UNIVERSIDAD DE HUÁNUCO

FACULTAD DE INGENIERÍA

ESCUELA ACADÉMICA PROFESIONAL DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

Trabajo de Suficiencia Profesional

PROPUESTA DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN PARA LA PROTECCIÓN DE ACTIVOS DE INFORMACIÓN BASADO EN LA NORMA ISO 27001 EN EL ÁREA DE INFORMÁTICA DE LA MUNICIPALIDAD PROVINCIAL DE HUÁNUCO

PARA OPTAR EL TÍTULO DE INGENIERO DE SISTEMAS E INFORMÁTICA

PRESENTADO POR EL BACHILLER

ARGÜEZO RAMIREZ, EDUARDO DANIEL

ASESOR:

JACHA ROJAS, JOHNNY PRUDENCIO

HUÁNUCO – PERÚ

2019

UNIVERSIDAD DE HUANUCO

Facultad de Ingeniería

E.A.P. DE INGENIERÍA DE SISTEMAS E INFORMATICA

ACTA DE SUSTENTACIÓN DE TRABAJO DE SUFICIENCIA PROFESIONAL PARA OPTAR EL TITULO PROFESIONAL DE INGENIERO (A) DE SISTEMAS E INFORMÁTICA

En la ciudad de Huánuco, siendo las 15:15 horas del día 11 del mes de OCTUBRE del año 2019, en el Auditorio de la Facultad de Ingeniería, en cumplimiento de lo señalado en el Reglamento de Grados y Títulos de la Universidad de Huánuco, se reunieron los Jurados Calificadores Nombrados mediante la Resolución N° 1201-2019-D-FI-UDH integrado por los docentes:

MG. BERTHA LUCILA CAMPOS RIOS (Presidente)

ING. ETHEL JHOVANI MANZANO LOZANO (Secretario)

ING. PAOLO EDUER SOLIS JARA (Vocal)

Para calificar el Trabajo de Suficiencia Profesional intitulada:

" PROPUESTA DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN PARA LA PROTECCIÓN DE ACTIVOS DE INFORMACIÓN BASADO EN LA NORMA ISO 27001 EN EL ÁREA DE INFORMÁTICA DE LA MUNICIPALIDAD PROVINCIAL DE HUÁNUCO" presentado por el (la) Bachiller EDUARDO DANIEL ARGÜERO ROMERO, para optar el Título Profesional de Ingeniero (a) de Sistemas e Informática.

Dicho acto de sustentación se desarrolló en dos etapas: exposición y absolución de preguntas: procediéndose luego a la evaluación por parte de los miembros del Jurado.

Habiendo absuelto las objeciones que le fueron formuladas por los miembros del Jurado y de conformidad con las respectivas disposiciones reglamentarias, procedieron a deliberar y calificar, declarándolo (a) APROBADO por UNANIMIDAD con el calificativo cuantitativo de CATORCE y cualitativo de SUFICIENTE

Siendo las 16:55 horas del día 11 del mes de OCTUBRE del año 2019, los miembros del Jurado Calificador firman la presente Acta en señal de conformidad.

Presidente

Secretario

Vocal

DEDICATORIA

Quiero, agradecer **A Dios,** por haberme dado la vida y las fuerzas necesarias para concluir satisfactoriamente este trabajo de investigación.

Quiero dedicar **a mis padres,** por demostrarme siempre su cariño, y su apoyo incondicional, ya que sin ellos no podía conseguir mis objetivos y metas alcanzadas.

Quiero dedicar **a mi esposa y mi hijo,** gracias a ambos por su paciencia y comprensión, ya que siempre me alentaron en concluir y seguir adelante con este trabajo de investigación.

AGRADECIMIENTO

Quiero agradecer a nuestra alma mater, Universidad de Huánuco por haberme aceptado y ser parte de ella y que nos dio la oportunidad de seguir y concluir nuestra formación académica.

A mis profesores que estuvieron a lo largo de mi carrera, que compartieron sus grandes conocimientos para convertirme en un profesional.

Quiero agradecer a la Municipalidad Provincial de Huánuco por permitirme realizar este trabajo de investigación.

INTRODUCCIÓN

Hoy en día, la seguridad informática es un pilar fundamental para el correcto funcionamiento de las empresas, ya que la información representa un capital muy importante y parte vital del rendimiento y rentabilidad de las empresas, como son las Mypes, financieras, clínicas municipalidades, etc., lo cual se encuentran con la necesidad de crear sistemas que puedan gestionarla y protegerla que garanticen confidencialidad, integración y disponibilidad de estos datos. La propuesta de un Sistema de Gestión Seguridad Información se basa en la identificación de datos importantes, sus propietarios y el lugar donde se encuentran. Actualmente es imposible crear un sistema perfecto, debido a los constantes avances tecnológicos, por lo que conocer los riesgos, debemos gestionarlos y mitigarlos.

Una forma de garantizar la seguridad de la información es conocer las normativas del **ISO 27001** y aplicarlo en el Sistema de Gestión de la Seguridad de la Información. Las empresas privadas como públicas deben estar al tanto de estas normas y formar al personal en ellas, desde el director hasta los operarios que manejarán el sistema. Asimismo, es importante contar con asesores que estén permanentemente actualizados para descubrir cualquier grieta dentro del sistema.

La mayoría de las organizaciones utiliza una red local, para mantener la información. Estas usan un firewall para salvaguardar los datos de la intrusión de personas ajenas dentro de Internet. No obstante, el cortafuego no puede proteger la información de todas las amenazas existentes, sobre todo de los hackers expertos o de las acciones de usuarios negligentes.

La presente investigación tiene como objetivo fundamental proponer un Sistema de Gestión de Seguridad de Información para mejorar la protección de activos de información basado en la norma **ISO 27001** en el área de informática de la Municipalidad Provincial de Huánuco.

La investigación se dividió en capítulos:

En el **capítulo I**, se detalla los aspectos de la entidad receptora nombre o razón social, rubro, ubicación, visión misión valores, objetivos estratégicos de la institución y organigrama.

En el **capítulo II**, se detalla de los aspectos del área como definir qué es lo que cuenta el área y que es lo que este encargado de velar.

En el **capítulo III**, se detalla de la identificación de la situación problemática, en este capítulo se detalla lo que es el problema de investigación, marco teórico, materiales y métodos.

En el **capítulo IV**, se detalla los aportes para la solución del problema, así como también la implementación del Sistema de Gestión Seguridad Información y los resultados.

RESUMEN

La presente investigación tiene como objetivo principal el desarrollo de un Sistema de Gestión de la Seguridad de la Información basado en la norma **ISO 27001** para la protección de los activos de información en el área de informática de la Municipalidad Provincial de Huánuco.

Donde se utilizó la metodología de Deming o PDCA sugerida por la norma **ISO 27001**, se dividió la investigación en cinco etapas:

En la primera se estableció el contexto, en la segunda se identificó y clasificación de los activos de información; en la tercera se siguió la metodología de análisis de riesgos, en la cuarta se siguió la metodología de evaluación de riesgo y en la quinta etapa el tratamiento de riesgo identificando los controles teniendo en cuenta el **ISO 27002:2013**.

Por otro lado, el presente trabajo nos permitió concluir en la importancia de contar con un Sistema de Gestión de la Seguridad de la Información para el área de informática de la Municipalidad Provincial de Huánuco, el sistema permite la protección de los activos de información garantizando la integración, disponibilidad y confidencialidad de estos.

Palabras claves: Sistema de Gestión de la Seguridad de la Información, ISO 27001, activos de información, PDCA

ABSTRACT

The main objective of this research is the development of an Information Security Management System based on the ISO 27001 standard for the protection of information assets in the information technology area of the Provincial Municipality of Huánuco.

Where the Deming or PDCA methodology suggested by ISO 27001 was used, the research was divided into five stages:

In the first one the context was established, in the second one the identification and classification of the information assets was identified; in the third, the risk analysis methodology was followed, in the fourth the risk assessment methodology was followed and in the fifth stage the risk treatment identifying the controls taking into account ISO 27002: 2013.

On the other hand, the present work allowed us to conclude on the importance of having an Information Security Management System for the IT department of the Provincial Municipality of Huánuco, the system allows the protection of information assets by guaranteeing the integration, availability and confidentiality of these.

Keywords: Information Security Management System, ISO 27001, information assets, PDCA

INDICE

INDICE DE FIGURAS

INDICE DE TABLAS

CAPITULO I

ASPECTOS DE LA ENTIDAD RECEPTORA

1.1. NOMBRE O RAZON SOCIAL

La Municipalidad Provincial de Huánuco Ubicado en el Departamento, Provincia y Distrito de Huánuco.

1.2. RUBRO

Administración Pública en General

1.3. UBICACIÓN / DIRECCIÓN

Jirón General Prado N° 750 – Huánuco

Figura 1. Plano de Ubicación

1.4. RESEÑA

1.4.1. CREACIÓN

La ciudad de Huánuco es fundada el 15 de agosto de 1539 por los conquistadores españoles con el nombre de "Huánuco de los Caballeros". De gran movimiento durante el periodo colonial, tuvo escritores importantes, descendientes de los españoles de la conquista. Durante la etapa de la emancipación, Huánuco fue una de las primeras ciudades en impulsar la independencia del Perú, a comienzos del siglo XIX. Inclusive figura como 15 de diciembre de 1820, la primera jura de independencia, tras una serie de levantamientos en Huamalíes, Huallanca y Ambo.

1.4.2. JURISDICCIÓN

La Provincia de Huánuco se encuentra asentada en la cuenca superior del río Huallaga. Está ubicada en la parte centro-oriental del Perú. Limita por el Norte con la provincia de Leoncio Prado; por el Sur, con la provincia de Ambo; por el Este, con la provincia de Pachitea y por el Oeste, con las provincias de Lauricocha y Yarowilca. Sus Distritos son: Huánuco, Chinchao (Acomayo), Churubamba, Santa María del Valle, Amarilis (Paucarbamba), San Francisco de Cayrán (Cayrán), Quisqui (Kichki), Margos, Yarumayo, San Pedro de Chaulán (Chaulán), Pillco Marca (Cayhuayna) y Yacus.

1.4.3. NATURALEZA

La Municipalidad Provincial de Huánuco es el Órgano de Gobierno Local emanado de la voluntad popular, con personería

jurídica de derecho público y con autonomía política, económica y administrativa en los asuntos de su competencia. Ejerce el gobierno local en su jurisdicción, la cual constituye una circunscripción político - administrativa de nivel provincial, que determina el ámbito territorial de gobierno y administración del Estado, que cuenta con una población caracterizada por su identidad histórico - cultural y un ámbito geográfico, que sirve de soporte de sus relaciones sociales, económicas y administrativas.

1.5. VISION

Figura 2. Visión Institucional

1.6. MISION

Figura 3. Misión Institucional

1.7. PRINCIPIO Y VALORES INSTITUCIONALES

Figura 4. Valores Institucionales

1.8. OBJETIVOS ESTRATEGICOS INSTITUCIONALES

Figura 5. Objetivos Estratégicos Institucionales

1.9. ORGANIGRAMA

ESTRUCTURA ORGÁNICA DE LA MUNICIPALIDAD PROVINCIAL DE HUÁNUCO

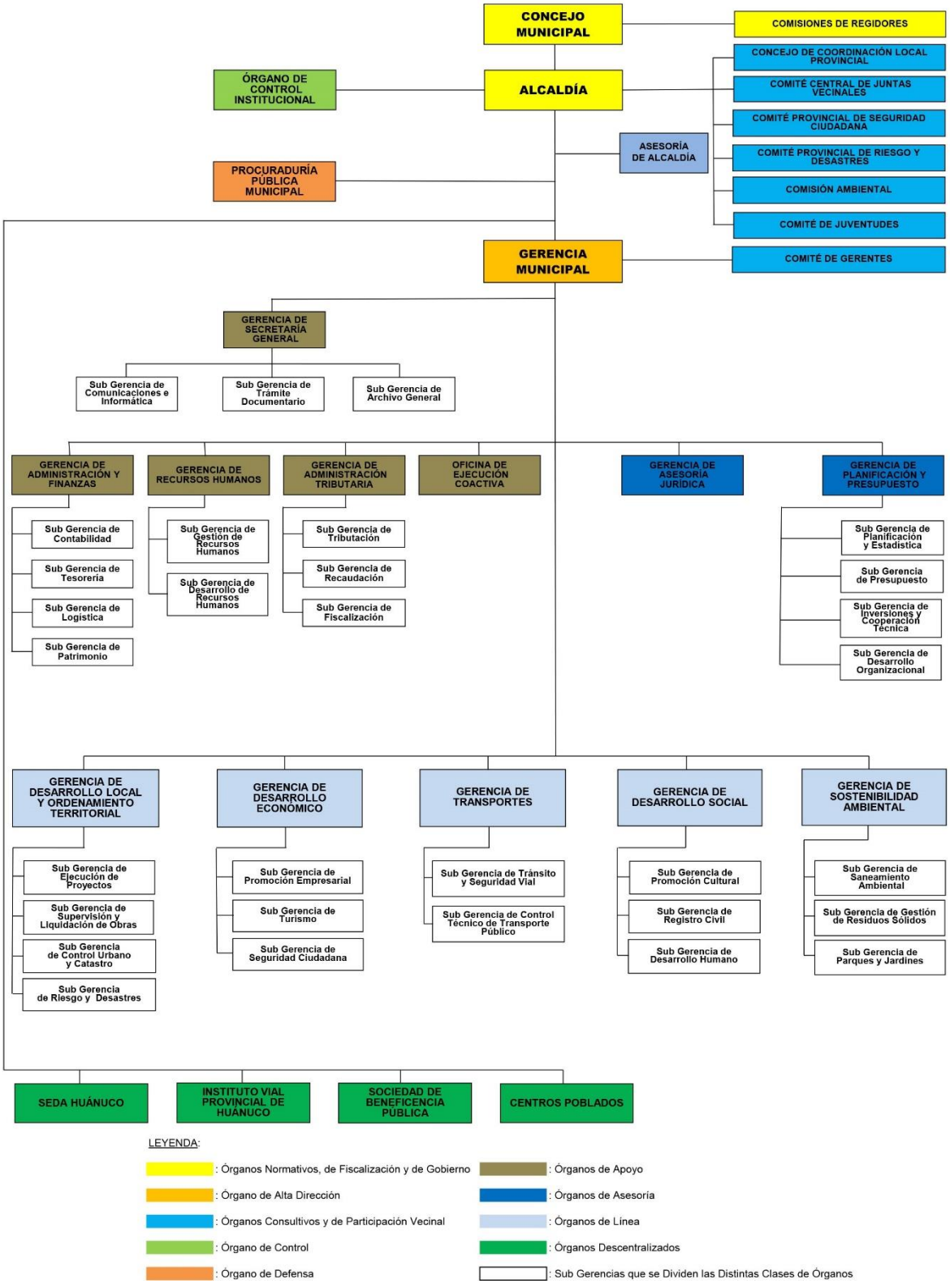

Figura 6. Estructura Orgánica

CAPITULO II

ASPECTOS DEL ÁREA

2.1. DESCRIPCIÓN DEL ÁREA

La oficina de informática se encuentra bajo la Gerencia de Secretaria General en el área de informática esta área se encarga de ver los siguientes aspectos:

Todo lo que son los equipos informáticos como ordenadores, laptop, impresoras, impresoras multifuncionales, escáner, proyectores multimedia, access point y otros equipos tecnológicos referentes al área.

El área de informática, también se encarga de la administración de la página web encargado, por un web master donde ahí se publican noticias boletines resoluciones ordenanzas, con el fin de informar a la ciudadanía de lo que sucede en la Municipalidad de Huánuco.

Como última tarea, el área de informática se encarga de realizar un análisis diseño y programación de aplicaciones para las distintas áreas con el fin de agilizar las búsquedas, guardar la información, imprimir reportes, teniendo un mejor manejo de la información para las gerencias que requieran.

CAPITULO III

IDENTIFICACIÓN DE LA SITUACIÓN PROBLEMATICA

3.1. PROBLEMA DE INVESTIGACIÓN

3.1.1. DESCRIPCIÓN DEL PROBLEMA

ISO 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2.

ISO 27001 puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Está redactada por los mejores especialistas del mundo en el tema y proporciona una metodología para implementar la gestión de la seguridad de la información en una organización. También permite que una empresa sea certificada; esto significa que una entidad de certificación independiente confirma que la seguridad de la información ha sido implementada en esa organización en cumplimiento con la norma ISO 27001.

En la actualidad, las empresas ya sean pública o privadas cuentan con sistemas de información que diariamente se enfrentan a factores internos y externos que amenazan la

integridad, disponibilidad y confidencialidad de su información. Siendo la información un activo fundamental para cualquier empresa, debiendo estar la información protegida bajo normas, controles y políticas de seguridad que garanticen la continuidad del negocio.

Con más frecuencia se han presentado incidentes a nivel mundial con respecto a ataque informáticos o fraudes, por eso es recomendable brindarle más importancia a la seguridad y si es necesario invertir para llevar una buena gestión, desarrollando las mejores prácticas para la prevención, detección y protección de los datos e información de la empresa.

En la actualidad la Municipalidad de Huánuco no cuenta con los controles, medidas o procedimientos de seguridad necesarios para resguardar sus activos de información. Barrantes (2012) indica que “tales como documentos, software, dispositivos físicos, personas, imagen, reputación y servicios, están expuestos a altos niveles de riesgos, frente a las diversas amenazas físicas y lógicas existentes:

- Estructurales (Incendios, inundaciones, humedad, cortes de electricidad, agua, refrigeración, comunicaciones, etc.)
- Hardware (fallo total o parcial de Servidores, Estaciones PC, portátiles, etc.)
- Software (Errores en los SO, BD, software base, Web servers, aplicaciones, elementos de seguridad, etc.)

- Información (Bases de datos, ficheros manuales, procedimientos, planes de contingencia, etc.)
- Personal (Errores y ataques de personal interno, externo, funciones, perfiles, formación, etc.)”(p.2)

El presente trabajo de investigación se basa en un Sistema de Gestión de Seguridad de la Información para la protección de los activos de la información enfocadas en la aplicación del estándar ISO 27001 en el área de informática.

La implementación de un sistema de gestión de seguridad en la información (Sistema de Gestión de Seguridad de la Información) es un punto clave con que debe trabajar el personal a cargo de la seguridad de la información en la institución, este sistema organiza los procedimientos para gestionar de una forma correcta la seguridad, permitiendo realizar análisis y autodiagnósticos para conocer el estado en que se encuentra, verificar falencias y establecer un plan de mejora.

3.1.2. FORMULACIÓN DEL PROBLEMA

3.1.2.1. PROBLEMA GENERAL

¿Cómo ayudará un Sistema de Gestión de la Seguridad de la Información basada en la norma **ISO 27001** para tener un control de los activos de información en el área de informática de la Municipalidad Provincial de Huánuco?

3.1.2.2. PROBLEMA ESPECIFICOS

- ¿Cuál es el alcance de las políticas del Sistema de Gestión de la seguridad de la Información para el área informática de la Municipalidad Provincial de Huánuco?
- ¿Qué metodología se usará para la gestión de los riesgos de los activos de información en el área de informática de la Municipalidad Provincial de Huánuco?
- ¿Cuáles son los controles adecuados para mitigar los riesgos de activos de información en el área de Informática de la Municipalidad Provincial de Huánuco?

3.1.3. OBJETIVO DE LA INVESTIGACIÓN

3.1.3.1. OBJETIVO GENERAL

Proponer un Sistema de Gestión de la Seguridad de la Información basado en la norma **ISO 27001** para la protección de los activos de información en el área de informática de la Municipalidad Provincial de Huánuco año **2019.**

3.1.3.2. OBJETIVOS ESPECIFICOS

- Definir las políticas y procedimientos para la protección de los activos en el área de informática de la Municipalidad Provincial de Huánuco.
- Identificar y evaluar los riesgos de seguridad de información para la protección de los activos en el

área informática de la Municipalidad Provincial de Huánuco.

- Diseñar los controles adecuados para mitigar los riesgos de los activos de información en el área de Informática de la Municipalidad Provincial de Huánuco.

3.1.4. JUSTIFICACIÓN DE LA INVESTIGACIÓN

Como la tecnología cada año avanza y se actualiza podemos estar expuestos a cualquier tipo de riesgos con los activos de información el impacto que puede causar, es muy dañino para la institución, para lo cual sería bueno utilizar una metodología y el uso de herramientas que nos ayuden a reducir cualquier riesgo.

El área de informática no tiene un diseño ni implementado un sistema de gestión de la seguridad de la información que garantice la integridad, disponibilidad y confidencialidad de la información mediante mecanismo de seguridad. Para esto se recomienda que se deben establecer lineamiento de seguridad de información para mitigar el riesgo.

La presente investigación busca mediante la aplicación del **ISO 27001** diseñar un sistema de gestión de la seguridad de la información (SGSI), que permita la buena gestión de los recursos informáticos asegurando su confidencialidad, integridad y disponibilidad.

El diseño de un Sistema de Gestión de la Seguridad de la Información será de vital importancia para salvaguardar la confidencialidad, integridad y disponibilidad de los activos de información en el área de informática de la Municipalidad Provincial de Huánuco.

3.1.5. LIMITACION DE LA INVESTIGACIÓN

3.1.5.1. ALCANCE DE LA INVESTIGACIÓN

La investigación se realizó en la Municipalidad Provincial de Huánuco en la Gerencia de Secretaria General, enfocado en el área de informática donde se propone un Sistema de Gestión de la Seguridad de la Información (SGSI), para mejorar la protección de los activos de la información.

3.1.5.2. LIMITACIONES DE LA INVESTIGACIÓN

Para la investigación a desarrollar se encontraron las siguientes limitaciones:

- Poca disponibilidad de tiempo para la investigación debido a la carga laboral del investigador.
- La investigación no tuvo dificultades con respecto al tema se contaba con el apoyo del área.

3.1.6. VIABILIDAD DE LA INVESTIGACIÓN

3.1.6.1. VIABILIDAD TÉCNICA

Es técnicamente posible la implementación de un sistema de gestión de la seguridad de la información

basado en la norma **ISO 27001** para mejorar la protección de los activos de Gestión de Seguridad de Información, ya que se dispone de los recursos físicos y lógicos necesarios para el desarrollo de la investigación.

3.1.6.2. VIABILIDAD ECONÓMICA

Es posible la implementación del Sistema de Gestión de la Seguridad de la Información debido a que la institución cuenta con los recursos necesarios para llevar dicha implementación.

3.2. MARCO TEORICO

3.2.1. ANTECEDENTES DE LA INVESTIGACIÓN

3.2.1.1. A NIVEL INTERNACIONAL

- **(Barragán Paguay, Góngora Zambrano, & Martínez Cárdenas, 2011)** desarrollo una investigación titulada "Implementación de Políticas de Seguridad Informática para la M.I. Municipalidad de Guayaquil aplicando la norma ISO/IEC 27002, previo a la obtención del título de Analista de Sistemas, el proyecto de titulación se pretende dar una adecuada solución de seguridad a la M.I. Municipalidad de Guayaquil, tomando base estándares internacionales.

  El primer capítulo presenta una introducción de lo que involucra un Sistema de Gestión de Seguridad de la

información, es decir concepciones básicas, consintiendo tener una visión general y clara en donde se establece objetivos y acciones forzosas para alcanzar que la entidad involucrada cuente con un acumulado de reglas y políticas para la seguridad y gestión de riesgos de la información.

En el segundo capítulo se presenta los antecedentes, objetivos y funciones desempeñadas dentro de la muy Ilustre Municipalidad de Guayaquil en donde se realizaría las Políticas de Seguridad de acuerdo a las Normas ISO/IEC 27001 y descripción de los departamentos y/o áreas en que se divide y su organigrama principal.

El capítulo tres del manual presenta la metodología PDCA y los conceptos por cada una de las etapas implicadas en el modelo. Se detalla el Alcance que se desea implantar indicando los lineamientos y principios a implementar, mantener y así mejorar la gestión de la seguridad de la información dentro del Municipio de Guayaquil.

El capítulo cuatro del presente proyecto describe la metodología MAGERIT con el concepto y ventajas principales de su implementación. Se detalla el inventario de Activos un exhaustivo análisis de Riesgo con sus apropiados Criterios de Valorización.

El capítulo cinco se explica la implementación de las Políticas, descripción y objetivos por cada una. Se especifica el Plan de tratamiento de Riesgos a utilizar para la gestión de riesgos que se encontró en el área de informática.

Y por último el capítulo seis son las estrategias de difusión que se aplicara para llegar a difundir las políticas dentro del departamento". (p.7)

- **(Romo Villafuerte & Valerezo Constante, 2012)**, previa la obtención del título de Ingeniero de Sistemas con mención en Telemática desarrollo una investigación titulada. "Análisis e implementación de la norma ISO 27002 para el departamento de sistemas de la Universidad Politécnica Salesiana Sede Guayaquil. El presente trabajo busca anunciar y orientar al lector en todo lo que corresponda las buenas prácticas de seguridad de la información las mismas que fueron creándose con el pasar del tiempo y todas los robos por fuga de información sean está impresa o no.

  En el primer capítulo podremos observar una pequeña pero importante introducción en la que se podrá recalcar la necesidad y evolución de la buena práctica de seguridad, así mismo se darán a conocer objetivos tanto generales como específicos que se tuvieron presentes en la elaboración de este proyecto, se

planeara algunos casos de los problemas más frecuentes que surgieron con la carencia de normas y/o políticas de seguridad de información.

En el segundo capítulo se ahondará más en el tema dando a conocer terminología básica y sustentando cada una de las partes que conforman esta tesis en las buenas prácticas de seguridad.

En el capítulo 3 se presentará una ruta para el cumplimiento de Políticas de Seguridad de la Información, donde se detallará las buenas prácticas que el departamento de sistemas de la Universidad Politécnica Salesiana sede Guayaquil debe seguir y cumplir paso a paso para poder adquirir el conocimiento necesario que le permitirá en base a las políticas establecer controles de seguridad y a su vez, para mitigar riesgos como por ejemplo perdida de información". (p.7)

3.2.1.2. A NIVEL NACIONAL

- **(Barrantes Porras & Hugo Herrera, 2012)**, para optar el título profesional de ingeniero de computación y sistemas. Desarrollo una investigación titulada "Diseño e Implementación de un Sistema de Gestión de Seguridad de Información en procesos Tecnológicos, para optar el título profesional de ingeniero de computación y sistemas en la actualidad, muchas empresas que están o desean

entrar en el ámbito financiero tiene problemas para proteger la seguridad de su información, en consecuencia, esta corre riesgos al igual que sus activos.

La intención de este trabajo se centró en la implementación de un Sistema de Gestión de la Seguridad de la información (SGSI), bajo una metodología de análisis y evaluación de riesgos desarrollada y planteada por los autores de este trabajo, también se usaron como referencias las normas ISO 27001_2005 e ISO 17799:2005.

Esta implementación permitió un gran aumento en la seguridad de los activos de información de la empresa Card Perú S.A., que garantiza que los riesgos de seguridad de información sean acreditados, asumidos, gestionados y minimizados de la forma documentada, sistemática, estructurada, repetible, eficiente y adaptable ante los cambios que se produzcan en los riesgos, entorno y las tecnologías". (p.3)

- **(Ccesa Quincho, 2017)**, para optar el título profesional de Ingeniero Informático. "Diseño de un Sistema de Gestión de la Seguridad de la Información bajo la NTP ISO/IEC 27001:2014 para la Municipalidad Provincial de Huamanga, 2016 para optar el título profesional de Ingeniero Informático, La información es considerada hoy en día el mayor activo que posee cualquier organización

y en consecuencia requiere de una protección adecuada. En el Perú, con el objetivo de establecer una adecuada gestión de la seguridad de la información que ayude a resguardar la confidencialidad, integridad y disponibilidad de la misma, se exige a las entidades públicas integrantes del sistema nacional de informática la implementación de la Norma Técnica Peruana NTP ISO/IEC 27001:2014 (Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información), pero el desconocimiento por parte de la alta dirección, la falta de presupuesto y falta de personal especializado ha ocasionado que no se cumplan con el cronograma establecido por el estado para su implementación. Se escogió como caso de estudio a la Municipalidad Provincial de Huamanga y para realizar el diseño de su SGSI se dividió la investigación en tres fases: en la primera fase se realizó el diagnóstico inicial de la entidad con respecto a la NTP ISO/IEC 27001:2014 y su posibilidad de aceptación, en la segundad fase se estudió a la organización y su contexto; se identificó el proceso crítico; se definió la política de seguridad, el alcance y se identificó al comité de seguridad de la información de la organización, en la tercera fase, siguiendo la metodología de análisis y gestión de riesgos adoptada, se identificó y valoró los

activos de información, se identificó las amenazas, se realizó el cálculo del impacto y del riesgo, se llegó a identificar las medidas de control necesarias para mitigar los riesgos a un nivel aceptable y finalmente se elaboró un documento denominado declaración de aplicabilidad que contiene la justificación de qué controles del Anexo A de la NTP ISO/IEC 27001:2014 pueden ser implementados en la organización". (p.12)

- **(Armas Huamán & Perez Romero, 2018)**, para optar el título de ingeniero de sistemas e informática. "Desarrollo de un SGSI para minimizar riesgos en los activos de información en la sub gerencia de informática y telecomunicaciones de la Municipalidad Distrital de Independencia 2016, para optar el título de ingeniero de sistemas e informática, el presente proyecto tiene como producto final el Desarrollo de un Sistema de Gestión de Seguridad de la Información para la Sub Gerencia de informática y telecomunicaciones de la Municipalidad Distrital de Independencia, el que se describe en el documento de aplicabilidad que al ser ejecutado tendrá como resultado un adecuado aseguramiento de la información manteniéndolo al margen o fuera de riesgos de activos de información.

  En este caso además de realizar el estudio en la subgerencia de Informática y Telecomunicaciones

realizaremos un estudio piloto, el área de Registro Civil ya que es uno de los procesos más vulnerables y expuesto, de esta manera se espera llegar a las otras dependencias y crear una cultura organizacional que involucre a la seguridad de la información.

Para este trabajo se desarrolló el Sistema de Gestión de Seguridad de la Información, se usó normas de la familia ISO/IEC 27000 y a su vez se utilizó la metodología MAGERIT, todo ello con el fin de poder identificar y mitigar los riesgos y amenazas a los que están expuestas la información, con las cuales se obtuvo como resultado la declaración de aplicabilidad". (p.7)

- **(Cruz Diaz & Fukusaki Infantas, 2017)**, para optar el título profesional de ingeniero de computación y sistemas. "Diseño e implementación de un sistema de gestión de seguridad de la información para proteger los activos de información de la clínica MEDCAM Perú S.A.C.

  La presente tesis tuvo como objetivo diseñar e implementar un Sistema de Gestión de Seguridad de la Información (SGSI) con el fin de salvaguardar los activos de información que influyan directamente en el cumplimiento de los objetivos de la empresa. Como metodología para el diseño de SGSI, se utilizó el método Deming o PDCA (Plan-Do-Check-Act), sugerida por la

norma ISO/IEC 27001, la cual parte de la identificación de los activos de información y, es a base de la clasificación de los mismos, que se determina el posible impacto ante un evento de pérdida, y se establecen acciones de respuesta para la mitigación de los riesgos a los que están expuestos los activos. Los controles en respuesta se obtuvieron un SGSI con lo que se logró minimizar los riesgos de amenazas y vulnerabilidades sobre los activos de información de MEDCAM Perú S.A.C. y así, lograr la confidencialidad, disponibilidad e integridad de la información. Concluimos que el beneficio más importante es asegurar los activos de información y así el cumplimiento de los objetivos de la empresa; así como, que cada SGSI debe estar acorde con el tamaño y madurez de los procesos de la empresa".(p.12)

3.2.1.3. A NIVEL LOCAL

- **(Paucar Falcón, 2017)**, para optar el título profesional de ingeniería de Sistema e Informática. "Implementación de un servidor de seguridad bajo el S.O. GNU/LINUX basado en la ISO 27002:2013 para mejorar la red de área local del área administrativa del Hospital de Contingencia Hermilio Valdizán Medrano de Huánuco, 2017. El presente estudio de investigación tuvo como fin el de implementar un servidor de seguridad utilizando el sistema operativo GNU/Linux bajo los controles del ISO

27002:2013, en el Hospital de Contingencia Hermilio Valdizán Medrano de la ciudad de Huánuco en el año 2017, en cuanto a la metodología se planteó bajo el enfoque cuantitativo, y el tipo aplicativo; porque se utilizó la tecnología para la solución de un problema, así mismo se empleó el diseño pre experimental de pre y post test se llevó a cabo un experimento en condiciones controladas. La población estuvo conformada por 320 trabajadores, solo del área administrativa del Hospital de Contingencia Hermilio Valdizán Medrano de la ciudad de Huánuco, y se determinó la muestra de forma no probabilística, de los cuales se permitió valorar algunos controles técnicos en base a las actividades de los trabajadores en la red de área local. En cuanto a la recolección de datos se usó la estadística descriptica mediante el uso de software SPSS. Se utilizó el sistema operativo GNU/Linux para dar soporte a la aplicación del servidor de seguridad usando los controles específicos números: 13.1.2 y 9.4 del ISO 27002:2013, se llevaron a cabo las pruebas de forma satisfactoria y cumpliendo el objetivo de dar seguridad a la red de área local del área administrativa del Hospital Mediante la implementación de dicho servidor".(p.8)

- **(Vilca Mosquera, 2017)**, para optar el título profesional de ingeniero de sistemas e informática. "Diseño e

implementación de un SGSI ISO 27001 para la mejora de la seguridad del área de recursos humanos de la empresa Geosurvey de la ciudad de Lima", La presente tesis tuvo como finalidad de implementar un sistema de gestión de la seguridad de la información bajo el ISO 27002 para mejorar la seguridad en cuanto al uso de los activos y tecnologías de la información en la empresa Geosurvey de la ciudad de Lima en el año 2016.

La metodología a emplearse fue bajo el enfoque cuantitativo y de tipo aplicativo; porque se manejó la tecnología como solución de un problema, así mismo se empleó el diseño pre experimental de pre y post test se llevó a cabo un experimento en condiciones controladas. Tanto la población como la muestra estuvo conformada por 33 empleados siendo no probabilística, se tomaron en cuenta todos los empleados de las diferentes áreas de la empresa. Para la recolección de datos se utilizó el cuestionario como técnica y el cuestionario de encuesta como instrumento para luego los datos ser procesados en el software estadístico SPSS. Se empleó las cuatro fases PDCA del ISO 27002, que permitió el diagnóstico de la gestión de riesgos de la empresa, la elaboración de la política de seguridad y así también el sistema de gestión de incidentes para poder controlar y mejorar la seguridad de la información de la empresa.(p.8)

3.2.2. BASES TEORICAS

Los conceptos a utilizar para el desarrollo de la tesina son los siguientes:

3.2.2.1. SGSI

El SGSI (Sistema de Gestión de la Seguridad de la Información) es el concepto central sobre el que se construye ISO 27001.

La gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización.

Este proceso es el que constituye un Sistema de Gestión de la Seguridad de la Información, que podría considerarse, por analogía con una norma tan conocida como ISO 9001, como el sistema de calidad para la seguridad de la información.

Garantizar un nivel de protección total es virtualmente imposible, incluso en el caso de disponer de un presupuesto ilimitado. El propósito de un sistema de gestión de la seguridad de la información es, por tanto, garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible,

eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

BENEFICIOS DE UN SGSI DE ACUERDO A ISO 27001

La certificación bajo la norma ISO 27001 de su Sistema de gestión de Seguridad de la Información aporta:

- Reduce el riesgo de que se produzcan pérdidas de información en las organizaciones. Por pérdidas también entendemos robos y corrupciones en la manipulación de la misma.
- Se hace una revisión continua de los riesgos a los que están expuestos los clientes. Adicionalmente, se hacen controles de manera periódica.
- Decretar una metodología gracias a la cual se puede gestionar la seguridad de la información de forma clara y concisa.
- Establece medidas de seguridad para que los propios clientes puedan acceder a la información.
- Al contar con dicho Sistema de Gestión, nos obliga a que se realicen auditorías externas de manera habitual y este hecho permite identificar las incidencias que pudiera haber en el Sistema de Gestión de Seguridad

de la Información, promoviendo de este modo a la mejora continua en la organización.

- Contar un Sistema de Gestión de la Seguridad de la Información da a la organización una garantía frente a clientes y socios estratégicos ya que muestra a la misma como un organismo preocupado por la confidencialidad y seguridad de la información que es depositada en la misma.

- Permite a las organizaciones proseguir operando con normalidad en caso de ocurrir problemas importantes.

- Se puede hacer una unificación conjunta con otros Sistemas de Gestión Normalizados tales como ISO 9001, ISO 14001, OHSAS 18001, entre otras.

- Permite que la organización esté cumpliendo con la legislación vigente sobre el manejo de información personal y propiedad intelectual.

- La seguridad en la información que ofrece constituir un Sistema de Gestión de la Seguridad de la Información de acuerdo a ISO 27001 beneficia a una reducción de los costes y un mejor funcionamiento de los procesos.

- Se convierte en un elemento próspero para la empresa frente a la competencia, pues el contar con un Sistema de Gestión de la Seguridad de la Información le hace ampliar su imagen a nivel internacional.

- Contribuye al incremento en la motivación del personal, ya que se desempeñan en una organización comprometida con la seguridad de la información.

3.2.2.2. SEGURIDAD INFORMATICA

Informática es el tratamiento automático de la información. Como tal, la informática designa a un grupo de conocimientos teóricos y prácticos, relativos al ámbito de la ciencia y de la tecnología, que se fusionan para posibilitar el tratamiento racional y automático de la información mediante sistemas informáticos o computadoras.

Las tareas principales de la informática son guardar, procesar y transferir la información.

Según la Real Academia Española de la Lengua, la palabra informática pasa al español a través del francés informatique, contracción de las palabras information, que traduce ‘información’, y automatique, ‘automática’, aunque su origen se registra en el alemán informatik.

Como disciplina de estudio, la ciencia de la informática o ciencia de la computación se encarga de aprender científicamente los límites físicos y teóricos de las computadoras, su procesamiento, la arquitectura de redes, el almacenamiento de la información, incluso, la inteligencia artificial, entre otros.

La ingeniería informática por otro lado aplica la teoría de la ciencia de la computación en métodos, técnicas, procesos, desarrollo y aplicación de la misma.

Por tanto, la informática es una de ciencia de vital importancia en la actualidad, ya que son muchas las aplicaciones que tiene a fin de facilitar el proceso, almacenamiento y análisis de datos, así como, la comunicación.

Informática también se refiere a lo que es perteneciente o relativo a la informática: “Javier es un experto en seguridad informática”. Por extensión, también es empleada, tanto en masculino como en femenino, para designar aquella persona que trabaja en informática.

3.2.2.3. SEGURIDAD DE LA INFORMACIÓN

Siempre que platicamos de una empresa, institución, organismo o entidad entre otras organizaciones similares, es importante que la información que se encuentre integrada en ellas esté resguardada bajo unas buenas medidas de seguridad. Es ahí donde brota la seguridad de la información para mantener a salvo todos los datos importantes de la empresa, desde los que pertenecen a la propia organización como los vinculados con trabajadores y clientes. A veces nos equivocamos este tipo de seguridad con la seguridad informática, pero hay que tener en cuenta que esta

última solo se centra en salvaguardar los datos dentro de un sistema informático, mientras que la información en general puede darse en otros muchos contextos entre los usuarios.

La seguridad de la información tiene como objetivo primordial proteger los datos de las empresas. Pero este concepto es en términos generales, puesto que el sistema lo que va a hacer es proteger tres aspectos fundamentales: la confidencialidad, la disponibilidad y la integridad. Para llevar a cabo estas acciones se deberán establecer estrategias donde se redacten las políticas de actuación para cada uno de estos casos. También habrá que establecer el uso de las tecnologías, incluir controles de seguridad y todos los procesos que se van a llevar a cabo para detectar los riesgos a los que se puede ver expuesto el sistema. Teniendo en cuenta todas estas cosas: ¿en qué consisten esos tres aspectos fundamentales?

Confidencialidad

A través de ella la seguridad de la información garantiza que los datos que están guardados en el sistema no se divulguen a otras entidades o individuos que no están autorizados para acceder a esa información.

Disponibilidad

Toda la información que se encuentre almacenada en el sistema debe de estar a disposición de los usuarios autorizados a cualquier momento que ellos necesiten acceder a ella.

Integridad

Para que el sistema sea veraz los datos no deben manipularse. Así se garantiza que la información recogida sea exacta y no haya sido modificada a no ser que algún usuario autorizado lo haya hecho por orden expresa.

3.2.2.4. ACTIVOS DE INFORMACIÓN

El concepto de activo son los bienes, derechos y otros recursos de los que cuenta una empresa, pudiendo ser, por ejemplo, muebles, construcciones, equipos informáticos o derechos de cobro por servicios prestados o venta de bienes a clientes. También, se incluirían aquellos de los que se espera obtener un beneficio económico en el futuro.

Los activos de información son los recursos que utiliza un Sistema de Gestión de la Seguridad de la Información para que las organizaciones funcionen y consigan los objetivos que se han propuesto por la alta dirección.

Los activos se encuentran asociados, de forma directa o indirectamente, con las demás entidades. Puede ser que le interese leer este artículo ISO 27001: ¿Cómo analizar y gestionar los riesgos en un SGSI?

Un proyecto de seguridad tiene el objetivo de controlar la seguridad de los activos de información que generan el dominio en el estudio de proyectos. El límite del conjunto de activos del dominio no imposibilita la consideración de las relaciones en materia de seguridad de dichos activos de información con el entorno. Uno de los primeros pasos que debe seguir la entidad para adaptarse a la norma **ISO 27001** es llevar a cabo un inventario de activos de información. Tendrán los activos de información que representan algún valor para la empresa y que quedan dentro del alcance del SGSI. En principio puede parecer un poco abrumador para un principiante, por la gran cantidad de activos que se van ocurriendo. Por este motivo se decide comenzar por clasificarlos de alguna forma. Entre las muchas formas que se encuentran podemos elegir la definida por los expertos. Parece la manera más completa. Muestra ejemplo de cada tipo y es válido para entidades de muy diferente naturaleza. Debido a que los activos de información son cambiantes, mañana puede ser que la situación sea

diferentes y mucho más distinta en unas semanas, meses o años. Así que es recomendable mantener vivo el inventario de activos que hagamos. Se debe incluir la revisión del Sistema de Gestión de Seguridad de la Información. Es necesario actualizar los procesos como parte de la mejora continua.

Activos de información pura

Datos digitales

- Personales
- Financieros
- Legales
- Investigación y desarrollo
- Estratégicos
- Comerciales
- Correo electrónico
- Contestadores automáticos
- Bases de datos
- Unidades lógicas
- Copias de seguridad

Activos tangibles

- Personales
- Financieros
- Legales
- Investigación y desarrollo
- Estratégicos y comerciales
- Correo electrónico
- Otros materiales de copia de seguridad
- Llaves de oficinas

- Otros medios de almacenamiento

Activos intangibles

- Conocimiento
- Relaciones
- Secretos comerciales
- Licencias
- Patentes
- Experiencia
- Conocimientos técnicos
- Imagen corporativa
- Marca
- Reputación comercial
- Confianza de los clientes
- Ventaja competitiva
- Ética
- Productividad

Software de aplicación

- Propietario desarrollo por la organización
- Cliente
- Planificación de recursos empresariales
- Gestión de la información
- Utilidades
- Herramientas de bases de datos
- Aplicaciones de comercio electrónico
- Middleware

Sistemas operativos

- Servidores
- Ordenadores de sobremesa
- Ordenadores contrales
- Dispositivos de red
- Dispositivos de mano e incrustados

Activos físicos

Infraestructura de TI

- Edificios
- Centros de datos
- Habitaciones de equipos y servidores
- Armarios de red
- Oficinas
- Escritorios
- Cajones
- Archivadores
- Salas de almacenamiento de medios físicos
- Cajas de seguridad
- Dispositivos de identificación
- Autentificación
- Control de acceso al personal

Controles de entorno de TI

- Equipos de alarma
- Supresión contra incendio
- Sistemas de alimentación ininterrumpida
- Alimentación de potencia
- Acondicionadores
- Filtros
- Supresores de potencia
- Deshumificadores
- Refrigeradores
- Alarmas de aire
- Alarmas de agua

Hardware de TI

- Dispositivos de almacenamiento
- Ordenadores de mesa
- Estaciones de trabajo
- Ordenadores portátiles

- Equipos de mano
- Servidores
- Módems
- Líneas de terminación de red
- Dispositivos de comunicaciones
- Equipos multifunción

Activos de servicios de TI

- Servicios de autenticación de usuario
- Administración de procesos
- Enlaces
- Cortafuegos
- Servidores proxy
- Servicios de red
- Servicios inalámbricos
- Anti-spam
- Virus
- Spyware
- Detección y prevención de intrusiones
- Teletrabajo
- Seguridad
- Correo electrónico
- Mensajería instantánea
- Servicios web
- Contratos de soporte
- Mantenimiento de software

Activos humanos

Empleados

- Personal y directivos
- Participar los que tienen roles de gestión como altos cargos
- Arquitectos de software y desarrolladores

- Administradores de sistemas
- Administradores de seguridad
- Operadores
- Abogados
- Auditores
- Usuarios con poder
- Expertos en general

Externos

- Trabajadores temporales
- Consultores externos
- Asesores especialistas
- Contratistas especializados
- Proveedores
- Socios

3.2.2.5. GESTIÓN DE RIESGO

La gestión de riesgos implica seleccionar e implantar las medidas técnicas y organizativas necesarias para impedir, reducir o controlar los riesgos identificados, de forma que los perjuicios que puedan causar se eliminen o, si esto no es posible, se reduzcan lo máximo posible.

Un resultado del análisis de riesgos habrá sido el criterio para establecer cuáles van a ser los niveles de riesgo aceptables y, en consecuencia, cuáles van a ser los niveles inaceptables y que por lo tanto son susceptibles de ser gestionados.

La gestión de los riesgos tiene como objetivo reducir los riesgos que estén por encima de los niveles

aceptables, a niveles que puedan ser asumidos por la organización.

Una vez que conocemos los riesgos de la organización y decidido el tratamiento que se le va a dar para cada uno de los activos, se deben tomar acciones en consecuencia. En resumen, la Gestión de Riesgo es un método para determinar, analizar, valorar y clasificar el riesgo, para posteriormente implementar mecanismos que permitan controlarlo.

Los cuatro tipos de tratamiento requieren de acciones de distinta naturaleza:

- **Mitigar el riesgo.**

Reducirlo mediante la implantación de controles que reduzcan el riesgo a un nivel aceptable, implica seleccionar dichos controles, definir y documentar los métodos para ponerlos en marcha y gestionarlos.

- **Asumir el riesgo.**

La Dirección asume el riesgo ya que está por debajo de un valor de riesgo aceptable, simplemente requiere que quede documentado que la dirección conoce y acepta estos riesgos. Los riesgos que se han asumido han de ser controlados y revisados periódicamente de cara a evitar que evolucionen y se conviertan en riesgos mayores.

- **Transferir el riesgo a un tercero.**

Como, ejemplo, asegurando el activo que tiene el riesgo o subcontratando el servicio. Deben evaluarse las opciones y tomar las acciones pertinentes para ejecutar la opción escogida, en función del valor del activo y del coste de realizar esta transferencia (no sólo coste económico sino también los riesgos que conlleva esta transferencia en cuanto a la inclusión de un tercero).

- **Eliminar el riesgo.**

Aunque no suele ser la opción más viable, ya que puede resultar difícil o demasiado costoso, si se cree posible o necesario, habrá que establecer los pasos para conseguirlo: eliminar el activo, eliminar el proceso o incluso el área de negocio que es la fuente del riesgo.

No caben más acciones a la hora de gestionar los riesgos para la correcta implantación de un sistema de gestión de la seguridad de la información, ya que una organización que conoce sus riesgos jamás podrá ignorarlos, puesto que, de este modo, no estaría vigilando que no se convirtiesen en riesgos que la organización no es capaz de asumir o que, por no haberlos tenido en cuenta, se materialicen y den lugar a un incidente de seguridad.

Una vez decididas las acciones a tomar, se debe realizar un nuevo análisis de riesgos, teniendo en cuenta la nueva situación considerando que los controles y medidas que se ha decidido implantar van a reducir en mayor o menor medida el riesgo que existía, ya que ese es su objetivo. El nivel de riesgo resultante de este segundo análisis es el riesgo residual. Este se define como el riesgo remanente que existe después de que se hayan tomado las medidas de seguridad apropiadas.

En una organización nunca se podrá eliminar totalmente el riesgo, siempre quedará un cierto nivel de riesgo, por lo que es importante que todos los riesgos residuales sean aceptados por la alta Dirección.

A continuación, algunas definiciones de términos importantes que se ven en la gestión de riesgos.

- **Amenazas**

En las organizaciones, los activos de información están sujetos a distintas formas de amenazas. Una amenaza es todo aquello, ya sea físico o lógico que puede causar un incidente no deseado, generando daños materiales o inmateriales a la organización y a sus activos, como la perdida de información, o de su privacidad, o bien un fallo en los equipos físicos.

Las amenazas conviene clasificarlas por su naturaleza, para así facilitar su ubicación. Se tienen seis tipos de amenazas:

- ✓ Amenazas naturales (inundaciones, tsunamis o maremotos, tornados, huracanes, sismos, tormentas, incendios forestales).
- ✓ Amenazas a instalaciones (fuego, explosión, caída de energía, daño de agua, perdida de acceso, fallas mecánicas).
- ✓ Amenazas humanas (huelgas, epidemias, materiales peligrosos, problemas de transporte, pérdida de personal clave).
- ✓ Amenazas tecnológicas (virus, hacking, pérdida de datos, fallas de hardware, fallas de software, fallas en la red, fallas en las líneas telefónicas).
- ✓ Amenazas operacionales (crisis financieras, perdida de suplidores, fallas en equipos, aspectos regulatorios, mala publicidad).
- ✓ Amenazas sociales (motines, (motines, protestas, sabotaje, vandalismo, bombas, violencia laboral, terrorismo).

- Vulnerabilidades

Las vulnerabilidades son debilidades de seguridad asociadas con los activos de información de una organización.

Las vulnerabilidades pueden clasificarse en las siguientes categorías:

- ✓ Seguridad de los recursos humanos (falta de entrenamiento en seguridad, carencia de toma de conciencia en seguridad, falta de mecanismos de monitoreo, falta de políticas para el uso correcto de las telecomunicaciones, no eliminar los accesos al término del contrato de trabajo, carencia de procedimiento que asegure la entrega de activos al término del contrato de trabajo, empleados desmotivados).
- ✓ Control de acceso (Segregación inapropiada de redes, falta de política sobre escritorio y pantalla limpia, falta de protección al equipo de comunicación móvil, política incorrecta para control de acceso, password sin modificarse).
- ✓ Seguridad física y ambiental (control de acceso físico inadecuado a oficinas, salones y edificios, ubicación en áreas sujetas a inundaciones, almacenes desprotegidos, carencia de programas

para sustituir equipos, mal cuidado de equipos, susceptibilidad de equipos a variaciones de voltaje).

- ✓ Gestión de operaciones y comunicación (complicadas interfaces para usuarios, control de cambio inadecuado, gestión de red inadecuada, carencia de mecanismos que aseguren el envío y recepción de mensajes, carencia de tareas segregadas, carencia de control de copiado, falta de protección en redes públicas de conexión).

- ✓ Mantenimiento, desarrollo y adquisición de sistemas de Información (protección inapropiada de llaves criptográficas, políticas incompletas para el uso de criptografía, carencia de validación de datos procesados, carencia de ensayos de software, documentación pobre de software, mala selección de ensayos de datos).

- Impacto

El impacto en un activo es la consecuencia sobre éste de la materialización de una amenaza. De forma dinámica, es la diferencia en las estimaciones del estado de seguridad del activo antes y después de la materialización de la amenaza sobre éste.

- Riesgos

El riesgo es la posibilidad de que se produzca un impacto determinado en un activo, en un dominio o en toda la organización.

En el cálculo del riesgo tiene gran influencia la evaluación del impacto, que es un proceso difícil. El nivel del riesgo depende de la vulnerabilidad y del impacto.

El proceso de identificación y evaluación de riesgos y el de clasificación de activos, permite determinar qué tan expuestos se encuentran los activos de información a ataques por la presencia de vulnerabilidades propias o inherentes a la actividad de la organización.

También podemos decir que es una situación que expone a un objeto a que pueda ser afectado o dañado. Extendiendo más el concepto de riesgo, se puede determinar que esta situación tiene cierto grado de probabilidad de generar un incidente en el cual el objeto de estudio – en el caso de un proyecto de Sistema de Gestión de la Seguridad de la Información sería el activo de información – pueda resultar afectado. De esta forma, en un sentido más amplio, se puede definir al riesgo como la combinación de la probabilidad de que ocurra un incidente con las consecuencias que generaría el mismo en el caso de que se materialice.

Existen muchas clasificaciones para tipificar los riesgos:

- ✓ Riesgo inherente: existencia de un error material o significativo sin un control compensatorio.
- ✓ Riesgos de control: existencia de un error que no pueda ser detectado por el sistema de controles establecido.
- ✓ Riesgos de detección: mal uso de procedimientos de detección de errores por parte de un auditor, que lleven a indicar que no existen errores donde si los haya.
- ✓ Riesgos de negocio.
- ✓ Otros riesgos generales propios de la naturaleza de la auditoría.

- Controles

Son las políticas, procedimientos, prácticas y estructuras organizacionales para reducir riesgos y que además proveen cierto grado de certeza de que se alcanzaran los objetivos del negocio.

Existen varias formas de establecer controles sobre riesgos:

- ✓ Disuasivos: su presencia disuade de la comisión de acciones en contra de alguna política o

procedimiento establecido y considerado correcto. Por ejemplo: cámaras de vigilancia.

- ✓ Preventivos: detectan problemas antes que ocurran por medio de monitoreo constante. Por ejemplo: políticas de contratación.
- ✓ Defectivos: detectan y reportan los problemas suscitados por errores u omisiones, en el momento en que éstos ocurren. Por ejemplo: Uso de antivirus.
- ✓ Correctivos: minimizan el impacto de una amenaza ya consumada. Por ejemplo: Planes de contingencia. Propios

3.2.2.6. FAMILIA ISO 27000

ISO 27000 es un conjunto de estándares internacionales sobre la Seguridad de la Información. La familia ISO 27000 contiene un conjunto de buenas prácticas para el establecimiento, implementación, mantenimiento y mejora de Sistemas de Gestión de la Seguridad de la Información.

Contiene el vocabulario en el que se apoyan el resto de normas. Es similar a una guía/diccionario que describe los términos de todas las normas de la familia.

Asimismo, los pilares principales de la familia 27000 son las normas 27001 y 27002. La principal diferencia entre estas dos normas, es que 27001 se basa en una

gestión de la seguridad de forma continuada apoyada en la identificación de los riesgos de forma continuada en el tiempo. En cambio, 27002, es una mera guía de buenas prácticas que describe una serie de objetivos de control y gestión que deberían ser perseguidos por las organizaciones.

3.2.2.7. FAMILIA ISO 27001

Es el conjunto de requisitos para implementar un SGSI. Es la única norma certificable de las que se incluyen en la lista y consta de una parte principal basada en el ciclo de mejora continua y un Anexo A, en el que se detallan las líneas generales de los controles propuestos por el estándar.

Análisis de riesgo

La norma exige que la empresa haga un análisis de riesgos de seguridad periódicamente y siempre que se propongan o se establezcan cambios significativos. Para que este análisis se haga de la manera correcta, es necesario establecer criterios de aceptación de riesgo, así como la definición de cómo esos riesgos serán medidos. También se deben evaluar las posibles consecuencias de los riesgos identificados, la probabilidad de que ocurran y sus niveles.

Compromiso de alta dirección

La norma también exige que la alta dirección demuestre compromiso con el SGSI, además de ser esa parte de la empresa ella misma la responsable por la seguridad de la información. Los líderes son también responsables de asegurar que todos los recursos para la implantación del sistema estén disponibles y asignados correctamente, y además tienen la obligación de orientar a los colaboradores para que el sistema sea verdaderamente eficiente.

Definición de objetivos y estrategias

Durante la planificación, la empresa necesita tener muy claro cuáles son sus objetivos de seguridad y cuáles serán las estrategias establecidas para alcanzar esos objetivos. Los objetivos, sin embargo, no pueden ser genéricos, deben ser mensurables y tener en cuenta los requisitos de seguridad.

Recursos y competencias

La organización también debe garantizar que todos los recursos necesarios no sólo para la implementación, sino que también para el mantenimiento del sistema estén disponibles. Además, es necesario establecer cuáles son las competencias necesarias y garantizar que las personas responsables sean suficientemente calificadas, incluso con documentación comprobatoria.

3.2.2.8. FAMILIA ISO 27002

Se trata de una recopilación de buenas prácticas para la Seguridad de la Información que describe los controles y objetivos de control. Actualmente cuentan con 14 dominios, 35 objetivos de control y 114 controles.

La parte principal de la norma se encuentra distribuida en las siguientes secciones, que corresponden a controles de seguridad de la información. Es importante recordar que la organización puede utilizar esas directrices como base para el desarrollo del SGSI. Como sigue:

Sección 5 – Política de Seguridad de la Información

Se debe crear un documento sobre la política de seguridad de la información de la empresa, que debe contener los conceptos de seguridad de la información, una estructura para establecer los objetivos y las formas de control, el compromiso de la dirección con la política, entre tantos otros factores.

Sección 6 – Organización de la Seguridad de la Información

Para implementar la Seguridad de la Información en una empresa, es necesario establecer una estructura para gestionarla de una manera adecuada. Para ello,

las actividades de seguridad de la información deben ser coordinadas por representantes de la organización, que deben tener responsabilidades bien definidas y proteger las informaciones de carácter confidencial.

Sección 7 – Gestión de activos

Activo, según la norma, es cualquier cosa que tenga valor para la organización y que necesita ser protegido. Pero para ello los activos deben ser identificados y clasificados, de modo que un inventario pueda ser estructurado y posteriormente mantenido. Además, deben seguir reglas documentadas, que definen qué tipo de uso se permite hacer con dichos activos.

Sección 8 – Seguridad en recursos humanos

Antes de la contratación de un empleado – o incluso de proveedores – es importante que sea debidamente analizado, principalmente si se trata de información de carácter confidencial. La intención de esta sección es mitigar el riesgo de robo, fraude o mal uso de los recursos. Y cuando el empleado esté trabajando en la empresa, debe ser consciente de las amenazas relativas a la seguridad de la información, así como de sus responsabilidades y obligaciones.

Sección 9 – Seguridad física y del medio ambiente

Los equipos e instalaciones de procesamiento de información crítica o sensible deben mantenerse en áreas seguras, con niveles y controles de acceso apropiados, incluyendo protección contra amenazas físicas y ambientales.

Sección 10 – Seguridad de las operaciones y comunicaciones

Es importante que estén definidos los procedimientos y responsabilidades por la gestión y operación de todos los recursos de procesamiento de la información. Esto incluye la gestión de servicios tercerizados, la planificación de recursos de los sistemas para minimizar el riesgo de fallas, la creación de procedimientos para la generación de copias de seguridad y su recuperación, así como la administración segura de las redes de comunicaciones.

Sección 11 – Control de acceso

El acceso a la información, así como a los recursos de procesamiento de la información y los procesos de negocios, debe ser controlado con base en los requisitos de negocio y en la seguridad de la información. Debe garantizarse el acceso de usuario autorizado y prevenido el acceso no autorizado a los sistemas de información, a fin de evitar daños a

documentos y recursos de procesamiento de la información que estén al alcance de cualquiera.

Sección 12 – Adquisición, desarrollo y mantenimiento de sistemas

Los requisitos de seguridad de los sistemas de información deben ser identificados y acordados antes de su desarrollo y/o de su implementación, para que así puedan ser protegidos para el mantenimiento de su confidencialidad, autenticidad o integridad por medios criptográficos.

Sección 13 – Gestión de incidentes de seguridad de la información

Los procedimientos formales de registro y escalonamiento deben ser establecidos y los empleados, proveedores y terceros deben ser conscientes de los procedimientos para notificar los eventos de seguridad de la información para asegurar que se comuniquen lo más rápido posible y corregidos en tiempo hábil.

Sección 14 – Gestión de continuidad del negocio

Los planes de continuidad del negocio deben ser desarrollados e implementados, con el fin de impedir la interrupción de las actividades del negocio y asegurar

que las operaciones esenciales sean rápidamente recuperadas.

Sección 15 – Conformidad

Es importante evitar la violación de cualquier ley criminal o civil, garantizando estatutos, regulaciones u obligaciones contractuales y de cualesquiera requisitos de seguridad de la información. En caso necesario, la empresa puede contratar una consultoría especializada, para que se verifique su conformidad y adherencia a los requisitos legales y reglamentarios.

3.2.2.9. FAMILIA ISO 27003

Es una guía de ayuda en la implementación de un SGSI. Sirve como apoyo a la norma 27001, indicando las directivas generales necesarias para la correcta implementación de un SGSI. Incluye instrucciones sobre cómo lograr la implementación de un SGSI con éxito.

3.2.2.10. FAMILIA ISO 27004

Describe una serie de recomendaciones sobre cómo realizar mediciones para la gestión de la Seguridad de la Información. Especifica cómo configurar métricas, qué medir, con qué frecuencia, cómo medirlo y la forma de conseguir objetivos.

3.2.2.11. FAMILIA ISO 27005

Es una guía de recomendaciones sobre cómo abordar la gestión de riesgos de seguridad de la información que puedan comprometer a las organizaciones. No especifica ninguna metodología de análisis y gestión de riesgos concreta, pero incluye ejemplos de posibles amenazas, vulnerabilidades e impactos.

3.2.2.12. FAMILIA ISO 27006

Es un conjunto de requisitos de acreditación para las organizaciones certificadoras.

3.2.2.13. FAMILIA ISO 27007

Es una guía para auditar SGSI. Establece qué auditar y cuándo, cómo asignar los auditores adecuados, la planificación y ejecución de la auditoría, las actividades claves, etc.

3.2.2.14. MAGERIT

El método MAGERIT, son las siglas de Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de la Administraciones, dicho método cubre la fase AGR (Análisis y Gestión de Riesgos). Si hablamos de Gestión global de la Seguridad de un Sistema de Seguridad de la Información basado en ISO 27001, MAGERIT, es el núcleo de toda actuación organizada en dicha materia, ya que influye en

todas las fases que sean de tipo estratégico y se condiciona la profundidad de las fases de tipo logístico.

El Consejo Superior de Informática ha sido el encargado de elaborar la primera versión de MAGERIT, con lo que promueve su utilización como respuesta a la dependencia creciente de toda la sociedad respecto a las Tecnologías de la Información. MAGERIT se encuentra muy relacionada con la generación en la que se utilizan los medios electrónicos, informáticos y telemáticos, lo que genera grandes beneficios para los empleados y los ciudadanos, aunque también puede dar lugar a diferentes riesgos que se tienen que minimizar con medidas de seguridad que generan confianza. **MAGERIT** facilita que se pueda llevar a cabo:

- El análisis de riesgo en cualquier tipo de Sistema de Seguridad de la Información (SSI), así como todos sus elementos, obteniendo un índice único en el que se realicen las estimaciones de su vulnerabilidad ante todas las posibles amenazas y el impacto que puede generar en la empresa.
- La gestión de riesgos, se basa en todos los resultados obtenidos durante el análisis que

hemos hecho anteriormente, se seleccionan medidas de seguridad adecuadas para poder conocer, prevenir, impedir, recudir o controlar todos los riesgos que se han identificado, pudiendo de este modo reducir al mínimo la potencialidad del riesgo.

El objetivo perseguido en sucesivas versiones de MAGERIT es la evaluación, homologación y certificación de Seguridad de Sistemas de Información (SSI) según ISO 27001:

- Se debe tener como referencia los criterios de ITSEC de Evaluación de la Seguridad de las Tecnologías de la Información, gracias a una recomendación del Consejo Europeo.
- Se tiene en cuenta también la referencia de los Criterios Comunes de Evaluación de la Seguridad de los Productos y Sistema de Información.
- Utilizando MAGERIT cuando se requiere un Análisis y Gestión de Riesgos (AGR) para poder evaluar los criterios de seguridad.

MAGERIT ha sido editado en un directorio que se encuentra compuesto por un conjunto de seis guías y un panel de herramientas de apoyo, con sus correspondientes guías de uso.

La Guía de Aproximación se encuentra orientada a identificar todas las existencias de posibles riesgos, se presenta de forma en la que la gestión de la Seguridad de Sistemas de Información (SSI) en la fase de análisis y gestión de riesgos que cubre MAGERIT establece un punto de arranque sobre las medidas que se deben tomar a la hora de disponer y ejecutar.

La Guía de Procedimientos junto a la Guía de Técnicas forman parte del núcleo del método. Ambas se unen en un conjunto perfectamente autosuficiente y con el contenido con el que cuenta basta para entender que la terminología y realizar el análisis y gestión de riesgo de cualquier Sistema de la Información. Es entonces donde enlazamos la utilización de herramientas construidas en torno a MAGERIT, por lo que es conveniente que se estudie el sistema.

La Guía de Procedimientos integra también, los resultados de las tareas que se indican en la Guía para responsables del dominio protegido y por otro lado se enlaza la Guía para desarrolladores de aplicaciones que facilitan la inserción de medidas de seguridad adecuadas en proyectos.

MAGERIT tiene una visión estratégica global de la Seguridad de los Sistemas de Información ISO 27001,

esta visión comienza en un modelo de análisis y gestión de riesgos que comprende tres modelos: entidades, eventos y procesos como podemos ver:

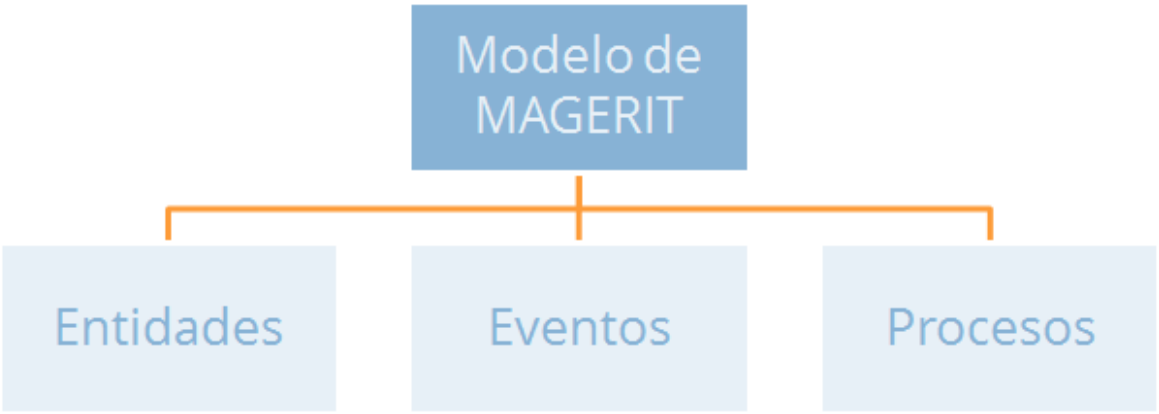

Figura 7. Visión Estratégica de Magerit

3.2.3. DEFINICION CONCEPTUAL

3.2.3.1. ISO

Las siglas ISO representan a la Organización Internacional para la Estandarización; organismo responsable de regular un conjunto de normas para la fabricación, comercio y comunicación en todas las industrias y comercios del mundo. Este término también se les adjudica a las normas fijadas por el

mismo organismo, para homogeneizar las técnicas de producción en las empresas y organizaciones internacionales.

Esta organización surge en 1947, una vez finalizada la segunda guerra mundial, transformándose en una entidad dedicada a fomentar la creación de normas y regulaciones de carácter internacional para la elaboración de todos los productos, a excepción de aquellos pertenecientes al área de la electrónica y la electricidad. De esta manera se garantiza calidad en todos los productos aunado al respeto por las políticas de protección ambiental.

En la actualidad la ISO tiene su sede en Ginebra, Suiza y cuenta con delegaciones de diversos gobiernos y otros entes similares. Sin embargo, y a pesar de su alta influencia a nivel mundial, el acatamiento de estas normas es de manera voluntaria, ya que la ISO no tiene poder para imponer sus regulaciones.

3.2.3.2. PDCA

El PDCA es una herramienta de la Calidad utilizada en el control de procesos, que tiene como foco la solución de problemas. Su aplicación consiste en cuatro fases:

P (Plan: Planificar): selección de un proceso, actividad o máquina que necesite de mejora y elaboración de

medidas claras y ejecutables, siempre orientadas hacia la obtención de los resultados esperados.

D (Do: Hacer): Implementación del plan elaborado y seguimiento de su progreso.

C (Check: Verificar): Análisis de los resultados obtenidos con la ejecución del plan y, en caso necesario, reevaluación del plan.

A (Act: Actuar): Si ha tenido éxito, el nuevo proceso se documenta y se transforma en un nuevo estándar.

3.2.3.3. SEGURIDAD

El término seguridad posee múltiples usos. A grandes rasgos, puede afirmarse que este concepto que proviene del latín securitas. En informática se habla de dos tipos de seguridades, la física (barreras físicas que impiden el paso al sistema de cualquier persona no acreditada. Se realiza a través de aplicaciones y procedimientos específicos que tienen el objeto de bloquear el acceso a dichos individuos) y la lógica (las formas en las que se desempeña este tipo de seguridad es a través de encriptación de códigos, de modo que no puedan ser leídos o traducidos por los intrusos que pudieran sobre pasar las barreras físicas, códigos de autenticación y antivirus o pared de fuego,

en el caso de usar un sistema operativo como Windows).

3.2.3.4. MAGERIT

Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.

3.2.3.5. VULNERABILIDAD

Vulnerabilidad es el riesgo que una persona, sistema u objeto puede sufrir frente a peligros inminentes, sean ellos desastres naturales, desigualdades económicas, políticas, sociales o culturales.

La palabra vulnerabilidad deriva del latín vulnerabilis. Está compuesto por vulnus, que significa 'herida', y el sufijo -abilis, que indica posibilidad; por lo tanto, etimológicamente, vulnerabilidad indica una mayor probabilidad de ser herido.

3.2.3.6. AMENAZA

Cualquier cosa que es capaz de actuar contra un activo de una manera que pueda dañarlo. Una causa potencial de un incidente no deseado.

3.2.3.7. ACTIVO DE INFORMACIÓN

Todo aquello que las entidades consideran importante o de alta validez para la misma ya que puede contener información importante.

3.2.3.8. RIESGO

Posibilidad de que se produzca un contratiempo o una desgracia, de que alguien o algo sufran perjuicio o daño.

3.2.3.9. CONFIDENCIALIDAD

Busca evitar que la información que puede ser conocida y utilizada sin autorización por cualquier persona, dentro o fuera de institución.

3.2.3.10. INTEGRIDAD

La información puede mantenerse en óptimas condiciones y evitar así una modificación no autorizada que afecte a las actividades de la institución.

3.2.3.11. DISPONIBILIDAD

Abarca la información cuya inaccesibilidad afecta la actividad normal de la institución, ya que podría impedir la ejecución de las actividades.

3.2.4. VARIABLES

3.2.4.1. VARIABLE DEPENDIENTE

Y: Activos de Información

3.2.4.2. VARIABLE INDEPENDIENTE

X: Sistema de Gestión de Seguridad de Información

3.2.5. OPERACIONALIZACIÓN DE VARIABLES

VARIABLE	TIPO DE	DIMENSIONES	INDICADORES

VARIABLES			
Activos de Información	Dependiente	Recursos Tecnológicos	Confidencialidad Integridad Disponibilidad
Sistema de Gestión de Seguridad de Información	Independiente	Gestión de Riesgos	Incidentes Reportados Vulnerabilidades y Amenazas

Tabla 1: Operacionalización de Variables

3.3. MATERIALES Y METODO

3.3.1. ENFOQUE

El enfoque para este trabajo de investigación es **cualitativo,** pues previo al análisis se realiza una auditoria, la cual permite conocer la problemática y los procesos de la institución así, conociendo el nivel de seguridad que cuenta la Municipalidad Provincial de Huánuco.

3.3.2. ALCANCE O NIVEL

El presente estudio es de nivel descriptivo, por qué prioriza describir. Unidades, características de un fenómeno o personas, su función principal es profundizar describir conceptos.

3.3.3. DISEÑO

El presente trabajo de investigación tiene por tipo de investigación **Descriptivo**, porque se analizó la realidad problemática y se logró comprender de forma íntegra.

M ⟶ **O**

Donde:

M: Muestra

O: Observación

3.3.4. TECNICAS E INSTRUMENTOS DE RECOLECCIÓN DE DATOS

3.3.4.1. POBLACIÓN - MUESTRA

La población de la presente investigación es finita está compuesta por el jefe de área más el personal del área; el tamaño de la población está constituido por 7 personas, está compuesto solo por el área de informática de la Municipalidad Provincial de Huánuco.

3.3.4.2. TECNICAS

Técnica	Justificación	Instrumentos	Aplicación
Observación	Es una técnica que se usa para estudiar la muestra en sus propias actividades de grupo	Fichas	Encargado del área de informática

Entrevista	Técnica que obtiene información a través de preguntas en forma personal, directa y verbal.	Entrevistas preparadas con preguntas y respuestas abiertas	Encargado del área de informática
Encuesta	Es una técnica para obtener información tomando una muestra de la población objetivo	Encuestas estructuradas de preguntas abiertas y cerradas	Trabajadores del área de informática

Tabla 2: Instrumentos de Recolección de Datos

CAPITULO IV

APORTES PARA LA SOLUCIÓN DEL PROBLEMA

4.1. IMPLEMENTACIÓN DEL SGSI

4.1.1. ETAPA 1: ESTABLECIMIENTO DEL CONTEXTO

4.1.1.1. OBJETIVO DEL SGSI

Establecer políticas y procedimientos para la adecuada gestión de los activos de información en el área de informática de la **MPHCO.**

4.1.1.2. ALCANCE DEL SGSI

En el presente documento se desarrolla un **SGSI** aplicando la norma **ISO 27001** con el fin de mejorar y establecer políticas para gestionar adecuadamente la protección de activos de información en el área de informática.

4.1.1.3. POLITICAS DEL SGSI

El área de informática es la encarga de proteger y salvaguardar la confidencialidad, disponibilidad e integridad de la información.

El área de informática es el responsable de la implementación de los requerimientos de seguridad con el fin de proteger la información.

4.1.1.4. COMITÉ DE SEGURIDAD DE INFORMACIÓN

El comité estará conformado de la siguiente manera:

Nombre	Unidad Organizativa	Cargo	Correo electrónico
José Luis Villavicencio Guardia	Alcaldía	Alcalde	alcaldia@munihuanuco.gob.pe
Aldo Fernando Reyes Viviano	Gerencia Municipal	Gerente General	gerenciamunicipal@munihuanuco.gob.pe
Néstor Gerardo Miraval Berrospi	Gerencia de Administración y Finanzas	Gerente	sglogistica@munihuanuco.gob.pe
Úrsula Mida Espinoza Torres	Gerencia de Asesoría Jurídica	Gerente	gaj@munihuanuco.gob.pe
Lorenzo Huánuco Silva	Gerencia de Planificación y Presupuesto	Gerente	sgict@munihuanuco.gob.pe
Leslye Miluska Rojas Guerra	Gerencia de Desarrollo Local y Ordenamiento Territorial	Gerente	licenciadeconstruccion@munihuanuco.gob.pe
Circe Gozar Rivera	Gerencia de Desarrollo Económico	Gerente	sgpe@munihuanuco.gob.pe
Irene Nieto Pérez	Gerencia de Desarrollo Social	Gerente	gds@munihuanuco.gob.pe

Tabla 3: Comité de Seguridad

4.1.2. ETAPA 2: IDENTIFICACIÓN DE RIESGOS

4.1.2.1. METODOLOGIA DE EVALUACION DE RIESGOS

El siguiente trabajo de investigación vamos a trabajar con la metodología **MAGERIT**; para el análisis y gestión de los riesgos esto debido a que:

- Esta metodología nos permite una identificación clara y definida del entorno de aplicación.
- Esta metodología identifica en su análisis, riesgos críticos para la entidad, con lo cual se puede identificar inmediatamente posibles soluciones.
- Esta metodología nos permite identificar valores cualitativos y cuantitativos, lo que hace fácil identificar las decisiones a tomar.

El uso de adecuado de **MAGERIT**:

El análisis de riesgo es una aproximación metódica para determinar el riesgo siguiendo unos pasos pautados los cuales son:

1. Inventario de activos.
2. Valoración de los activos.
3. Amenazas (identificación y valorización).
4. Salvaguardar.

4.1.2.2. IDENTIFICACIÓN DE RIESGO

- **INVENTARIO DE ACTIVOS**

De acuerdo a la metodología de análisis y gestión adoptada por (**Magerit V.3**) se definió la siguiente clasificación de activos:

Categoría	Tipo de Activo
Información	Copias de respaldo
	Información escrita
	Código fuente de los sistemas de información
Software	Servidor de aplicaciones
	Sistema de Gestión de Base de datos
	Antivirus
	Ofimática
	Sistema Operativo
	Autocad, Adobe
	Sistema de Tramite Documentario
	SIAF
Físicos	Equipo de procesamiento
	Equipo de comunicaciones
	Medio de Almacenamiento
	Equipos de escritorio
	Impresoras y Escáner
Servicios	Procesamiento y comunicaciones
	Correo Electrónico
Personal	Personal Interno
	Administrador de Sistemas

Tabla 4: Inventario de Activos

- **VALORIZACIÓN DE LOS ACTIVOS**

Se consideró las dimensiones de confidencialidad, integridad y disponibilidad para la valorización de los activos de información.

Valor	Confidencialidad	Integridad	Disponibilidad
1 (Muy Bajo)	La información asociada al activo es **pública** y cualquiera puede acceder a ella, pues no impacta a la institución.	El activo puede tolerar un máximo de pérdida o alteración de sus componentes en un **100%**.	Se considera que como máximo el activo puede estar no indisponible por tiempo **indefinido**, pues su carencia no impacta a la institución.
2 (Bajo)	La información asociada al activo es de uso **interno** y solo personal de la entidad puede acceder a ella.	El activo puede tolerar un máximo de pérdida o alteración de sus componentes en un **85%.**	Se considera que como máximo el activo puede estar no disponible por una semana.
3 (Medio)	La información asociada al activo es **confidencial** y solo personal de algunas áreas internas pueden acceder a ella.	El activo puede tolerar un máximo de pérdida o alteración de sus componentes en un **50%**.	Se considera que como máximo el activo puede estar no disponible por un día.
4 (Alto)	La información asociada al activo es restringida y solo personal de un proyecto específico crítico para la institución.	El activo puede tolerar un máximo de pérdida o alteración de sus componentes en un **15%**.	Se considera que como máximo el activo puede estar no disponible por cuatro horas.
5 (Muy Alto)	La información asociada al activo es restringida y	El activo no puede tolerar pérdida o alteración de	Se requiere que el activo siempre esté disponible.

	accedida por personal de alto rango.	sus componentes.	

Tabla 5: Escala de Valor de los Activos

Se estima el valor del activo como el promedio de sumar los valores del nivel de relevancia respecto a la confidencialidad, integrad y disponibilidad, se muestra en la siguiente fórmula:

$$\boldsymbol{Valor\ del\ Activo} = \frac{(Valor\ Confidencialidad + Valor\ Integridad + Valor\ Disponibilidad)}{3}$$

Para valorar los activos de información se emplea la siguiente escala.

Nivel de Importancia	Valor Color	Rango del Valor	Criticidad
Muy Alto (MA)	**5**	4.001 – 5.000	Extremadamente Alto
Alto (A)	**4**	3.001 – 4.000	Alto
Mediano (M)	**3**	2.001 – 3.000	Mediano
Bajo (B)	**2**	1.001 – 2.000	Bajo
Muy Bajo (MB)	**1**	1.000 – 1.000	Muy Bajo

Tabla 6: Valor de Activo de Información

Esta tabla permite evaluar los activos de información mediante la relación a las dimensiones de confidencialidad, integridad y disponibilidad.

Categoría	Tipo de Activo	Confidencialidad	Integridad	Disponibilidad	Criticidad
Información	Copias de respaldo	4	5	5	M. A.
	Código fuente de los sistemas de información	4	5	5	M. A.
	Información escrita	4	4	4	A.
Software	Servidor de aplicaciones	5	5	4	M.A.
	Sistema de Gestión de Base de datos	5	5	5	M.A.
	Antivirus	4	4	3	A.
	Ofimática	3	3	3	M.
	Sistema Operativo	3	3	3	M.
	AutoCAD, Adobe	3	3	3	M.
	Sistema de Tramite Documentario	4	4	4	A.
	SIAF	4	4	4	A.
Físicos	Equipo de procesamiento	4	4	5	M.A.
	Equipo de comunicaciones	4	4	5	M.A.
	Medio de Almacenamiento	4	4	5	M.A.
	Equipos de escritorio	3	3	3	M.
	Impresoras y Escáner	2	2	2	B.
Servicios	Procesamiento y Comunicaciones	4	4	4	A.
	Correo Electrónico	3	3	3	M.

Personal	Personal Interno	3	3	3	M.
	Administrador de Sistemas	4	4	4	A.

Tabla 7: Valoración de los Activos de Información

4.1.3. ETAPA 3: ANÁLISIS DE RIESGOS

En esta etapa se identifican las amenazas y vulnerabilidades para los activos de información que puedan afectar con un impacto negativo sobre la confidencialidad, integridad y disponibilidad de los mismos.

El análisis de los riesgos de seguridad de información se inicia con el cuestionamiento de lo que puede fallar a causa de las amenazas que pueden explotar en vulnerabilidades de los activos y la consecuencia de la falla.

El enfoque metodológico de la etapa de análisis de riesgos de seguridad de información, se despliega a través de las siguientes actividades:

1. Identificar amenazas.
2. Identificar vulnerabilidades
3. Identificar controles de riesgo

4.1.3.1. IDENTIFICACIÓN DE AMENAZAS

En base a la lista de activos que se han identificado como relevantes, se realizará la identificación de las amenazas asociados a los activos de información.

Tipo	N°	TIPOLOGÍA DE AMENAZA
AMENAZAS A LA	1	Acceso no autorizado a la información

INFORMACIÓN	2	Eliminación no autorizada a la información
	3	Modificación no autorizada a la información
	4	Robo de activos de información
	5	Inadecuada eliminación de activos de información
	6	Corrupción de datos por error de procesamiento
	7	Uso extra laboral de la información
	8	Ataques de hacking/cracking sobre la información
	9	Virus informáticos que alteran o eliminan la información
	10	Fuga de información
AMENAZAS AL SOFTWARE	11	Adulteración del software
	12	Cambios no autorizados sobre el software
	13	Actualizaciones no controladas del software
	14	Instalación de software no licenciado o autorizado
	15	Copia no controlada del código fuente del software
	16	Saturación de la operación del software
	17	Hacking/Cracking
	18	Virus informáticos
	19	Error humano en los cambios en el software
	20	Incompatibilidad en la operación con otro Software
AMENAZAS A ACTIVOS FÍSICOS (EQUIPOS)	21	Corto Circuito
	22	Filtraciones de agua
	23	Filtraciones de polvo
	24	Corrosión de equipos
	25	Desconexión de equipos
	26	Saturación de humedad en ambientes
	27	Fallas del sistema de aire acondicionado
	28	Radiación electromagnética
	29	Robo de equipos o de sus componentes

	30	Incumplimiento del plan de mantenimiento
	31	Uso inadecuado de los equipos
	32	Desconfiguración del equipo
	33	Obsolescencia de los componentes del equipo
AMENAZAS A SERVICIOS	34	Falla de servicios para las telecomunicaciones
	35	Degradación de servicios para las telecomunicaciones
	36	Falla de la provisión de energía eléctrica
	37	Incumplimiento de fechas por parte de proveedores
	38	Provisión de servicios defectuosos(personal)
	39	Provisión de recursos defectuosos(material)
	40	Falla en servicios de información
AMENAZAS A PERSONAL	41	Contaminación del ambiente
	42	Uso de credenciales falsificadas
	43	Bloqueo del acceso al centro de trabajo
	44	Dificultad en el desplazamiento hacia el centro de trabajo
	45	Asaltos
AMENAZAS A UBICACIONES FÍSICAS	46	Sismo
	47	Inundación
	48	Hundimiento de suelos
	49	Incendio
	50	Destrucción intencional de los ambientes (protestas)

Tabla 8: Tipo de Amenazas

El nivel de amenaza se estima en base a la frecuencia con que la amenaza puede afectar el activo de información, se emplea la siguiente escala de valor:

Nivel de Amenaza	
Muy Alto	Una o más veces a la semana

Alto	Una vez al mes
Medio	Una vez al año
Bajo	Ha sucedido alguna vez
Muy Bajo	Nunca ha ocurrido

Tabla 9: Nivel de Amenaza

4.1.3.2. IDENTIFICAR VULNERABILIDADES

Las vulnerabilidades son debilidades de seguridad asociadas con los activos de información críticos. Para facilitar la identificación de las vulnerabilidades se clasifican de acuerdo con las distintas fuentes que las puedan originar, tal como se propone a continuación:

Tipo	N°	VULNERABILIDADES	EJEMPLO AMENAZAS
HARDWARE	1	Mantenimiento insuficiente	Ruptura de la mantenibilidad del sistema de información
	2	Falta de esquema de reemplazo periódicos	Destrucción de equipos o medio
	3	Susceptibilidad a la humedad, al polvo y a la suciedad	Polvo, corrosión, congelamiento
	4	Sensibilidad a la radiación electromagnética	Radiación electromagnética
	5	Falta de control eficiente del cambio de configuración	Error en el uso
	6	Susceptibilidad a variaciones de voltaje	Pérdida del suministro eléctrico

	7	Susceptibilidad a variaciones de temperatura	Fenómeno meteorológico
	8	Almacenamiento no protegido	Robo de medios
	9	Falta de cuidado al descartarlo	Robo de medios
	10	Copia no controlada	Robo de medios
SOFTWARE	11	Errores conocidos en el software	Abuso de derechos
	12	No hacer “logout” cuando se sale de las estaciones de trabajo	Abuso de derechos
	13	Software ampliamente distribuido	Corrupción de datos
	14	Asignación equivocada de derechos de acceso	Abuso de derechos
	15	Falta de documentación	Error en uso
	16	Configuración incorrecta de parámetros	Error en uso
	17	Mala administración de claves	Falsificación de datos
	18	Especificaciones no claras o incompletas para los desarrolladores	Mal funcionamiento del software
	19	Falta de copias de respaldo	Adulteración del software
	20	Líneas de comunicación no protegidas	Intercepción
	21	Pruebas al software inexistentes o insuficientes	Abuso de derechos
	22	Punto de falla único	Falla del equipo de telecomunicaciones
RED	23	Falta de identificación y autentificación de receptor y destinatario	Falsificación de derechos

	24	Arquitectura de red insegura	Espionaje remoto
	25	Transferencia de contraseñas autorizadas	Espionaje remoto
	26	Gestión inadecuada de la red	Saturación del sistema de información
	27	Conexión de red pública sin protección	Uso no autorizado del equipo
PERSONAL	28	Ausencia de personal	Ruptura de la disponibilidad del personal
	29	Procedimientos inadecuados de contratación	Destrucción de equipos o medio
	30	Capacitación insuficiente en seguridad	Error en el uso
	31	Uso incorrecto de Software y Hardware	Error en el uso
	32	Falta de conciencia de seguridad	Error en el uso
SITIO	33	Uso inadecuado o descuido del control de acceso a las edificaciones o recintos	Inundación
	34	Red inestable de energía eléctrica	Perdida de suministro eléctrico
	35	Falta de protección física del edificio puertas y ventanas.	Robo de equipos
ORGANIZACIÓN	36	Falta de un procedimiento formal para el registro y baja de los usuarios.	Abuso de derechos
	37	Falta de proceso formal para revisar el derecho de acceso	Abuso de derechos

	38	Falta de procesamiento de monitoreo de las instalaciones de procesamiento de la información.	Abuso de derechos
	39	Falta de informes de fallas registradas en los registros del administrador y del operador.	Abuso de derechos
	40	Falta de procedimientos en el control de cambios.	Ruptura de mantenibilidad del sistema de información
	41	Falta de procedimiento formal para la supervisión del registro.	Corrupción de datos
	42	Falta de proceso formal para autorización de información pública disponible.	Datos de fuentes no confiables
	43	Falta de procedimientos para manejo de la información clasificada	Error en el uso
	44	Falta de políticas formal sobre el uso de ordenadores portátiles.	Robo de equipos
	45	Inexistencia o insuficiencia de la política de “Escritorios despejado y pantalla despejada”	Robo de medios

Tabla 10: Catálogo de Vulnerabilidades

El nivel de vulnerabilidad se pondera de la siguiente manera:

Nivel de vulnerabilidad	Descripción
Muy Alto	Muy alta facilidad de explotación de la vulnerabilidad.
Alto	Alta facilidad de explotación de la vulnerabilidad.

Medio	Mediana facilidad de explotación de la vulnerabilidad.
Bajo	Baja facilidad de explotación de la vulnerabilidad.
Muy Bajo	Muy baja facilidad de explotación de la vulnerabilidad.

Tabla 11: Nivel de Vulnerabilidad

4.1.3.3. IDENTIFICAR CONTROLES

Una vez identificadas las amenazas y vulnerabilidades relacionadas con los activos de información, se procede a detallar el riesgo de seguridad de la información.

4.1.4. ETAPA 4: EVALUACIÓN DE RIESGOS

La evaluación del riesgo es el componente por el cual se estima la valoración del riesgo del activo de soporte, mediante técnicas cualitativas de valorización del riesgo, con la finalidad de estimar el impacto si llegase a ocurrir, y con qué frecuencia (dentro de período de tiempo de un año) para cada riesgo. En un segundo nivel de evaluación, también se tiene en cuenta los controles existentes, así como su efectividad.

El enfoque metodológico, considera criterios para la evaluación y calificación de los riesgos, los cuales están en función de dos variables: la frecuencia e impacto, que permiten construir la metodología de la exposición del riesgo. Es importante considerar lo siguiente:

Frecuencia (probabilidad): Es el número de veces que puede materializarse el riesgo, considerando la frecuencia de las amenazas y vulnerabilidades.

Impacto: Es una estimación de la magnitud de la consecuencia si se materializa el riesgo, expresada en términos de impacto de la pérdida de la confidencialidad, integridad y disponibilidad del activo.

FRECUENCIA						
	CASI SEGURO	ALTO	ALTO	EXTREMO	EXTREMO	EXTREMO
	PROBABLE	MODERADO	ALTO	ALTO	EXTREMO	EXTREMO
	POSIBLE	BAJO	MODERADO	ALTO	EXTREMO	EXTREMO
	IMPROBABLE	BAJO	BAJO	MODERADO	ALTO	EXTREMO
	RARO	BAJO	BAJO	MODERADO	ALTO	ALTO
		INSIGNIFICANTE	*MENOR*	*MODERADO*	*MAYOR*	*CATASTRÓFICO*
		IMPACTO				

A continuación, se presenta la matriz de calor:

Tabla 12: Matriz de Calor

Nivel de Riesgo	Descripción
Extremo	Si el riesgo llega a materializarse tendría un impacto o efecto extremo
Alto	Si el riesgo llega a materializarse, tendría un alto impacto.

Moderado	Si el riesgo llega a materializarse, tendría impacto moderado.
Bajo	Si el riesgo llega a materializarse, tendría un efecto bajo.

Tabla 13: Niveles de riesgo

El riesgo de un activo de información corresponde al nivel de riesgos sin considerar los controles existentes o planificados para disminuir la frecuencia.

El valor de la frecuencia se estima mediante el valor la frecuencia el cálculo del promedio del valor de la frecuencia de la vulnerabilidad y el valor de la amenaza.

$$\boldsymbol{Valor\ de\ la\ Frecuencia} = \frac{(Valor\ de\ la\ Vulnerabilidad) + (Valor\ de\ Amenaza)}{2}$$

Para determinar el nivel de frecuencia se utiliza la siguiente tabla:

Nivel	Valor	Compatibilidad
Raro	1	Raro
Improbable	2	Improbable
Posible	3	Moderado

Probable	4	Probable
Casi Seguro	5	Casi Certeza

Tabla 14: Frecuencia de Riesgo

El nivel de impacto se estima como la magnitud de la consecuencia de la perdida de la confidencialidad, integridad y disponibilidad del activo de información.

Nivel de Importancia	Valor	Nivel de Impacto
Muy Alto	5	Catastrófico
Alto	4	Mayor
Mediano	3	Moderado
Bajo	2	Menor
Muy Bajo	1	Insignificante

Tabla 15: Nivel de Importancia

El valor del riesgo se estima mediante una función de los valores de la frecuencia y el impacto del riesgo. A continuación, se describe la fórmula:

$$\boldsymbol{Nivel\ del\ riesgo\ inherente} = f(\text{Frecuencia} \times \text{Impacto})$$

A continuación, se presenta la matriz de riesgo de los activos de información:

Matriz de Riesgo						
Id de Riesgo	**Activo**	**Vulnerabilidad**	**Amenaza**	**Posible Amenaza**	**Impacto**	**Nivel de Riesgo**
R1	Hardware	Mantenimiento insuficiente	Ruptura de la mantenibilidad del	Posible	Menor	Moderado

			sistema de información			
R2	Hardware	Falta de esquema de reemplazo periódicos	Destrucción de equipos o medio	Improbable	Moderado	Moderado
R3	Hardware	Susceptibilidad a la humedad, al polvo y a la suciedad	Polvo, corrosión, congelamiento	Posible	Moderado	Alto
R4	Hardware	Sensibilidad a la radiación electromagnética	Radiación electromagnética	Posible	Menor	Moderado
R5	Hardware	Falta de control eficiente del cambio de configuración	Error en el uso	Probable	Moderado	Alto
R6	Hardware	Susceptibilidad a variaciones de voltaje	Pérdida del suministro eléctrico	Probable	Menor	Alto
R7	Hardware	Susceptibilidad a variaciones de temperatura	Fenómeno meteorológico	Probable	Insignificante	Moderado
R8	Hardware	Almacenamiento no protegido	Robo de medios	Probable	Moderado	Alto
R9	Hardware	Falta de cuidado al descartarlo	Robo de medios	Probable	Moderado	Alto
R10	Hardware	Copia no controlada	Robo de medios	Probable	Menor	Alto
R11	Software	Errores conocidos en el software	Abuso de derechos	Probable	Insignificante	Moderado
R12	Software	No hacer “logout” cuando se sale de las estaciones de trabajo	Abuso de derechos	Casi Seguro	Menor	Alto
R13	Software	Software ampliamente distribuido	Corrupción de datos	Raro	Moderado	Moderado
R14	Software	Asignación equivocada de derechos de acceso	Abuso de derechos	Improbable	Mayor	Alto
R15	Software	Falta de documentación	Error en uso	Posible	Menor	Moderado
R16	Software	Configuración incorrecta de parámetros	Error en uso	Posible	Menor	Moderado
R17	Software	Mala administración de claves	Falsificación de datos	Probable	Moderado	Alto
R18	Software	Especificaciones no claras o incompletas para los desarrolladores	Mal funcionamiento del software	Posible	Menor	Moderado
R19	Software	Falta de copias de respaldo	Adulteración del software	Probable	Moderado	Alto

R20	Software	Líneas de comunicación no protegidas	Intercepción	Posible	Menor	Moderado
R21	Software	Pruebas al software inexistentes o insuficientes	Abuso de derechos	Raro	Moderado	Moderado
R22	Software	Punto de falla único	Falla del equipo de telecomunicaciones	Improbable	Menor	Bajo
R23	Red	Falta de identificación y autentificación de receptor y destinatario	Falsificación de derechos	Probable	Menor	Moderado
R24	Red	Arquitectura de red insegura	Espionaje remoto	Improbable	Moderado	Moderado
R25	Red	Transferencia de contraseñas autorizadas	Espionaje remoto	Probable	Moderado	Alto
R26	Red	Gestión inadecuada de la red	Saturación del sistema de información	Probable	Menor	Alto
R27	Red	Conexión de red pública sin protección	Uso no autorizado del equipo	Posible	Menor	Moderado
R28	Personal	Ausencia de personal	Ruptura de la disponibilidad del personal	Raro	Moderado	Moderado
R29	Personal	Procedimientos inadecuados de contratación	Destrucción de equipos o medio	Probable	Moderado	Alto
R30	Personal	Capacitación insuficiente en seguridad	Error en el uso	Probable	Insignificante	Moderado
R31	Personal	Uso incorrecto de Software y Hardware	Error en el uso	Posible	Menor	Moderado
R32	Personal	Falta de conciencia de seguridad	Error en el uso	Probable	Menor	Alto
R33	Sitio	Uso inadecuado o descuido del control de acceso a las edificaciones o recintos	Inundación	Casi Seguro	Menor	Alto
R34	Sitio	Red inestable de energía eléctrica	Perdida de suministro eléctrico	Probable	Moderado	Alto
R35	Sitio	Falta de protección física del edificio puertas y ventanas.	Robo de equipos	Probable	Moderado	Alto
R36	Organización	Falta de un procedimiento formal para el registro y baja de los usuarios.	Abuso de derechos	Posible	Moderado	Alto
R37	Organización	Falta de proceso formal para	Abuso de derechos	Casi	Menor	Alto

		revisar el derecho de acceso		Seguro		
R38	Organización	Falta de procesamiento de monitoreo de en las instalaciones de procesamiento de la información.	Abuso de derechos	Raro	Mayor	Alto
R39	Organización	Falta de informes de fallas registradas en los registros del administrador y del operador.	Abuso de derechos	Probable	Moderado	Alto
R40	Organización	Falta de procedimientos en el control de cambios.	Ruptura de mantenibilidad del sistema de información	Probable	Menor	Alto
R41	Organización	Falta de procedimiento formal para la supervisión del registro.	Corrupción de datos	Probable	Insignificante	Moderado
R42	Organización	Falta de proceso formal para autorización de información pública disponible.	Datos de fuentes no confiables	Posible	Menor	Moderado
R43	Organización	Falta de procedimientos para manejo de la información clasificada	Error en el uso	Probable	Menor	Alto
R44	Organización	Falta de políticas formal sobre el uso de computadoras portátiles.	Robo de equipos	Probable	Moderado	Alto
R45	Organización	Inexistencia o insuficiencia de la política de “Escritorios despejado y pantalla despejada”	Robo de medios	Probable	Moderado	Alto

Tabla 16: Lista de Riesgos

4.1.5. ETAPA 5: TRATAMIENTO DE RIESGOS

4.1.5.1. PLAN DE TRATAMIENTO DE RIESGOS

A continuación, se presenta la matriz de los activos críticos que se encontraron en el análisis de riesgo.

Matriz de Riesgo						
Id de Riesgo	**Activo**	**Vulnerabilidad**	**Amenaza**	**Posible Amenaza**	**Impacto**	**Nivel de Riesgo**
R3	Hardware	Susceptibilidad a la humedad, al polvo y a la suciedad	Polvo, corrosión, congelamiento	Posible	Moderado	Alto
R5	Hardware	Falta de control eficiente del cambio de configuración	Error en el uso	Probable	Moderado	Alto
R6	Hardware	Susceptibilidad a variaciones de voltaje	Pérdida del suministro eléctrico	Probable	Menor	Alto
R8	Hardware	Almacenamiento no protegido	Robo de medios	Probable	Moderado	Alto
R9	Hardware	Falta de cuidado al descartarlo	Robo de medios	Probable	Moderado	Alto
R10	Hardware	Copia no controlada	Robo de medios	Probable	Menor	Alto
R12	Software	No hacer “logout” cuando se sale de las estaciones de trabajo	Abuso de derechos	Casi Seguro	Menor	Alto
R14	Software	Asignación equivocada de derechos de acceso	Abuso de derechos	Improbable	Mayor	Alto
R17	Software	Mala administración de claves	Falsificación de datos	Probable	Moderado	Alto
R19	Software	Falta de copias de respaldo	Adulteración del software	Probable	Moderado	Alto
R25	Red	Transferencia de contraseñas autorizadas	Espionaje remoto	Probable	Moderado	Alto
R26	Red	Gestión inadecuada de la red	Saturación del sistema de información	Probable	Menor	Alto

R29	Personal	Procedimientos inadecuados de contratación	Destrucción de equipos o medio	Probable	Moderado	Alto
R32	Personal	Falta de conciencia de seguridad	Error en el uso	Probable	Menor	Alto
R33	Sitio	Uso inadecuado o descuido del control de acceso a las edificaciones o recintos	Inundación	Casi Seguro	Menor	Alto
R34	Sitio	Red inestable de energía eléctrica	Perdida de suministro eléctrico	Probable	Moderado	Alto
R35	Sitio	Falta de protección física del edificio puertas y ventanas.	Robo de equipos	Probable	Moderado	Alto
R36	Organización	Falta de un procedimiento formal para el registro y baja de los usuarios.	Abuso de derechos	Posible	Moderado	Alto
R37	Organización	Falta de proceso formal para revisar el derecho de acceso	Abuso de derechos	Casi Seguro	Menor	Alto
R38	Organización	Falta de procesamiento de monitoreo en las instalaciones de procesamiento de la información.	Abuso de derechos	Raro	Mayor	Alto

R39	Organización	Falta de informes de fallas registradas en los registros del administrador y del operador.	Abuso de derechos	Probable	Moderado	Alto
R40	Organización	Falta de procedimientos en el control de cambios.	Ruptura de mantenibilidad del sistema de información	Probable	Menor	Alto
R43	Organización	Falta de procedimientos para manejo de la información clasificada	Error en el uso	Probable	Menor	Alto
R44	Organización	Falta de políticas formal sobre el uso de computadoras portátiles.	Robo de equipos	Probable	Moderado	Alto
R45	Organización	Inexistencia o insuficiencia de la política de "Escritorios despejado y pantalla despejada"	Robo de medios	Probable	Moderado	Alto

Tabla 17: Lista de Riesgos No Aceptables

Una vez realizado el análisis y evaluación de riesgo en base a los criterios de aceptación de riesgos, se debe decidir cuales acciones se han de tomar con los riesgos priorizados, las opciones de tratamiento se presentan en la tabla.

Medida Frente al riesgo	
Aceptar	Aceptar la posibilidad que pueda ocurrir el riesgo sin tomar medidas de acción concretas.
Mitigar	Mitigar el impacto o la probabilidad de ocurrencia mediante la implementación de un control de seguridad de información.
Evitar	Eliminar la fuente del proceso que genera la amenaza, se utiliza cuando el nivel de riesgo es alto, la actividad del proceso o sistema que lo genera no es de gran impacto.
Transferir	Transferir el impacto de riesgo a terceros. Se utiliza cuando no se puede mitigar la probabilidad de ocurrencia de un riesgo.

Tabla 18: Opciones de Tratamiento

En el presente trabajo de investigación se estableció que a los niveles alto y extremo se aplicaran controles, que ayuden a reducir el riesgo producido por las amenazas a un nivel aceptable.

Se priorizará el tratamiento de riesgo del nivel alto, aplicará de manera urgente las medidas de seguridad. Así mismo el nivel moderado y bajo serán monitoreados.

4.1.5.2. DETERMINAR LOS CONTROLES

Se determinaron los controles que ayudarán a reducir los riesgos a un nivel aceptable. Se detallan en el **ANEXO N° 05** los controles para reducir los riesgos.

Finalmente se elaboró la declaración de aplicabilidad cual incluye todos los controles identificados. Este

documento puede ser estudiado en el **ANEXO N° 06** del presente trabajo de investigación.

4.2. RESULTADOS

4.2.1. OBJETIVO ESPECÍFICO 1:

Definir las políticas y procedimientos para la protección de los activos en el área de informática de la Municipalidad Provincial de Huánuco.

Se desarrolló el Sistema de Gestión de Seguridad de Información según los alcances establecidos en el trabajo de investigación. Se identificaron los activos de información, se valorizaron según el impacto que causaban a la institución en base a la disponibilidad, integridad y confidencialidad. Se especifica en la **Tabla 7.**

Así mismo para identificar que los trabajadores del área de informática si contaban con el conocimiento de políticas de seguridad de información se realizaron las encuestas. Esta especificado en el **ANEXO N° 02.**

4.2.2. OBJETIVO ESPECÍFICO 2:

Identificar y evaluar los riesgos de seguridad de información para la protección de los activos en el área informática de la Municipalidad de Huánuco.

Se identificaron las amenazas y vulnerabilidades de los activos de información. Se especifica en la **Tabla 8** y **Tabla 10.**

Se realizó la matriz de riesgo. Se especifica en la **Tabla 16.**

4.2.3. OBJETIVO ESPECÍFICO 3:

Diseñar los controles adecuados para mitigar los riesgos de los activos de información en el área de Informática de la Municipalidad Provincial de Huánuco.

Se realizó el análisis de riesgo donde se identificaron los controles, el cual se encuentra en el **ANEXO N° 05.**

Se desarrolló la declaración de aplicabilidad el cual se encuentra en el **ANEXO N° 06.**

CONCLUSIONES

- Se desarrolló las políticas de seguridad que son de gran utilidad, para la protección de activos de información además los colaboradores deben tener conocimiento para el buen manejo y uso de los activos.
- En la investigación se pudo identificar y evaluar los riesgos a los que están expuesto los activos de información, con el cual se realizó la matriz de amenazas de los activos viendo la probabilidad de ocurrencia de cada uno de ellos.
- El prevenir y mitigar los riesgos identificados forman parte del plan de tratamiento de riesgos, se aprecia que en su mayoría están en estado alto, se desarrolla el plan de tratamiento de riesgos. asegurando la protección de los activos de información.

RECOMENDACIONES

- Se recomienda la implementación del Sistema de Gestión de la Seguridad de la Información para mitigar los riesgos de los activos de información en la Municipalidad Provincial de Huánuco.
- Se recomienda que se establezca un comité de seguridad conformada por los Gerentes, Sub Gerentes y el Alcalde para la implementación del Sistema de Gestión de la Seguridad de la Información el cual debe tener un seguimiento constante.
- Se recomienda concientizar a los trabajadores en seguridad de información mediante charlar informativas y/o capacitaciones.
- Se recomienda que se implementen los controles del Sistema de Gestión de la Seguridad de la Información, mantenerlo actualizado con la finalidad de alcanzar la excelencia y a futuro lograr la certificación en Seguridad de la información ISO 27001.

BIBLIOGRAFIA

- **Aguirre, D. (2014).** "*Diseño de un sistema de gestión de seguridad de información para servicios postales del Perú S.A.* Tesis de licenciatura, Facultad de Ciencias e Ingeniería, Universidad Católica del Perú. Lima, Perú".

- **Ampuero, C. (2011).** "*Diseño de un sistema de gestión de seguridad de información para una compañía de seguros*. Tesis de licenciatura, Facultad de Ciencias e Ingeniería, Universidad Católica del Perú. Lima, Perú".

- **Barrantes, C; Hugo, J. (2012).** "*Diseño e implementación de un Sistema de Gestión de Seguridad de Información en Procesos Tecnológicos.* Facultad de Ingeniería y Arquitectura, Universidad de San Martin de Porres. Lima, Perú".

- **Chávez Paz, J. H. & Nepo López, G. A. (Julio de 2015).** "Sistema de Gestión de Seguridad de Información basado en la Norma ISO/IEC 27001 para la Superintendencia de Transporte Terrestre de Personas, Carga y Mercancías (SUTRAN) – Región Lambayeque".

- **Congreso de la Republica. (2011).** Ley 29733. Ley de protección de datos personales. Lima.

- **De la Cruz Guerrero, C. W; & Vásquez Montenegro, J. C. (2008).** "Elaboración y Aplicación de un Sistema de Gestión de

la seguridad de información (SGSI) Para la realidad Tecnológica de la USAT", Chiclayo.

- ISO 27001 En *ISO27000.es.*

  - Disponible en: http://www.iso27000.es/.

- Leyva, R. (2016). " *Diseño de un Sistema de Gestión de Seguridad de la Información basado en las Normas ISO/IEC 27001 e ISO/IEC 27002 para proteger los activos de información en el proceso de suministros de medicamentos de la Red de Salud de Lambayeque 2015.* Facultad de Ciencias Físicas y Matemáticas, Universidad Nacional Pedro Ruiz Gallo. Lambayeque, Perú".

ANEXOS

ANEXO N° 01 - MATRIZ DE CONSISTENCIA

PROBLEMA GENERAL	OBJETIVO GENERAL	TIPO DE VARIABLES	VARIABLE	DIMENSIONES	INDICADORES	METODOLOGÍA
¿Cómo ayudará un Sistema de Gestión de la Seguridad de la Información basada en la norma ISO 27001 para tener un control de los activos de información en el área de informática de la Municipalidad Provincial de Huánuco?	Proponer un Sistema de Gestión Seguridad Información basado en la norma ISO 27001 para la protección de los activos de información en el área de informática de la Municipalidad Provincial de Huánuco año 2019.	Dependiente	Activos de Información	Recursos Tecnológicos	Confidencialidad Integridad Disponibilidad	Tipo de Investigación **Aplicada** Alcance y Nivel **Aplicativo** Diseño **Descriptivo** Enfoque **Cualitativo** Muestras **Encuestas** **Cuestionario** Gráfico de la Muestra M → O
		Independiente	Sistema de Gestión de Seguridad de Información	Gestión de Riesgos	Incidentes Reportados Vulnerabilidades y Amenazas	
PROBLEMAS ESPECÍFICOS	**OBJETIVOS ESPECÍFICOS**					
¿Cuál es el alcance de las políticas del Sistema de Gestión de la seguridad de la información para el área informática de la Municipalidad Provincial de Huánuco?	Definir las políticas y procedimientos para la protección de los activos en el área de informática de la Municipalidad Provincial Huánuco.				Controles de Seguridad	
¿Qué metodología se usará para la gestión de los riesgos de los activos de información en el área de informática de la Municipalidad Provincial de Huánuco?	Identificar y evaluar los riesgos de seguridad de información para la protección de los activos en el área informática de la Municipalidad Provincial Huánuco.					
¿Cuáles son los controles adecuados para mitigar los riesgos de activos de información en el área de Informática de la Municipalidad Provincial Huánuco?	Diseñar los controles adecuados para mitigar los riesgos de los activos de información en el área de Informática de la Municipalidad Provincial Huánuco.					

ANEXO N° 02 - ENCUESTA SOBRE SEGURIDAD DE LA INFORMACIÓN

La siguiente encuesta tiene por finalidad saber si el personal administrativo que labora en el área de informática conoce, utiliza y salvaguarda la información de manera óptima y adecuada.

Instrucciones:

Para desarrollar la encuesta, usted debe leer cada pregunta y escoger una las alternativas propuestas con un "**X**" dentro de los paréntesis.

1. ¿Ud. tiene conocimiento si en la Municipalidad Provincial de Huánuco existe un sistema de gestión de seguridad de la información?

   Si ( ) No ( )

2. ¿Cree usted que implementado un SGSI mejorara la seguridad de información de su área de informática?

   Si ( ) No ( )

3. ¿Aprobaría usted la implementación del SGSI en el área de informática?

   Si ( ) No ( )

4. ¿Cree Ud. que en su área de trabajo se lograra un cambio positivo con la aplicación de este SGSI?

   Si ( ) No ( )

5. ¿Considera Ud. que en su área de trabajo existe información que debe ser protegida?

   Si ( ) No ( )

6. ¿Cuenta Ud. con un computador para realizar sus funciones?

   Si ( ) No ( )

7. Usted apaga los equipos informáticos debidamente después de utilizarlos

   Si ( ) No ( )

8. Se siente seguro en los ambientes donde se encuentran los equipos informáticos dentro del área de informática

   Si ( ) No ( )

9. Ha observado algún extinguidor cerca de los equipos informáticos.

   Si ( ) No ( )

10. Ha participado de algún simulacro frente a cualquier desastre natural o humano, especialmente en el área de informática.

Si ( ) No ( )

ANEXO N° 03 - CUESTIONARIO PARA IDENTIFICAR LOS ACTIVOS

Dependencia: _____

Instrucciones: En cada tabla marque (**x**) con los activos que se cuentan.

CUESTIONARIO DE TIPOS DE ACTIVOS
¿Qué activos son fundamentales para el área de informática?
Marque con (**x**) los activos que cuenta el área de Informática. ( ) Datos de interés para la administración pública. ( ) Datos de carácter personal (información concerniente al personal) ( ) Datos clasificados (aquellos sometidos a normatividad especifica de la Municipalidad y que determina su control de acceso y distribución)

CUESTIONARIO DE TIPO DATO / INFORMACIÓN
¿Qué activos de tipo dato/información son fundamentales para el área de informática?
Marque con (**x**) los activos que cuenta el área de Informática. ( ) Ficheros o bases de datos ( ) Copias de respaldo ( ) Datos de configuración de los sistemas de información ( ) Datos de gestión interna ( ) Datos de control de acceso (Ejemplo: contraseñas) ( ) Datos de validación de credenciales ( ) Código fuente de los sistemas de información ( ) Código ejecutable de los sistemas de información

CUESTIONARIO DE TIPO SERVICIO
¿Qué activos de tipo servicio son fundamentales para el área de informática?
Marque con (**x**) los activos que cuenta el área de Informática. ( ) Internet ( ) Intranet ( ) Acceso remoto ( ) Correo electrónico ( ) Almacenamiento de ficheros (File Server) ( ) Intercambio electrónico de datos

CUESTIONARIO DE TIPO SOFTWARE / APLICACIONES UTILIZADAS
¿Qué activos de tipo software son fundamentales para el área de informática?
Marque con (**x**) los activos que cuenta el área de Informática. ( ) ERP ( ) Páginas Web ( ) Software de desarrollo propio ( ) Intranet ( ) Servidor de aplicaciones ( ) Servidor de correo electrónico ( )Sistema de gestión de bases de datos ( ) Anti-Virus, Autocad, Adobe pdf,

( ) Sistema Operativo, Ofimática

CUESTIONARIO DE TIPO EQUIPOS INFORMÁTICOS
¿Qué tipo de hardware son fundamentales para el área de informática?
Marque con (**x**) los activos que cuenta el área de Informática. ( ) Equipos medios ( ) Informática personal ( ) Informática móvil ( ) Equipo virtual ( ) Equipamiento de respaldo ( ) Medios de impresión ( ) Escáneres ( ) Módems ( ) Concentradores (Hub) ( ) Conmutadores (Switch) ( ) Encaminadores (Router) ( ) Pasarelas (Bridge) ( ) Cortafuegos (Firewall) ( ) Punto de acceso inalámbrico ( ) Centralita telefónica ( ) Teléfonos IP

CUESTIONARIO DE TIPO DE REDES DE COMUNICACIONES
¿Qué medios de transporte utiliza la dependencia para transmitir información?
Marque con (**x**) los activos que cuenta el área de Informática. ( ) Red telefónica ( ) ADSL ( ) Punto a punto ( ) Red inalámbrica ( ) Red local ( ) Internet

CUESTIONARIO DE TIPO SOPORTE DE INFORMACIÓN
¿Qué dispositivos físicos utiliza la dependencia para el área de informática?
Marque con (**x**) los activos que cuenta el área de Informática. ( ) Discos ( ) Discos virtuales ( ) Almacenamiento en red ( ) Disquetes ( ) CD-ROM ( ) Memorias USB ( ) DVD ( ) Cinta magnética

( ) Tarjetas de memoria

CUESTIONARIO DE TIPO EQUIPAMIENTO

Marque con (**x**) los activos que cuenta el área de Informática.

( ) Fuentes de alimentación

( ) Sistemas de alimentación ininterrumpida

( ) Generadores eléctricos

( ) Equipos de climatización

( ) Cable eléctrico

( ) Fibra óptica

( ) Suministros esenciales

( ) Equipos de destrucción de soportes de información

( ) Mobiliario: armarios, gabinetes, escritorios, etc.

CUESTIONARIO DE TIPO PERSONAL

Marque con (**x**) los activos que cuenta el área de Informática.

( ) Usuarios externos

( ) Usuarios internos

( ) Operadores

( ) Administradores de sistemas

( ) Administradores de comunicaciones

( ) Administradores de BBDD

( ) Desarrolladores / Programadores

( ) Proveedores

ANEXO N° 04 - ISO/IEC 27002:2013

ISO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES

5. POLÍTICAS DE SEGURIDAD.
- 5.1 Directrices de la Dirección en seguridad de la información.
  - 5.1.1 Conjunto de políticas para la seguridad de la información.
  - 5.1.2 Revisión de las políticas para la seguridad de la información.

6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.
- 6.1 Organización interna.
  - 6.1.1 Asignación de responsabilidades para la segur. de la información.
  - 6.1.2 Segregación de tareas.
  - 6.1.3 Contacto con las autoridades.
  - 6.1.4 Contacto con grupos de interés especial.
  - 6.1.5 Seguridad de la información en la gestión de proyectos.
- 6.2 Dispositivos para movilidad y teletrabajo.
  - 6.2.1 Política de uso de dispositivos para movilidad.
  - 6.2.2 Teletrabajo.

7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.
- 7.1 Antes de la contratación.
  - 7.1.1 Investigación de antecedentes.
  - 7.1.2 Términos y condiciones de contratación.
- 7.2 Durante la contratación.
  - 7.2.1 Responsabilidades de gestión.
  - 7.2.2 Concienciación, educación y capacitación en segur. de la informac.
  - 7.2.3 Proceso disciplinario.
- 7.3 Cese o cambio de puesto de trabajo.
  - 7.3.1 Cese o cambio de puesto de trabajo.

8. GESTIÓN DE ACTIVOS.
- 8.1 Responsabilidad sobre los activos.
  - 8.1.1 Inventario de activos.
  - 8.1.2 Propiedad de los activos.
  - 8.1.3 Uso aceptable de los activos.
  - 8.1.4 Devolución de activos.
- 8.2 Clasificación de la información.
  - 8.2.1 Directrices de clasificación.
  - 8.2.2 Etiquetado y manipulado de la información.
  - 8.2.3 Manipulación de activos.
- 8.3 Manejo de los soportes de almacenamiento.
  - 8.3.1 Gestión de soportes extraíbles.
  - 8.3.2 Eliminación de soportes.
  - 8.3.3 Soportes físicos en tránsito.

9. CONTROL DE ACCESOS.
- 9.1 Requisitos de negocio para el control de accesos.
  - 9.1.1 Política de control de accesos.
  - 9.1.2 Control de acceso a las redes y servicios asociados.
- 9.2 Gestión de acceso de usuario.
  - 9.2.1 Gestión de altas/bajas en el registro de usuarios.
  - 9.2.2 Gestión de los derechos de acceso asignados a usuarios.
  - 9.2.3 Gestión de los derechos de acceso con privilegios especiales.
  - 9.2.4 Gestión de información confidencial de autenticación de usuarios.
  - 9.2.5 Revisión de los derechos de acceso de los usuarios.
  - 9.2.6 Retirada o adaptación de los derechos de acceso
- 9.3 Responsabilidades del usuario.
  - 9.3.1 Uso de información confidencial para la autenticación.
- 9.4 Control de acceso a sistemas y aplicaciones.
  - 9.4.1 Restricción del acceso a la información.
  - 9.4.2 Procedimientos seguros de inicio de sesión.
  - 9.4.3 Gestión de contraseñas de usuario.
  - 9.4.4 Uso de herramientas de administración de sistemas.
  - 9.4.5 Control de acceso al código fuente de los programas.

10. CIFRADO.
- 10.1 Controles criptográficos.
  - 10.1.1 Política de uso de los controles criptográficos.
  - 10.1.2 Gestión de claves.

11. SEGURIDAD FÍSICA Y AMBIENTAL.
- 11.1 Áreas seguras.
  - 11.1.1 Perímetro de seguridad física.
  - 11.1.2 Controles físicos de entrada.
  - 11.1.3 Seguridad de oficinas, despachos y recursos.
  - 11.1.4 Protección contra las amenazas externas y ambientales.
  - 11.1.5 El trabajo en áreas seguras.
  - 11.1.6 Áreas de acceso público, carga y descarga.
- 11.2 Seguridad de los equipos.
  - 11.2.1 Emplazamiento y protección de equipos.
  - 11.2.2 Instalaciones de suministro.
  - 11.2.3 Seguridad del cableado.
  - 11.2.4 Mantenimiento de los equipos.
  - 11.2.5 Salida de activos fuera de las dependencias de la empresa.
  - 11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.
  - 11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.
  - 11.2.8 Equipo informático de usuario desatendido.
  - 11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.

12. SEGURIDAD EN LA OPERATIVA.
- 12.1 Responsabilidades y procedimientos de operación.
  - 12.1.1 Documentación de procedimientos de operación.
  - 12.1.2 Gestión de cambios.
  - 12.1.3 Gestión de capacidades.
  - 12.1.4 Separación de entornos de desarrollo, prueba y producción.
- 12.2 Protección contra código malicioso.
  - 12.2.1 Controles contra el código malicioso.
- 12.3 Copias de seguridad.
  - 12.3.1 Copias de seguridad de la información.
- 12.4 Registro de actividad y supervisión.
  - 12.4.1 Registro y gestión de eventos de actividad.
  - 12.4.2 Protección de los registros de información.
  - 12.4.3 Registros de actividad del administrador y operador del sistema.
  - 12.4.4 Sincronización de relojes.
- 12.5 Control del software en explotación.
  - 12.5.1 Instalación del software en sistemas en producción.
- 12.6 Gestión de la vulnerabilidad técnica.
  - 12.6.1 Gestión de las vulnerabilidades técnicas.
  - 12.6.2 Restricciones en la instalación de software.
- 12.7 Consideraciones de las auditorías de los sistemas de información.
  - 12.7.1 Controles de auditoría de los sistemas de información.

13. SEGURIDAD EN LAS TELECOMUNICACIONES.
- 13.1 Gestión de la seguridad en las redes.
  - 13.1.1 Controles de red.
  - 13.1.2 Mecanismos de seguridad asociados a servicios en red.
  - 13.1.3 Segregación de redes.
- 13.2 Intercambio de información con partes externas.
  - 13.2.1 Políticas y procedimientos de intercambio de información.
  - 13.2.2 Acuerdos de intercambio.
  - 13.2.3 Mensajería electrónica.
  - 13.2.4 Acuerdos de confidencialidad y secreto.

14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.
- 14.1 Requisitos de seguridad de los sistemas de información.
  - 14.1.1 Análisis y especificación de los requisitos de seguridad.
  - 14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.
  - 14.1.3 Protección de las transacciones por redes telemáticas.
- 14.2 Seguridad en los procesos de desarrollo y soporte.
  - 14.2.1 Política de desarrollo seguro de software.
  - 14.2.2 Procedimientos de control de cambios en los sistemas.
  - 14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
  - 14.2.4 Restricciones a los cambios en los paquetes de software.
  - 14.2.5 Uso de principios de ingeniería en protección de sistemas.
  - 14.2.6 Seguridad en entornos de desarrollo.
  - 14.2.7 Externalización del desarrollo de software.
  - 14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.
  - 14.2.9 Pruebas de aceptación.
- 14.3 Datos de prueba.
  - 14.3.1 Protección de los datos utilizados en pruebas.

15. RELACIONES CON SUMINISTRADORES.
- 15.1 Seguridad de la información en las relaciones con suministradores.
  - 15.1.1 Política de seguridad de la información para suministradores.
  - 15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.
  - 15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.
- 15.2 Gestión de la prestación del servicio por suministradores.
  - 15.2.1 Supervisión y revisión de los servicios prestados por terceros.
  - 15.2.2 Gestión de cambios en los servicios prestados por terceros.

16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.
- 16.1 Gestión de incidentes de seguridad de la información y mejoras.
  - 16.1.1 Responsabilidades y procedimientos.
  - 16.1.2 Notificación de los eventos de seguridad de la información.
  - 16.1.3 Notificación de puntos débiles de la seguridad.
  - 16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.
  - 16.1.5 Respuesta a los incidentes de seguridad.
  - 16.1.6 Aprendizaje de los incidentes de seguridad de la información.
  - 16.1.7 Recopilación de evidencias.

17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.
- 17.1 Continuidad de la seguridad de la información.
  - 17.1.1 Planificación de la continuidad de la seguridad de la información.
  - 17.1.2 Implantación de la continuidad de la seguridad de la información.
  - 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.
- 17.2 Redundancias.
  - 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.

18. CUMPLIMIENTO.
- 18.1 Cumplimiento de los requisitos legales y contractuales.
  - 18.1.1 Identificación de la legislación aplicable.
  - 18.1.2 Derechos de propiedad intelectual (DPI).
  - 18.1.3 Protección de los registros de la organización.
  - 18.1.4 Protección de datos y privacidad de la información personal.
  - 18.1.5 Regulación de los controles criptográficos.
- 18.2 Revisiones de la seguridad de la información.
  - 18.2.1 Revisión independiente de la seguridad de la información.
  - 18.2.2 Cumplimiento de las políticas y normas de seguridad.
  - 18.2.3 Comprobación del cumplimiento.

ANEXO N° 05 - TRATAMIENTO DE RIESGO

Controles para el tratamiento de Riesgo

Id de Riesgo	Activo	Vulnerabilidad	Amenaza	Posible Amenaza	Impacto	Nivel de Riesgo	Jerarquía de Control	Control Especifico	Control Alineado al ISO 27002:2013	Responsable
R3	Hardware	Susceptibilidad a la humedad, al polvo y a la suciedad	Polvo, corrosión, congelamiento	Posible	Moderado	Alto	Mitigar	11 seguridad física y Ambiental	11.2.4 Mantenimiento de equipos	Jefe de área de Informática / Soporte Técnico
R5	Hardware	Falta de control eficiente del cambio de configuración	Error en el uso	Probable	Moderado	Alto	Mitigar	12 seguridad Operativa	12.1.2 Gestión de cambios	Jefe de área Informática / Soporte Técnico
R6	Hardware	Susceptibilidad a variaciones de voltaje	Pérdida del suministro eléctrico	Probable	Menor	Alto	Mitigar	11 seguridad física	11.1.4 Protección contra las amenazas y ambientales	Soporte Técnico / Mantenimiento
R8	Hardware	Almacenamiento no protegido	Robo de medios	Probable	Moderado	Alto	Mitigar	12 seguridad Operativa	12.3.1 Copia de seguridad de la información	Administrador de servidores BD
R9	Hardware	Falta de cuidado al descartarlo	Robo de medios	Probable	Moderado	Alto	Mitigar	8 gestión de activos	8.3.1 Gestión de soporte extraíbles	Jefe de área Informática
R10	Hardware	Copia no controlada	Robo de medios	Probable	Menor	Alto	Mitigar	12 seguridad Operativa 8 Gestión de activos	12.5.1 Control de Software en explotación 8.3.1 Gestión de soporte extraíble	Administrador de Servidores
R12	Software	No hacer “logout” cuando se sale de las estaciones de trabajo	Abuso de derechos	Casi Seguro	Menor	Alto	Mitigar	9 control de Acceso	9.4.2 Procedimiento seguro de inicio de sesión	Webmaster / Administrador de Servidores BD
R14	Software	Asignación equivocada de derechos de acceso	Abuso de derechos	Improbable	Mayor	Alto	Mitigar	9 control de Acceso	9.2.2 Gestión de los derechos acceso asignado a usuario	Jefe de área Informática
R17	Software	Mala administración de claves	Falsificación de datos	Probable	Moderado	Alto	Mitigar	9 control de Acceso	9.4.3 Gestión de Contraseña de usuarios	Jefe de área de Informática
R19	Software	Falta de copias de respaldo	Adulteración del software	Probable	Moderado	Alto	Mitigar	12 seguridad Operativa	12.3.1 Copia de seguridad de la información	Administrador de servidores BD
R25	Red	Transferencia de contraseñas autorizadas	Espionaje remoto	Probable	Moderado	Alto	Mitigar	13 seguridad en las telecomunicaciones 9 Control de Acceso	13.1.2 Mecanismo de seguridad asociados a servicios en red 9.1.2 Control de acceso a las redes y servicios asociados	Jefe de área Informática
R26	Red	Gestión inadecuada de la red	Saturación del sistema de información	Probable	Menor	Alto	Mitigar	13 seguridad en las telecomunicaciones	13.1.1 Controles de red	Jefe de área de Informática / Soporte Técnico
R29	Personal	Procedimientos inadecuados de contratación	Destrucción de equipos o medio	Probable	Moderado	Alto	Mitigar	8 gestión de activos	8.3.2 Eliminación de soporte	Jefe de área de Informática / Soporte Tecnico

R32	Personal	Falta de conciencia de seguridad	Error en el uso	Probable	Menor	Alto	Mitigar	7 seguridad ligada a los RRHH	7.2.2 Concienciación educación capacitación en seguridad de la información	Jefe de área de Informática
R33	Sitio	Uso inadecuado o descuido del control de acceso a las edificaciones o recintos	Inundación	Casi Seguro	Menor	Alto	Mitigar	11 seguridad física ambiental	11.1.2 Controles físicos de entrada	Jefe de área de Informática
R34	Sitio	Red inestable de energía eléctrica	Perdida de suministro eléctrico	Probable	Moderado	Alto	Mitigar	11 seguridad física	11.1.4 Protección contra las amenazas y ambientales	Soporte Técnico / Mantenimiento
R35	Sitio	Falta de protección física del edificio puertas y ventanas.	Robo de equipos	Probable	Moderado	Alto	Mitigar	11 seguridad física	11.1.3 Seguridad de Oficina, despacho y recursos	Jefe de área de Informática
R36	Organización	Falta de un procedimiento formal para el registro y baja de los usuarios.	Abuso de derechos	Posible	Moderado	Alto	Mitigar	9 control de Acceso	9.2.1 Gestión de altas / bajas en el registro de usuarios	Webmaster / Administrador de Servidores BD
R37	Organización	Falta de proceso formal para revisar el derecho de acceso	Abuso de derechos	Casi Seguro	Menor	Alto	Mitigar	9 control de Acceso	9.2.5 Revisión de los derechos de acceso a los usuarios	Webmaster / Administrador de Servidores BD
R38	Organización	Falta de procesamiento de monitoreo de las instalaciones de procesamiento de la información.	Abuso de derechos	Raro	Mayor	Alto	Mitigar	9 control de Acceso	9.1.2 Control de acceso a las redes y asociados	Soporte Técnico
R39	Organización	Falta de informes de fallas registradas en los registros del administrador y del operador.	Abuso de derechos	Probable	Moderado	Alto	Mitigar	14 adquisición, desarrollo y mantenimiento de los sistemas de información	14.2.1 Política de desarrollo seguro de software	Jefe de área Informática / Administrador de Servidores BD
R40	Organización	Falta de procedimientos en el control de cambios.	Ruptura de mantenibilidad del sistema de información	Probable	Menor	Alto	Mitigar	9 control de Acceso	9.4.5 Control de Acceso al código fuente a los programas	Jefe de área Informática / Administrador de Servidores BD
R43	Organización	Falta de procedimientos para manejo de la información clasificada	Error en el uso	Probable	Menor	Alto	Mitigar	8 gestión de activos	8.2.1 Directrices de clasificación	Jefe de área Informática
R44	Organización	Falta de políticas formal sobre el uso de computadoras portátiles.	Robo de equipos	Probable	Moderado	Alto	Mitigar	11 seguridad física Ambiental	11.2.6 Seguridad de los equipos y activos fuera de las instalaciones	Jefe de área Informática / Soporte Técnico
R45	Organización	Inexistencia o insuficiencia de la política de “Escritorios despejado y pantalla despejada”	Robo de medios	Probable	Moderado	Alto	Mitigar	11 seguridad física Ambiental	11.2.9 Política de puesto de trabajo y pantalla despejada	Jefe de área Informática / Soporte Técnico

ANEXO N° 06 - APLICABILIDAD

"DESCRIPCIÓN DE CONTROLES ISO/IEC 27002:2013 APLICADOS AL ÁREA DE INFORMÁTICA DE LA MUNICIPALIDAD PROVINCIAL DE HUÁNUCO"

7. Seguridad en los Recursos Humanos

7.1 Generalidades: Debe educarse e informar al personal desde su ingreso y en forma continua, cualquiera sea su situación de actividad, acerca de las medidas de seguridad que afectan al desarrollo de sus funciones y de las expectativas depositadas en ellos en materia de seguridad y asuntos de confidencialidad.

7.2. Objetivo: Reducir los riesgos de error humano, comisión de actos ilícitos, uso inadecuado de instalaciones y recursos, manejo no autorizado de la información, junto a la definición de posibles sanciones que se aplicarán en caso de incumplimiento.

7.3. Alcance: La política de seguridad de la institución debe ser aplicada por todos los trabajadores, en el transcurso de sus actividades y tareas involucradas.

7.4. Responsables:

7.4.1. El responsable del Área informática: Se encargará de entregar y hacer de conocimiento de la política de seguridad al área de recursos humanos para su adaptación a las funciones de puesto.

7.4.2. Área de Recursos Humanos: Es su responsabilidad incluir las funciones relativas a la seguridad de la información en las descripciones de puestos de los empleados, informar a todo el personal que ingresa de sus obligaciones respecto del cumplimiento de la Política de Seguridad de la Información, gestionar los Compromisos de Confidencialidad con el personal y coordinar las tareas de capacitación de usuarios respecto a las necesidades actuales en seguridad.

7.4.3. Área Jurídica: Se encargará de la confección del Compromiso de Confidencialidad a firmar por los empleados y terceros que desarrollen funciones en el organismo, en el asesoramiento sobre las sanciones a ser aplicadas por incumplimiento de las Políticas en seguridad y en el tratamiento de incidentes de seguridad que requieran de su intervención.

	7.2 DURANTE LA CONTRATACIÓN	
7. SEGURIDAD EN LOS RECURSOS HUMANOS	7.2.2 Concienciación educación capacitación en seguridad de la información.	Se debe definir un plan de capacitación para los trabajadores.

8. Gestión de Activos

8.1. Generalidades: La institución debe clasificar los activos de información de acuerdo a la sensibilidad y criticidad de la información que contienen con el objeto de señalar cómo ha de ser tratada y protegida dicha información.

8.2. Objetivo: La institución debe tener el conocimiento preciso sobre los activos que posee como parte importante de la administración de riesgos.

8.3. Alcance: La clasificación de activos abarca a toda la institución porque cuenta con al menos cada área con un activo físico o lógico en riesgo.

8.4. Responsables:

8.4.1. El responsable del Área informática: Se encargará de elaborar y mantener un inventario de activos de información, mostrando los propietarios de los activos del área (directivos o gestores responsables de proteger sus activos).

8. GESTIÓN DE ACTIVOS	**8.2 CLASIFICACIÓN DE LA INFORMACIÓN**	
	8.2.1 Clasificación de la información	Se debe realizar una clasificación de los activos identificados según la criticidad de la institución.
	8.3 MANEJO DE MEDIOS	
	8.3.1 Gestión de medios removibles (extraíbles)	Se deberían establecer procedimientos para la gestión de los medios informáticos removibles.
	8.3.2 Eliminación de medios	Para eliminar los medios que contienen información confidencial se debe seguir un protocolo que asegure su correcto desecho.

9. Control de Acceso

9.1. Generalidades: cada institución debe aplicar el impedimento el acceso no autorizado a los sistemas de información, así también se deberían implementar procedimientos formales para controlar la asignación de derechos de acceso a los sistemas de información, bases de datos y servicios de información, y estos deben estar claramente documentados, comunicados y controlados en cuanto a su cumplimiento.

9.2. Objetivo: Controlar el acceso por medio de un sistema de restricciones y excepciones a la información como base de todo sistema de seguridad informática.

9.3. Alcance: Los procedimientos comprenden todas las etapas del ciclo de DEMING de los accesos de los usuarios de todos los niveles, desde el registro inicial de nuevos usuarios hasta la privación final de derechos de los usuarios que ya no requieren el acceso.

9.4. Responsables:

9.4.1. El responsable de redes y telecomunicaciones: Sera el encargado de controlar el flujo de la información en los diferentes niveles de acceso, comprendiendo todas las etapas del ciclo de DEMING de los accesos de los usuarios.

9.4.2. El responsable del Área informática: Se encargará de concientizar a los mismos acerca de sus responsabilidades por el mantenimiento de controles de acceso eficaces, en particular aquellos relacionados con el uso de contraseñas y la seguridad del equipamiento.

9. CONTROL DE ACCESO	**9.1 REQUERIMIENTOS DE NEGOCIO PARA EL CONTROL DE ACCESOS**	
	9.1.2 Control de acceso a las redes y servicios asociados	Establecer una política de accesos a nivel de red que nos permita establecer los lineamientos en cuanto a segmentación de redes, accesos de externos a la red interna, monitoreo, etc.
	9.2 GESTIÓN DE ACCESO DE USUARIO	
	9.2.1 Gestión de altas/bajas en el registro de usuarios	Para poder mitigar el riesgo de acceso no autorizado, se debe mantener un procedimiento de altas y sobre todo bajas de usuarios de los sistemas que maneja la Municipalidad.
	9.2.2 Gestión de los derechos de acceso asignados a usuarios	Contar con una correcta gestión de privilegios que permitirá limitar el acceso según las funciones o áreas a las cuales cada colaborador pertenece.
	9.2.5 Revisión de los derechos de acceso de los usuarios	Los propietarios de los activos deberían revisar con regularidad los derechos de acceso de los usuarios.
	9.4 CONTROL DE ACCESO A SISTEMAS Y APLICACIONES	
	9.4.2 Procedimientos de inicio de sesión segura	Cuando sea requerido por la política de control de accesos se debería controlar el acceso a los sistemas y aplicaciones mediante un procedimiento seguro enfocado a proteger la información de inicio de sesión del usuario en los sistemas.
	9.4.3 Sistema de gestión de contraseña	Los sistemas de gestión de contraseñas deberían ser interactivos y asegurar

		contraseñas de calidad. Establecer requisitos mínimos en cuanto a la complejidad de contraseñas.
	9.4.5 Control de acceso al código fuente del programa	Se debería restringir el acceso al código fuente de las aplicaciones software.

11. Seguridad Física y del Entorno

11.1. Generalidades: Establecimiento de perímetros de seguridad y áreas protegidas facilita la implementación de controles de protección de las instalaciones de procesamiento de información crítica. El control de los factores ambientales de origen interno y/o externo permite garantizar el correcto funcionamiento de los equipos de procesamiento y minimizar las interrupciones de servicio.

11.2. Objetivo: Minimizar los riesgos de daños e interferencias a la información y a las operaciones.

11.3. Alcance: Los controles de protección de la información se enfocarán en las áreas que cuenten con información sensible con riesgo de pérdida.

11.4. Responsables:

11.4.1. El responsable de redes y telecomunicaciones: Sera el encargado de definir los controles de protección de la información y telecomunicaciones.

11.4.2. El responsable del Área informática: Se encargará del transporte y la disposición final presentan riesgos que deben ser evaluados.

11. SEGURIDAD FÍSICA Y DEL ENTORNO	**11.1 ÁREAS SEGURAS**	
	11.1.2 Controles físicos de entrada	Las áreas seguras deberían estar protegidas mediante controles de entrada adecuados para garantizar que solo el personal autorizado dispone de permiso de acceso. El personal debe estar debidamente identificado en todo momento.
	11.1.3 Seguridad de oficinas, despachos y recursos	Se debería diseñar y aplicar un sistema de seguridad física a las oficinas e instalaciones de la Municipalidad.
	11.1.4 Protección contra las amenazas externas y ambientes	Se debería diseñar y aplicar una protección física contra desastres naturales, ataques maliciosos o accidentes, que puedan afectar tanto natural como provocados (incendios).
	11.2 SEGURIDAD DE LOS EQUIPOS	
	11.2.4 Mantenimiento de los equipos	Los equipos que cuenten con acceso a información crítica deberán seguir un procedimiento de mantenimiento adecuado de manera que la información que contienen no sea comprometida.
	11.2.6 Seguridad de los equipos y activos fuera de las instalaciones	La municipalidad debe asegurar que cualquier uso externo de la información que maneja la oficina de registros, haya sido previamente autorizado por las

		personas correspondientes.
	11.2.9 Políticas de puesto de trabajo despejado y bloqueo de pantalla	Los usuarios deberán mantener sus escritorios libres de cualquier información sensible que pueda usar un agente externo como consecuencia de sus exposiciones como parte de un olvido o mala gestión

12. Seguridad en la operativa

12.1. Generalidades: La Municipalidad Provincial de Huánuco debe crear condiciones que garanticen la confidencialidad, integridad y disponibilidad de la información que se produce y se recibe a través de diferentes canales de operación.

12.2. Objetivo: Adoptar medidas de seguridad encaminadas a prevenir la proliferación y expansión de software malicioso que son catalogadas como amenazas en potencia, garantizar el adecuado funcionamiento de los sistemas de información y designar responsables encargados de adoptar todas las medidas de seguridad necesarias para prevenir posibles ataques.

12.3. Alcance: Esta política se debe aplicar a todo el sistema informático (red, servidores, comunicaciones y equipos) etc.

12.4. Responsables:

12.4.1. El responsable de la seguridad informática: Sera el encargado de definir procedimientos para el control

actualización y modificación de los sistemas operativos tanto de servidores como ordenadores.

- Para la actualización, modificación y mantenimiento debe estar debidamente documentada.
- Se debe tener mecanismos para el reporte y manejo de incidentes
- Se debe tener políticas de control para el uso de correo electrónico, consulta de páginas, navegación en internet y uso de redes sociales.
- Adquirir antivirus licenciado y verificar que las actualizaciones se estén realizando periódicamente.
- Establecer y verificar políticas de control de usuarios mediante contraseñas y gestión de privilegios.
- Controlar la realización de copias de seguridad.
- Todo procedimiento debe ser debidamente documentado.

12.4.2. El responsable del Área informática: Se encargará de adoptar todas las políticas establecidas por el responsable de la seguridad y verificará el cumplimiento de las mismas.

12. SEGURIDAD EN LA OPERATIVA	**12.1 RESPONSABILIDADES Y PROCEDIMIENTOS DE OPERACIÓN**	
	12.1.2 Gestión de Cambios	Los cambios deben ser evaluados y aprobados previamente y se tendrán en cuenta los siguientes aspectos: evaluación del cambio y posible impacto, planificación, prueba, e identificación de responsabilidades en caso de que el cambio sea fallido.
	12.3 COPIAS DE SEGURIDAD	
	12.3.1 Copias de seguridad de la información	Es necesario realizar y pruebas regulares de las copias de la información, del software y de las imágenes del sistema de relación a una política de respaldo (Backup) convenida
	12.5 CONTROL DE SOFTWARE EN EXPLOTACIÓN	
	12.5.1 Instalación del software en sistemas en producción	Se deberían implementar procedimientos para controlar la instalación de software en sistemas operacionales.

13. Seguridad en las telecomunicaciones

13.1. Generalidades: La Municipalidad Provincial de Huánuco debe crear condiciones que garanticen la seguridad en cuanto a las telecomunicaciones.

13.2. Objetivo: Adoptar medidas de seguridad encaminadas a prevenir la mala implementación de redes de telecomunicaciones dentro de la entidad para poder garantizar su debida seguridad.

13.3. Alcance: Esta política se debe aplicar a todo el sistema de redes y telecomunicaciones.

13.4. Responsables:

13.4.1. El responsable de redes y telecomunicaciones: Sera el encargado de definir procedimientos para el control implementación y modificación de las telecomunicaciones.

13.4.2. El responsable del Área informática: Se encargará de adoptar todas las políticas establecidas por el responsable de las redes y verificará el cumplimiento de las mismas.

13. SEGURIDAD EN LAS TELECOMUNICACIONES	**13.1 Gestión de la seguridad en las redes**	
	13.1.1 Controles de red	Se deberían administrar y controlar las redes para proteger la información en sistemas y aplicaciones.
	13.1.2 Mecanismos de seguridad asociados a servicios en red	Se deberían identificar e incluir en los acuerdos de servicios (SLA) los mecanismos de seguridad, los niveles de servicio y los requisitos de administración de todos los servicios de red, independientemente de si estos servicios se entregan de manera interna o están externalizados.

14. Adquisición, desarrollo y mantenimiento de sistemas de información

14.1. Generalidades: Se debe documentar y aprobar los requerimientos de seguridad a aplicar en la implementación de los sistemas de información; se debe llevar a cabo adecuadas políticas de seguridad para las bases de datos, los sistemas operativos, todo esto con el fin de evitar que personas conocedoras de los procesos puedan cometer fraudes o ilícitos y si es el caso identificarlos de manera inmediata.

14.2. Objetivo: Adoptar medidas de seguridad en la implementación de los sistemas de información.

14.3. Alcance: Esta política se debe aplicar a todos los sistemas informáticos tanto sistemas operativos como software requerido para la Municipalidad.

14.4. Responsables:

14.4.1. Responsable de la seguridad informática: El propietario de la información y el área de auditoría interna se encargarán de definir e implementar controles en el desarrollo y mantenimiento de sistemas de información.

14.4.2. El responsable del Área informática: Se encargará de definir el procedimiento para asignar claves, de garantizar el cumplimiento de los requisitos de seguridad del software, de controlar los cambios en los sistemas etc.

14.4.3. El responsable del área legal y administrativa: Se encargará del licenciamiento del software adquirido y en el caso del software desarrollado por la organización de establecer las políticas de derechos de autor y fijar las condiciones de los contratos y de entrega.

14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN	**14.2 SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y SOPORTE**	
	14.2.1 Políticas de desarrollo seguro de software	Se deberían establecer y aplicar reglas para el desarrollo de software y sistemas dentro de la Municipalidad.