B150	Intel Core i7-6700 3.40GHz	DDR4 16 Gbytes	1024 Gbytes	LG22	johny.lazo	UNIDAD DE ESTADISTICA Y SISTEMAS	PALACIO MUNICIPAL	UES01	
3	2	DESKTOP		Intel DB75EN	Intel Core i7-3770 3.40GHz	DDR3 24 Gbytes	512 Gbytes	LG22	jhan.huerta	UNIDAD DE ESTADISTICA Y SISTEMAS	PALACIO MUNICIPAL	UES02	
4	3	DESKTOP		Gigabyte H81M-E33 (MS-7817	Intel Core i3-4160 3.60GHz	DDR3 4 Gbytes	512 Gbytes	LG21	janet.hidalgo	ADMINISTRACION DEL MERCADO Y CAMAL	MERCADO MUNICIPAL	ADM01	
5	4	DESKTOP		Gigabyte H81M-E33 (MS-7817	Intel Core i7-2600 3.40GHz	DDR3 2 bytes	512 Gbytes	LG22	yuriro.llanto	ADMINISTRACION DEL MERCADO Y CAMAL	MERCADO MUNICIPAL	ADM02	
6	5	LAPTOP	LENOVO	Intel DB75EN	AMD A6-9225 RADEON R4	DDR3 4 Gbytes	512 Gbytes	14	jhan.figueroa	DIVISION DE SERVICIOS SOCIALES	CENTRO RECREACIONAL	DSS01	
7	6	LAPTOP	LENOVO	LENOVO LNVNB161216	Intel Core i5-7200U 2.50GHz	DDR4 4 Gbytes	1024 Gbytes	15.6	jhan.figueroa	DIVISION DE SERVICIOS SOCIALES	CENTRO RECREACIONAL	DSS02	
8	7	LAPTOP	TOSHIBA	TOSHIBA Type 2	Intel Core i3-4005U 1.70GHz	DDR3 4 Gbytes	700 Gbytes	15.6	lizlo.gonzalez	DIVISION DE SERVICIOS SOCIALES	CENTRO RECREACIONAL	DSS06	
9	8	LAPTOP	ASUS	X507UF	Intel Core i7-8550U 1.80GHz	DDR4 8 Gbytes	1024 Gbytes	15.6	alexir.principe	AREA TECNICA MUNICIPAL	SEDE PARROQUIAL	ATM01	
10	9	DESKTOP		PRIME H310M-E	Intel Core i5-9400F 2.90GHz	DDR4 8 Gbytes	1024 Gbytes	LG21	alexir.principe	AREA TECNICA MUNICIPAL	SEDE PARROQUIAL	ATM03	
11	10	DESKTOP		Gigabyte H61M-E33	Intel Core i3-4160 3.60GHz	DDR3 4 Gbytes	512 Gbytes	LG21	luz.flores	DIVISION DE DESARROLLO ECONOMICO Y FOMENTO E	SEDE PARROQUIAL	DEFE03	
12	11	DESKTOP		Gigabyte H61M-HD2	Intel Core i7-3770 3.40GHz	DDR3 4 Gbytes	512 Gbytes	LG21	haydi.ramos	AREA DE PSICOLOGIA	CENTRO RECREACIONAL	PSICOLOGIA01	
13	12	LAPTOP	TOSHIBA	TOSHIBA Type 2	Intel Core i3-4005U 1.70GHz	DDR3 4 Gbytes	512 Gbytes	15.6		DIVISION DE PARTICIPACION VECINAL, EDUCACION, (	CENTRO RECREACIONAL	EDUCACION01	
14	13	DESKTOP		Gigabyte H61M-K	Intel Core i5-3330 3.00GHz	DDR3 4 Gbytes	512 Gbytes	LG21		DIVISION DE PARTICIPACION VECINAL, EDUCACION, (	CENTRO RECREACIONAL	EDUCACION02	
15	14	DESKTOP		Gigabyte H61M-DS2	Intel Core i5-3470 3.20GHz	DDR3 4 Gbytes	512 Gbytes	LG21		GERENCIA DE DESARROLLO SOCIAL	CENTRO RECREACIONAL	GDS-SEC01	
16	15	LAPTOP	TOSHIBA	TOSHIBA Type 2	Intel Core i5-5200U 2.20GHz	DDR3 4 Gbytes	512 Gbytes	L21		GERENCIA DE DESARROLLO SOCIAL	CENTRO RECREACIONAL	GDS02	
17	16	LAPTOP	LENOVO	LENOVO LNVNB161216	Intel Core i5-8250U 1.60GHz	DDR4 8 Gbytes	1024 Gbytes	15.6	frank.quispe	DIVISION DE TURISMO	SEDE PARROQUIAL	TURISMO01	
18	17	LAPTOP	HP	HP 84A7	Intel Core i5-8250U 1.60GHz	DDR4 8 Gbytes	1024 Gbytes	15.6	delsy.monocha	DIVISION DE TURISMO	SEDE PARROQUIAL	TURISMO02	
19	18	DESKTOP		B85M-D3V	Intel Core i5-4460 3.20GHz	DDR3 4 Gbytes	1024 Gbytes	SAMSUNG 17	mario.campos	GERENCIA DE PLANIFICACION Y PRESUPUESTO	PALACIO MUNICIPAL	GPP-SEC01	
20	19	DESKTOP		DH61WW	Intel Core i7-2600 3.40GHz	DDR3 8 Gbytes	512 Gbytes	NOC21	alex.dominguez	UNIDAD DE IMAGEN INSTITUCIONAL	CENTRO CULTURAL	IMAGEN01	
21	20	DESKTOP		787-UP2B	Intel Core i5-6400 2.70GHz	DDR3 16 Gbytes	2072 Gbytes	SAMSUNG 22		UNIDAD DE IMAGEN INSTITUCIONAL	CENTRO CULTURAL	MKTI1	

COMPUTADORAS | IMPRESORAS | SEDES | OFICINAS | TIPO-COMPU | TIPO-PRINT

Matriz de consistencia de la investigación.

TITULO	PROBLEMA	OBJETIVOS	HIPÓTESIS	VARIABLES	INDICADORES
Modelo De Seguridad De La Información Para Mejorar La Gestión Informática En La Municipalidad Provincial De Yungay, 2022.	**PROBLEMA GENERAL** ¿De qué manera el modelo de seguridad de la información mejorara LA GESTIÓN INFORMÁTICA EN LA MUNICIPALIDAD PROVINCIAL DE YUNGAY, 2022? **PROBLEMAS ESPECÍFICOS**	**OBJETIVO GENERAL** Mejorar la gestión informática de la Municipalidad Provincial de Yungay a través de la aplicación de un modelo de seguridad de la información basado en la Norma ISO 27002:2013. **OBJETIVOS ESPECÍFICOS**	**HIPÓTESIS GENERAL** El modelo de seguridad de la información para mejorar la gestión informática en la Municipalidad Provincial De Yungay, 2022. **HIPÓTESIS ESPECIFICAS**	**VARIABLE DEPENDIENTE** Seguridad de la información **VARIABLE INDEPENDIENTE**	a) Nivel de confidencialidad de Hardware y Software b) Nivel de integridad de Hardware y Software c) Nivel de disponibilidad de Hardware y Software

	¿De qué manera se puede determinar el Modelo actual de la seguridad de la información de la Municipalidad Provincial de Yungay?	Determinar el modelo de seguridad de la información actual en la municipalidad Provincial de Yungay en todos sus dominios y controles de seguridad.	Se determino el modelo de seguridad de la información actual en la municipalidad Provincial de Yungay en todos sus dominios y controles de seguridad.	Gestión informática	a) Cantidad de Incidentes reportados b) Nivel de Conocimiento de RRHH c) Cantidad de controles implantados
	¿De qué manera se evaluarán los Modelos de Seguridad de la Información existentes en el mercado informático orientado a la gestión segura y efectiva de los procesos ediles de un municipio?	Evaluar los modelos de seguridad de la información existentes en el mercado informático orientado a la gestión segura y efectiva de los procesos ediles de un municipio.	Se evaluó los modelos de seguridad de la información existentes en el mercado informático orientado a la gestión segura y efectiva de los procesos ediles de un municipio.		

	¿Cómo se diseñará el nuevo Modelo de Seguridad de la Información en la Gestión informática de la Municipalidad provincial de Yungay?	Diseñar el modelo de gestión de seguridad de la información orientándolo a la mejora de la gestión informática para la Provincial de Yungay.	Se diseño el modelo de gestión de seguridad de la información orientándolo a la mejora de la gestión informática para la Provincial de Yungay.