UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR

FACULTAD DE INGENIERÍA Y GESTIÓN

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

"PLAN DE LA SEGURIDAD DE LA INFORMACÍON BASADO EN LA NORMA ISO 27001 PARA LA SUB GERENCIA DE INFORMÁTICA Y TECNOLOGÍAS DE LA INFORMACIÓN DE LA MUNICIPALIDAD DE PUNTA HERMOSA"

TRABAJO DE SUFICIENCIA PROFESIONAL

Para optar el Título Profesional de

INGENIERO DE SISTEMAS

PRESENTADO POR EL BACHILLER

MEDRANO FLORES, YAMIR ADOLFO

Villa El Salvador

2019

DEDICATORIA

Dedico este trabajo en primer lugar a mi Padre Celestial por un día más de vida y su ayuda de poder lograr mis metas; a mis padres por su esfuerzo y dedicación durante todo el tiempo.

AGRADECIMIENTO

Agradezco a mi Universidad Nacional Tecnológica de Lima Sur (UNTELS), ya que me abrió las puertas durante estos 5 años, las cuales me han formado como profesional.

A mis docentes universitarios por el apoyo y ser mi guía en este periodo de estudio.

A mis compañeros de trabajo del área de informática por brindarme su apoyo y colaboración.

Al Dr. Igor Aguilar Alonso (asesor) por ser una guía y darme las pautas necesarias para desarrollar este proyecto.

ÍNDICE

LISTADO DE TABLAS

LISTADO DE FIGURAS

INTRODUCCIÓN

El proyecto de investigación lleva como título: “Plan de la Seguridad de Información basado en la Norma ISO 27001 para la Sub Gerencia de Informática y Tecnologías de la Información de la Municipalidad de Punta Hermosa”, la cual me ayudará a obtener el título de Ingeniero de Sistemas”, realizado por el Bachiller Medrano Flores, Yamir Adolfo.

Una de las funciones más esenciales de la Municipalidad de Punta Hermosa es proveer al ciudadano un ambiente óptimo para desenvolverse y satisfacer las necesidades esenciales de las familias. Esto quiere decir que no sólo se basa en la seguridad, sino también en la salubridad, equipamiento, recreación e igualdad en sus derechos. La Municipalidad Distrital de Punta Hermosa ejerce a través de sus Órganos las funciones generales establecidas en los Artículos 195° y 197° de Ia Constitución Política, Ley N° 27783 Ley de Bases de Ia Descentralización, Ley N° 27972 Ley Orgánica de Municipalidades y demás normas pertinentes.

Según el Artículo 64° del Reglamento de Organización y Funciones (ROF), la Municipalidad Distrital de Punta Hermosa cuenta con la Sub Gerencia de Informática y Tecnologías de la Información, cabe recalcar que es un órgano de apoyo de tercer nivel teniendo como asignación de dirigir y efectuar el mantenimiento de la infraestructura informática y de telecomunicaciones basado a las políticas y el planeamiento estratégico institucional (PEI); cabe mencionar que es el ejecutor de las normas emitidas por el ente rector del Sistema Nacional de Informática y los conceptos de Gobierno Electrónico en los servicios y procesos de la Municipalidad. La Sub gerencia siempre estará bajo la supervisión de la Gerencia de Administración y Finanzas.

La Municipalidad Distrital de Punta Hermosa, es integrante del Sistema Nacional de Informática, pero aún no tiene un sistema de Gestión de Seguridad de la Información en el marco de la norma NTP-

ISO/IEC 27001:2014, que permita establecer una adecuada gestión de seguridad de la información para así cumplir con la normativa vigente. Finalmente, no se ha efectuado ningún procedimiento para la mejora de la seguridad de información, anular la fuga de información a través de políticas; con lo cual es totalmente claro que existe una alta probabilidad de perdida de la información.

Como solución a los descrito líneas arriba, se propone realizar un plan de seguridad de información que permita identificar los activos, amenazas, vulnerabilidades; para así poder conocer, gestionar y minimizar todos los riesgos que perjudiquen a la seguridad de la información en la Municipalidad, donde se establecerán mecanismos alineados basadas en la Norma ISO 27001, cabe señalar que es indispensable tener los documentos normativos para una eficaz administración de los procesos.

En el primer capítulo trataremos la realidad problemática, justificación del problema, las delimitaciones y se plantearan los objetivos generales y específicos. En el segundo capítulo se desarrollará los antecedentes de esta investigación, contando con las bases teóricas y el marco conceptual que se usará como base para el proceso de la investigación. En el tercer capítulo abordamos el desarrollo de la metodología y finalmente concluimos con la revisión y consolidación de los resultados, las conclusiones, recomendaciones.

CAPÍTULO I: PLANTEAMIENTO DEL PROBLEMA

1.1 Descripción de la Realidad Problemática

Hoy en día las tecnologías de información han ido evolucionando haciendo que sea más intenso el poder manipular y manejar la información, generando beneficios para las organizaciones como la mejora de su servicio, operatividad y creando procesos más eficientes; por lo que se puede decir que aplicar la seguridad de la información es de mucha importancia en las organizaciones.

Para Erb, Markus (2014) la seguridad informática debe proteger los activos informáticos como:

- La infraestructura computacional: Es la parte esencial para el almacenamiento y administración de la información, debe ser asegurada por un área encargada el cual se asegurará que los equipos funcionen adecuadamente, y protegerlos en casos de robos, fallas en el suministro eléctrico y cualquier otro factor que amenace la infraestructura informática.

- Los usuarios: Se les deben diseñar protocolos que permitan proteger la información que ellos utilizan, para que esta no se convierta vulnerable y a su vez instruirlos sobre las posibles amenazas existentes. Existen también errores de programación siendo usados como exploits por los crackers dando como resultado el robo de la información o la alteración del funcionamiento.

Según el Computer Security Institute (CSI) de San Francisco; Aproximadamente entre el 60 y el 80% de los incidentes de red son causados desde dentro de la misma.

“Existe una amenaza informática del futuro, anteriormente el

objetivo de los ataques era cambiar las plataformas tecnológicas, ahora existen tendencias cibercriminales señalando que la nueva moda indica es manipular los certificados que contienen la información digital. Antes el área semántica que era reservada para las personas los humanos se han convertido en el centro de los ataques como consecuencia al desarrollo de la web y de las redes sociales". (Ramírez, E. & Aguilera, A. 2009)

La Sub Gerencia de Informática y Tecnologías de la Información de la Municipalidad evidencia que tiene una red de datos desprotegida en algunas áreas funcionales, carece de planes de respaldo adecuados ante la posible falla del sistema, ausencia de mantenimiento y actualización del software y hardware, y cuenta con escasas políticas para realizar copias de seguridad.

La poca seguridad física en que hay en lagunas áreas ocasiona la probabilidad de robo de información y/o la omisión de concientización y capacitación a las gerencias y el personal respecto a la seguridad de información.

En términos generales la Municipalidad Distrital de Punta Hermosa carece de un plan de seguridad de la información que le pueda permitir proteger la confidencialidad, disponibilidad e integridad que se gestiona diariamente, es por ello que se sugiere dicho plan de seguridad para poder identificar los activos de información y los riesgos a través de selección de controles. Esta situación no permite poder cumplir con lo que establece la ONGEI en la **Resolución Ministerial N° 004-2016-PCM.**

1.2 Justificación del Problema

La justificación de esta investigación es poder establecer un plan para la Seguridad de Información que es indispensable en cualquier organización estatal o privada a tal grado que no es suficiente hacer grandes inversiones en sistemas y dispositivos de seguridad, asegurando la integridad, disponibilidad y confidencialidad de estos, protegiendo de esta forma la información de todas las partes interesadas, haciendo cumplir la norma ISO 27001. El plan de seguridad de la información buscará mejorar la efectividad de todos los procesos, tanto en la parte administrativa, operativa y tecnológica dentro y fuera de la Municipalidad; con el fin de mantener el riesgo de la información por debajo del nivel asumible, la cual generará confianza en sus partes interesadas siendo fundamental para el crecimiento y sostenibilidad de la institución.

1.2.1. Justificación operativa: siempre se debe recordar el uso obligatorio de la Norma Técnica Peruana NTP-ISO/IEC 27001:2014 en todas las instituciones integrantes del Sistema Nacional de Informática, permitiendo incluir a la alta dirección, en ese aspecto al Sub Gerente de Informática y Tecnologías de la Información.

1.2.2. Justificación tecnológica: la propuesta de políticas basadas en la norma ISO 27001 en la Municipalidad de Punta Hermosa, brindará a la organización una herramienta de soporte de información cumpliendo así con los objetivos tales como el poder minimizar el riesgo de pérdida de la información, principios e innovación tecnológica para poder resguardar la efectividad de la disponibilidad, confidencialidad e integridad de las mismas.

1.2.3. Justificación institucional: se debe considerar que la Municipalidad de Punta Hermosa, debe estar alineada a las normas técnicas internacionales, considerando que en **la Resolución Ministerial N° 004-2016-PCM** con fecha 08 de enero del 2016 se

aprobó el uso obligatorio 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. Requisitos. 2a. Edición”, en todas las entidades integrantes del Sistema Nacional de Informática; considerando que existen plazos a las entidades públicas para que puedan implementar y adecuar a la norma.

1.3 Delimitación del Proyecto

1.3.1. Teórica:

Este proyecto es de actualidad, ya que se está realizando un plan de seguridad de la información basado en la norma ISO 27001 para la Sub Gerencia de Informática y Tecnologías de la Información de la Municipalidad de Punta Hermosa.

- **Plan de Seguridad de la Información:** Es un documento que sirve para poder proteger la información, asegurando la confidencialidad, disponibilidad e integridad. (Leyva, 2016)
- **Sistema de Gestión de Seguridad de la Información (SGSI):** Es el diseño, implantación y mantenimiento de un conjunto de procedimientos para gestionar eficientemente la accesibilidad de la información, minimizando los riesgos a los que están expuestos los activos de información. (ISO27000.es)

1.3.2. Temporal:

Aproximadamente, el proyecto de plan de implementación de seguridad de la información se ejecutó durante de 5 meses, desde el mes de enero del 2019 a mayo del 2019.

1.3.3. Espacial:

La investigación se realizó en la Municipalidad Distrital de Punta Hermosa ubicado en la parte central de la Provincia y Departamento de Lima, a la altura de los Km 42 al 46 de la Antigua Panamericana Sur. Limita con el Norte con el Distrito de Lurín, por el sur, con el Distrito de Punta Negra, por el este con el Distrito de Santo Domingo de Olleros de la Provincia de Huarochirí y por el Oeste con el Océano Pacifico.

1.4 Formulación del Problema

1.4.1 Problema general

¿Un Plan de Seguridad de la Información basado en la norma ISO 27001 permitirá mantener y mejorar la disponibilidad, confidencialidad e integridad de la información de la Sub Gerencia de Informática y Tecnologías de la Información de la Municipalidad de Punta Hermosa?

1.4.2 Problemas específicos

- ¿Con el plan de seguridad de la información basado en la norma ISO 27001 se permitirá identificar los activos de información que serán de gran ayuda para la mejora de la seguridad de la información?

- ¿Con el plan de seguridad de la información basado en la norma ISO 27001 se permitirá reconocer y evaluar los riesgos de la Sub Gerencia de Informática y Tecnologías de la Información?

- ¿Con el plan de seguridad de la información basado en la norma ISO 27001 se ayudará a definir políticas y controles que logren reducir los riesgos de la seguridad de información?

1.5 Objetivos

1.5.1 Objetivo General

Proponer un Plan de Seguridad de Información basado en la norma ISO 27001 para mantener y mejorar la disponibilidad, confidencialidad e integridad de la información para la Sub Gerencia de Informática y Tecnologías de la Información de la Municipalidad de Punta Hermosa.

1.5.2 Objetivos Específicos

- Reconocer y valorar los activos de información, de la sub gerencia de informática y tecnologías de la información de la municipalidad de Punta Hermosa.

- Analizar y valorar los riesgos identificando las vulnerabilidades, amenazas que enfrentan los activos de información de la municipalidad de Punta Hermosa.

- Diagnosticar y sugerir políticas y controles apropiados para reducir los riesgos de la seguridad de la información para a sub gerencia de informática y tecnologías de la información de la municipalidad de Punta Hermosa.

CAPÍTULO II: MARCO TEÓRICO

2.1 Antecedentes de la Investigación

2.1.1. Antecedentes Internacionales

Para elaborar la propuesta de Plan de la seguridad de la información basada en la norma ISO 27001, es conveniente referirnos a tesis realizados que guarden relación con los objetivos de este proyecto.

(Moyano Orjuela & Suárez Cárdenas, 2017) , en su tesis **plan de implementación del SGSI basado en la norma ISO 27001:2013 para la empresa Interfaces y Soluciones**, en esta investigación se llegó a determinar que el problema era el siguiente: ¿De qué manera la implementación de un SGSI puede garantizar la integridad, confidencialidad y disponibilidad de su información? , donde el objetivo era establecer un sistema de gestión de la seguridad de la información (SGSI) basado en la norma ISO 27001:2013, siendo la metodología a emplear MAGERIT. Se concluye que: Al iniciar el plan de implementación del SGSI, para la empresa interfaces y Soluciones, la identificación de necesidades y requerimientos permitió evidenciar la preocupación de la gerencia por los temas relacionados con la seguridad de la información, también la gestión de riesgos realizada en la compañía estableció las bases para la mejora continua del SGSI. Por lo tanto, se identificaron y clasificaron los activos. Se resalta una alta probabilidad e impacto de la materialización de amenazas relacionadas con abuso de información privilegiada y actos no autorizados, ataques internos, ataques externos, intrusión física y/o robo, errores y omisiones, fallos en el sistema y en el medio ambiente, mientras no se siga el plan de tratamiento y recomendaciones realizadas.

(Picón Carrascal, 2016), en su trabajo para titularse como **máster sobre Elaboración de un plan de Implementación de la ISO/IEC 27001:2013**, la investigación tuvo como objetivo establecer compromiso de la dirección e identificar el enfoque en la gestión de la seguridad de la información, de tal manera que todos los miembros de la organización preserven la confidencialidad, integridad y

disponibilidad de la información. La metodología que se empleó fue de Análisis de Riesgos. Como conclusión se tiene que: El SGSI, sin duda alguna es de las prácticas más eficientes que nos permite una correcta gestión de riesgos dentro de la organización y el cumplimiento de la seguridad de la información bajo un marco de referencia que cerciora su gestión y permanencia en el tiempo. El Sistema de Gestión de Seguridad de la Información se inicia bajo una normativa reconocida como la ISO/IEC 27001 cuya implementación asegurará a la organización de gozar de un adecuado gobierno de seguridad de la información protegiendo los activos, mejorará el negocio, maximizará el retorno de las inversiones asegurando la perpetuidad del negocio.

(Tola Franco, 2015), **Implementación de un sistema de gestión de seguridad de la información para una empresa de consultoría y auditoría, aplicando la Norma ISO/IEC 27001**, la investigación aplico las metodologías del PDCA, gestión del riesgo y MAGERIT. Donde se concluye que es importante establecer los objetivos y políticas del SGSI, pues estos nos señalan la ruta que la organización debe seguir para mantener la confidencialidad, integridad y disponibilidad de la información y por lo tanto es de vital importancia la participación de la alta gerencia. Dentro del ciclo de un SGSI, basado en ISO 27001, se halla el mejoramiento continuo por lo que se hace indispensable que la organización cree procedimientos para el monitoreo y revisión del sistema, los mismos que deben cubrir incidentes de seguridad, auditorías internas y revisiones gerenciales. Estos elementos cooperan con la retroalimentación al Sistema pues hacen posible conocer su estado y efectuar las correcciones necesarias para que se cumplan los planes y objetivos.

(Mesquida Calaft, 2012), en su **tesis de doctor Un Modelo para Facilitar la Integración de Estándares de Gestión de TI en entornos maduros,** el problema principal es que las empresas de desarrollo de software no solo están interesadas en la mejora, sino también en la calidad de los servicios, los modelos de mejora de procesos podrían ser ampliados para poder incluir los procesos de gestión de servicios de TI,

siendo la metodología la PDCA. El cual concluye que se ha dado una visión de la situación actual de los estándares de gestión de TI para identificar sus factores comunes y crear un nuevo modelo integrado que ofrezca la implantación de estos estándares reduciendo esfuerzos y duplicidades. El nuevo modelo integrado de estándares de gestión de TI está realizado por un modelo de referencia de procesos y prácticas que su base son los procesos del ciclo de vida del software; y un sistema de gestión integrado a partir de los requisitos de los sistemas de gestión propuestos por las normas ISO 9001.Una vez desarrollado el modelo integrado, se procedió a validarlo mediante la aplicación real en dos empresas de desarrollo de software, donde se pudo constatar que: el tener determinados procesos de la norma ISO 15004-5 a un cierto nivel de capacidad facilita la implantación de las normas ISO 20000 e ISO 27001; y el poder implantar los procesos de la norma ISO 15504-5, que ya integran las buenas prácticas y requisitos propios de las normas ISO 20000 o ISO 27001, permite reducir gran cantidad de esfuerzos, recursos humanos y recursos materiales por lo tanto también un importante ahorro de costos.

(Polanco Velez, 2013), **Diseño de un manual de procedimientos del sistema contable en la empresa FEVECOMEX S.A.S. basado en la norma técnica colombiana para la seguridad de la información NTC- ISO/IEC 27001/2006**, la investigación identifico que como problema principal no cuenta con un manual de procedimientos del sistema contable, por lo tanto, el objetivo es diseñar un manual que contribuya al mejoramiento del dpto. de contabilidad y satisfaga las necesidades del negocio. La metodología es Inductivo-Deductivo. Se concluye que: Como medida utilizada para manejar el éxito de la organización se establecieron indicadores de gestión en la caracterización de los procesos, clasificados intrínsecamente en: EFICIENCIA organizando los procesos para dar como resultado los mejores resultados posibles con los recursos disponibles y en efectividad en el nivel de logro de los requerimientos u objetivos propuestos. Igualmente se hace seguimiento a la perspectiva del cliente

y se busca la mejora continua de los procesos sin dejar de un lado los indicadores financieros clásicos como son: el aumento de ventas y la disminución de costos, pero exigiéndole al encargado realizar un seguimiento mucho más amplio que incluya otras variables de interés para la organización a través de la interacción con todas las actividades de la empresa.

2.1.2. Antecedentes Nacionales

(Aguirre Mollehuanca, 2014), en su **tesis Diseño de un Sistema de Gestión de Seguridad de Información para Servicios Postales del Perú S.A.**, el problema identificado fue que en primera instancia no se contaba con un sistema de gestión de seguridad de información, pero luego el objetivo fue diseñarla. La Metodología que se empleó fue la del PCDA y MAGERIT. Donde se concluyó que: La alta gerencia era de vital importancia para el modelo de este sistema de gestión, debido a que su participación era concientizar tanto a los jefes de área como a los dueños de los procesos a que participen de las entrevistas de levantamiento de información. Es evidente que hay necesidad en la organización de contratar personal especializado para dar soporte a los procesos involucrados en el SGSI, pues es notorio que los recursos con los que se cuentan no son suficientes para atender todos los requerimientos de los usuarios, que como consecuencia de ello en muchos casos se ha utilizado como excusa para realizar actos que perjudican la seguridad de la información como el préstamo de credenciales de usuarios, uso de un correo para varias personas o el abandono en la generación de respaldos de información del área.

Espinoza (2013), en su **tesis titulada "Análisis y diseño de un sistema de gestión de seguridad de información basado en la norma ISO/IEC 27001: 2005 para una empresa de producción y comercialización de productos de consumo masivo**, se pudo identificar que el objetivo principal fue analizar y diseñar un sistema de seguridad de la información, donde se aplicó las metodologías de MAGERIT y la del PDCA. Se concluye que la adecuada gestión de

seguridad de la información siempre debe estar incluida en la cultura de la organización de las empresas y se debe concientizar a los colaboradores de las empresas sobre la seguridad de la información y su importancia. El proyecto abarca solamente el análisis y diseño del SGSI, basado en la norma ISO/IEC 27001:2005 y está dirigido a procesos, activos, riesgos, y demás consideraciones, de una empresa de producción y comercialización de productos de consumo masivo. El proyecto contribuyó al uso de técnicas necesarias para el levantamiento de los activos de información y el análisis de riesgos, donde se permitió la adecuada definición de controles en base a lo que se encontró.

Alcántara Flores (2015), realizó su trabajo para **titularse "Guía de Implementación de la Seguridad basado en la Norma ISO/IEC 27001, para apoyar la seguridad en los Sistemas Informáticos de la Comisaria del Norte P.N.P en la Ciudad de Chiclayo",** la investigación llego a la siguiente conclusión: Que gracias a la Guía , se pudo lograr aumentar la seguridad en las aplicaciones informáticas de la institución policial, viéndose reflejado el aumento de políticas de seguridad que fueron puestas en marcha que beneficiando a la institución y ayudaron a incrementar el nivel de seguridad en la misma. Con el uso de la Guía, mejoró el proceso para encontrar las anomalías en la seguridad de la información, reflejado en distintos mecanismos de seguridad para salvaguardarla y prevenir su mal uso y divulgación no adecuada.

2.2. Bases Teóricas

2.2.1. Sistema de Gestión de Seguridad de Información

Según Martelo, Madera y Betín (2015), define que el SGSI es un conjunto de políticas que establece la alta dirección con el propósito de definir, construir, desarrollar y mantener la seguridad de los activos de información y asegurar la continuidad de la operatividad de la organización.

Según la ISO (2017), el objetivo de un SGSI es respaldar que los riesgos de la seguridad de la información sean conocidos y asumidos por la institución de una forma sistemática, eficiente y adecuada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías. El sistema de Gestión de la Seguridad de la Información (SGSI) ayuda a establecer políticas y procedimientos en relación a los objetivos de negocio de la institución.

Según Quintero Parra (2015), Un SGSI se define como un sistema que comprende la política, la estructura organizativa, los recursos, los procedimientos y los procesos fundamentales para implantar la gestión de la seguridad de la información en una organización. Para dar trámite de manera efectiva a la seguridad de la información es de mucha importancia considerar una serie de protocolos que permitan dar garantía de los niveles óptimos de seguridad que exige la organización, teniendo en cuenta que no se puede lograr un nivel de seguridad al 100% ya que los riesgos nunca serán eliminados en su totalidad. Las políticas orientadas a la Gestión de Seguridad de la Información están conformadas por el conjunto de normas reguladoras y buenas prácticas que definen el modelo en que todos los activos y recursos de la organización considerando la información misma son gestionados, protegidos y distribuidos.

Para implementar un SGSI, toda organización debe considerar lo siguiente:

1). Determinar la gestión de la seguridad de la información.

2). Examinar y resolver los riesgos.

3). Entablar métodos de gestión de la seguridad siguiendo el ciclo Deming o metodología del PDCA:

* Plan: Selección y definición de medidas y procedimientos.

* Do: Establecer medidas y procesos de mejora.

* Check: Comprobar y verificar las medidas que se han Implantado.

* Act: Actuar para hacer la corrección de las fallas ubicadas en el sistema.

4). Autenticación de la gestión de la seguridad.

2.2.1.1. Beneficios del SGSI para las organizaciones

Según ISO27000.ES, indica que las ventajas de SGSI para las organizaciones son los siguientes:

- Se establece una metodología de gestión de la seguridad clara y estructurada.
- Se reduce el riesgo de pérdida de información.
- Los clientes tienen acceso a la información a través medidas de seguridad.
- Los riesgos tienen sus controles que son revisados continuamente.
- Lealtad de los clientes y socios, por la garantía de calidad y confidencialidad comercial.
- Debe llevarse a cabo auditorías externas ya que ayudan a identificar las debilidades del sistema y las áreas a mejorar.
- Habrá la posibilidad de integrar otros sistemas de gestión (ISO 9001, ISO 14001, OHSAS 18001).
- Prolongación de las operaciones necesarias de negocio tras incidentes de gravedad.

- Aprobación de la legislación vigente sobre información personal, propiedad intelectual y otras.
- Crece la motivación y satisfacción del personal.
- Minimiza los costes, mejora los procesos y servicios.

2.2.1.2. Actividades relevantes de un SGSI

Según ISO27000.ES, indica que las actividades relevantes de un SGSI son los siguientes:

- Implicación de la Dirección.
- Alcance del SGSI y política de seguridad.
- Inventario de todos los activos de información.
- Metodología de evaluación del riesgo.
- Identificación de amenazas, vulnerabilidades e impactos.
- Análisis y evaluación de riesgos.
- Selección de controles para el tratamiento de riesgos.
- Aprobación por parte de la dirección del riesgo residual.
- Declaración de aplicabilidad.
- Plan de tratamiento de riesgos.
- Implementación de controles, documentación de políticas, procedimientos e instrucciones de trabajo.
- Definición de un método de medida de la eficacia de los controles y puesta en marcha del mismo.
- Formación y concienciación en lo relativo a seguridad de la información a todo el personal.
- Monitorización constante y registro de todas las incidencias.
- Realización de auditorías internas.
- Mejora continua del SGSI.

2.2.2. Estándares de seguridad de la información

Dentro de los estándares más conocidos tenemos la MAGERIT 3.0, COBIT y la Familia ISO.

2.2.2.1. MAGERIT 3.0

Según el Ministerio de Hacienda y Administraciones Publicas (2012), Magerit responde a lo que se señala “Proceso de Gestión de los Riesgos”, sección 4.4 (“Implementación de la Gestión de los Riesgos”), MAGERIT incorpora el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo siempre presente los riesgos producidos del uso de tecnologías de la información.

El método de análisis de riesgos que proporciona MAGERIT consiste en cinco (5) pasos (Ministerio de Hacienda y Administraciones Publicas, 2012):

1. Determinar los activos relevantes para la organización, sus relaciones entre si y el valor que tienen.
2. Determinar las amenazas a las que se exponen los activos.
3. Determinar las salvaguardas disponibles y que tan eficaces son frente al riesgo.
4. Estimar el impacto que tendría una amenaza al dañar un activo.
5. Estimar el riesgo.

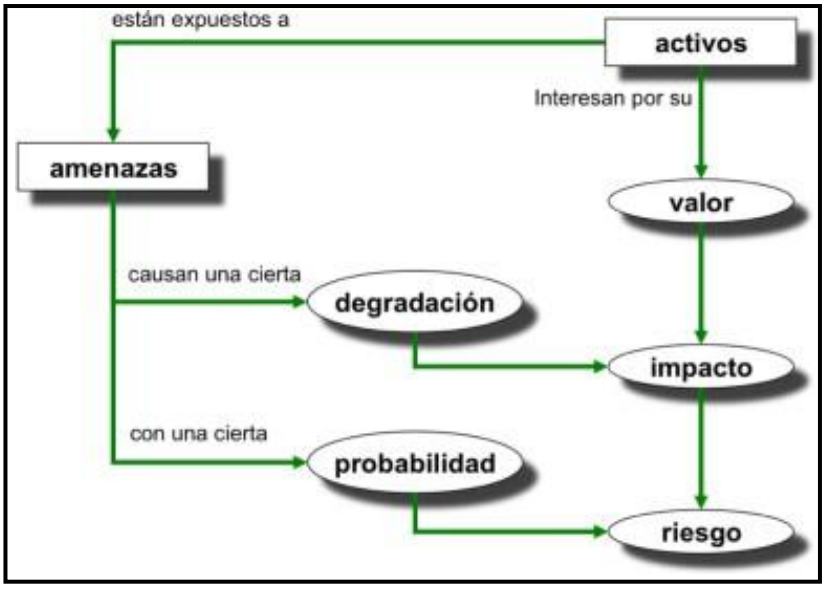


Figura 1 Elementos del análisis de riesgos potenciales

Fuente: Ministerio de Hacienda y Administraciones Públicas – MAGERIT- Libro I - Método

2.2.2.2. COBIT

Según Gualsaqui Vivar (2013), COBIT 5 basa su metodología en cinco principios claves para el gobierno y la gestión de las TI a nivel organizacional.

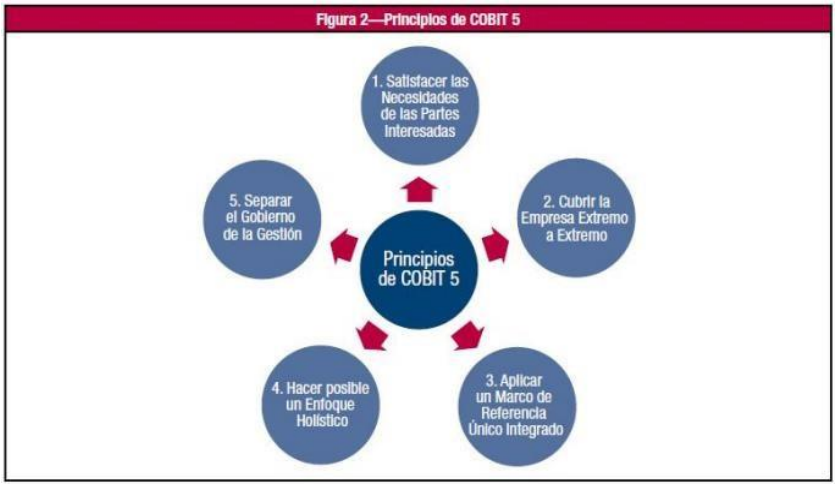


Figura 2 Principios de Cobit 5

Fuente: Cobit 5 Framework-spanish.pdf

Principio 1. Satisfacer las Necesidades de las Partes Interesadas

Según Gualsaqui Vivar (2013), El marco de referencia Cobit 5.0 facilita los procedimientos y actividades necesarios para permitir la creación de valor del negocio mediante el uso de las Tecnologías de Información, dando como resultado la consecución de beneficios y reduciendo el riesgo y uso de recursos.

Principio 2: Cubrir la Empresa Extremo-a-Extremo

Según Gualsaqui Vivar (2013), COBIT 5 permite acaparar la empresa de extremo a extremo, incluyendo todas las áreas funcionales de TI, personal interno y externo, todo cuanto sea de vital importancia para el gobierno y la gestión de las TI.

Principio 3: Aplicar un Marco de Referencia único integrado

Según Gualsaqui Vivar (2013), El marco de referencia Cobit 5.0 aplica un marco de referencia único integrando estándares, marcos de trabajo y buenas prácticas relacionadas con TI, tiene como fin ser un marco principal para el gobierno y administración de las TI de la empresa u organización.

Principio 4: Hacer Posible un Enfoque Holístico

Según Gualsaqui Vivar (2013), El marco de referencia Cobit 5.0 ofrece varios métodos de apoyo en la implementación de un sistema de gobierno y gestión para las TI de las instituciones, esto tiene base en principios, políticas, marcos de trabajo, procesos, estructuras organizativas, cultura, ética, comportamiento, información, servicios, infraestructuras, aplicaciones, personas, habilidades y competencias.

Principio 5: Separar el Gobierno de la Gestión

Según Gualsaqui Vivar (2013), COBIT 5 distribuye visiblemente al gobierno y la gestión, ya que cada uno de estos conceptos involucra diferentes estructuras y propósitos organizacionales diferentes.

2.2.3. Familia ISO 27000

2.2.3.1. ISO 27001

Según ISO (2017), consiste en la conservación de su confidencialidad, integridad y disponibilidad, como también de los sistemas implicados en su tratamiento, dentro de una empresa u organización. Así mismo, estos tres términos constituyen la base sobre la que se cimienta todo el edificio de la seguridad de la información: Confidencialidad: la información no puede ser otorgada a personas, organizaciones que no estén autorizados. Integridad: mantiene una información exacta y completa y sus procesos. Disponibilidad: poder acceder al uso de la información y los sistemas de tratamiento por ellos mismos y las organizaciones cuando lo necesiten. Para poder tener la certeza que la información está siendo gestionada correctamente se necesita usar un procedimiento sistemático, que esté documentado y se halla dado a conocer a la entidad., desde un enfoque de riesgo empresarial. Este proceso es el que constituye un Sistema de Gestión de Seguridad de la Información.

2.2.3.2. ISO 27002

Es una guía de buenas prácticas que explica los objetivos de control y recomienda controles en cuanto a seguridad de la información. No es certificable. Está hecha en base a la norma BS 7799-1 e ISO/IEC 17799:2005. La norma ISO/IEC 27001:2005 contiene un anexo que resume los controles de ISO/IEC 17799:2005, a diferencia que en la primera los requerimientos son específicos y obligatorios para la organización que desee certificar. (Pantaleone y Silva, 2013).

Cordero (Cordero, 2015), indica que la norma ISO 27002 contiene:

- Introducción: conceptos generales de seguridad de la información y SGSI.

- Campo de aplicación: se especifica el objetivo de la norma.

- Términos y definiciones: breve descripción de los términos más usados en la norma.

- Estructura del estándar: describe la estructura de la norma.

- Evaluación y tratamiento del riesgo: pautas para evaluar los riesgos de seguridad de la información.

- Política de seguridad: documento de política de seguridad y su gestión.

- Aspectos organizativos de la seguridad de la información: organización interna; terceros.

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

- Seguridad correspondiente a los recursos humanos: antes del empleo; durante, al término del empleo o cambio de puesto.

- Seguridad física y ambiental: áreas seguras; seguridad de los equipos.

- Gestión de comunicaciones y operaciones: responsabilidades y procedimientos de operación; gestión de la provisión de servicios por terceros; planificación y aceptación del sistema; protección contra código malicioso y descargable; copias de seguridad; gestión de la seguridad de las redes; manipulación de los soportes; intercambio de información; servicios de comercio electrónico; supervisión.

- Control de acceso: requisitos de negocio para el control de acceso; gestión de acceso de usuario; responsabilidades de usuario; control de acceso a la red; control de acceso al sistema operativo; control de acceso a las aplicaciones y a la información; ordenadores portátiles y teletrabajo.

- Adquisición, desarrollo y mantenimiento de los sistemas de información: requisitos de seguridad de los sistemas de información; tratamiento correcto de las aplicaciones; controles criptográficos; seguridad de los archivos de sistema; seguridad en los procesos de desarrollo y soporte; gestión de la vulnerabilidad técnica.

- Gestión de incidentes de seguridad de la información: notificación de eventos y puntos débiles de la seguridad de la información; gestión de

incidentes de seguridad de la información y mejoras.

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

- Cumplimiento: cumplimiento de los requisitos legales; cumplimiento de las políticas y normas de seguridad y cumplimiento técnico; consideraciones sobre las auditorías de los sistemas de información.

- Bibliografía: normas y publicaciones de referencia.

2.2.3.3. ISO 27003

Consiste en una guía de implementación de SGSI e información acerca del uso del modelo PDCA y de los requerimientos de sus diferentes fases. Tiene su origen en el anexo B de la norma BS7799-2 y en la serie de documentos publicados por BSI a lo largo de los años con recomendaciones y guías de implantación. (Aguirre y Zambrano, 2015)

2.2.3.4. ISO 27004

Especifica las métricas y las técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles relacionados. Estas métricas se usan fundamentalmente para la medición de los componentes de la fase “Do” (Implementar y Utilizar) del ciclo PDCA. (Chacón, 2012).

2.2.3.5. ISO 27000

Según la ISO27000.ES, ISO/IEC 27000 es un conjunto de estándares desarrollados -o en fase de desarrollo por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada.

2.2.3.6. ISO 27005

Según ISO27000.ES, fue publicada el 4 de Junio de 2008. Establece las instrucciones para la gestión del riesgo en la seguridad de la

información. Sostiene que los conceptos generales especificados en la norma ISO/IEC 27001 están diseñadas para ayudar a la seguridad de la información basada en un enfoque de gestión de riesgos. El conocimiento de los conceptos, modelos, procesos y términos descritos en la norma ISO/IEC 27001 e ISO/IEC 27002 es importante para un completo entendimiento de la norma ISO/IEC 27005:2008, se aplica a cualquier tipo de organización que tienen la intención de resolver los riesgos que puedan comprometer a la organización en temas de seguridad de información.

2.2.3.7. ISO 27006

Según ISO27000.ES, fue publicada el 13 de febrero de 2007. Especifica los requisitos para la acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información. Es decir, ayuda a interpretar los criterios de acreditación de ISO/IEC 17021cuando se aplican a entidades de certificación de ISO 27001, pero no es una norma de acreditación por sí misma.

2.2.3.8. ISO 27007

Consiste en una guía para la auditoría de un Sistema de Gestión de Seguridad de la Información.

2.2.4. Metodología PDCA - Ciclo Deming

La presente metodología tiene 4 pasos fundamentales que se adaptan de una forma muy sencilla a los sistemas de gestión siendo usados por las normas ISO, incluyendo la de gestión de seguridad de información. Conocido como ciclo de Deming o circulo de PDCA, por sus siglas en ingles que son PLAN, DO, CHEK y ACT, debido a que nace en Japón.

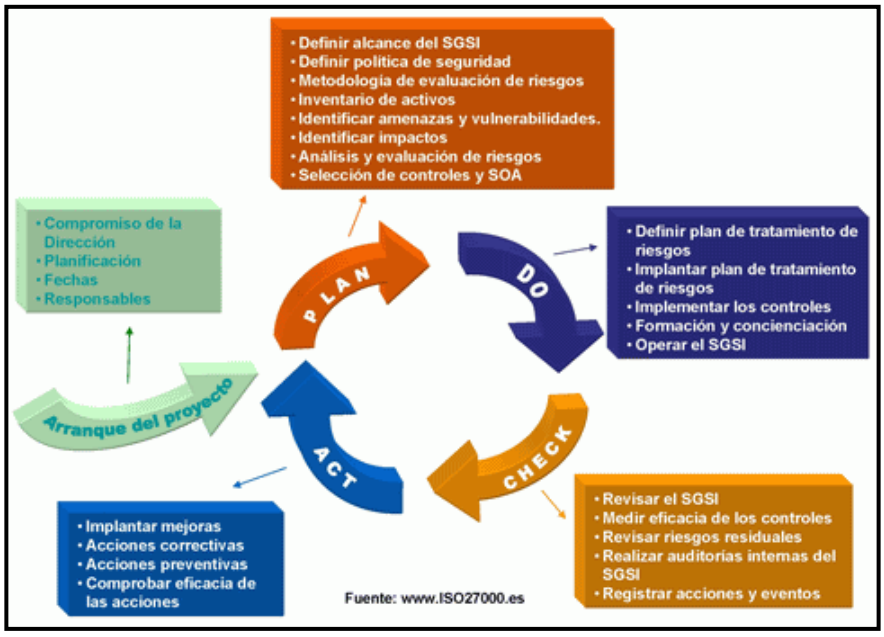


Figura 3 Ciclo de Mejora Continua del SGSI

Fuente: http://www.iso27000.es/sgsi.html

a) Etapas:

- **Planificar(PLAN)**

En primer lugar se debe hacer un análisis y un estudio del proceso decidiendo así que mejoras se deben hacer y como lo llevarlo a cabo. (M.Alemany, 2004) Esta etapa se divide en 5 pasos sucesivos que son:

- Definir el objetivo.
- Recopilar los datos.
- Elaborar el diagnostico.
- Elaborar pronósticos.
- Planificar los cambios.

- **Hacer (DO)**

Es aquí donde se deben realizar el cambio tomando en cuenta la decisión que se haya tomado y la planificación que se ha efectuado. Siempre se recomienda hacerlo en pequeñas escalas para que de este modo podamos verificar los resultados y hacer algunos cambios en los modelos si es necesario, para trasladarlos a situaciones reales de trabajo mostrando mayor seguridad en el resultado final. (M. Alemany, 2004)

- **Chequear (CHECK)**

Una vez efectuado el acto, debemos verificar. Esto involucra el análisis y la medición de los afectos producidos por el cambio realizado al proceso, sin dejar pasar la comparación de las metas prospectadas con los resultados obtenidos chequeando si se ha logrado el objetivo del previsto. (M.Alemany, 2004) Se indica realizar los siguientes procesos:

- Se realizará la Ejecución de procedimientos de seguimiento y revisión de controles.
- Se debe realizar revisiones regulares de cumplimiento.
- Se debe medir la eficacia de los controles y verificación de satisfacción.
- Se debe realizar evaluación de riesgos según calendarios
- Se debe realizar auditorías internas.
- Se debe actualizar los planes de seguridad y registrar.

- **Actuar (ACTION)**

Para terminar el periodo debemos analizar los resultados, viendo que se puede mejorar, implementar, realizar acciones, etc., lo cual permitirá la mejora continua (M.Alemany, 2004)

Se debe seguir los siguientes procesos:

- Implementar las mejoras identificadas para el plan de seguridad de información.
- Implementar las acciones correctivas y preventivas pertinentes.

- Comunicar acciones y mejoras a todas las partes involucradas.
- Asegurarse que las mejoras logren los objetivos previstos.

2.2.5. Municipalidad de Punta Hermosa

Según el Reglamento de Organización y Funciones (ROF), la municipalidad tiene como funciones generales, planificar y ejecutar a través de los órganos competentes, programas, proyectos, actividades y una serie de actividades que puedan proporcionar al vecino el mejor ambiente para la satisfacción de sus necesidades vitales.

La municipalidad tiene como misión brindar servicios públicos de calidad, promoviendo el desarrollo de los vecinos, procurando oportunidades de desarrollo social y económico con participación plena y organizada de la sociedad civil; teniendo como pilares fundamentales la eficiencia y la transparencia.

La municipalidad tiene como visión ser líder en promover el desarrollo de la sociedad, con una administración óptima, donde pueda notar total transparencia y participación en la comunidad, posicionándose como ciudad ordenada, segura, turística, moderna, inclusiva y saludable, donde se fomente la cultura diaria.

La estructura Orgánica de la Municipalidad Distrital de Punta Hermosa es la siguiente:

ORGANO DE GOBIERNO

- Concejo Municipal

ORGANOS DE ALTA DIRECCION

- Alcaldía
- Gerencia Municipal

ORGANOS CONSULTIVOS DE COORDINACION

- Consejo de Coordinación Local Distrital
- Junta de Delegados Vecinales Comunales
- Comité Distrital de Seguridad Ciudadana

• Plataforma de Defensa Civil
• Comité de Administración del Programa del Vaso de Leche
• Comisión Ambiental Distrital

ORGANO DE CONTROL

• Órgano de Control Institucional

ORGANO DE DEFENSA JUDICIAL

• Procuraduría Pública Municipal

ORGANO DE ASESORAMIENTO

• Gerencia de Asesoría Jurídica
• Gerencia de Planeamiento y Presupuesto
  - Oficina de Programación Multianual de Inversiones (OPMI)

ORGANOS DE APOYO

■ Secretaria General de Consejo
■ Secretaria General Administrativa
  - Subgerencia de Gestión Documentaria
  - Subgerencia de Imagen Institucional

■ Gerencia de Administración y Finanzas
  - Subgerencia de Logística y Control Patrimonial
  - Subgerencia de Contabilidad
  - Subgerencia de Tesorería
  - Subgerencia de Recursos Humanos
  - Subgerencia de Informática y Tecnologías de la Información

- Subgerencia de Fiscalización Administrativa

ORGANOS DE LINEA

■ Gerencia de Desarrollo Urbano y Control Territorial
  - Subgerencia de Obras Privadas
  - Subgerencia de Catastro

- Subgerencia de Obras Públicas y Proyectos
- Subgerencia de Comercialización
- Subgerencia de Defensa Civil y Gestión de Riesgos de Desastres

■ Gerencia de Administración Tributaria
- Subgerencia de Registro y Fiscalización Tributaria
- Subgerencia de Recaudación y Control Tributario
- Subgerencia de Ejecutoria Coactiva

■ Gerencia de Desarrollo Humano y Social
- Subgerencia de DEMUNA y OMAPED
- Subgerencia de Programas Sociales y Alimentarios
- Subgerencia de Participación Vecinal
- Subgerencia de Educación, Cultura, Salud, Deporte y Turismo

■ Gerencia de Seguridad Ciudadana
- Subgerencia de Serenazgo
- Subgerencia de Transporte y Seguridad Vial

■ Gerencia de Servicios Públicos y Gestión Ambiental
- Subgerencia de Limpieza Pública y Áreas Verdes

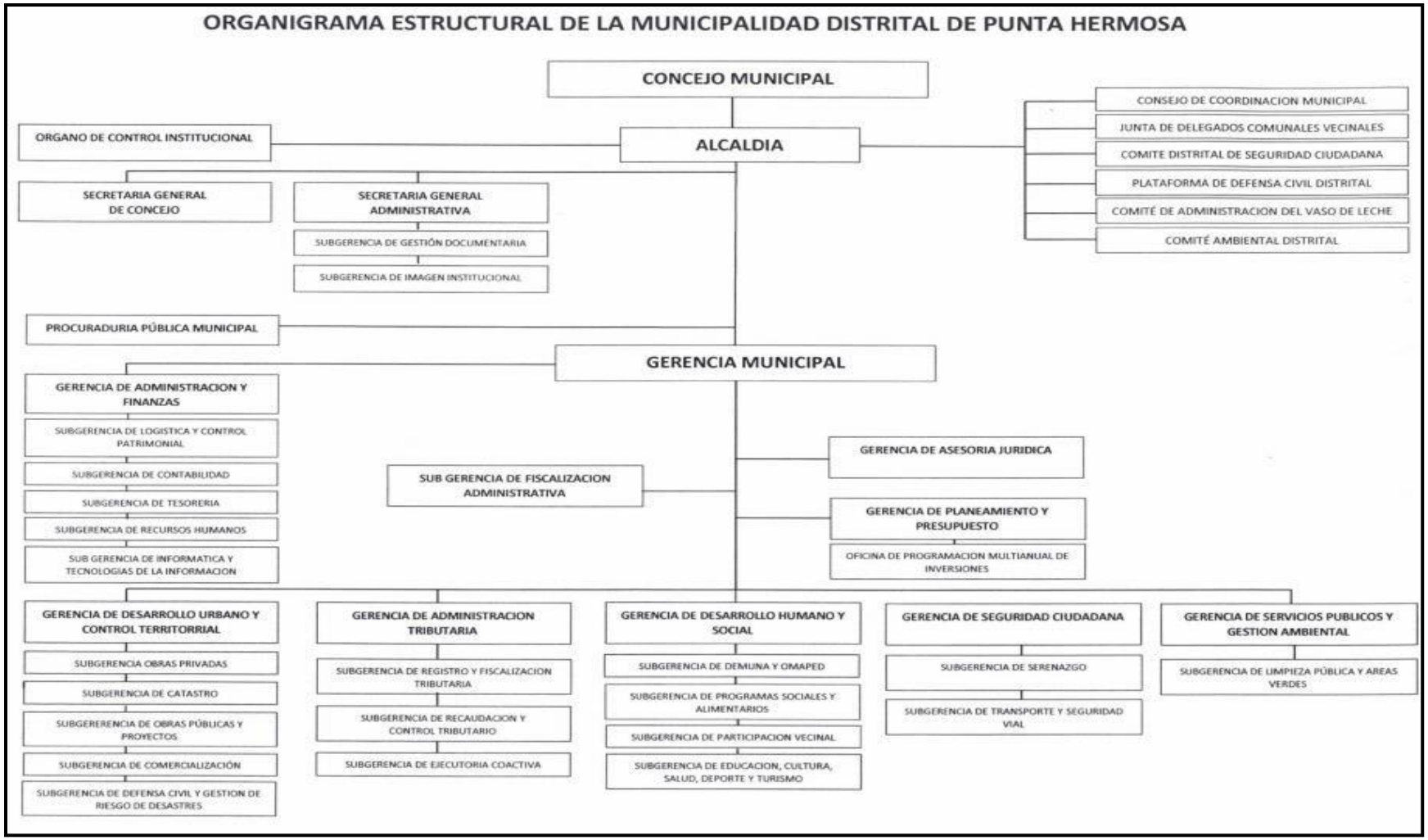


Figura 4 Organigrama de la Municipalidad de Punta Hermosa

Fuente: http://www.munipuntahermosa.gob.pe/pdf/transparencia/Estructura_Organica.PDF

Según el Reglamento de Organización y Funciones (ROF) de la Municipalidad de Punta Hermosa, **LA SUB GERENCIA DE INFORMATICA Y TECNOLOGIAS DE LA INFORMACION**, tiene las siguientes funciones:

a) Proponer, formular, organizar, dirigir e implementar las políticas y planes de aplicación y de uso de tecnologías de la información y de las comunicaciones, de manera que estos provean soporte a la operación de la Municipalidad.
b) Planear, organizar, dirigir, ejecutar y controlar las actividades relacionadas con los sistemas de información.
c) Planear, organizar, dirigir, ejecutar y controlar las actividades técnicas relacionadas con los sistemas de comunicación de voz y de datos.
d) Formular, proponer y dirigir el desarrollo y aplicación de políticas, prácticas, procedimientos y funciones que aseguren los niveles adecuados de confidencialidad, integridad y disponibilidad de los sistemas de información de los datos y de las comunicaciones de la Municipalidad.
e) Planear y desarrollar sistemas informáticos e implementar nuevas tecnologías para optimizar los existentes.
f) Dirigir las políticas de procesamiento electrónico y aseguramiento de calidad de datos de la Municipalidad.
g) Desarrollar el Portal Web Institucional, en concordancia con la normatividad aplicable vigente, Secretaria General Administrativa y la Subgerencia de Imagen Institucional.
h) Brindar a la Secretaria General Administrativa y a la Subgerencia de Imagen Institucional el soporte técnico oportuno para mantener debidamente actualizado el Portal Institucional.
i) Formular, actualizar y proponer la normatividad interna de su competencia, atraves de Reglamentos, Directivas, Manuales de Procedimientos y otros documentos, con el asesoramiento de la Gerencia de Planeamiento y Presupuesto, dentro del marco de sus competencias, propendiendo a la mejora continua de la

gestión.

j) Formular, implementar, ejecutar y supervisar los planes de contingencia y de seguridad de la información que aseguren la continuidad de la gestión, en concordancia con las normas técnicas peruanas y estándares internacionales.

k) Dirigir, ejecutar y supervisar Ia administración de Ia red de conectividad, generación de archivos de respaldo (backups), niveles de acceso y seguridades, así como dirigir y administrar los servicios internos de telefonía, comunicaciones y mensajería electrónica.

l) Conducir y ejecutar las actividades, servicios y proyectos, en concordancia con los lineamientos de política y objetivos generales institucionales aprobados y con Ia Política Nacional Informática y el Plan Estratégico Informático.

m) Cumplir con las directivas, lineamientos y normas emitidas por Ia Oficina Nacional de Gobierno Electrónico e Informática (ONGEI), ente rector del Sistema Nacional Informático (SNI).

n) Conducir y ejecutar la aplicación de los conceptos de Gobierno Electrónico (GE) en los servicios y procesos de la Municipalidad.

o) Identificar y proponer las tecnologías de información aplicables a cada proceso sometido a mejoramiento.

p) Conducir Ia aplicación de Tecnologías de Información y Comunicaciones (TICs) en los procesos de la Municipalidad.

q) Formular el plan anual de desarrollo de sistemas de información en base a los requerimientos de información de las áreas usuarias de Ia Municipalidad, acorde con los lineamientos institucionales.

r) Desarrollar Ia sistematización de los procesos de Ia Municipalidad, en coordinación con Ia Gerencia de Planeamiento y Presupuesto, de acuerdo con los planes aprobados y los estándares y directivas o lineamientos establecidos por Ia entidad.

s) Ejecutar las fases del desarrollo de los sistemas de información aprobados, que comprenden el análisis, diseño, programación,

carga de datos, pruebas y afinamiento en casos de desarrollo propio.

t) Supervisar y controlar el cumplimiento de las fases de desarrollo de los sistemas de información en caso de ser desarrollados por terceros, responsabilizándose de obtener y mantener en custodia la documentación, manuales y los códigos fuentes que permitan el mantenimiento y/o mejora de los sistemas.

u) Brindar el mantenimiento y soporte a los sistemas de información de las unidades orgánicas, controlando su permanente operatividad.

v) Documentar las fases de desarrollo de los sistemas de información, en caso de desarrollo propio, elaborando los respectivos manuales de programación, manuales de variables estandarizadas, manuales de usuarios y demasdocumentaci6n inherente al desarrollo de sistemas de información.

w) Emitir opinión técnica sobre la conveniencia de implementar soluciones informáticas existentes en el mercado.

x) Implementar y ejecutar Ia Gestión por Procesos, según los lineamientos y metodologías establecidas.

y) Formular, actualizar y proponer la normatividad interna de su competencia.

z) Elaborar y ejecutar su Plan Operativo Institucional y Presupuesto Anual, en el ámbito de su competencia.

aa) Proponer, coordinar e implementar mejoras en los procesos y procedimientos de su competencia.

bb) Proponer, coordinar y ejecutar las normas de control interno aplicables a su unidad orgánica.

cc) Promover el cumplimiento de Ia normatividad vigente inherente a seguridad y salud en el trabajo.

dd) Cumplir con las demás funciones que le asigne Ia Gerencia de Administración y Finanzas o que le sean dadas por las normas sustantivas en materia de su competencia.

2.3. Definición de términos básicos

- Controles: Son Procesos de verificación del desempeño tanto de las áreas como de las funciones de una entidad u empresa; naturalmente se realiza con la comparación entre un rendimiento esperado y un rendimiento obtenido, para constatar si se están llegando a los objetivos de forma correcta y tomar acciones de mejoramiento". (Anzil, 2010)

- Implementación: En el ámbito del software, la implementación se define con la instalación del software: colocar los archivos de la aplicación en donde lo necesitamos. Sin embargo, en dicho ámbito, la implementación también incluye otras actividades. (Adobe Creative Suite 5, 2010)

- Información: "Son datos que responden a una serie de preguntas incrementando así nuestro conocimiento sobre algo en específico. La información es un mensaje que tiene un significado definido para poder ser usado de forma inmediata dándonos orientación a nuestras decisiones". (Chiavenato, 2006)

- ISO: La ISO (Organización Internacional de Normalización) es una federación mundial de organismos nacionales de normalización (comités miembros de la ISO). La creación de las Normas Internacionales con normalidad siempre es designada a los comités técnicos de la ISO. Cada integrante del comité que tenga interés por un estudio tiene el derecho de formar parte del comité técnico creado para este efecto. (Fernandez Jimenez & Muñoz Cornejo, 1974)

- Norma: Tiene como base resultados de experiencias aprobado por un organismo de normalización reconocido

"Las normas hacen que las empresas puedan tener posición en un mejor mercado y forma parte de la fuente de para los profesionales de

cualquier actividad económica.” (AENOR, 2016)

- Políticas de seguridad de información: Estas permiten cumplir con requisitos que mejorarán el sistema de gestión de seguridad de la información. La política debe adaptarse a la organización mostrando el compromiso de la alta dirección.

- Riesgo: Es cuando existe la probabilidad de que una amenaza se convierta en desastre. Cuando la vulnerabilidad y la amenaza se encuentran separadas no nos muestran mayor peligro, sin embargo al poder unirse forman un riesgo y existe una gran posibilidad que se convierta en desastre. También se debe recordar que estos riesgos se pueden minimizar y manejar. (UNISDR, 2004)

- Seguridad: La seguridad es importante en el área de sistemas, ya que es una disciplina que tiene la responsabilidad de proteger y salvaguardar la privacidad e integridad de la información.

- Sistema: Son elementos relacionados entre sí, buscando un fin en común. Un sistema puede ser cualquier objeto, cualquier cantidad de materia, etc. (Jaramillo, 2007)

- Sistema de gestión: Es una herramienta que permitirá a la organización optimizar recursos, reducir costes y mejorar la productividad de la organización u empresa.

CAPÍTULO III: DESCRIPCIÓN DEL MODELO METODOLÓGICO

3.1 Diagnóstico

Para poder conocer el grado de conocimiento en cuanto a seguridad de la información dentro de la Municipalidad de Punta Hermosa, se aplicó un cuestionario a 30 empleados de áreas administrativas y de la sub gerencia de informática y tecnologías de la información sobre seguridad de la información en la institución. Asimismo, las respuestas serán graficadas con estadísticas mostrando los resultados de la investigación. (Anexo 1).

Pregunta 1:

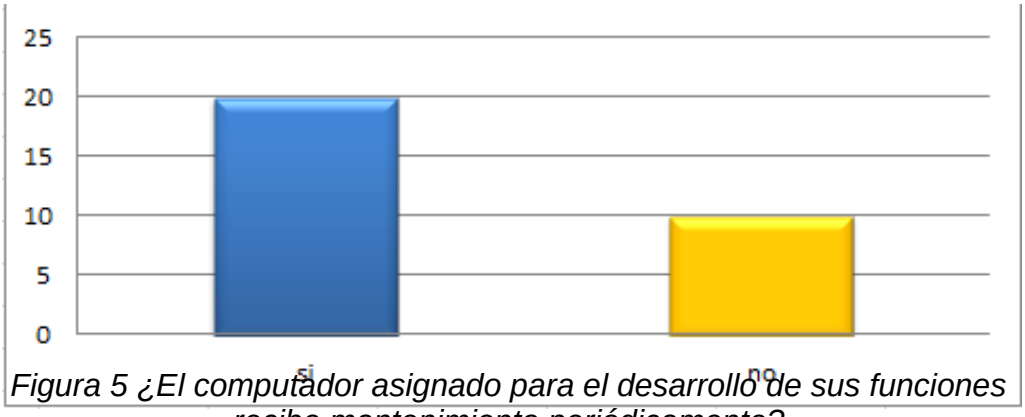


Figura 5 ¿El computador asignado para el desarrollo de sus funciones recibe mantenimiento periódicamente?

Fuente: Elaboración Propia

Interpretación: de los 30 empleados, 20 mencionan que se realiza mantenimiento cada mes, 10 manifiestan que no se realiza mantenimiento periódicamente.

Pregunta 2:

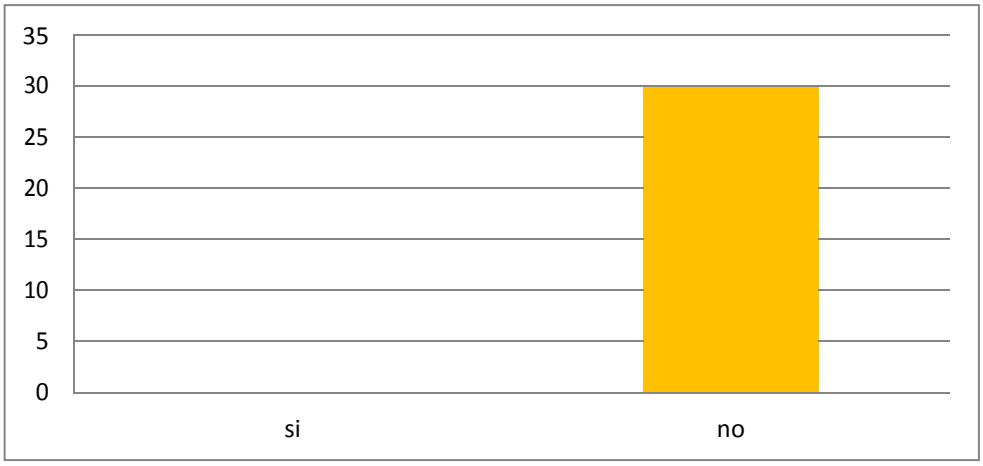


Figura 6 ¿Existe un SGSI en la Municipalidad?

Fuente: Elaboración Propia

Interpretación: de los 30 empleados, 30 mencionaron que no existe o no conocen que se halla ejecutado un sistema de seguridad informática.

Pregunta 3:

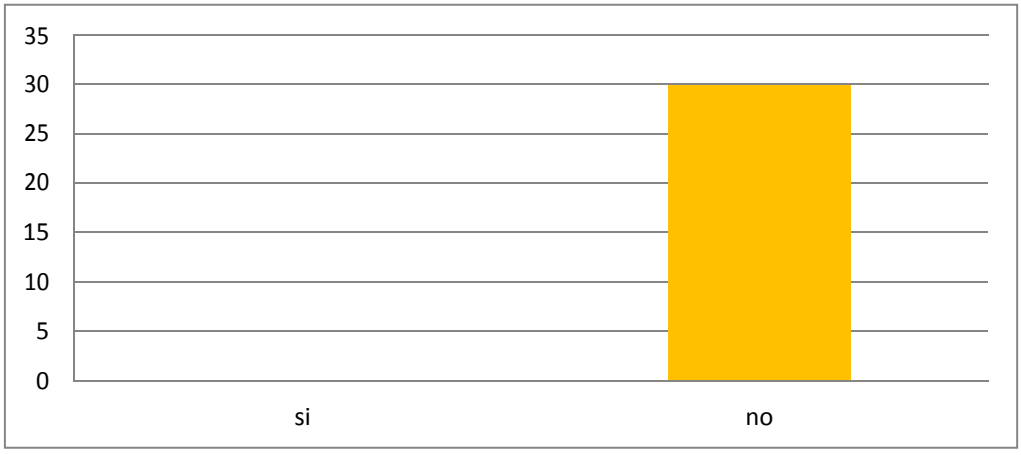


Figura 7¿La Municipalidad capacita al personal en temas de seguridad informática?

Fuente: Elaboración Propia

Interpretación: de los 30 empleados, 30 dijeron que nunca se ha realizado capacitaciones en aspectos de seguridad informática.

Pregunta 4:

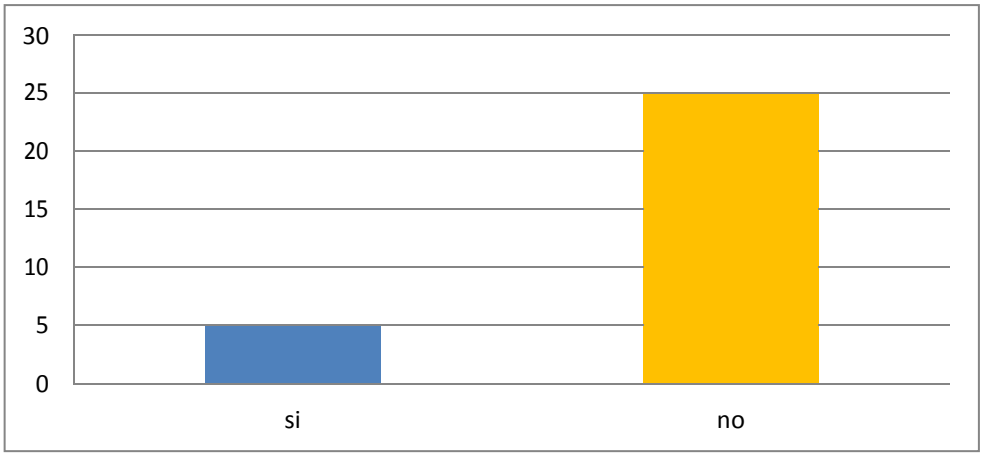


Figura 8 ¿Existe alguna política para el cambio regular de las contraseñas?

Fuente: Elaboración Propia

Interpretación: de los 30 empleados, 5 mencionaron que si cuentan con políticas de cambio de contraseñas y 25 manifiestan que si fueron informados verbalmente pero no se aplican de forma regular.

Pregunta 5:

Figura 9¿Antes y después de la contratación del personal se hace entrega de un manual de funciones y responsabilidades de seguridad de la información?

Fuente: Elaboración Propia

Interpretación: de los 30 empleados, 30 mencionaron que no conocen manuales de funciones y responsabilidades de seguridad de la información.

Pregunta 6:

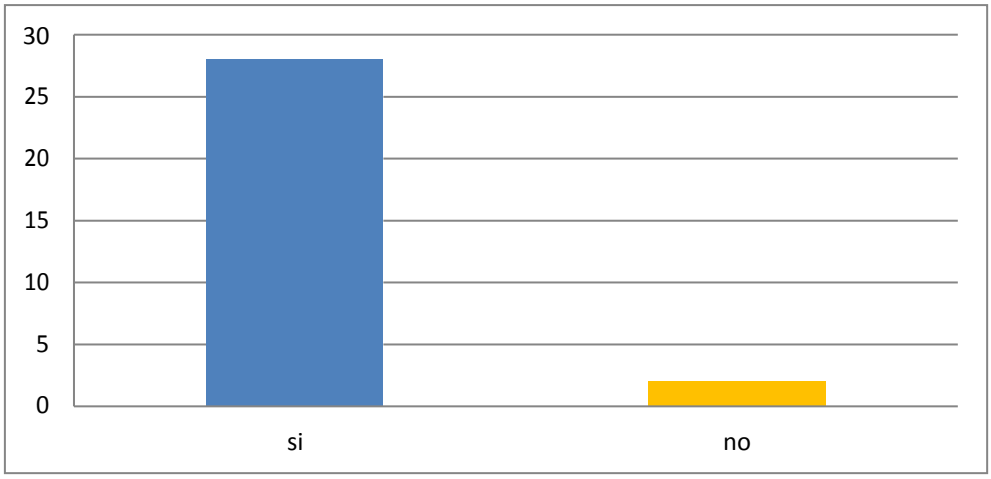


Figura 10 ¿Cuándo ocurre un imprevisto relacionado con seguridad de la información sabe a quién reportarlo?

Fuente: Elaboración Propia

Interpretación: de los 30 empleados, 28 dijeron que cuando ocurre un imprevisto relacionado con seguridad se reporta al área de sistemas y 2 mencionaron que no saben a quién reportarlo.

Pregunta 7:

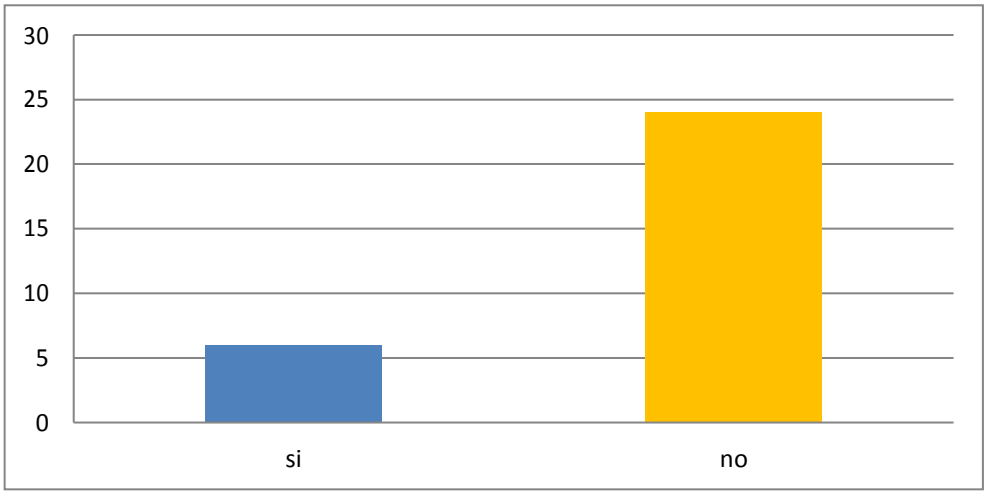


Figura 11 ¿Realiza copias de la información?

Fuente: Elaboración Propia

Interpretación: de los 30 empleados, 24 mencionaron que nunca se realizan copias y 6 dijeron que se realizan copias de seguridad en algunas ocasiones.

Pregunta 8:

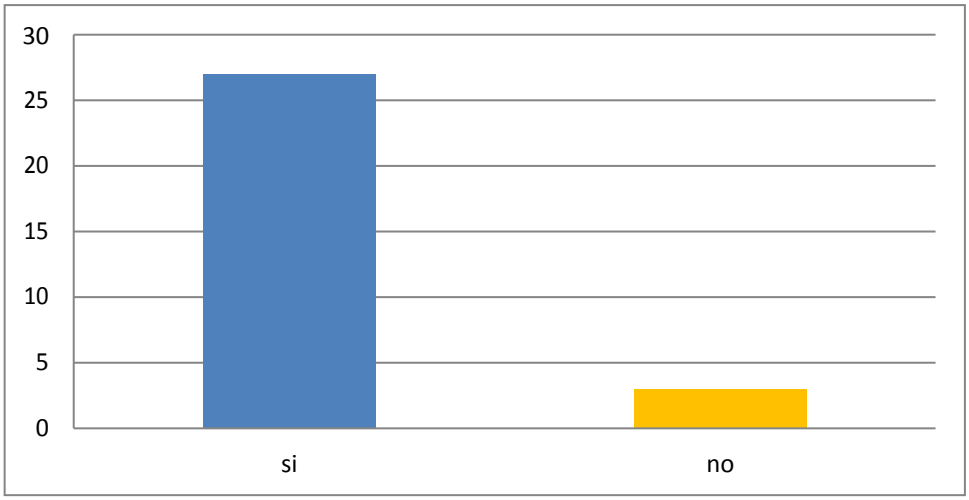


Figura 12 ¿Considera necesario que la Municipalidad invierta en la implementación de un Sistema de Gestión de Seguridad de la Información?

Fuente: Elaboración Propia

Interpretación: de los 30 empleados, 27 mencionaron que si es importante inversión de este tipo, mientras que 3 manifiestan que el dinero se podría invertir en otra cosa.

Pregunta 9:

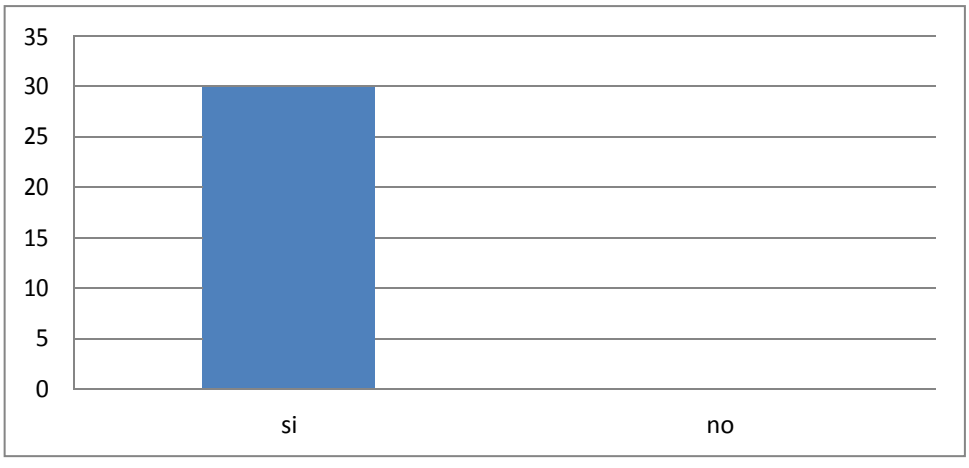


Figura 13 ¿Tiene antivirus la computadora asignada?

Fuente: Elaboración Propia

Interpretación: de los 30 empleados, 30 mencionaron que si se cuenta con un programa de antivirus.

Pregunta 10:

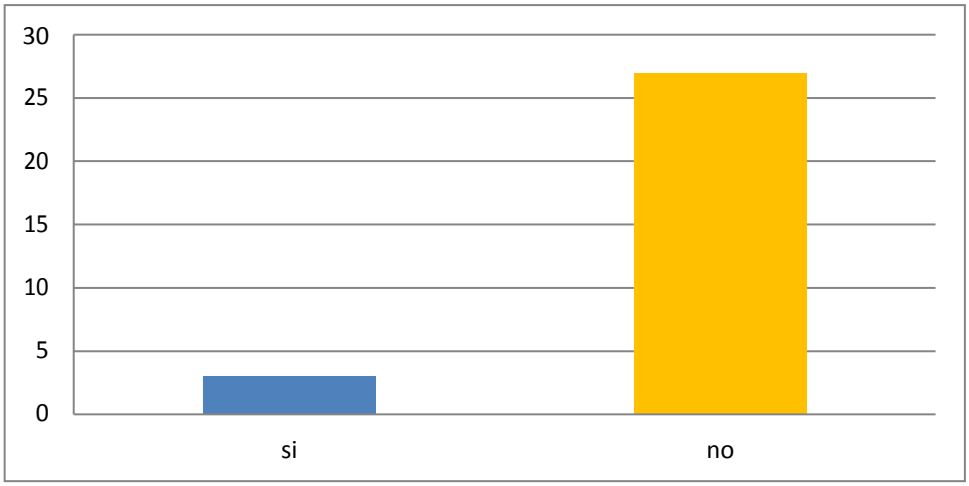


Figura 14 ¿La Municipalidad tiene software legal en su totalidad?

Fuente: Elaboración Propia

Interpretación: de los 30 empleados, 3 mencionaron que si hay software legal y 27 dicen que la municipalidad no tiene software legal.

Pregunta 11:

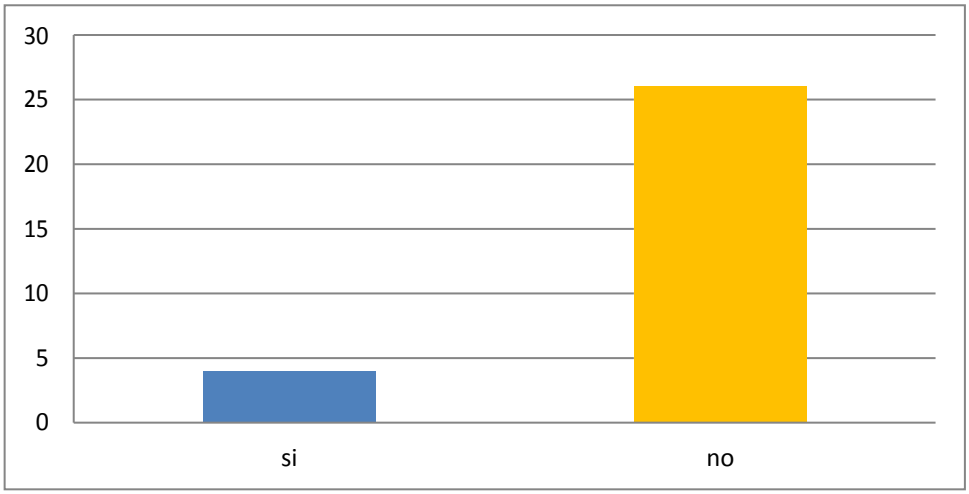


Figura 15 ¿Existen zonas restringidas de acceso de personal?

Fuente: Elaboración Propia

Interpretación: de los 30 empleados, 4 mencionaron que si cuenta con zonas restringidas, mientras que 26 empleados manifiestan que no cuentan con sitios restringidos.

Pregunta 12:

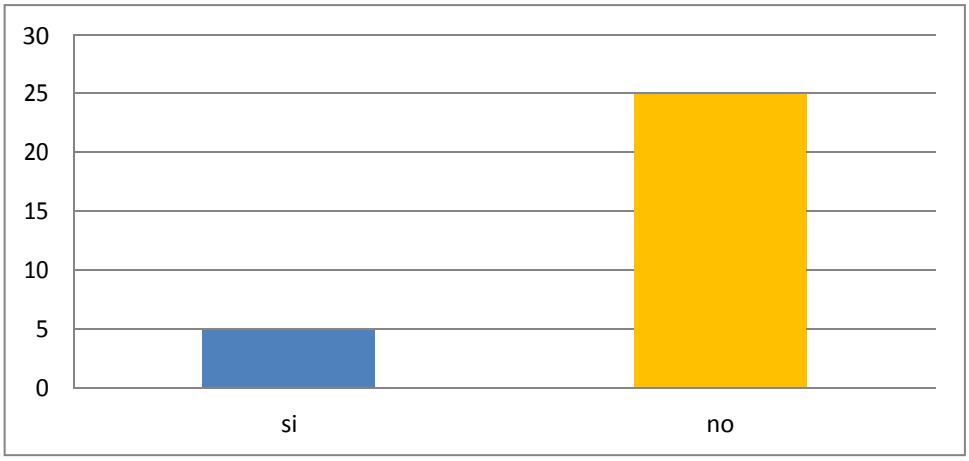


Figura 16 ¿Se realiza mantenimiento preventivo y correctivo a la UPS?

Fuente: Elaboración Propia

Interpretación: de los 30 empleados, 5 mencionaron que si se realiza mantenimiento de la UPS, mientras que los 25 restantes manifiestan que no se realiza ningún mantenimiento.

Pregunta 13:

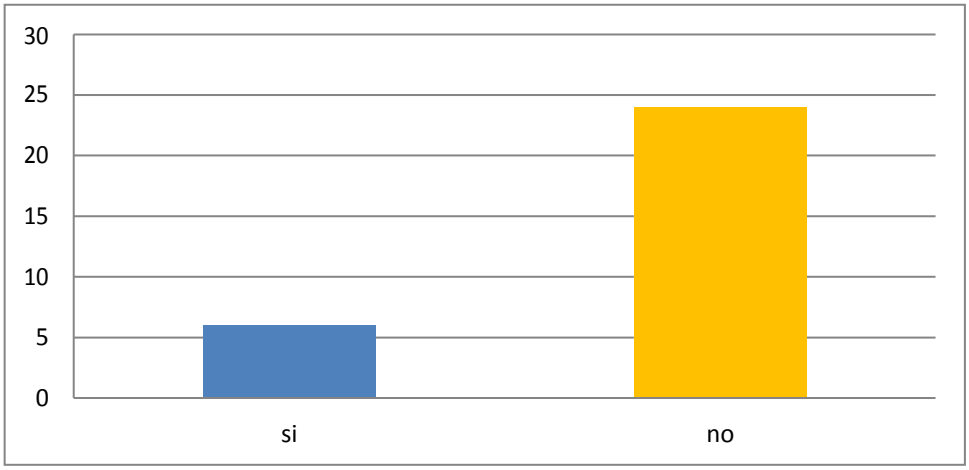


Figura 17 ¿Existen sistemas de seguridad que impidan el acceso a lugares restringidos?

Fuente: Elaboración Propia

Interpretación: de los 30 empleados, 6 mencionaron que si hay sistemas de seguridad, mientras que los 24 restantes manifiestan que no hay dispositivos de control de acceso.

Pregunta 14:

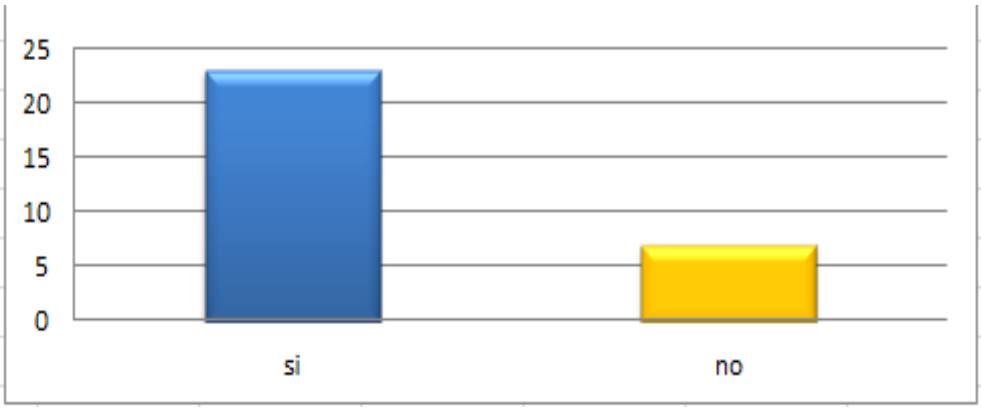


Figura 18 ¿Se cuenta con sistemas de alarma como detectores de humo, humedad en todos los locales de la Municipalidad?

Fuente: Elaboración Propia

Interpretación: de los 30 empleados, 23 mencionaron que si hay sistemas de alarmas, mientras que los 7 restantes manifiestan que no poseen alarmas.

Pregunta 15:

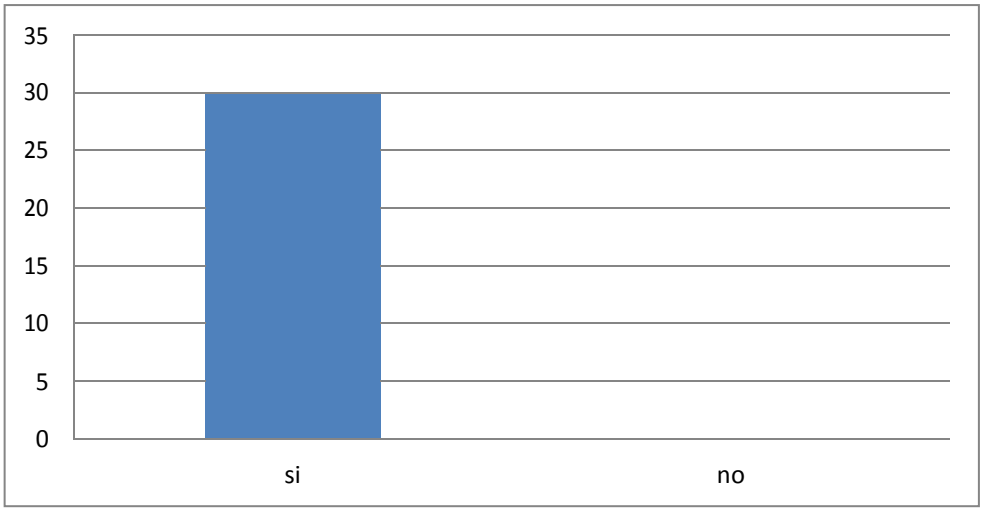


Figura 19 ¿Existe vigilancia en la entrada del edificio?

Fuente: Elaboración Propia

Interpretación: de los 30 empleados, 30 manifiestan que si se cuenta con vigilancia al ingreso de la institución.

Pregunta 16:

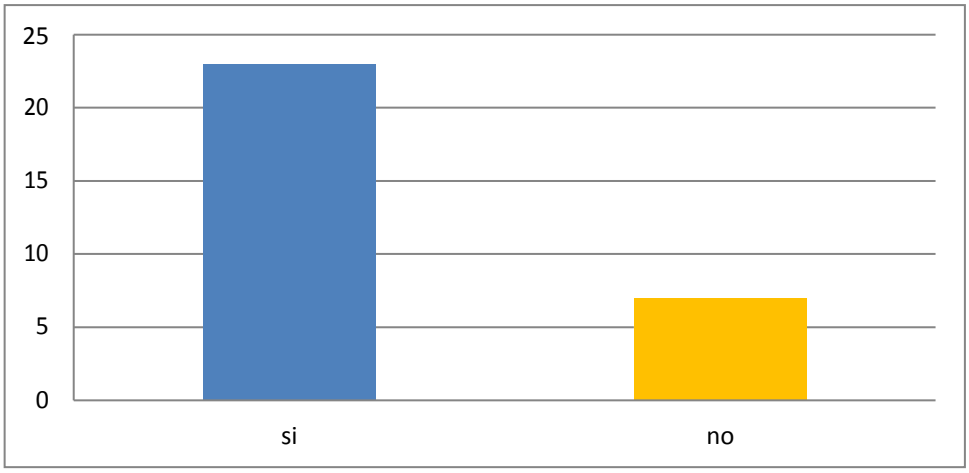


Figura 20 ¿Los sitios donde están los equipos de cómputo cuentan con aire acondicionado?

Fuente: Elaboración Propia

Interpretación: de los 30 empleados, 23 manifiestan que si se cuenta con aire acondicionado, mientras que los 7 restantes dicen que no cuentan con aire acondicionado.

Pregunta 17:

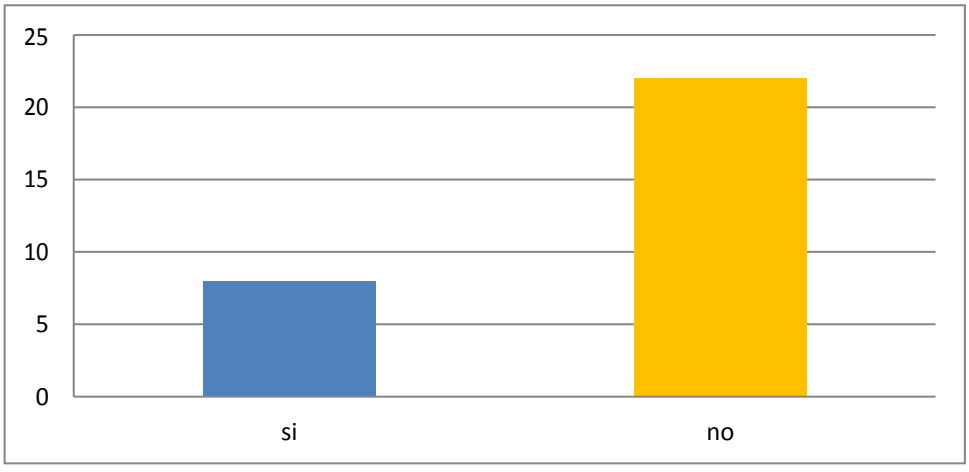


Figura 21 ¿Se encuentra asegurados mediante pólizas los equipos de cómputo?

Fuente: Elaboración Propia

Interpretación: de los 30 empleados, 8 manifiestan que si cuentan con pólizas de protección de equipos y 22 empleados dicen que no cuentan con ninguna póliza de protección de equipos.

Pregunta 18:

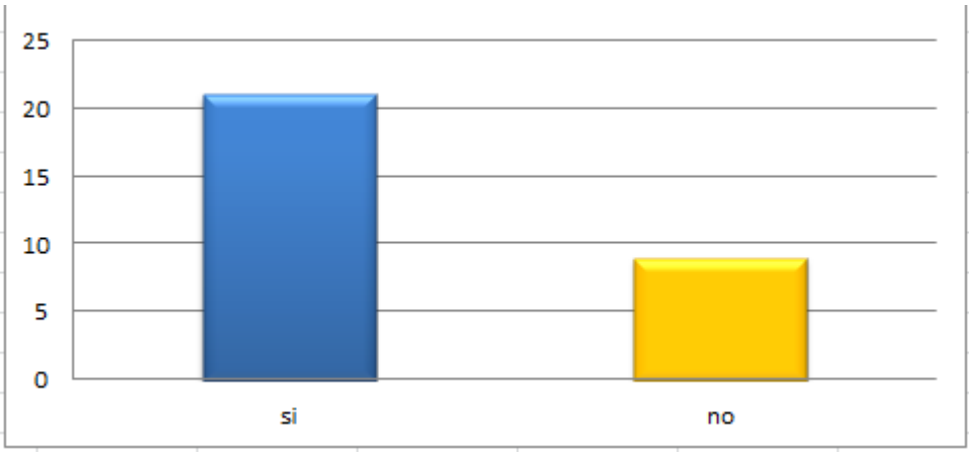


Figura 22 ¿Existe algún control para navegar en internet?

Fuente: Elaboración Propia

Interpretación: de los 30 empleados, 21 manifiestan que si cuentan con controles para navegar en internet y 9 dicen que no cuentan con ninguna restricción.

3.2 Modelo de solución propuesto

En este proyecto de investigación se realizará el diagnóstico del conocimiento sobre sistemas de seguridad de la información y se aplicará la metodología de evaluación y Análisis de riesgo de los activos identificados, para determinar cuales deberán ser protegidos y así poder mitigar los riesgos en la institución.

Para la elaboración del plan de seguridad de la información se tiene en cuenta 4 aspectos cruciales, los cuales son:

- Objetivos del plan de seguridad de la información.
- Descripción de las fases seguidas para el manejo de la Metodología de evaluación y análisis de riesgo.
- Definir las políticas de seguridad para un buen funcionamiento de la seguridad.
- Proponer la formación de un Comité de Seguridad de la Información según la ISO 27001.

3.2.1. Objetivos del Plan de Seguridad de la Información

Los objetivos del plan de seguridad de la información son los siguientes:

- Fomentar la cultura de seguridad de la información en la Municipalidad de Punta Hermosa, estableciendo procesos internos quienes se encargarán de garantizar la seguridad, es decir se protegerá la confidencialidad, integridad y disponibilidad.
- Que todo el personal de la municipalidad relacionado directamente con información confidencial, tome conciencia en materia de seguridad.
- Que se cumpla la legislación vigente respecto a seguridad de la información y protección de datos personales.
- Registrar la documentación respecto a los procedimientos relacionados con la seguridad de la información.
- Cumplir con los requerimientos legales aplicables a la municipalidad, correspondientes al sistema de gestión de

seguridad de la información.

- Garantizar el acceso a la información de acuerdo a las políticas, normativa y criterios de seguridad que establezca la sub gerencia de informática y tecnologías de la información.
- Mantener la integridad de la información de la municipalidad, teniendo en cuenta los requisitos y resultados de la valoración y tratamiento de los riesgos identificados.

3.2.2. Descripción de las fases seguidas para el manejo de la Metodología de Evaluación y Análisis de Riesgo

El resultado importante de todo proceso de evaluación de riesgos es la información que es utilizada para generar políticas y controles de seguridad.

El procedimiento de evaluación de riesgo que permitirá a la municipalidad resolver el riesgo y estar conforme con los requerimientos normativos, se aplicará a través de un proceso de análisis metodológico de nueve fases.

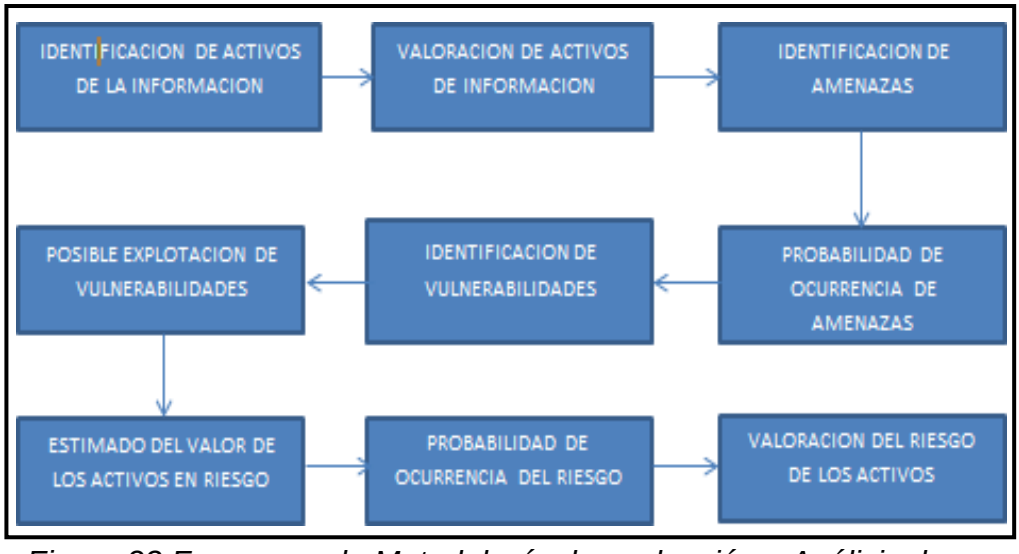


Figura 23 Fases para la Metodología de evaluación y Análisis de Riesgo

Fuente: Elaboración propia

3.2.2.1. Identificación de activos de la Información

Se reconoce a los activos importantes y se asignan la responsabilidad por el mantenimiento de los controles apropiados.

Tabla 1 Listado de Activos de Información- área de desarrollo-soporte técnico

Nro.	Activo de Información	Tipo
1	Equipos de escritorio	**Hardware**
2	Laptops	**Hardware**
3	Impresoras	**Hardware**
4	Disco Duro externo	**Hardware**
5	Equipos de comunicaciones	**Hardware**
6	Switch de 24 puertos	**Hardware**
7	Switch de 16 puertos	**Hardware**
8	Switch de 8 puertos	**Hardware**
9	Servidor de Archivos	**Hardware**
10	Servidor de temas Administrativos	**Hardware**
11	Servidor SIAF	**Hardware**
12	Teléfonos IP	**Hardware**
13	Red Wifi corporativo	**Hardware**
14	Red LAN	**Hardware**
15	Servidor Web,dhcp,dns	**Hardware**
16	Microsoft Office 2013 y 2010	**Software**
17	Antivirus McAfee, Eset, Avast, Comodo, AVG	**Software**
18	Microsoft Windows server 2012 y 2008	**Software**
19	Sql Express edition	**Software**
20	Simunet	**Software**
21	Team Viewer 11	**Software**
22	Anydesk	**Software**
23	Librerías SIAF	**Software**
24	Registros de planilla	**Documentos físicos**
25	Documentos de compras	**Documentos físicos**

26	Cotizaciones	**Documentos físicos**
27	Registros de RRHH	**Documentos físicos**
28	Registros de cobranza	**Documentos físicos**
29	Actas de Requerimientos	**Documentos físicos**
30	Actas de Implementación	**Documentos físicos**
31	Historial de Modificaciones	**Documentos digital**
32	Historial de Soportes	**Documento digital**
33	Historial de Actualizaciones	**Documento digital**
34	Solicitudes de Cambio	**Documento físicos**
35	Agenda Telefónica	**Documento digital**
36	Estado de soporte del cliente	**Documento digital**

Fuente: Elaboración Propia

3.2.2.2. Valoración de Activos de Información

La valoración es el atributo que hace valioso a un activo de información para la institución. A través de su dimensionamiento nos permite valorar las consecuencias de la materialización de una amenaza. Para darle valor a los activos de información se tiene en cuenta la siguiente escala.

Tabla 2 Criterios de valoración de los activos de información

Escala de Valoración	Valor	Criterio
MA	MUY ALTO	Daño muy grave a la institución
A	ALTO	Daño grave a la institución
M	MEDIANO	Daño importante a la institución
B	BAJO	Daño menor a la institución
MB	MUY BAJO	Irrelevante

Fuente: Elaboración Propia

En esta actividad se asignará por importancia en términos que tenga para la institución, se mirará el impacto con respecto a su confidencialidad, integridad y confidencialidad.

Tabla 3 Valoración de los activos de información

Nro.	Activo de Información	C	I	D	Total
1	Equipos de escritorio	A	A	A	A
2	Laptops	A	A	A	A
3	Impresoras	B	MB	B	B
4	Disco Duro externo	A	A	M	A
5	Equipos de comunicaciones	A	A	A	A
6	Switch de 24 puertos	A	A	A	A
7	Switch de 16 puertos	A	A	A	A
8	Switch de 8 puertos	A	A	A	A
9	Servidor de Archivos	MA	MA	MA	MA

10	Servidor de temas Administrativos	MA	MA	MA	MA
11	Servidor SIAF	MA	MA	MA	MA
12	Teléfonos IP	B	B	B	B
13	Red Wifi corporativo	A	A	A	A
14	Red LAN	A	A	A	A
15	Servidor Web,dhcp,dns	MA	MA	MA	MA
16	Microsoft Office 2013 y 2010	B	M	M	M
17	Antivirus McAfee, Eset, Avast, Comodo, AVG	M	M	M	M
18	Microsoft Windows server 2012 y 2008	A	MA	MA	MA
19	Sql Express edition	MA	MA	A	MA
20	Simunet	MA	MA	MA	MA
21	Team Viewer 11	M	B	M	M
22	Anydesk	M	B	M	M
23	Librerías SIAF	A	A	A	A
24	Registros de planilla	A	A	A	A
25	Documentos de compras	A	A	A	A
26	Cotizaciones	A	A	A	A
27	Registros de RRHH	A	A	A	A
28	Registros de cobranza	A	A	A	A
29	Actas de Requerimientos	A	A	A	A
30	Actas de Implementación	M	A	A	A
31	Historial de Modificaciones	M	A	A	A
32	Historial de Soportes	M	M	A	M
33	Historial de Actualizaciones	M	M	A	M
34	Solicitudes de Cambio	A	A	A	A
35	Agenda Telefónica	M	M	B	M
36	Estado de soporte del cliente	M	B	M	M

Fuente: Elaboración Propia

3.2.2.3 Identificación de Amenazas

La amenaza es un potencial evento no deseado. Las amenazas son ser externas e internas a la organización y pueden ser mal intencionadas o accidentales. Se pude identificar a una amenaza porque generará daño a la organización y sus activos.

Los tipos de amenazas:

- Amenazas Lógicas.
- Suplantación identidad por internos.
- Suplantación identidad por contratistas.
- Suplantación identidad por externos.
- Uso no autorizado de una aplicación.
- Software malicioso.
- Abuso de los recursos de los sistemas.

- Amenazas a las Comunicaciones
- Infiltración comunicaciones.
- Interceptación comunicaciones.
- Alteración comunicaciones.
- Repudio.
- Fallo comunicaciones.
- Inclusión de código malicioso.
- Entrega incorrecta.

- Amenazas Físicas
- Fuego.
- Inundación.
- Desastre natural.
- Ausencia de persona.
- Robo por internos.
- Robo por externos.
- Daño intencionado por internos.

- Daño intencionado por externos.
- Terrorismo.

- Fallos Técnicos
- Fallo host, impresora, almacenamiento.
- Fallo de elemento de red, interfaz de red.
- Fallo de pasarela de red.
- Fallo de gestión de red.
- Fallo de servicios de red.
- Fallo electricidad.
- Fallo aire acondicionado.
- Fallo de software de sistema.
- Fallo de software de red.
- Fallo de aplicación.

- Errores Humanos
- Error de operador.
- Error mantenimiento hardware.
- Error mantenimiento software.
- Error de usuario.

En la siguiente tabla se identificará las amenazas para cada grupo de activo de información.

Tabla 4 Identificación de amenazas a los activos de información

Nº	GRUPO DE ACTIVO DE INFORMACION	AMENAZAS
1	PROGRAMAS FUENTE	Control de cambios.
		Modificación mal intencionada.
		Error de programación
		Software malicioso
2	DOCUMENTOS FISICOS	Alteración de información
		Destrucción o eliminación mal intencionada
		Destrucción de la información por error
		Incendio, desastres naturales
3	SERVIDORES	Error en el mantenimiento de hardware
		Acceso no autorizado
		Interferencia electromagnética
		Falla de software aplicación
		Incendio y/o desastres naturales
		Falla por error
		Abuso de los recursos del sistema y repudio
4	EQUIPOS	Corte o fallas del suministro eléctrico
		Violación de derechos de autor
		Suplantación identidad
		Abuso de los recursos del sistema y repudio
		Falla de equipo por error
5	INFORMACION ALMACENADA	Fuga de información mal intencionada
		Falla en dispositivo de almacenamiento

		Backup no autorizado
6	SOFTWARE	Ataque informático
		Malware
		Suplantación de identidad
		Uso no autorizado.
7	SWITCH/ROUTER	Alteración comunicaciones
		Entrega incorrecta
		Error de operador
		Fallo de electricidad
		Interceptación comunicaciones
		Repudio
		Fallo de equipos

Fuente: Elaboración Propia

3.2.2.4. Probabilidad de ocurrencia de amenazas

Se ha podido revisar las distintas potenciales amenazas que pueden afectar a la institución y se ha logrado identificar exposiciones específicas que puedan requerir medidas de protección y así minimizar la probabilidad que las amenazas pudiesen causar daño a la institución.

Por cada amenaza que hay se mide su posibilidad de ocurrencia, utilizando la siguiente escala:

Tabla 5 Valoración de ocurrencias de amenazas

VALOR		CRITERIO
A	ALTO	**Daño grave a la institución**
M	MEDIO	**Daño importante a la institución**
B	BAJO	**Daño menor a la institución**

Fuente: Elaboración Propia

En la siguiente tabla se aplicará la escala de valoración de amenazas para cada grupo de activo de información.

Tabla 6 Evaluación de ocurrencias de amenazas

Nº	GRUPOS DE ACTIVOS DE INFORMACION	AMENAZAS	POSIBILIDAD DE OCURRENCIA
1	PROGRAMAS FUENTE	Control de cambios	**A**
		Modificación mal intencionada	**A**
		Error de programación	**B**
		Software malicioso	**M**
		Alteración de información	**M**

2	DOCUMENTOS FÍSICOS	Destrucción o eliminación mal intencionada	**A**
		Destrucción de la información por error	**M**
		Incendio, desastres naturales	**M**
3	SERVIDORES	Error en el mantenimiento de hardware	M
		Acceso no autorizado	B
		Interferencia electromagnética	M
		Falla de software aplicación	A
		Incendio y/o desastres naturales	A
		Falla por error	M
		Abuso de los recursos del sistema y repudio	B
4	EQUIPOS	Corte o fallas del suministro eléctrico	M
		Violación de derechos de autor	B
		Suplantación identidad	M
		Abuso de los recursos del sistema y repudio	M
		Falla de equipo por error	M
5	INFORMACION ALMACENADA	Fuga de información mal intencionada	M
		Falla en dispositivo de almacenamiento	B
		Backup no autorizado	M
6	SOFTWARE	Ataque informático	A
		Malware	A
		Suplantación de identidad	A
		Uso no autorizado.	B
		Alteración comunicaciones	A
		Entrega incorrecta	A

7	SWITCH/ROUTER	Error de operador	B
		Fallo de electricidad	M
		Interceptación comunicaciones	A
		Repudio	A
		Fallo de equipos	A

Fuente: Elaboración Propia

3.2.2.5. Identificación de vulnerabilidades

Se define como debilidades de seguridad, vinculadas con los activos de información de la institución. Se clasifican:

- Física y Ambiental
- Gestión de operaciones y comunicación
- Adquisición, desarrollo y mantenimiento de sistemas de información
- Red
- Seguridad de los RR.HH

Tabla 7 Identificación de vulnerabilidades de los activos de información

Nº	GRUPOS DE ACTIVOS DE INFORMACION	VULNERABILIDADES
1	PROGRAMAS FUENTE	Política de control de cambios inexistentes
		Inadecuado manejo
		Error de diseño
		Falta de Seguridad del sistema
2	DOCUMENTOS FISICOS	Inadecuado manejo
		Política de integridad inexistente
		Política de integridad inexistente
		Falta de uso de EPP(Elemento de Protección Personal)
		Falta de manual de mantenimiento

3	SERVIDORES	Política de control de identidad inexistentes
		Falta de equipos de red de respaldo
		Falta de manual de contingencias
		Falta de uso de EPP(Elemento de Protección Personal)
		Inadecuado manejo de la información
		Políticas de seguridad deficientes o inexistentes
4	EQUIPOS	Falta de manual de mantenimiento
		Política de control de identidad inexistentes
		Política de control de identidad inexistentes
		Configuración de perfiles deficiente
		Falta de equipos de respaldo
5	INFORMACION ALMACENADA	Política de control de identidad inexistentes
		Falta de equipos de respaldo
		Políticas de backup inexistente
6	SOFTWARE	Falta de Seguridad del sistema
		Falta de licencias vigentes
		Falta de manual de usuario
		Configuración de perfiles deficiente
7	SWITCH/ROUTER	Políticas de seguridad deficientes o inexistentes
		Falta de capacitación
		Fallos en la autenticación
		Protocolos de red sin cifrar
		Políticas de seguridad deficientes o inexistentes
		Desastres naturales
		Inexistencia de sistemas contra incendios

Fuente: Elaboración Propia

3.2.2.6. Posible explotación de Vulnerabilidades

Siendo las vulnerabilidades debilidades asociadas con los activos, éstas pueden ser explotadas causando incidentes no deseados que pudieran terminar causando pérdidas, daño o deterioro de los activos.

Recordemos que la vulnerabilidad como tal, no causa daño, es simplemente una condición o conjunto de condiciones que pueden permitir que una amenaza afecte un activo.

Tabla 8 Probabilidad de ocurrencia de la vulnerabilidad

VALOR		CRITERIO
A	ALTO	**Vulnerabilidad muy deficiente**
M	MEDIO	**Vulnerabilidad deficiente**
B	BAJO	**Vulnerabilidad controlada**

Fuente: Elaboración Propia

A continuación se realizará una evaluación de las posibilidades de explotación de las vulnerabilidades como se muestra en la siguiente tabla.

Tabla 9 Evaluación de posibilidad de explotación de vulnerabilidades

Nº	GRUPOS DE ACTIVOS DE INFORMACION	VULNERABILIDADES	POSIBILIDAD DE EXPLOTACION
1	PROGRAMAS FUENTE	Política de control de cambios inexistentes	A
		Inadecuado manejo	M
		Error de diseño	A
		Falta de Seguridad del sistema	A
		Inadecuado manejo	A

2	DOCUMENTOS FISICOS	Política de integridad inexistente	M
		Política de integridad inexistente	M
		Falta de uso de EPP(Elemento de Protección Personal)	B
3	SERVIDORES	Falta de manual de mantenimiento	M
		Política de control de identidad inexistentes	A
		Falta de equipos de red de respaldo	A
		Falta de manual de contingencias	A
		Falta de uso de EPP(Elemento de Protección Personal)	B
		Inadecuado manejo de la información	M
		Configuración de perfiles deficiente	B
4	EQUIPOS	Falta de manual de mantenimiento	M
		Políticas de control de usuarios inexistentes	A
		Políticas de control de usuarios inexistentes	A
		Configuración de perfiles deficiente	M
		Falta de equipos de respaldo	M
5	INFORMACION ALMACENADA	Política de control de identidad inexistentes	A
		Falta de equipos de respaldo	M
		Políticas de backup inexistente	A
		Falta de licencias vigentes	M

6	SOFTWARE	Falta de manual de usuario	M
		Configuración de perfiles deficiente	M
		Política de actualizaciones inexistentes	M
7	SWITCH/ROUTER	Políticas de seguridad deficientes o inexistentes	A
		Falta de capacitación	M
		Fallos en la autenticación	B
		Protocolos de red sin cifrar	A
		Políticas de seguridad deficientes o inexistentes	A
		Desastres naturales	B
		Inexistencia de sistemas contra incendios	A

Fuente: Elaboración Propia

3.2.2.7. Estimado del Valor de los Activos en Riesgo

En la siguiente tabla el objetivo es determinar el daño económico que el riesgo pueda causar a los activos de información.

Tabla 10 Evaluación de los Activos en Riesgo

Nº	GRUPOS DE ACTIVO DE INFORMACION	AMENAZAS	POSIBILIDAD DE OCURRENCIA DE AMENAZAS	POSIBILIDAD EXPLOTACION DE VULNERAVILIDAD	VALOR ACTIVO
1	PROGRAMAS FUENTE	Control de cambios	A	A	MA
		Modificación mal intencionada	A	M	
		Error de programación	B	A	
		Software malicioso	M	A	
2	DOCUMENTOS FISICOS	Alteración de información	M	A	A
		Destrucción o eliminación mal intencionada	A	M	
		Destrucción de la información por error	M	M	
		Incendio, desastres naturales	M	B	
3	SERVIDORES	Error en el mantenimiento de hardware	M	M	MA
		Acceso no autorizado	B	A	
		Interferencia electromagnética	M	A	
		Falla de software de aplicación	A	A	
		Incendio, desastres naturales	A	B	

		Falla por error	M	M	
		Abuso de los recursos del sistema y repudio	B	B	
4	EQUIPOS	Corte o fallas del suministro eléctrico	M	M	**A**
		Violación de derechos de autor	B	A	
		Suplantación identidad	M	A	
		Abuso de los recursos del sistema y repudio	M	M	
		Falla de equipo por error	M	M	
5	INFORMACION ALMACENADA	Fuga de información mal intencionada	M	A	**M**
		Falla en dispositivo De almacenamiento	B	M	
		Backup no autorizado	M	A	
6	SOFTWARE	Ataque informático	A	M	**M**
		Malware	A	M	
		Suplantación de identidad	A	M	
		Uso no autorizado	B	M	
7	SWITCH/ROUTER	Alteración comunicaciones	A	A	**A**
		Entrega incorrecta	A	M	
		Error de operador	B	B	
		Fallo de electricidad	M	A	
		Interceptación comunicaciones	A	A	
		Repudio	A	B	
		Fallo de equipos	A	A	

Fuente: Elaboración Propia

3.2.2.8. Probabilidad de Ocurrencia del Riesgo

La probabilidad de que haya riesgo se basa en las vulnerabilidades y amenazas y la escala de valoración que se le ha calculado.

Tabla 11 Evaluación de la probabilidad de ocurrencia del riesgo

N°	GRUPOS DE ACTIVOS DE INFORMACION	AMENAZAS	VULNERABILIDADES	V. ACTIVO DE INFORMACION	PROBABILIDAD DE OCURRENCIA
1	PROGRAMAS FUENTE	Control de Cambios	Política de control de cambios inexistentes	MA	M
		Modificación mal intencionada	Inadecuado manejo		
		Error de programación	Error de diseño		
		Software malicioso	Falta de seguridad del sistema		
2	DOCUMENTOS FISICOS	Alteración de información	Inadecuado manejo	A	M
		Destrucción o eliminación mal intencionada	Política de integridad inexistente		
		Destrucción de la información por error	Integridad inexistente		
		Incendio, desastres naturales	Falta de uso de EPP(Elemento de Protección Personal)		
		Error en el mantenimiento de hardware	Falta de manual de mantenimiento		
		Acceso no autorizado	Política de control de identidad inexistentes		

3	SERVIDORES	Interferencia electromagnética	Falta de equipos de red de respaldo	MA	M
		Falla de software de aplicación	Falta de manual de contingencias		
		Incendio, desastres naturales	Falta de uso de EPP(Elemento de Protección Personal)		
		Falla por error	Inadecuado manejo de la información		
		Abuso de los recursos del sistema y repudio	Configuración de perfiles deficiente		
4	EQUIPOS	Corte o fallas del suministro eléctrico	Falta de Manual de mantenimiento	A	M
		Violación de derechos de autor	Políticas de control de usuarios inexistentes		
		Suplantación identidad	Políticas de control de usuarios		
		Abuso de los recursos del sistema y repudio	Configuración de perfiles deficiente		
		Falla de equipo por error	Falta de equipos de respaldo		
5	INFORMACION ALMACENADA	Fuga de información mal intencionada	Política de control de identidad inexistentes	M	M
		Falla en dispositivo de almacenamiento	Falta de equipos de respaldo		
		Backup no autorizado	Políticas de backup inexistente		

6	SOFTWARE	Ataque informático	Falta control de activos	M	M
		Malware	Falta de licencias vigentes		
		Suplantación de identidad	Falta de manual de usuario		
		Uso no Autorizado	Configuración de perfiles deficiente		
		Denegación del servicio por error	Política de actualizaciones inexistente		
7	SWITCH/ ROUTER	Alteración comunicaciones	Políticas de seguridad deficientes o inexistentes	A	A
		Entrega incorrecta	Falta de capacitación		
		Error de operador	Fallos en la autenticación		
		Fallo de electricidad	Protocolos de red sin cifrar		
		Interceptación comunicaciones	Políticas de seguridad deficientes o inexistentes		
		Repudio	Desastres naturales		
		Fallo de equipos	Inexistencia de sistemas contra incendios		

Fuente: Elaboración Propia

3.2.2.9. Valoración del Riesgo de los Activos

El análisis del riesgo busca prevenir los riesgos y las consecuencias, calificándolos y evaluándolos con el único fin de poder establecer el nivel de riesgo y las posibles acciones que se puede implementar. Se tiene dos aspectos dentro de los riesgos identificados uno es la probabilidad, entendido como la posibilidad de ocurrencia y el otro es impacto entendido como la consecuencia que puede ocasionar a la empresa la materialización del riesgo.

Análisis cuantitativo: hace referencia a valores numéricos que contribuyen a la calidad en la exactitud y evaluación de los riesgos.

Análisis cualitativo: se refiere a la utilización de formas descriptivas para dar a conocer las consecuencias potenciales y la posibilidad de ocurrencia.

Tabla 12 Valoración de la probabilidad de ocurrencia

VALOR	PROBABILIDAD		CRITERIO
3	A	ALTA	**EVITAR RIESGO**
2	M	MEDIA	**REDUCIR EL RIESGO**
1	B	BAJA	**ASUMIR RIESGO**

Fuente: Elaboración Propia

Tabla 13 Valoración del impacto

VALOR	IMPACTO		CRITERIO
3	A	ALTA	**IMPLICA MÁS DE UN PROCEDIMIENTO PARA SU CORRECCIÓN**
2	M	MEDIO	**IMPLICA UN PROCEDIMIENTO PARA SU CORRECCIÓN.**
1	B	BAJA	**RIESGO CONTROLADO**

Fuente: Elaboración Propia

Tabla 14 Resultados de Valoración

Nº	ACTIVO DE INFORMACIÓN	PROBABILIDAD DE OCURRENCIA		IMPACTO	
1	Equipos de Escritorio	2	**M**	3	**A**
2	Laptops	2	**M**	2	**M**
3	Impresoras	2	**M**	2	**M**
4	Disco Duro externo	2	**M**	2	**M**
5	Equipos de comunicación	2	**M**	3	**A**
6	Switch de 24 puertos	2	**M**	3	**A**
7	Switch de 16 puertos	2	**M**	3	**A**
8	Switch de 8 puertos	2	**M**	3	**A**
9	Servidor de Archivos	2	**M**	3	**A**
10	Servidor de temas Administrativos	3	**A**	3	**A**
11	Servidor SIAF	3	**A**	3	**A**
12	Teléfonos IP	**2**	**M**	**3**	**A**
13	Red Wifi corporativo	**3**	**A**	**3**	
14	Red LAN	**3**	A	**3**	**A**
15	Servidor Web, dhcp,dns	**2**	M	**3**	**A**
16	Microsoft Office 2013 y 2010	1	**B**	2	**M**
17	Antivirus McAfee,Eset,Avast,Comodo, AVG	2	**M**	2	**M**
18	Microsoft Windows Server 2012 y 2008	1	**B**	**3**	**A**

19	Sql Express edition	1	**B**	2	**M**
20	Simunet	2	**M**	**3**	**A**
21	Team Viewer 11	2	**M**	**1**	**B**
22	Anydesk	2	**M**	1	**B**
23	Librerías SIAF	2	**M**	**3**	**A**
24	Registros de planilla	2	**M**	**3**	**A**
25	Documentos de compras	2	**M**	3	**A**
26	Cotizaciones	2	**M**	2	**M**
27	Registros de RRHH	2	**M**	3	**A**
28	Registros de cobranza	2	**M**	3	**A**
29	Actas de Requerimientos	2	**M**	2	**M**
30	Actas de Implementación	1	**B**	2	**M**
31	Historial de modificaciones	1	**B**	2	**M**
32	Historial de Soportes	1	**B**	2	**M**
33	Historial de Actualizaciones	**1**	B	**2**	**M**
34	Solicitudes de Cambio	**3**	A	**3**	**A**
35	Agenda Telefónica	2	M	3	A
36	Estado de soporte del cliente	2	M	3	A

Fuente: Elaboración Propia

Resultados

Después de evaluar las amenazas y vulnerabilidades que tienen los activos de información, mediante una matriz de evaluación de riesgo se obtiene la siguiente tabla con la evaluación de los riesgos.

Tabla 15 Matriz de Evaluación de Riesgo

PROBABILIAD	**Alta**	MEDIO	ALTO	CRÍTICO
	Media	BAJO	MEDIO	ALTO
	Baja	BAJO	BAJO	MEDIO
		Bajo	**Medio**	**Alta**
		IMPACTO		

Fuente: Elaboración Propia

Tabla 16 Riesgo de los Activos de Información

Nº	ACTIVO DE INFORMACIÓN	RIESGO
1	Equipos de Escritorio	ALTO
2	Laptops	MEDIO
3	Impresoras	MEDIO
4	Disco Duro externo	MEDIO
5	Equipos de comunicación	ALTO
6	Switch de 24 puertos	ALTO
7	Switch de 16 puertos	ALTO
8	Switch de 8 puertos	ALTO
9	Servidor de Archivos	ALTO
10	Servidor de temas Administrativos	CRÍTICO
11	Servidor SIAF	CRÍTICO
12	Teléfono IP	ALTO
13	Red Wifi corporativo	CRÍTICO
14	Red LAN	CRÍTICO
15	Servidor Web, dhcp,dns	ALTO
16	Microsoft Office 2013 y 2010	BAJO
17	Antivirus McAfee,Eset,Avast,Comodo, AVG	MEDIO
18	Microsoft Windows Server 2012 y 2008	MEDIO
19	Sql Express edition	BAJO
20	Simunet	ALTO
21	Team Viewer 11	BAJO
22	Anydesk	BAJO
23	Librerías SIAF	ALTO
24	Registros de planilla	ALTO

25	Documentos de compras	**ALTO**
26	**Cotizaciones**	**MEDIO**

27	**Registros de RRHH**	**ALTO**
28	Registros de cobranza	**ALTO**
29	Actas de Requerimientos	**MEDIO**
30	Actas de Implementación	**BAJO**
31	Historial de Modificaciones	**BAJO**
32	Historial de Soportes	**BAJO**
33	Historial de Actualizaciones	**BAJO**
34	Solicitudes de Cambio	**CRÍTICO**
35	Agenda Telefónica	**ALTO**
36	**Estado de soporte del cliente**	**ALTO**

Fuente: Elaboración Propia

3.2.3. Políticas de seguridad de información

Según (Moyano Orjuela & Suárez Cárdenas, 2017) , El plan de implementación del SGSI, exige el desarrollo de una política de seguridad en la que se establezcan las reglas necesarias para garantizar la confidencialidad, integridad y disponibilidad de la información en todos los procesos. Por tanto, esta debe ser definida, asignada y comunica a todos los miembros de la institución.

Figura 24 Ciclo de Políticas de Seguridad

Fuente: Elaboración Propia

3.2.3.1. Políticas Generales de Seguridad de la Información

Con el fin de optimizar el uso de la información, se debe garantizar la confidencialidad, integridad y disponibilidad en las actividades de la municipalidad; se dan a conocer las siguientes políticas de observancia general y obligatoria:

1. Antes de asignar algún equipo de cómputo a un nuevo usuario, la Sub Gerencia de Informática y Tecnologías de la información

debe asegurarse que no exista información de suma importancia, en caso contrario, debe ser respaldada de forma inmediata y posteriormente se procederá a borrarla del equipo.

2. La Sub Gerencia de Informática y Tecnologías de la información tiene la obligación de adoptar todas las medidas de control y mecanismos, seguridad y monitoreo, ya sea para el uso de correo electrónico o sitios web con contenidos sospechosos.
3. El personal de soporte debe realizar pruebas (mínimo dos veces al año), así como un análisis de las vulnerabilidades de la red ante un posible ataque desde el exterior de la municipalidad.
4. El administrador de la seguridad es el único autorizado para habilitar las paginas o sitios web que se encuentran bloqueadas, siempre y cuando el acceso a estos esté debidamente autorizadas por el encargado respectivo, existiendo una justificación para ello.
5. El personal de Soporte y desarrollo debe asegurarse que los componentes de red cuenten con las configuraciones respectivamente, contemplando las actualizaciones de parches y de versiones.
6. La Sub Gerencia de Informática y Tecnologías de la información debe tener un registro de todas las personas que tienen algún privilegio de acceso.
7. La Sub Gerencia de Informática y Tecnologías de la información debe tener un registro de todos los activos de información, este debe incluir clasificación, ubicación y usuario designado. El inventario debe actualizarse constantemente.
8. El personal de la empresa debe utilizar el correo de trabajo solo para fines laborales.
9. El uso de internet debe estar debidamente controlado por un proxy, permitiendo solamente acceder a los usuarios autorizados.
10. No está permitido usar el internet para fines personales o de lucro.

11. En caso de sospecha de revelación de contraseñas a personas ajenas a la empresa, estas contraseñas deben ser cambiadas inmediatamente.
12. Antes de descargar cualquier archivo a las computadoras se debe escanear con el antivirus para evitar los virus maliciosos o malware.
13. Esta estrictamente prohibido usar el internet para acceder o descargar contenido pornográfico, descargar cualquier tipo de software sin autorización del área de sistemas, o descargando software comercial violando las leyes de derecho de autor.
14. Se prohíbe ingresar a las áreas de trabajo sin autorización correspondiente o extraer de las instalaciones medios removibles como el CD, USB, DVD, disco duro, Zip, etc., sin una debida autorización.
15. La clave del usuario es única para cada tipo de acceso que desee.
16. Cualquier salida de algún equipo de cómputo fuera de la municipalidad debe estar autorizada por el sub gerente.
17. Los sub gerentes y gerentes deberán garantizar que se ha comunicado a todo el personal de la municipalidad las responsabilidades relacionadas a la seguridad de la información antes de poder brindarles acceso a la información.
18. Los puntos de acceso inalámbricos deben estar configurados de manera segura, para ello se debe tomar en cuenta lo siguiente: máximo de dispositivos que puedan conectarse a la red, filtrar las direcciones MAC de los equipos conectados y por ultimo utilizar una encriptación de 128 bits mínimo.
19. Se debe tener instalado y configurados como mínimo Firewalls y sistemas de prevención y detección de intrusos para poder salvaguardar los datos que se transmiten por la red.
20. Cuando algún usuario este usando información reservada o confidencial, no podrá abandonar su lugar de trabajo sin antes bloquear el sistema.

3.2.3.2. Políticas Específicas de Seguridad de la Información

Todo los usuarios de la municipalidad deben de cumplir con las políticas y los estándares de seguridad para poder proteger y controlar la información siendo aplicable a todo su personal regular, no regular, contratistas y consultores que utilicen los sistemas e instalaciones.

1. Los sistemas, la red de comunicación y la información de la municipalidad solamente serán utilizadas para fines laborales aprobados por los responsables del área.
2. Políticas para un mejor control de accesos: todo usuario y software debe contar con autorización detallada para el uso de los sistemas y espacios dentro de la municipalidad, este privilegio solo será otorgado cuando se realiza una función específica. Las personas ajenas a la institución o llamados terceros solo podrán hacer uso de los sistemas e instalaciones con una autorización específica y durante un tiempo determinado.
3. Para asegurarse que el personal sea correctamente contratado se debe cumplir con ciertos estándares, para que así sean identificados mientras laboran en la institución, por ende esta política se debe aplicar a todos los empleados de la institución y proveedores.
4. Los empleados de la municipalidad pueden utilizar sus propias computadoras, dispositivos periféricos, o software en las instalaciones de la municipalidad siempre y cuando tengan autorización de su Sub Gerencia o Gerencia a la cual corresponden.
5. Cada puesto que desempeñe el personal de la municipalidad debe estar descrito y por ende se debe cumplir con las responsabilidades. La alta dirección debe conocer las responsabilidades del personal que tiene a su supervisión; se debe contar con TDR (Términos de Referencia) el cual cuenta con las descripciones del puesto y responsabilidades que tiene

que cumplir.

3.2.3.3. Selección de controles para mitigar los riesgos

Una vez identificado los requerimientos de seguridad, se seleccionan controles que garanticen la reducción de los riesgos a niveles aceptables. A continuación los controles seleccionados son:

3.2.3.3.1. Seguridad Lógica

Objetivo: Controlar los accesos a la información mediante la aplicación de mecanismos de seguridad establecidos para evitar la modificación, destrucción de los archivos y datos.

Los procedimientos formales se mencionan a continuación:

1. Los usuarios del sistema informático deben mantener en secreto sus contraseñas personales y las que se comparten de forma grupal solo entre los miembros del grupo, este compromiso está contemplado en los términos y condiciones del contrato o resolución. Responsable: Sub Gerencia de Informática y Tecnologías de la Información.
2. Cada usuario de la municipalidad pertenecerá a un grupo de trabajo donde poseerá un perfil, el que permitirá accesos a los mismos recursos y servicios informáticos, de acuerdo a las funciones del área que pertenece y de acuerdo al rol correspondiente a su cargo. Los accesos personalizados deberán contar con la autorización y aprobación del Jefe Inmediato. Responsable: Sub Gerencia de Informática y Tecnologías de la Información.
3. Solo se podrá realizar tres intentos como máximo para poder acceder a la red, luego el sistema bloqueará automáticamente la cuenta. Responsable: Sub Gerencia de Informática y Tecnologías de la Información.
4. Todo acceso a la red y al sistema, deberá pedir un usuario y contraseña, la cual deberá tener una caducidad de 30 días, no pudiendo utilizar contraseñas anteriores. Responsable: Sub

Gerencia de Informática y Tecnologías de la Información.

5. Cada usuario de la municipalidad tendrá una sola clave de acceso, la cual también será utilizado para correo corporativo, ingreso a la red y al sistema. Responsable: Sub Gerencia de Informática y Tecnologías de la Información.
6. Después de haber creado una cuenta para un nuevo usuario se activará el pedido de cambio de contraseña. Responsable: Sub Gerencia de Informática y Tecnologías de la Información.
7. Los accesos a la red y al sistema serán bloqueados desde las 11:00 p.m hasta las 7:00 a.m de lunes a sábado, y los días domingos todo el día a excepción que sea autorizado por el Alcalde. Responsable: Sub Gerencia de Informática y Tecnologías de la Información.
8. Los usuarios tendrán al acceso del internet a las paginas definidas por la municipalidad, el acceso a otras webs deberán ser autorizadas por cada Gerencia, a través del formato establecido. Responsable: Sub Gerencia de Informática y Tecnologías de la Información.
9. Los usuarios que tengan acceso a internet solo usaran para fines netamente laborales. Responsable: Sub Gerencia de Informática y Tecnologías de la Información.
10. Está totalmente prohibido el uso de internet para descargar archivos de video, imagen, audio, programas ejecutables, etc., que no estén aprobados por el área de sistemas. Responsable: Sub Gerencia de Informática y Tecnologías de la Información.

3.2.3.3.2. Seguridad Personal

Objetivo: Asegurar que todo el personal de la municipalidad, contratistas, proveedores y terceros entiendan sus responsabilidades y asuman los roles por la cual han sido contratados, para que así puedan ser identificados mientras que laboren en la municipalidad reduciendo algún fraude, mal uso de las instalaciones o riesgo de hurto.

Definición de roles y responsabilidades establecidos sobre la seguridad

de información.

1. La seguridad es responsabilidad de todo el personal, por ende, todos aquellos con acceso a las instalaciones e información deben acatar los estándares documentados en la política de seguridad e incluirla como una de sus responsabilidades principales. Responsables: Gerentes de área.
2. Cuando se adquiera el servicio de un personal, se debe de entregar la política de seguridad de la información, así como las normas y procedimientos para el uso de las aplicaciones y los sistemas de información de la municipalidad. También, se debe entregar un resumen de las medidas básicas de seguridad de la información, una copia firmada de las políticas de seguridad de información que deben ser guardadas en el archivo del personal. Responsable: Sub Gerencia de Recursos Humanos.
3. El personal Contratista o tercero deberá recibir una copia del acuerdo de no divulgación firmado por la municipalidad y por el proveedor de servicios que tendrá la responsabilidad de la confidencialidad de la información. Responsable: Sub Gerencia de Recursos Humanos.

Verificación de los antecedentes.

1. Todo empleado que labora en la municipalidad deberá mantener su curriculum vitae actualizado y correctamente documentado. Responsable: Sub Gerencia de Recursos Humanos.
2. Todo empleado que trabaje en la municipalidad deberá comunicar inmediatamente al área de Recursos Humanos los cambios ocurridos en su curriculum vitae. Responsable: Sub Gerencia de Recursos Humanos.

Concientización y entrenamiento.

1. Es responsabilidad de la Sub Gerencia de Informática y Tecnologías de la Información el promover la importancia de la seguridad a todos los empleados. Dicho programa de concientización en seguridad

debe brindar continuas capacitaciones, charlas, afiches, etc., los cuales hagan recordar constantemente el rol importante que cumplen con el mantenimiento de la seguridad de la información. Responsable: Sub Gerencia de Informática y Tecnologías de la Información.

2. Es responsabilidad del personal que capacita proveer de material escrito; los materiales pueden ser manuales, guías, separatas, entre otros. Responsables: Gerentes de área.
3. El personal que capacita debe ser elegido de acuerdo a la experiencia y conocimiento que posee de un tema específico. Responsable: Sub Gerencia de Recursos Humanos y Sub Gerencia de Informática y Tecnologías de la Información.

3.2.3.3.3. Seguridad Física y Ambiental

Objetivo: Evitar accesos no autorizados, daños e interferencias contra los ambientes y la información de la municipalidad.

Para evitar el acceso físico no autorizado, daños o interferencias a las áreas de trabajo y a la información de la municipalidad se brindará controles.

1. Se debe establecer un registro de entrada y salida de visitas a las áreas administrativas. Responsable: Gerencia de Seguridad Ciudadana.
2. Implementar un sistema de vigilancia con cámaras de seguridad en lugares estratégicos, a fin de mantener un mejor control del movimiento de las personas dentro de la empresa. Responsable: Sub Gerencia de Informática y Tecnologías de la Información.

Se brindará controles para prevenir pérdidas, daños o robos de los activos de información. Se dará protección a los equipos frente a amenazas físicas y ambientales.

1. Cuando el personal se traslade a diferentes áreas dentro de la

municipalidad, deberá asegurarse de activar el protector de pantalla pulsando las teclas: Ctrl + Alt + Supr para evitar la pérdida de algún tipo de información. Responsable: Gerencias y Sub Gerencias.

2. Bajo ninguna circunstancia, ningún personal deberá retirar un equipo o componente de la municipalidad sin una guía de salida autorizada por la dependencia en cuestión. Responsable: Sub Gerencia de Recursos Humanos y Sub Gerencia de Informática y Tecnologías de la Información.
3. Se deberá apagar los equipos de cómputo cuando se dejen de utilizar por un tiempo prolongado, en especial cuando sean días no laborales. Responsable: Gerencias y Sub Gerencias.
4. Los equipos deben tener una identificación única para cada usuario de la municipalidad y deben registrarse en el control de inventario. Responsable: Sub Gerencia de Informática y Tecnologías de la Información.
5. La pérdida o robo de algún componente de hardware o software debe ser reportado inmediatamente. Responsable: Gerencias y Sub Gerencias.

Controles para establecer medidas de seguridad en la Sub Gerencia de Informática y Tecnologías de la Información.

1. Las autorizaciones hacia el área de sistemas deben ser aprobadas por el responsable de la gerencia o sub gerencia. Responsable: Sub Gerencia de Informática y Tecnologías de la Información.
2. La limpieza de la oficina deberá realizarse en presencia de algún empleado del área. Responsable: Sub Gerencia de Informática y Tecnologías de la Información.
3. El empleado deberá conocer las zonas de seguridad en caso de cualquier evento causado o natural, identificando las señalizaciones. Responsable: Sub Gerencia de Defensa Civil y Gestión de Riesgos de Desastres.
4. El personal deberá informar cualquier obstáculo que se encuentre en las rutas de salida, sobre las condiciones inseguras encontradas,

con la finalidad que sean reubicadas o se retire de la zona. Responsable: Sub Gerencia de Defensa Civil y Gestión de Riesgos de Desastres.

3.2.3.3.4. Inventario de los activos y clasificación de la información

Objetivo: Asegurar que la información que se reciba tenga un nivel de protección adecuada.

1. Todo documento debe ser etiquetado como “Restringido”, “Confidencial”, de “Uso interno” o de “Acceso General”, dependiendo de la clasificación asignada. Responsable: Gerencias y Sub Gerencias.
2. Todo documento que presente información clasificada como “Confidencial” o “Restringida”, debe ser etiquetado en la parte superior e inferior de cada página con la clasificación correspondiente. Responsable: Gerencias y Sub Gerencias.
3. Todo documento clasificado como “Confidencial” o “Restringido” debe contar con una carátula en la cual se muestre la clasificación de la información que contiene. Responsable: Gerencias y Sub Gerencias.
4. El ambiente donde se almacena la información clasificada como “Restringida”, debe contar con adecuados controles de acceso y asegurado cuando se encuentre sin vigilancia. El acceso debe ser permitido solo al personal autorizado. El personal de limpieza de la oficina deberá ingresar solo cuando halla un personal autorizado. Responsable: Sub Gerencia de Informática y Tecnologías de la Información.
5. El área de sistemas a través del responsable designado deberá mantener actualizada la relación de software base necesario para cada nuevo usuario o grupo de usuarios.
6. El área de sistemas a través del responsable designado deberá actualizar constantemente el inventario de los equipos de cómputo, periféricos, equipos de comunicación, redes, UPS y archivos como (*.INI, *.CNF, *.SYS, *.DLL, *.EXE, *.BAT, otros).

3.2.3.3.5. Administración de las comunicaciones

Objetivo: Asegurar un adecuado nivel de servicio a los clientes.

1. El correo corporativo, es una herramienta de comunicación e intercambio de información entre personas o grupos. Responsable: Gerencias y Sub Gerencias.
2. Nunca se deben descargar programas o archivos adjuntos (en correos electrónicos) cuya procedencia y fiabilidad no ofrezcan todas las garantías. Responsable: Gerencias y Sub Gerencias.
3. Todos los intentos de conexión, desconexión, cambios de contraseña, fallas en los cambios de contraseña, reinstalación de contraseñas, registro de usuarios y supresión de usuarios, serán registrados. Responsable: Sub Gerencia de Informática y Tecnologías de la Información.

3.2.3.3.6. Adquisición y mantenimiento de sistemas informáticos

Objetivo: La seguridad debe estar imbuida dentro de los sistemas de información.

1. En la municipalidad, la información confidencial debe ser diariamente encriptado, antes de que viaje a través de la red. Responsable: Sub Gerencia de Informática y Tecnologías de la Información.
2. La información crítica debe ser encriptado cuando se vaya a respaldar o guardar. Responsable: Sub Gerencia de Informática y Tecnologías de la Información.
3. Los sistemas aplicativos deben ser probados en forma exhaustiva, antes de ser liberados a producción, en ambientes controlados de pruebas (Test y Calidad). Responsable: Sub Gerencia de Informática y Tecnologías de la Información.
4. La municipalidad deberá implantar mecanismos que permitan llevar controles de las modificaciones y accesos a los programas producto y programas fuente con el objeto de mantener integridad sobre los

ambientes de prueba y producción. Responsable: Sub Gerencia de Informática y Tecnologías de la Información.

5. Cada software elaborado por desarrolladores propios de la municipalidad o por desarrolladores externos contratados, debe de contener la información de derecho de autor correspondiente. Responsable: Sub Gerencia de Informática y Tecnologías de la Información.

3.2.3.3.7. Procedimiento de respaldo

Objetivo: Establecer un conjunto de controles que permitan gestionar adecuadamente el respaldo de la información producida en la municipalidad.

1. El área de Sistemas a través de un responsable llevará una bitácora actualizada de la realización de backups de bases de datos detallando la fecha de backup, la hora, el tamaño, el responsable de la operación, el contenido, la fecha de registro, y observaciones en el caso que estas existieran.
2. Se realizará comprobaciones puntuales para asegurar que las copias de seguridad se realicen correctamente, considerando lo siguiente:

- Organizar pruebas periódicas de hardware y software para la recuperación de la información.
- Establecer y ejecutar procedimientos para la restauración de la información de la municipalidad.
- Participar en pruebas y simulacros de desastres en la municipalidad, donde se pueda verificar un buen funcionamiento de los procedimientos de backups.

3. El procedimiento de backup, debe ser difundido a todas las personas involucradas, teniendo como responsable de tal difusión a la Sub Gerencia de Informática y Tecnologías de la Información.

3.2.3.3.8. Gestión de incidentes de seguridad de la información

Objetivo: Asegurar que los eventos y debilidades sean asociados con los sistemas de información, sean comunicados de una manera que permita que se realice una acción correctiva a tiempo.

1. Luego de reportado el incidente de seguridad, éste debe ser investigado por el personal técnico del Área de Sistemas en forma rápida y confidencial. Se debe identificar la gravedad del incidente para la toma de medidas correctivas.
2. Se debe mantener una documentación de todos los incidentes de seguridad ocurridos en la empresa.

Procedimientos establecidos para dar una respuesta adecuada a los incidentes y vulnerabilidades de seguridad reportadas.

1. Luego de la investigación realizada por el personal designado, se elaborará un informe al Sub Gerente indicando la severidad del incidente.
2. El Sub Gerente de Informática y Tecnologías de la Información reportará sobre los avances en los tratamientos a los incidentes y vulnerabilidades que son reportadas.

3.2.3.3.9. Cumplimiento Normativo y de Auditoria

Objetivo: Evitar los incumplimientos de cualquier ley civil o penal, requisito reglamentario, regulación u obligación contractual, y de todo requisito de seguridad.

1. Los gerentes y Sub Gerentes deben asegurarse que las responsabilidades respecto a la seguridad deben cumplirse y las funciones que estén relacionadas se ejecuten correctamente. Responsable: Gerencias y Sub Gerencia de Unidad.
2. Es responsabilidad del personal encargado de la administración de la seguridad y de auditoria interna verificar el cumplimiento de las políticas de seguridad. Las excepciones deben ser reportadas a la

gerencia apropiada.

3. Es responsabilidad del personal encargado de la administración de la seguridad y de auditoria interna verificar el cumplimiento de las políticas de seguridad. Las excepciones deben ser reportadas a la gerencia apropiada.
4. Todos los registros de auditoría de los sistemas, serán recopilados en una base de datos que facilite la generación de informes. Responsable: Sub Gerencia de Informática y Tecnologías de la Información.
5. Es necesario identificar y desarrollar modelos de informes de auditorías. Responsable: Sub Gerencia de Informática y Tecnologías de la Información.

Las siguientes tablas muestran la relación de las políticas propuestas con sus respectivos controles.

Tabla 17 Controles de Política General

CONTROLES			
POLÍTICAS GENERALES DE SEGURIDAD DE LA INFORMACIÓN			
3.2.3.3.1 Seguridad Lógica			
Objetivo: Controlar los accesos a la información mediante la aplicación de mecanismos de seguridad establecidos para evitar la modificación, destrucción de los archivos y datos.			
3.3.1.1	Antes de asignar algún equipo de cómputo a un nuevo usuario, el área de sistemas debe asegurarse que no exista información de suma importancia, en caso contrario, debe ser respaldada de forma inmediata y posteriormente se procederá a borrarla del equipo.	**Control:** Los usuarios del sistema informático deben mantener en secreto sus contraseñas personales y las que se comparten de forma grupal solo entre los miembros del grupo, este compromiso está contemplado en los términos y condiciones del contrato o resolución	Responsable: Sub Gerencia de Informática y Tecnologías de la Información.
3.3.1.2	La Sub Gerencia de Informática y Tecnologías de la Información tiene la obligación de adoptar todas las medidas de control y mecanismos, seguridad y monitoreo, ya sea para el uso de correo electrónico o sitios web con contenidos sospechosos.	**Control:** Cada usuario de la municipalidad pertenecerá a un grupo de trabajo donde poseerá un perfil, el que permitirá accesos a los mismos recursos y servicios informáticos. **Control:** Solo se podrá realizar tres intentos como máximo para poder acceder a la red, luego el sistema bloqueara automáticamente la cuenta. **Control:** todo acceso a la red y al sistema, deberá pedir un usuario y contraseña, la cual deberá tener una caducidad de 30 días. **Control:** cada usuario de la municipalidad tendrá una sola clave de acceso.	Responsable: Sub Gerencia de Informática y Tecnologías de la Información.
3.3.1.3	El personal de soporte debe realizar pruebas (mínimo dos veces al año), así como un análisis de las vulnerabilidades de la red ante un posible ataque desde el exterior de la municipalidad.	**Control:** Después de haber creado una cuenta para un nuevo usuario se activará el pedido de cambio de contraseña. **Control:** los accesos a la red y al sistema serán bloqueados desde las 11:00 p.m hasta las 7:00 a.m y los días domingos todo el día a excepción que sea autorizado.	Responsable: Sub Gerencia de Informática y Tecnologías de la Información.

3.3.1.4	El administrador de la seguridad es el único autorizado para habilitar las paginas o sitios web que se encuentran bloqueadas, siempre y cuando el acceso a estos esté debidamente autorizadas por el encargado respectivo, existiendo una justificación para ello.	**Control:** los usuarios tendrán el acceso del internet a las páginas definida por la municipalidad, el acceso a otras webs deberán ser autorizadas por cada Gerencia.	Responsable: Sub Gerencia de Informática y Tecnologías de la Información.
3.3.1.5	El personal de Soporte y desarrollo debe asegurarse que los componentes de red cuenten con las configuraciones respectivamente, contemplando las actualizaciones de parches y de versiones.	**Control:** Los usuarios que tengan acceso a internet solo usaran para fines netamente laborales.	
3.3.1.6	El área de sistemas debe tener un registro de todas las personas que tienen algún privilegio de acceso.	**Control:** Esta totalmente prohibido el uso de internet para descargar archivos que no estén aprobados por el área de TI.	
POLÍTICAS GENERALES DE SEGURIDAD DE LA INFORMACIÓN			
3.2.3.3.2 Seguridad Personal			
Objetivo: Asegurar que todo el personal de la municipalidad, contratistas, proveedores y terceros entiendan sus responsabilidades y asuman los roles por la cual han sido contratados, para que así puedan ser identificados mientras que laboren en la empresa reduciendo algún fraude, mal uso de las instalaciones o riesgo de hurto.			
3.3.1.7	El área de administración debe tener un registro de todos los activos de información, este debe incluir clasificación, ubicación y usuario designado. El inventario debe actualizarse constantemente.	**Control:** La seguridad es responsabilidad de todo el personal de la municipalidad, por ende, todos aquellos con acceso a las instalaciones e información deben acatar los estándares documentados en la política de seguridad.	Responsable: Gerentes de área.
		Control: Cuando se adquiera el servicio de un personal, se debe de entregar la política de seguridad de la información, así como las normas y procedimientos para el uso de las aplicaciones y los sistemas de información de la municipalidad.	Responsable: Sub gerencia de Recursos Humanos.

		Control: El personal Contratista o tercero deberá recibir una copia del acuerdo de no divulgación firmado por la empresa y por el proveedor de servicios que tendrá la responsabilidad de la confidencialidad de la información. Responsable: Sub Gerencia de Recursos Humanos.	
3.3.1.8	El personal de la municipalidad debe utilizar el correo de trabajo solo para fines laborales.	**Control:** Es responsabilidad de la Sub Gerencia de Informática y Tecnologías de la Información el promover la importancia de la seguridad a todos los empleados.	Responsable: Sub Gerencia de Informática y Tecnologías de la Información.
POLÍTICAS GENERALES DE SEGURIDAD DE LA INFORMACIÓN			
3.2.3.3.3 Seguridad Física y Ambiental			
Objetivo: Evitar accesos no autorizados, daños e interferencias contra los ambientes y la información de la municipalidad.			
3.3.1.9	El uso de internet debe estar debidamente controlado por un proxy, permitiendo solamente acceder a los usuarios autorizados.	**Control:** Cuando el personal se traslade a diferentes áreas dentro de la municipalidad, deberá asegurarse de activar el protector de pantalla pulsando las teclas: Ctrl + Alt + Supr para evitar la pérdida de algún tipo de información.	Responsable: Gerencias y Sub Gerencias.
3.3.1.10	No está permitido usar el internet para fines personales o de lucro.	**Control:** Implementar un sistema de vigilancia con cámaras de seguridad en lugares estratégicos, a fin de mantener un mejor control del movimiento de las personas dentro de la municipalidad.	Responsable: Sub Gerencia de Informática y Tecnologías de la Información.
3.3.1.11	En caso de sospecha de revelación de contraseñas a personas ajenas a la municipalidad, estas contraseñas deben ser cambiadas inmediatamente.	**Control:** Los equipos deben tener una identificación única para cada usuario de la municipalidad y deben registrarse en el control de inventario.	Responsable: Gerencias y Sub Gerencias.

3.3.1.13	Esta estrictamente prohibido usar el internet para acceder o descargar contenido pornográfico, descargar cualquier tipo de software sin autorización del área de sistemas, o descargando software comercial violando las leyes de derecho de autor.	**Control:** Las autorizaciones hacia el área de sistema deben ser aprobadas por el responsable de la Gerencia o Sub Gerencia.	Responsable: Sub Gerencia de Informática y Tecnologías de la Información.
3.3.1.16	Cualquier salida de algún equipo de cómputo fuera de la municipalidad debe estar autorizada por el sub gerente.	**Control:** Bajo ninguna circunstancia, ningún personal deberá retirar un equipo o componente de la municipalidad sin una guía de salida autorizada por la dependencia en cuestión.	Responsable: Sub Gerencia de Recursos Humanos y Sub Gerencia de Informática y Tecnologías de la Información.
3.3.1.14	Se prohíbe ingresar a las áreas de trabajo sin autorización correspondiente o extraer de las instalaciones medios removibles como el CD, USB, DVD, disco duro, Zip, etc., sin una debida autorización.	**Control:** La pérdida o robo de algún componente de hardware o software debe ser reportado inmediatamente.	Responsable: Gerencias y Sub Gerencia.
POLÍTICAS GENERALES DE SEGURIDAD DE LA INFORMACIÓN			
3.2.3.3.4 Inventario de los Activos y clasificación de la información			
Objetivo: Asegurar que la información que se reciba tenga un nivel de protección adecuada.			
3.3.1.15	La clave del usuario es única para cada tipo de acceso que desee.	**Control:** El ambiente donde se almacena la información clasificada como “Restringida”, debe contar con adecuados controles de acceso y asegurado cuando se encuentre sin vigilancia	Responsable: Sub Gerencia de Informática y Tecnologías de la Información.
POLÍTICAS GENERALES DE SEGURIDAD DE LA INFORMACIÓN			
3.2.3.3.5 Administración de las Comunicaciones			
Objetivo: Asegurar un adecuado nivel de servicio a los clientes.			
3.3.1.12	Antes de descargar cualquier archivo a las computadoras se debe escanear con el antivirus para evitar los virus maliciosos o malware.	**Control:** Nunca se deben descargar programas o archivos adjuntos (en correos electrónicos) cuya procedencia y fiabilidad no ofrezcan todas las garantías.	Responsable: Gerencias y Sub Gerencias.

3.3.1.17	Los jefes de área, coordinadores y gerentes deberán garantizar que se ha comunicado a todo el personal de la municipalidad las responsabilidades relacionadas a la seguridad de la información antes de poder brindarles acceso a la información.	**Control:** Nunca se deben descargar programas o archivos adjuntos (en correos electrónicos) cuya procedencia y fiabilidad no ofrezcan todas las garantías.	Responsable: Gerencias y Sub Gerencias.
POLÍTICAS GENERALES DE SEGURIDAD DE LA INFORMACIÓN			
3.2.3.3.6 Adquisición y mantenimiento de sistemas informáticos.			
Objetivo: La seguridad debe estar imbuida dentro de los sistemas de información.			
3.3.1.20	Cuando algún usuario este usando información reservada o confidencial, no podrá abandonar su lugar de trabajo sin antes bloquear el sistema.	**Control:** En la municipalidad, la información confidencial debe ser diariamente encriptado, antes de que viaje a través de la red.	Responsable: Sub Gerencia de Informática y Tecnologías de la Información.
POLÍTICAS GENERALES DE SEGURIDAD DE LA INFORMACIÓN			
3.2.3.3.8 Gestión de incidentes de seguridad de la información			
Objetivo: Asegurar que los eventos y debilidades sean asociados con los sistemas de información, sean comunicados de una manera que permita que se realice una acción correctiva a tiempo.			
3.3.1.18	Los puntos de acceso inalámbricos deben estar configurados de manera segura, para ello se debe tomar en cuenta lo siguiente: máximo de dispositivos que puedan conectarse a la red, filtrar las direcciones MAC de los equipos conectados y por ultimo utilizar una encriptación de 128 bits mínimo.	**Control:** Luego de reportado el incidente de seguridad, éste debe ser investigado por el personal técnico del Área de Sistemas en forma rápida y confidencial. Se debe identificar la gravedad del incidente para la toma de medidas correctivas.	Responsable: Sub Gerencia de Informática y Tecnologías de la Información.
3.3.1.19	Se debe tener instalado y configurados como mínimo Firewalls y sistemas de prevención y detección de intrusos para poder salvaguardar los datos que se transmiten por la red.	**Control:** La Sub Gerencia de Informática y Tecnologías de la Información reportara sobre los avances en los tratamientos a los incidentes y vulnerabilidades que son reportadas.	Responsable: Sub Gerencia de Informática y Tecnologías de la Información.

Fuente: Elaboración propia

Tabla 18 Controles de Política Especifica 1

N°	Políticas Específicas de Seguridad de la Información		Responsable
1	Los sistemas, la red de comunicación y la información de la municipalidad solamente serán utilizados para fines laborales aprobados por los responsables de área.		Sub Gerencia de Informática y Tecnologías de la Información.
Dominio	**N°**	**Control**	
Inventario de los activos y clasificación de la información	**5**	El área de sistemas a través del responsable designado deberá mantener actualizada la relación de software base necesario para cada nuevo usuario o grupo de usuarios.	
	6	El área de sistemas a través del responsable designado deberá actualizar constantemente el inventario de los equipos de cómputo, periféricos, equipos de comunicación, redes, UPS y archivos como (*.INI, *.CNF, *.SYS, *.DLL, *.EXE, *.BAT, otros).	

Fuente: Elaboración propia

Tabla 19 Controles de Política Especifica 2

N°	Políticas Específicas de Seguridad de la Información		Responsable
2	Políticas para el control de accesos: todo usuario y software debe contar con autorización explícita para el uso de los sistemas y espacios dentro de la municipalidad, este privilegio solo será otorgado cuando se realiza una función específica. Las personas ajenas a la institución o llamados terceros solo podrán hacer uso de los sistemas e instalaciones con una autorización específica y durante un tiempo determinado.		Sub Gerencia de Informática y Tecnologías de la Información.
Dominio	**N°**	**Control**	
Inventario de los activos y clasificación de la información	**4**	El ambiente donde se almacena la información clasificada como “Restringida”, debe contar con adecuados controles de acceso y asegurado cuando se encuentre sin vigilancia. El acceso debe ser permitido solo al personal autorizado.	

Fuente: Elaboración propia

Tabla 20 Controles de Política Especifica 3

N°	Políticas Específicas de Seguridad de la Información		Responsable
3	Políticas de seguridad de la información para la promoción, vacaciones, rotación y/o cese del personal.		Sub Gerencia de Recursos Humanos
Dominio	**N°**	**Control**	
Seguridad Personal	**2**	Cuando se adquiera el servicio de un personal, se debe de entregar la política de seguridad de la información, así como las normas y procedimientos para el uso de las aplicaciones y los sistemas de información de la municipalidad.	
	5	Todo empleado que trabaje en la municipalidad deberá comunicar inmediatamente al área de Recursos Humanos los cambios ocurridos en su curriculum vitae.	

Fuente: Elaboración propia

Tabla 21 Controles de Política Especifica 4

N°	Políticas Específicas de Seguridad de la Información		Responsable
4	Cada puesto que desempeñe el personal de la municipalidad debe estar descrito y por ende se debe cumplir con las responsabilidades. La alta directiva debe conocer las responsabilidades del personal que tiene a su supervisión; se debe contar TDR (términos de referencia) el cual cuenta con las descripciones del puesto y responsabilidades que tiene que cumplir.		Gerencias y Sub Gerencias.
Dominio	**N°**	**Control**	
Seguridad Personal	**1**	La seguridad es responsabilidad de todo el personal de la municipalidad, por ende, todos aquellos con acceso a las instalaciones e información deben acatar los estándares documentados en la política de seguridad e incluirla como una de sus responsabilidades principales.	

Fuente: Elaboración propia

Tabla 22 Controles de Política Especifica 5

N°	Políticas Específicas de Seguridad de la Información		Responsable
5	Los empleados pueden utilizar sus propias computadoras, dispositivos periféricos, o software en las instalaciones de la municipalidad siempre y cuando cuenten con la autorización de sub Gerencia o Gerencias a la cual corresponden.		Sub Gerencia de Informática y Tecnologías de la Información.
Dominio	**N°**	**Control**	
Administración de las comunicaciones	**3**	Todos los intentos de conexión, desconexión, cambios de contraseña, fallas en los cambios de contraseña, reinstalación de contraseñas, registro de usuarios y supresión de usuarios, serán registrados.	

Fuente: Elaboración propia

3.2.4. Propuesta del Comité de Seguridad de la Información según ISO 27001

Según el la Oficina Nacional de Gobierno Electrónico e Informática, el Comité de Gestión de Seguridad de la Información es el órgano máximo sobre la seguridad de la información. Deberá tener una reunión durante el mes para poder evaluar la situación de la entidad en temas de seguridad de la información y sobre el plan de acción para mejorarla constantemente.

Las funciones del Comité de Gestión de Seguridad de la Información son las siguientes:

- Informar cómo se encuentra la municipalidad en temas de seguridad de la información.
- Designar a un oficial de seguridad de la información.
- Proponer a los integrantes del Comité Técnico de Seguridad de la información.
- Patrocinar y participar activamente en la implementación y mejora continua del SGSI.

CONCLUSIONES

Se logró proponer un plan de la seguridad de la información basado en la ISO 27001 aplicando la metodología de Evaluación y Análisis de Riesgos, logrando implementar políticas de seguridad para mantener y mejorar la integridad, confidencialidad y disponibilidad de la información de la municipalidad distrital de Punta Hermosa.

Se concluye que al realizar el estudio de investigación se ha identificado para un mejor análisis de los riesgos existentes, clasificando las amenazas, vulnerabilidades y la estimación de los riesgos de acuerdo a los criterios de confidencialidad, disponibilidad e integridad en la municipalidad de Punta Hermosa.

Se concluye que se ha definido las políticas y controles para reducir los riesgos de la confiabilidad e integridad de la información ya que se protege los activos y los intereses de la Municipalidad Distrital de Punta Hermosa.

Por último, se ha analizado y valorado los riesgos, identificando las vulnerabilidades y amenazas que enfrentan los activos de información de la municipalidad de Punta Hermosa.

RECOMENDACIONES

Se recomienda tener en la municipalidad un Plan de Seguridad de la Información basado en la norma ISO 27001.

Además, se recomienda formar un Comité de Seguridad de la Información según la norma ISO 27001, para así tener un mejor control con la información y se pueda evitar posibles riesgos.

Por ende, se recomienda establecer mecanismos que ayuden a identificar nuevos activos de información, y también la cultura organizacional para tomar acciones correctivas frente a nuevas vulnerabilidades, amenazas o riesgos detectados y sobre eso tomar acciones preventivas.

Luego se deben seguir realizando evaluaciones constantes a las políticas de seguridad de la información, con el único fin de mantenerlas actualizadas y ajustadas a las necesidades del área.

Finalmente, se recomienda contar con el apoyo del alcalde ya que es de suma importancia, para implementar a futuro el plan de seguridad de la información en la Sub Gerencia de Informática y Tecnologías de la Información.

BIBLIOGRAFÍA

1. (Alcántara Flores, 2015) Guía de implementación de la seguridad basado en la norma ISO/IEC 27001, para apoyar la seguridad en los sistemas informáticos de la Comisaria del Norte P.N.P en la ciudad de Chiclayo. Tesis de Grado.

2. (Aguirre Mollehuanca, 2014), Diseño de un Sistema de Gestión de Seguridad de Información para Servicios Postales del Perú S.A. Tesis de grado.

3. Briceño A. (2013) Deming y la prevención de riesgos laborales. En Prevencionar.com.
   Disponible en http://prevencionar.com/2013/05/13/deming-y- la-prevención-de-riesgos-laborales.

4. Cordero, K. (2015). Estudio comparativo entre las metodologías MAGERIT y CRAMM, utilizadas para análisis y gestión de riesgos de seguridad de la información (Tesis de Grado, Universidad del Azuay).Recuperado de http://dspace.uazuay.edu.ec/bitstream/datos/5051/1/11490.pdf.

5. Chacón, P. (2012). Propuesta de un modelo de sistema de gestión de seguridad de la información para institutos superiores tecnológicos de educación aeronáutica (Tesis de Maestría, Escuela Politécnica Nacional de Ecuador). Recuperado de http://bibdigital.epn.edu.ec/bitstream/15000 /7807/1/CD-4189.pdf.

6. Deming, E. (1989). Calidad, Productividad y Competitividad: la salida de la crisis. Madrid, España: Ediciones Díaz de Santos.

7. Espinoza, H. (2013). Análisis y diseño de un sistema de gestión de seguridad de información basado en la norma ISO/IEC 27001: 2005 para una empresa de producción y comercialización de productos de consumo masivo. (Tesis de Grado, Pontificia Universidad Católica del Perú). Recuperado de http://tesis.pucp.edu.pe/repositorio/handle/123456789/4957.

8. (Gualsaqui Vivar, 2013) Desarrollo del Marco de Referencia Cobit 5.0 para la Gestión del Área de TI de la Empresa Blue Card. Tesis de Grado para la obtención del Título de Ingeniero en Sistemas. Pontificia Universidad Católica del Ecuador.

9. International Organization of Standardization and International Electrotechnical Commission. ISO 27001:2005. Tecnología de la

información Técnicas de seguridad Sistemas de gestión de seguridad de la información Requerimientos (2005). Primera edición.

10. (ISOTools, 2015) Blog especializado en Sistemas de Gestión de Seguridad de la Información. Disponible en https://www.pmg-ssi.com/2015/10/la-norma-iso-27001-version-2013/.

11. ISO 27001. En ISO27000.es. Consultado el 15 de Marzo de 2019. Disponible en http://www.iso27000.es/.

12. Leyva, R. (2016). Diseño de un Sistema de Gestión de Seguridad de la información basado en las Normas 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.

13. Martelo, R., Madera, J. y Betín, A. (2015). Software para Gestión Documental, un Componente Modular del Sistema de Gestión de Seguridad de la Información (SGSI). *Información tecnológica*, 26(2). Recuperado de http://dx.doi.org/10.4067/S0718-07642015000200015.

14. (Mesquida Calaft, 2012) Un Modelo para facilitar la Integración de Estándares de Gestión de TI en entornos maduros. Tesis de Doctorado

15. (Ministerio de Hacienda y Administraciones Públicas, 2012) MAGERIT – Versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro III- Guía DE Técnicas.

16. (Moyano Orjuela & Suárez Cárdenas, 2017) Plan de Implementación del SGSI basado en la Norma ISO 27001 para la empresa Interfaces y Soluciones. Tesis de Titulación, Facultad Tecnológica, Universidad Distrital Francisco José de Caldas, Bogotá D.C.

17. (Picón Carrascal, 2016) Elaboración de un Plan de Implementación de la ISO 27001.Master Universitario en Seguridad de las Tecnologías de la Información de las Comunicaciones, Instituto Colombiano para la Evaluación de la Educación ICFEES.

18. (Polanco Vélez, 2013) Diseño de un manual de procedimientos del sistema contable en la empresa FEVECOMEX S.A.S basado en la norma técnica colombiana para la seguridad de la información NTC-ISO/IEC 27001/2006. Tesis desde Grado.

19. Project Management Institute. Guía de los fundamentos para la dirección de proyectos (Guía del PMBOK). (2013) Quinta edición.

20. Ramírez, E. & Aguilera, A. (2009). Los delitos informáticos. Tratamiento internacional. Edumet.net: Contribuciones a las Ciencias Sociales. Recuperado de http://www.eumed.net/rev/cccss/04/rbar2.htm.

21. (Tola Franco, 2015) Implementación de un Sistema de Gestión de Seguridad de la Información para una empresa de Consultoría y Auditoría, Aplicando la Norma ISO/IEC 27001. Facultad de Ingeniería en Electricidad y Computación, Escuela Superior Politécnica del Litoral, Guayaquil-Ecuador.

ANEXOS

ANEXO 1: ENCUESTA PARA EL PERSONAL DE LA MUNICIPALIDAD DE PUNTA HERMOSA

N°	PREGUNTAS	RESPUESTA	
		SI	NO
1	¿El computador asignado para el desarrollo de sus funciones recibe mantenimiento periódicamente?		
2	¿Existe un SGSI en la Municipalidad?		
3	¿La Municipalidad capacita al personal en temas de seguridad informática?		
4	¿Existe alguna política para el cambio regular de las contraseñas?		
5	¿Antes ydespués de la contrataciónde l personal se hace entrega de un manual de funciones y responsabilidades de seguridad de la información?		
6	¿Cuándo ocurre un evento relacionado con seguridad de la información sabe a quién reportarlo?		
7	¿Realiza copias de la información?		
8	¿Considera necesario que la Municipalidad invierta en la implementación de un Sistema de Gestión de Seguridad de la Información?		
9	¿Tiene antivirus la computadora asignada?		
10	¿La Municipalidad tiene software legal en su totalidad?		
11	¿Existen zonas restringidas de acceso de personal?		
12	¿Se realiza mantenimiento preventivo y correctivo a la UPS?		
13	¿Existen sistemas de seguridad que impidan el acceso a lugares restringidos?		
14	¿Se cuenta con sistemas de alarma como detectores de humo, humedad?		
15	¿Existe vigilancia en la entrada del edificio?		
16	¿Los sitios donde están los equipos de cómputo cuentan con aire acondicionado?		
17	¿Se encuentra asegurados mediante pólizas los equipos de cómputo?		
18	¿Existe algún control para navegar en internet?		

Anexo 2: Glosario de términos

1. Acción correctiva: medida orientada a eliminar la causa de una no conformidad, con el fin de prevenir su repetición.

2. Acción preventiva: medida orientada a prevenir potenciales no conformidades asociadas a la operación e implementación de un SGSI.

3. Activo: se hace referencia a cualquier información o sistema relacionado que tenga valor para la empresa.

4. Amenaza: causa potencial de un incidente no deseado, el cual puede causar un daño en la empresa.

5. Auditor: persona encargada de verificar, de manera totalmente independiente la calidad del trabajo que se ha realizado en un área particular.

6. Auditoria: es un proceso en el cual un auditor obtiene evidencias objetivas y claras que le permitan emitir un juicio informado sobre el estado y efectividad de un SGSI de una empresa u organización.

7. Confidencialidad: acceso a la información de las personas que estén autorizadas.

8. Control: los riesgos de seguridad de la información debe estar por debajo del nivel de riesgo asumido.

9. Disponibilidad: acceso a la información y a los sistemas de tratamiento de la misma por parte del personal autorizados cuando lo requieran.

10. Evaluación de riesgos: proceso de comparar el riesgo

estimado contra un criterio de riesgo con el objetivo de determinar la importancia del riesgo.

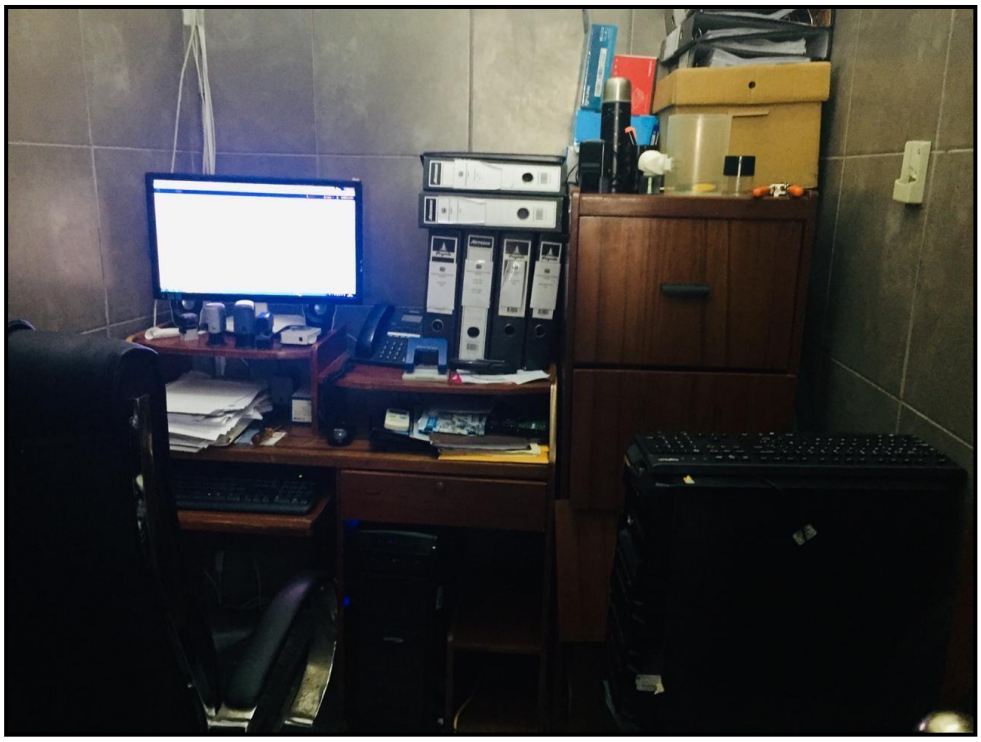
11. Gestión de riesgos: proceso de identificación, control, minimización y eliminación aun coste aceptable. Incluye la valoración de riesgos y el tratamiento.

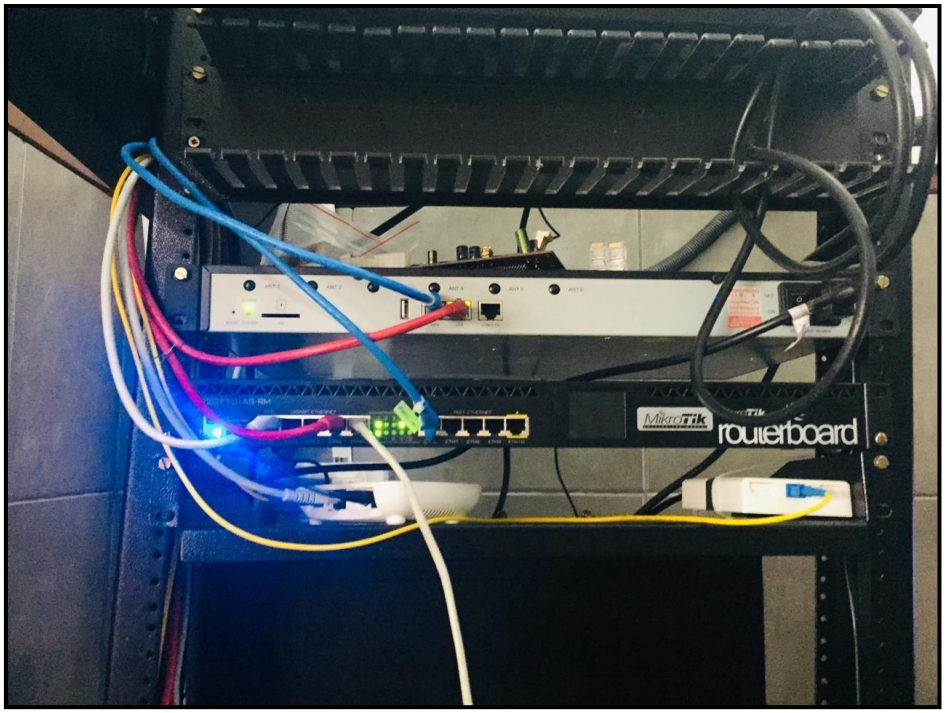
12. Integridad: exactitud de la información.

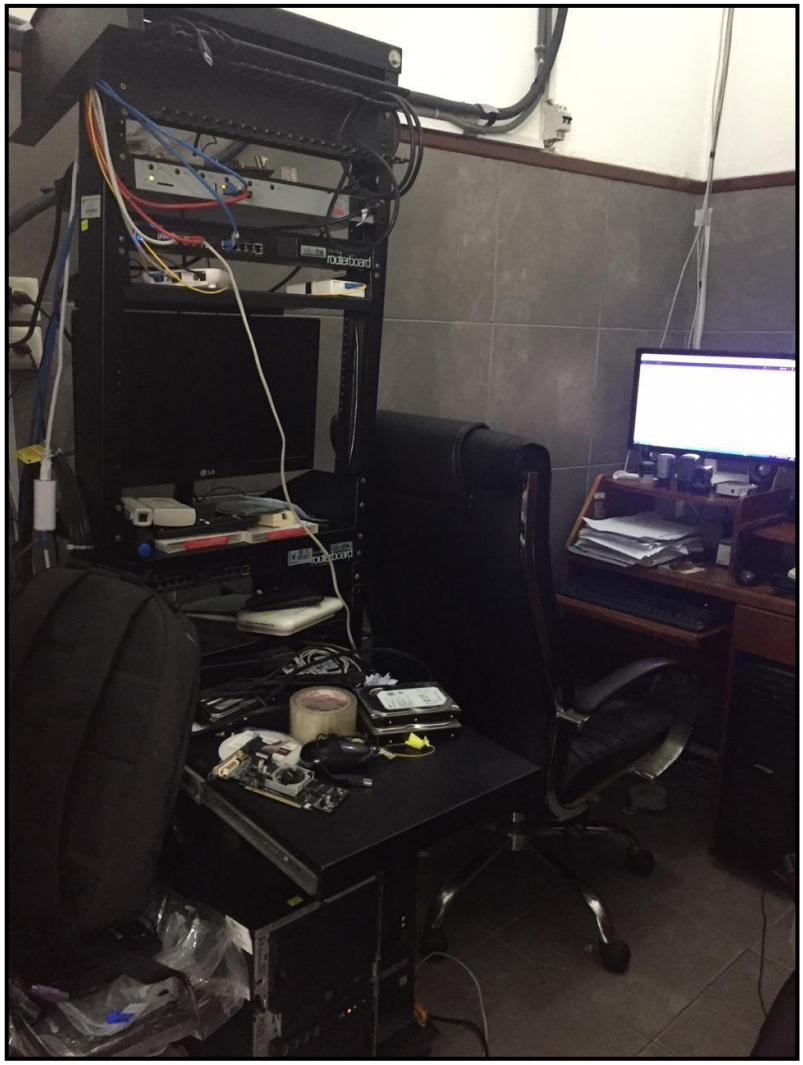
13. Inventario de activos: lista de todos aquellos recursos físicos, software, servicios, documentos, personas, etc. dentro del alcance del SGSI, para que así sean protegidos de potenciales riesgos.

Anexo 3

El ambiente donde se trabaja es el siguiente:

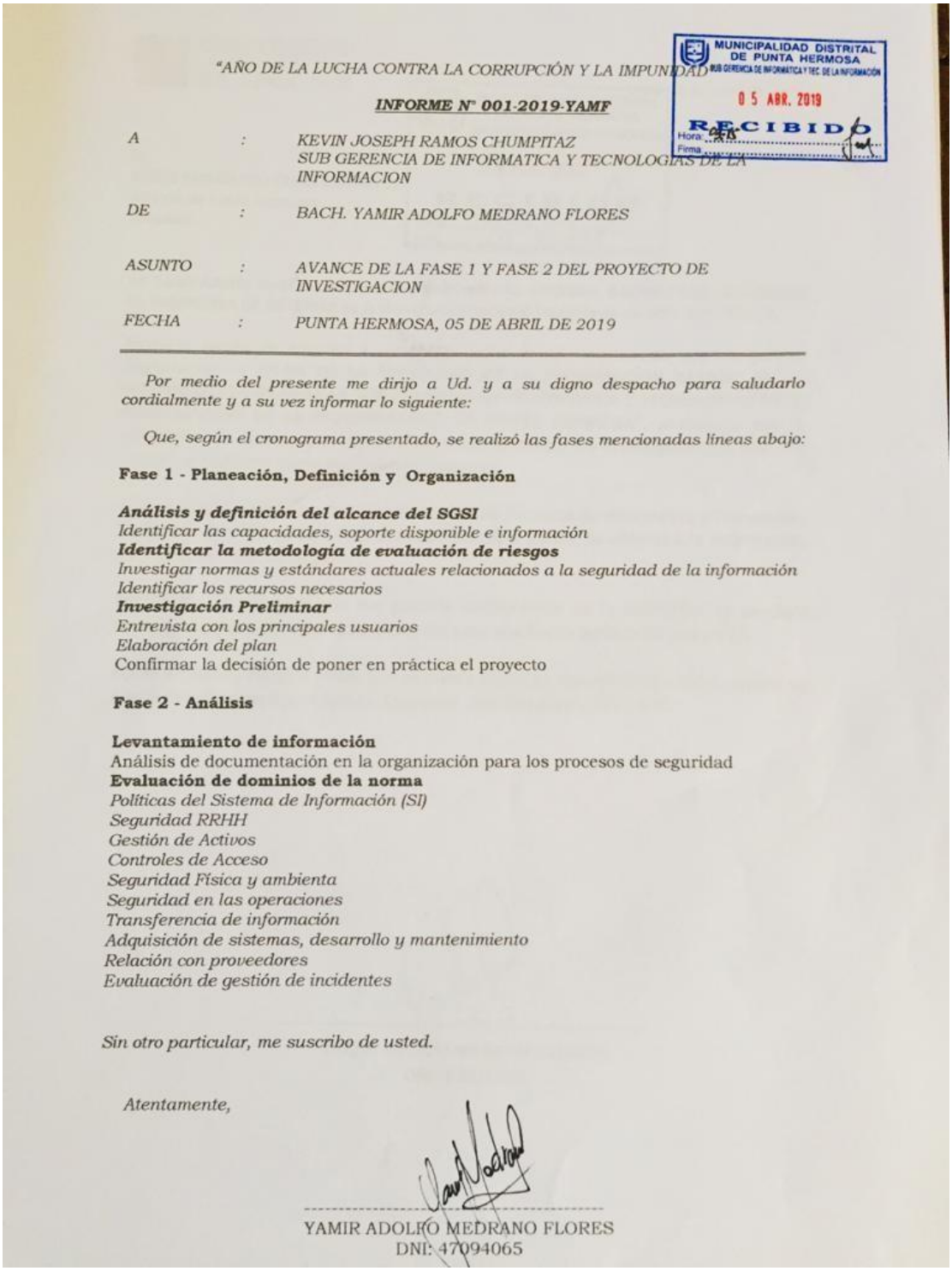



MikroTik
routerboard


routerboard

Anexo 4

Sustento como modo probatorio a mi avance de mi proyecto de investigación.



"AÑO DE LA LUCHA CONTRA LA CORRUPCIÓN Y LA IMPUNIDAD"

MUNICIPALIDAD DISTRITAL DE PUNTA HERMOSA
SUB GERENCIA DE INFORMATICA Y TEC. DE LA INFORMACIÓN
05 ABR. 2019
RECIBIDO
Hora: 04:15
Firma:

INFORME N° 001-2019-YAMF

A : KEVIN JOSEPH RAMOS CHUMPITAZ
SUB GERENCIA DE INFORMATICA Y TECNOLOGIAS DE LA INFORMACION

DE : BACH. YAMIR ADOLFO MEDRANO FLORES

ASUNTO : AVANCE DE LA FASE 1 Y FASE 2 DEL PROYECTO DE INVESTIGACION

FECHA : PUNTA HERMOSA, 05 DE ABRIL DE 2019

Por medio del presente me dirijo a Ud. y a su digno despacho para saludarlo cordialmente y a su vez informar lo siguiente:

Que, según el cronograma presentado, se realizó las fases mencionadas líneas abajo:

Fase 1 - Planeación, Definición y Organización

Análisis y definición del alcance del SGSI
Identificar las capacidades, soporte disponible e información
Identificar la metodología de evaluación de riesgos
Investigar normas y estándares actuales relacionados a la seguridad de la información
Identificar los recursos necesarios
Investigación Preliminar
Entrevista con los principales usuarios
Elaboración del plan
Confirmar la decisión de poner en práctica el proyecto

Fase 2 - Análisis

Levantamiento de información
Análisis de documentación en la organización para los procesos de seguridad
Evaluación de dominios de la norma
Políticas del Sistema de Información (SI)
Seguridad RRHH
Gestión de Activos
Controles de Acceso
Seguridad Física y ambienta
Seguridad en las operaciones
Transferencia de información
Adquisición de sistemas, desarrollo y mantenimiento
Relación con proveedores
Evaluación de gestión de incidentes

Sin otro particular, me suscribo de usted.

Atentamente,

YAMIR ADOLFO MEDRANO FLORES
DNI: 47094065

"AÑO DE LA LUCHA CONTRA LA CORRUPCIÓN Y LA IMPUNIDAD"

INFORME N° 002-2019-YAMF

MUNICIPALIDAD DISTRITAL DE PUNTA HERMOSA
SUB GERENCIA DE INFORMATICA Y TEC. DE LA INFORMACIÓN
24 MAYO 2019
RECIBIDO
Hora: 9:00 pm
Firma:

A	:	*KEVIN JOSEPH RAMOS CHUMPITAZ* *SUB GERENCIA DE INFORMATICA Y TECNOLOGIAS DE LA INFORMACION*
DE	:	*BACH. YAMIR ADOLFO MEDRANO FLORES*
ASUNTO	:	*AVANCE DE LA FASE 3 Y FASE 4 DEL PROYECTO DE INVESTIGACION*
FECHA	:	*PUNTA HERMOSA, 23 DE MAYO DE 2019*

Por medio del presente me dirijo a Ud. y a su digno despacho para saludarlo cordialmente y a su vez informar lo siguiente:

Que, según el cronograma presentado, se realizó las fases mencionadas lineas abajo:

Fase 3 - Gestión

Interpretar y gestionar el riesgo
Identificar y estimar las funciones para proteger la información
Identificar controles de seguridad convenientes
Definición de métricas para determinar la eficacia de los controles
Definición de procedimientos para detectar y gestionar incidentes de seguridad
Documentación del SGSI

Fase 4 – Selección de Salvaguardas y Evaluación

Plan de tratamiento
Identificar mecanismos para protección de información
Selección de mecanismos de protección
Priorizar y evaluar los mecanismos
Integración de resultados
Identificación de oportunidades de mejora
Actualización de los planes de seguridad
Comunicación a los grupos de interés

Sin otro particular, me suscribo de usted.

Atentamente,

YAMIR ADOLFO MEDRANO FLORES
DNI: 47094065

Anexo 5

El presente documento es de modo sustentatorio, para poder regularizar que se viene trabajando de forma coordinada con el Sub Gerente de Sistemas.

UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR

Lima, 04 de Abril de 2019

MUNICIPALIDAD DISTRITAL DE PUNTA HERMOSA
SUB GERENCIA DE GESTION DOCUMENTARIA
04 ABR. 2019
RECIBIDO
Exped.: 2652 Firma:
Folio: 01 12:13

Sr.
JORGE HUMBERTO OLAECHEA REYES
Alcalde de Punta Hermosa
Presente.-

Yo, **Yamir Adolfo Medrano Flores** identificado con DNI: 47094065, **BACHILLER DE LA CARRERA DE INGENIERIA DE SISTEMAS** de la Universidad Nacional Tecnológica de Lima Sur (UNTELS).

Tengo el agrado de dirigirme a usted para poner en su conocimiento que me gustaría implementar un "**PLAN DE LA SEGURIDAD DE LA INFORMACÍON BASADO EN LA NORMA ISO 27001 PARA LA SUB GERENCIA DE INFORMATICA Y TECNOLOGIAS DE LA INFORMACION DE LA MUNICIPALIDAD DE PUNTA HERMOSA",** analizando que la institución no cuenta con dicho plan; como proyecto de investigación el cual me permitirá titularme como Ingeniero de Sistemas.

El presente proyecto será coordinado con la Sub Gerencia de Informática y Tecnologias de la Información, ya que será el medio principal donde se obtendrá la información para implementar dicho plan.

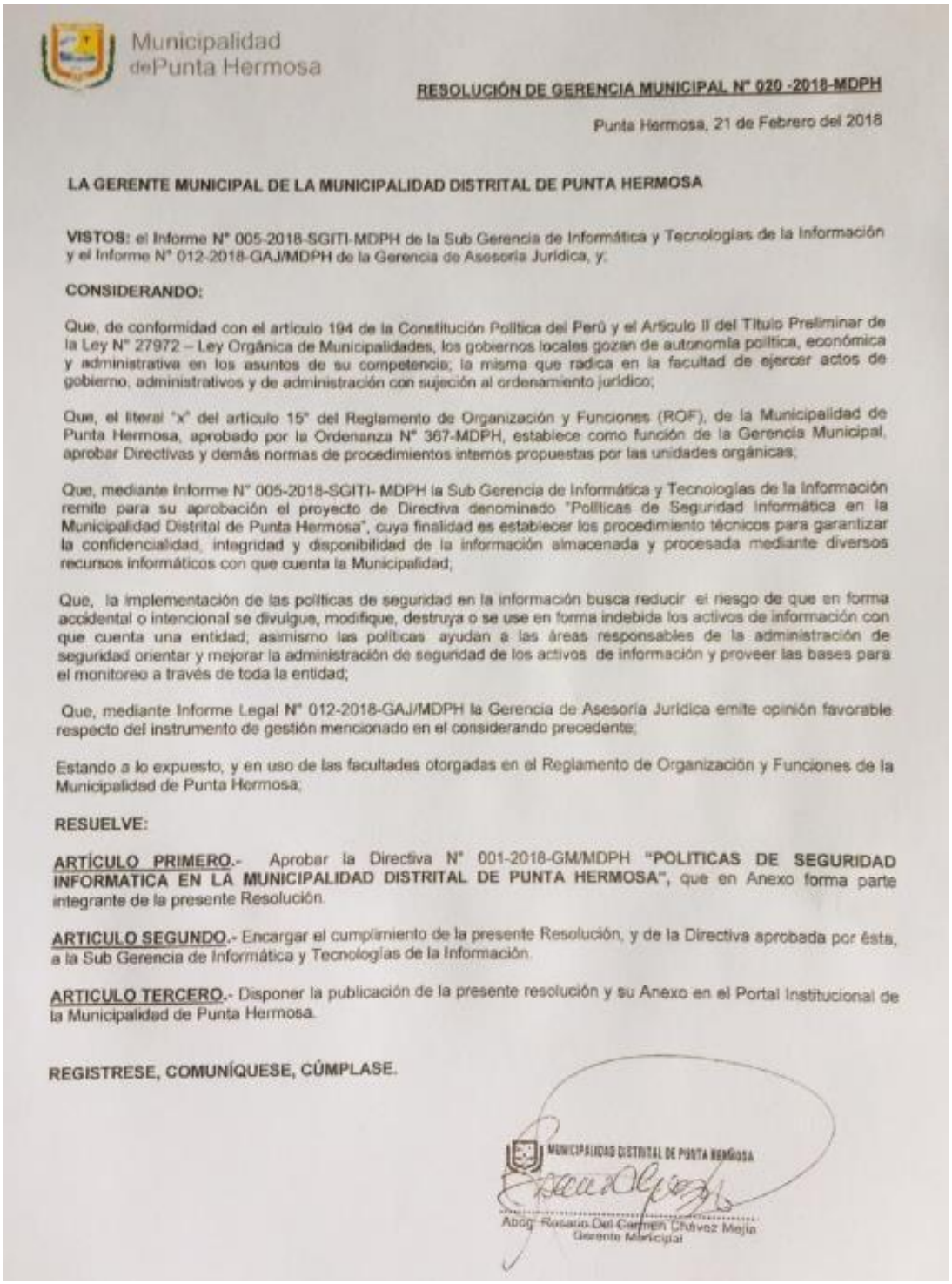
Por último, el proyecto que me gustaría implementar en la institución se quedará como documentación a ejecutar y cumplir para una buena gestión de Seguridad.

Por lo expuesto, ruego a usted, que se pueda tomar en consideración dicho pedido, ya que el beneficio será para ambos. Cualquier consulta al cel.: 991719457.

YAMIR ADOLFO MEDRANO FLORES
DNI: 47094065

Anexo 6

Resolución de Gerencia Municipal N° 020-2018-MDPH
Directiva N° 001-2018 MDPH
Política de Seguridad Informática en la Municipalidad Distrital de Punta Hermosa



Municipalidad
dePunta Hermosa

RESOLUCIÓN DE GERENCIA MUNICIPAL N° 020 -2018-MDPH

Punta Hermosa, 21 de Febrero del 2018

LA GERENTE MUNICIPAL DE LA MUNICIPALIDAD DISTRITAL DE PUNTA HERMOSA

VISTOS: el Informe N° 005-2018-SGITI-MDPH de la Sub Gerencia de Informática y Tecnologías de la Información y el Informe N° 012-2018-GAJ/MDPH de la Gerencia de Asesoría Jurídica, y;

CONSIDERANDO:

Que, de conformidad con el artículo 194 de la Constitución Política del Perú y el Artículo II del Título Preliminar de la Ley N° 27972 – Ley Orgánica de Municipalidades, los gobiernos locales gozan de autonomía política, económica y administrativa en los asuntos de su competencia; la misma que radica en la facultad de ejercer actos de gobierno, administrativos y de administración con sujeción al ordenamiento jurídico;

Que, el literal "x" del artículo 15° del Reglamento de Organización y Funciones (ROF), de la Municipalidad de Punta Hermosa, aprobado por la Ordenanza N° 367-MDPH, establece como función de la Gerencia Municipal, aprobar Directivas y demás normas de procedimientos internos propuestas por las unidades orgánicas;

Que, mediante Informe N° 005-2018-SGITI- MDPH la Sub Gerencia de Informática y Tecnologías de la Información remite para su aprobación el proyecto de Directiva denominado "Políticas de Seguridad Informática en la Municipalidad Distrital de Punta Hermosa", cuya finalidad es establecer los procedimiento técnicos para garantizar la confidencialidad, integridad y disponibilidad de la información almacenada y procesada mediante diversos recursos informáticos con que cuenta la Municipalidad;

Que, la implementación de las políticas de seguridad en la información busca reducir el riesgo de que en forma accidental o intencional se divulgue, modifique, destruya o se use en forma indebida los activos de información con que cuenta una entidad; asimismo las políticas ayudan a las áreas responsables de la administración de seguridad orientar y mejorar la administración de seguridad de los activos de información y proveer las bases para el monitoreo a través de toda la entidad;

Que, mediante Informe Legal N° 012-2018-GAJ/MDPH la Gerencia de Asesoría Jurídica emite opinión favorable respecto del instrumento de gestión mencionado en el considerando precedente;

Estando a lo expuesto, y en uso de las facultades otorgadas en el Reglamento de Organización y Funciones de la Municipalidad de Punta Hermosa;

RESUELVE:

ARTÍCULO PRIMERO.- Aprobar la Directiva N° 001-2018-GM/MDPH **"POLITICAS DE SEGURIDAD INFORMATICA EN LA MUNICIPALIDAD DISTRITAL DE PUNTA HERMOSA"**, que en Anexo forma parte integrante de la presente Resolución.

ARTICULO SEGUNDO.- Encargar el cumplimiento de la presente Resolución, y de la Directiva aprobada por ésta, a la Sub Gerencia de Informática y Tecnologías de la Información.

ARTICULO TERCERO.- Disponer la publicación de la presente resolución y su Anexo en el Portal Institucional de la Municipalidad de Punta Hermosa.

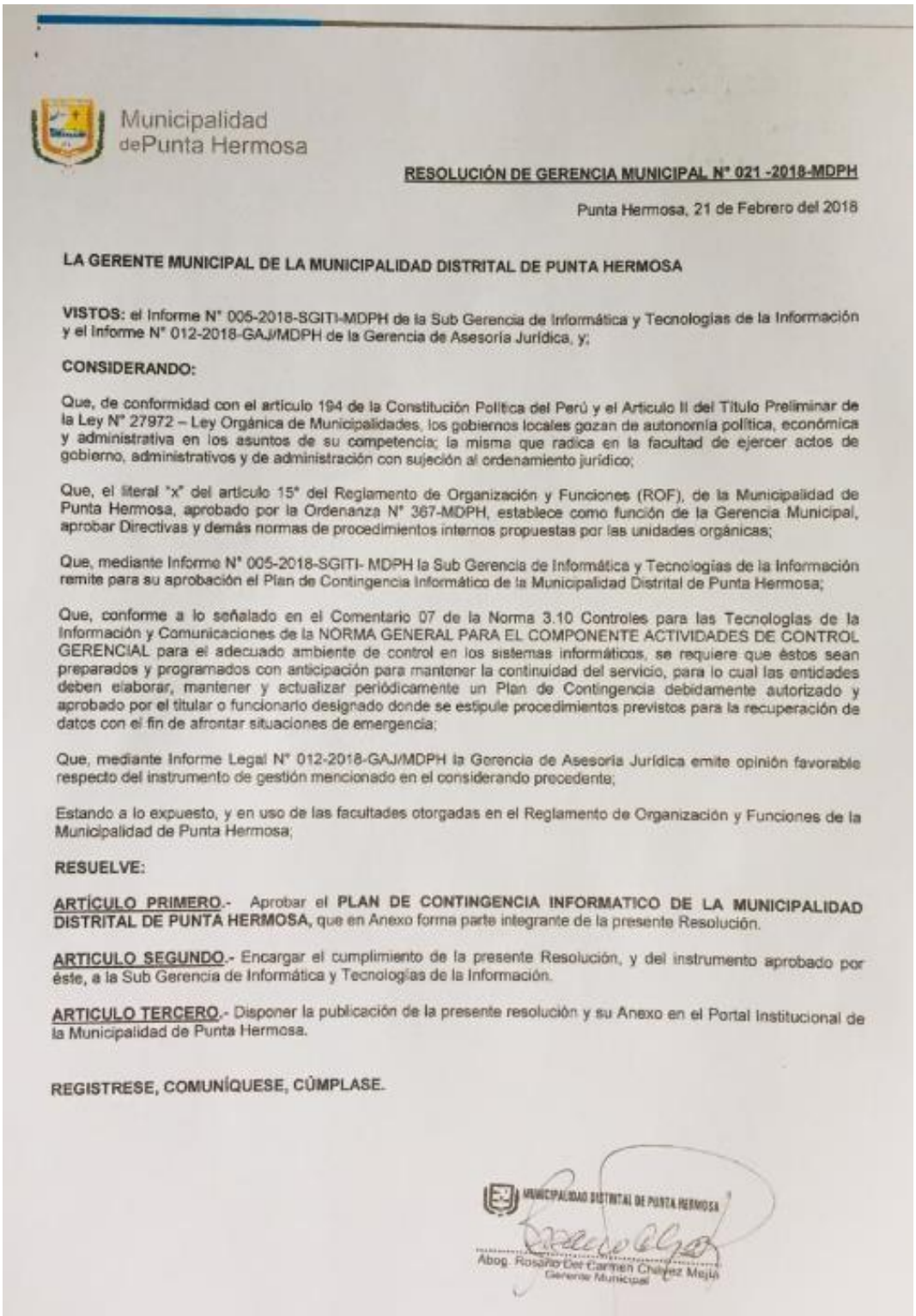
REGISTRESE, COMUNÍQUESE, CÚMPLASE.

MUNICIPALIDAD DISTRITAL DE PUNTA HERMOSA

Abog. Rosario Del Carmen Chávez Mejía
Gerente Municipal

Anexo 7

Resolución de Gerencia Municipal 021-2018-MDPH
Plan de Contingencia Informático



Municipalidad
dePunta Hermosa

RESOLUCIÓN DE GERENCIA MUNICIPAL N° 021 -2018-MDPH

Punta Hermosa, 21 de Febrero del 2018

LA GERENTE MUNICIPAL DE LA MUNICIPALIDAD DISTRITAL DE PUNTA HERMOSA

VISTOS: el Informe N° 005-2018-SGITI-MDPH de la Sub Gerencia de Informática y Tecnologías de la Información y el Informe N° 012-2018-GAJ/MDPH de la Gerencia de Asesoría Jurídica, y;

CONSIDERANDO:

Que, de conformidad con el artículo 194 de la Constitución Política del Perú y el Artículo II del Título Preliminar de la Ley N° 27972 – Ley Orgánica de Municipalidades, los gobiernos locales gozan de autonomía política, económica y administrativa en los asuntos de su competencia; la misma que radica en la facultad de ejercer actos de gobierno, administrativos y de administración con sujeción al ordenamiento jurídico;

Que, el literal "x" del artículo 15° del Reglamento de Organización y Funciones (ROF), de la Municipalidad de Punta Hermosa, aprobado por la Ordenanza N° 367-MDPH, establece como función de la Gerencia Municipal, aprobar Directivas y demás normas de procedimientos internos propuestas por las unidades orgánicas;

Que, mediante Informe N° 005-2018-SGITI- MDPH la Sub Gerencia de Informática y Tecnologías de la Información remite para su aprobación el Plan de Contingencia Informático de la Municipalidad Distrital de Punta Hermosa;

Que, conforme a lo señalado en el Comentario 07 de la Norma 3.10 Controles para las Tecnologías de la Información y Comunicaciones de la NORMA GENERAL PARA EL COMPONENTE ACTIVIDADES DE CONTROL GERENCIAL para el adecuado ambiente de control en los sistemas informáticos, se requiere que éstos sean preparados y programados con anticipación para mantener la continuidad del servicio, para lo cual las entidades deben elaborar, mantener y actualizar periódicamente un Plan de Contingencia debidamente autorizado y aprobado por el titular o funcionario designado donde se estipule procedimientos previstos para la recuperación de datos con el fin de afrontar situaciones de emergencia;

Que, mediante Informe Legal N° 012-2018-GAJ/MDPH la Gerencia de Asesoría Jurídica emite opinión favorable respecto del instrumento de gestión mencionado en el considerando precedente;

Estando a lo expuesto, y en uso de las facultades otorgadas en el Reglamento de Organización y Funciones de la Municipalidad de Punta Hermosa;

RESUELVE:

ARTÍCULO PRIMERO.- Aprobar el **PLAN DE CONTINGENCIA INFORMATICO DE LA MUNICIPALIDAD DISTRITAL DE PUNTA HERMOSA,** que en Anexo forma parte integrante de la presente Resolución.

ARTICULO SEGUNDO.- Encargar el cumplimiento de la presente Resolución, y del instrumento aprobado por éste, a la Sub Gerencia de Informática y Tecnologías de la Información.

ARTICULO TERCERO.- Disponer la publicación de la presente resolución y su Anexo en el Portal Institucional de la Municipalidad de Punta Hermosa.

REGISTRESE, COMUNÍQUESE, CÚMPLASE.

MUNICIPALIDAD DISTRITAL DE PUNTA HERMOSA
Abog. Rosario Del Carmen Chávez Mejía
Gerente Municipal