UNIVERSIDAD ANDINA DEL CUSCO

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

TESIS

"DISEÑO DEL PLAN DE SEGURIDAD INFORMATICA BASADO EN LA NTP ISO/IEC 27001:2014 PARA LA MUNICIPALIDAD DEL CENTRO POBLADO DE SALCEDO - PUNO"

PRESENTADO POR:

BR. ABDON ANDERS CAMAPAZA QUISPE

PARA OPTAR AL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS

ASESOR:

ING. LUIS ALBERTO SOTA ORELLANA

CUSCO – PERÚ

2019

Dedicatoria

A mis padres Abdón y Leonor por su apoyo, comprensión, amor, motivación para poder conseguir cada una de mis metas, por inculcarme valores para ser una mejor persona y sobre todo porque son el pilar fundamental en mi vida.

A mis hermanas Mirella y Ariana por toda la confianza y el amor que me brindan, el cual mayor fuente de inspiración para seguir adelante.

A mi novia y futura esposa Melissa por todo el amor, cariño, compresión y apoyo para poder cumplir mis metas y sobre todo por ser parte de mi vida .

Agradecimientos

En primer lugar, quiero agradecer a Dios por permitir tener y disfrutar de mi hermosa familia, por derramar sus bendiciones, por estar en los momentos de difíciles y felices de mi vida, por nunca abandonarme cuando más te necesitaba.

A mi familia por darme el apoyo incondicional para poder culminar esta etapa de mi vida, ya que sin ellos no lo hubiera podido lograr y concluir.

A mi asesor Ingeniero Luis Alberto Sota Orellana por el apoyo y asesoramiento en todo el proceso de desarrollo de mi tesis.

A los Ingenieros Adriel Ramirez y Carlos Zambrano por su tiempo y conocimientos para poder corregir y concluir mi tesis.

A mis amigos y compañeros por su apoyo en cada etapa de mi vida, ya que aprendí muchas cosas las cuales me sirven en mi desarrollo personal y profesional .

Índice General

Índice de Figuras

Índice de Tablas

Introducción

Actualmente la continuidad del negocio se basa en la información, que es considerada como el mayor activo que poseen las empresas, por tal motivo requieren una protección adecuada ante cualquier evento que puede causar daños en los datos. Esta importancia que tiene hoy en día la información, ha hecho que las organizacionales internacionales de estandarización elaboren normativas y estándares que permiten el resguardo y buen uso de la información y de los activos en general.

Con la finalidad de resguardar la confidencialidad, integridad y disponibilidad gestión de la información, es necesario establecer una adecuada gestión de la seguridad de la información. En el Perú se exige a las entidades públicas integrantes del sistema nacional de informática la implementación de la Norma Técnica Peruana NTP ISO/IEC 27001:2014 (Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información); Sin embargo, la falta de conocimiento de la alta dirección, así como la falta de presupuesto y falta de personal especializado ha ocasionado que no se cumplan con el cronograma establecido por el gobierno para su implementación.

El presente diseño del plan de seguridad informática basado en la norma NTP ISO/IEC 27001:2014, se realizará para la Municipalidad del Centro Poblado de Salcedo Puno, con el propósito de aplicar las mejores prácticas en la gestión de la seguridad de la información, priorizando los procesos críticos de la Municipalidad del Centro Poblado de Salcedo Puno.

Se desarrollará un Plan de Seguridad Informática basado en la NTP ISO/IEC 27001:2014, en el cual inicialmente se realizará un diagnostico situacional de la Municipalidad del Centro Poblado de Salcedo Puno para poder identificar las debilidades y amenazas en temas de seguridad de la información. Luego se preparará el plan de seguridad informática con el propósito de definir el alcance del plan, identificar los requisitos legales, elaborar políticas de seguridad y proponer un plan de seguridad informática evaluando los riegos de seguridad informática para elaborar los controles respectivos que permitan mitigarlos .

Resumen

En el Perú toda organización publica está obligado a implementar Planes de Seguridad Informática o Sistemas de Gestión de la Seguridad de la Información, que permita preservar las dimensiones de confidencialidad, integridad y disponibilidad de la información, basada en la de la Norma Técnica Peruana NTP ISO/IEC 27001:2014, pero por diversos motivos causas y circunstancias esto no sucede, aduciendo la falta de presupuesto, la falta de conocimiento, la falta de personal capacitado para implementar, consultores en seguridad muy caros, etc. Motivo por el algún organismo del estado no cumplen con la implementación de su Plan de Seguridad Informática.

Es el caso de la Municipalidad del Centro Poblado de Salcedo Puno, que por falta de conocimiento no tenía en sus planes a corto ni a mediano plazo el diseño, menos la implementación de un Plan de Seguridad Informática, lo que motivo el presente trabajo de investigación. El objetivo de este trabajo es desarrollar un Plan de Seguridad Informática basado en la NTP ISO/IEC 27001:2014, en el cual inicialmente se realizará un diagnostico situacional de la Municipalidad del Centro Poblado de Salcedo Puno para poder identificar las debilidades y amenazas en temas de seguridad de la información. Luego se preparará el plan de seguridad informática con el propósito de definir el alcance del plan, identificar los requisitos legales, elaborar políticas de seguridad y proponer un plan a la Oficina de Administración y Finanzas de la Municipalidad del Centro Poblado de Salcedo Puno. Por último, se terminará el plan de seguridad informática evaluando los riegos de seguridad informática para elaborar los controles respectivos que permitan mitigarlos.

Abstract

In Peru, every public organization is obliged to implement Information Security Plans or Information Security Management Systems, which allow the preservation of the dimensions of confidentiality, integrity and availability of information, based on that of the Peruvian Technical Standard NTP ISO / IEC 27001: 2014, but for various reasons causes and circumstances this does not happen, citing lack of budget, lack of knowledge, lack of trained personnel to implement, very expensive security consultants, etc. Reason by the state agency does not comply with the implementation of its Computer Security Plan.

This is the case of the Municipality of the Salcedo-Puno Town Center, which, due to lack of knowledge, did not have the design in its short-term or medium-term plans, less the implementation of an Information Security Plan, which motivated the present work of investigation. The objective of this work is to develop a Computer Security Plan based on the NTP ISO / IEC 27001: 2014, in which initially a situational diagnosis will be made of the Municipality of the Salcedo Town Center to identify weaknesses and threats in matters of security of the information. The computer security plan will then be prepared with the purpose of defining the scope of the plan, identifying legal requirements, developing security policies and proposing a plan to the Office of Administration and Finance of the Municipality. Finally, the computer security plan will be completed by evaluating the computer security risks to develop the respective controls that allow mitigating them

Capítulo 1 - Problema de investigación

1.1. Ámbito de influencia

1.1.1. Ámbito de influencia teórica.

El ámbito de influencia teórica del presente proyecto de tesis, está enfocada a temas relacionados a las Tecnologías de Comunicación y la Seguridad Informática basados en la norma NTP ISO/IEC 27001:2014.

1.1.2. Área de dominio.

El Área o dominio de conocimiento, está centrada específicamente al área de Tecnologías de Comunicación, ya que se trata de ver los temas relacionados a la seguridad informática, teniendo como objetivo disminuir los posibles riesgos, mediante procedimientos establecidos sistemáticamente.

1.1.3. Línea de investigación.

La línea de investigación del presente proyecto de tesis está relacionada con la Seguridad en tecnologías de información y comunicación, ya que se tocarán temas relacionados a esta línea de investigación como: Seguridad Informática, Sistema de Gestión de la Seguridad de la Información y la NTP ISO/IEC 27001:2014.

1.2. Planteamiento del problema

1.2.1. Descripción de la situación actual del lugar de intervención.

En la actualidad la parte operativa de toda organización pública o privada tiene obligatoriamente una dependencia directa con el nivel tecnológico que esta tenga. Gracias a la informática los procesos y el manejo de la información se han automatizado y sistematizado, generando muchos beneficios económicos y utilidades a las empresas, pues en la actualidad sin el uso de las mismas no se puede realizar ningún proceso o mantener un negocio, incluso la informática ha traspasado límites al integrarse al Internet, pues los procesos se vuelven más dinámicos; sin embargo, por la falta de políticas de seguridad, los procedimientos de seguridad en muchas ocasiones no se toman en cuenta.

En el Perú, desde el año 2004 la Secretaría de Gobierno Digital (SeGDi) por ser ente rector del Sistema Nacional de Informática, ha ido publicando normas relacionadas a la seguridad de la información a través de publicaciones en el Diario Oficial "El Peruano" y a través de su página Web.

Publicaron normas como: NTP ISO/IEC 17799:2004, NTP ISO/IEC 17799:2007, NTP ISO/IEC 27001:2008 y la NTP ISO/IEC 27001:2014 (que reemplaza a la NTP ISO/IEC 27001:2008), que mediante la implementación de un sistema de gestión de seguridad de la información ayudan a las entidades del estado a resguardar y proteger su información sensible y confidencial.

Todo ello sumado a que mediante la Norma Técnica Peruana (NTP) ISO/IEC 27001:2014 aprobada mediante la Resolución Ministerial Nº 004-2016-PCM el 8 de enero de 2016, se obliga actualmente las entidades públicas a diseñar e implementar un sistema de gestión de seguridad de la información (SGSI).

1.3. Descripción del problema

Conforme a un análisis preliminar de la situación actual de la infraestructura de comunicaciones y servicios de la Municipalidad del Centro Poblado de Salcedo Puno, se ha podido identificar algunas dificultades operativas, resultado de un cierto nivel de inseguridad de la información, cabe mencionar que muchas por no decir todas las operaciones municipales son apoyadas por las tecnologías de información y comunicaciones y entre las dificultades encontradas están:

- Debido a accesos indebidos a los recursos compartidos de la red se han alterado la información, razón por la cual muchas veces se ha dejado de atender a los usuarios.
- La conectividad a Internet, que hoy en día es inevitable, hace que se tenga accesos externos, los mismos que en muchas ocasiones no pueden o no han podido ser controlados adecuadamente, ocasionando pérdida de información por software maliciosos o accesos indebidos.
- Sus redes inalámbricas no poseen clave de acceso, por lo que cualquier persona que esté en el área de cobertura de sus Access Point, pueden tener acceso a Internet y con ello se puede generar los inconvenientes mencionados anteriormente.
- La falta de conocimiento muchas veces hace que los usuarios internos no tengan una cultura de seguridad informática en el desempeño de sus funciones, además, difícilmente se tiene cuentas de usuario y claves de acceso en los equipos y muchas veces no están

activos los protectores de pantalla con clave, lo cual genera una posibilidad de que el equipo pueda ser mal utilizado y se pueda acceder fácilmente a la información que contiene.

- La falta de infraestructura básica de seguridad como redes perimetrales (DMZ), y firewall en el Municipio del Centro Poblado de Salcedo está generando enormes vulnerabilidades en su red.

Se ha podido observar también, que los funcionarios del órgano de informática de la Municipalidad del Centro Poblado de Salcedo Puno desconocen de la existencia de estas normas, y no han establecido lineamientos de seguridad de la información conforme a los estándares, que les ayude en la prevención y en la recuperación ante desastres o ataques (internos y externos) que pudieran afectar a la información que manejan.

Se hace necesario conocer las amenazas a las que se enfrenta y los activos en riesgo de la Municipalidad del Centro Poblado de Salcedo Puno para poder afrontarlas. Para ello se debe diseñar un Plan de Seguridad Informática, que permita implementar adecuadamente algunos controles de seguridad basándose en la evaluación de riesgos.

Contextualizada la situación actual, se presenta como trabajo de tesis el diseño de un Plan de Seguridad Informática basado en la Norma Técnica Peruana vigente del sector, que permita cubrir todos los requerimientos de seguridad en los procesos del negocio de la Municipalidad del Centro Poblado de Salcedo Puno. Asimismo, el documento que resulte de esta investigación deberá servir como un marco de referencia en su implementación.

1.3.1. Formulación interrogativa del problema general.

¿Cómo disminuir los elevados niveles de riesgo de seguridad informática, que se generan en los diferentes procesos de negocio de la Municipalidad del Centro Poblado de Salcedo Puno?

1.3.2. Formulación interrogativa de los problemas específicos.

- ¿Cuál es el alcance del diseño del Plan de Seguridad Informática para la Municipalidad del Centro Poblado de Salcedo Puno?
- ¿Cuáles son los resultados del análisis de riesgos de la seguridad informática para la Municipalidad del Centro Poblado de Salcedo Puno?

- ¿Qué controles de seguridad son aplicables en el plan de seguridad informática para la Municipalidad del Centro Poblado de Salcedo Puno?

1.4. Objetivos

1.4.1. Objetivo general.

Diseñar un plan de seguridad informática basado en la NTP-ISO/IEC 27001:2014, para que en base a su aplicación se logre la disminución de los niveles de riesgo de seguridad informática en los procesos de negocios de la Municipalidad del Centro Poblado de Salcedo Puno .

1.4.2. Objetivos específicos.

- Analizar las áreas funcionales y definir el alcance del diseño del plan de seguridad para la Municipalidad del Centro Poblado de Salcedo Puno.
- Realizar la evaluación de riesgos de la seguridad informática para la Municipalidad del Centro Poblado de Salcedo Puno.
- Elaborar la lista de controles de seguridad para mitigar los riesgos identificados en el diseño del plan de seguridad informática para la Municipalidad del Centro Poblado de Salcedo Puno .

1.5. Justificación

Considero que es deber de las instituciones públicas o privadas de hoy en día, invertir en el aseguramiento de su información y considerar a ésta, como uno de los activos más importante de una organizacion.

En ese sentido, la NTP-ISO/IEC 27001:2014 sirve como modelo o guia para el establecimiento, implementación, mejora y seguimiento de un sistema de gestión de seguridad de la información en cualquier tipo de organización.

El presente trabajo de investigación se origina a partir de la necesidad creada por la Secretaría de Gobierno Digital (SeGDi), al declarar el uso obligatorio de la NTP-ISO/IEC 27001:2014, en las entidades que pertenecen al sistema nacional de informática con la finalidad de coadyuvar con la implementación del gobierno electrónico en nuestro País, ya que se considera a la seguridad de la información, como un componente crucial para dicho objetivo propuesto.

Con este proyecto se quiere que la Municipalidad del Centro Poblado de Salcedo Puno de un primer paso en la implantación de un Plan de Seguridad Informática basado en la NTP ISO/IEC 27001:2014.

1.6. Alcances y limitaciones

La presente investigación se realizará en el Área de Informática y Elaboración de Datos de la Oficina de Administración y Finanzas de la Municipalidad del Centro Poblado de Salcedo Puno. A razón de que dicha área que es la responsable de formular, proponer y ejecutar lineamientos para el desarrollo y aplicación de procedimientos, políticas, prácticas y funciones que aseguren los niveles adecuados de integridad, confidencialidad y disponibilidad de los sistemas de información, los datos y de las comunicaciones en la Municipalidad del Centro Poblado de Salcedo Puno .

Capítulo 2 – Marco teórico de la Tesis

2.1. Antecedentes del desarrollo, implementación o transferencia tecnológica

2.1.1. Antecedentes regionales.

(Ariasca Suma & Quispe Borda, 2017), en la Ciudad de Cusco (Perú), en su tesis "Desarrollo de una Propuesta de Implementación de la NTPISO/IEC 27001:2014, Sistema de Gestión de Seguridad de la Información, para la Oficina Funcional de Informática del Gobierno Regional del Cusco", concluyeron que la aplicación de la NTP ISO/IEC 27001:2014, permite definir los procesos y actividades requeridos para el diseño y planificación del Sistema de Gestión de Seguridad de la Información, así como identificar los activos de información críticos, los riegos asociados a estos, los propietarios de cada riesgo y así definir los controles de seguridad requeridos para garantizar un nivel de seguridad adecuado para la elaboración del Plan de Tratamiento de Riesgos y así lograr desarrollar y documentar los procesos, procedimientos y actividades del diseño y planificación del Sistema de Gestión de Seguridad de la Información en cumplimiento respecto a la documentación requerida por la norma

2.1.2. Antecedentes nacionales.

(Justino Salinas, 2015), en la Ciudad de Lima (Perú), en su tesis "Diseño de un sistema de gestión de seguridad de información para una empresa inmobiliaria alineado a la NORMA ISO/IEC 27001:2013, concluyó que el papel de la alta dirección es muy importante en el SGSI, porque además de tomar las decisiones estratégicas en la organización, el nivel de compromiso que tenga será fundamental para llevar a cabo el SGSI y mucho más importante para la implementación de los controles. Menciona también la importancia de establecer políticas de seguridad de la información que contengan los lineamientos para una administración eficiente de la información con el fin de garantizar la seguridad de los sistemas y mantener la integridad de la información, de la infraestructura de procesamiento, así como minimizar el impacto de vulnerabilidades e incidentes de seguridad, asimismo considera importante establecer algunos roles y responsabilidades que ayuden a garantizar el cumplimiento de las políticas y el monitoreo de los riesgos a los que se encuentra expuesta la información

(Ccesa Quincho, 2017), en la Ciudad de Huamanga (Perú) en sus tesis "Diseño De Un Sistema De Gestión De Seguridad De La Información Bajo La NTP ISO/IEC 27001:2014

Para La Municipalidad Provincial De Huamanga, concluyo que el análisis y gestión de riesgos es la columna vertebral de un sistema de gestión de seguridad de la información, porque permite cuantificar el riesgo ya que es un indicador estadístico que mide la incertidumbre. La evaluación de riesgos permitió identificar y valorar los activos, identificar y valorar las amenazas, calcular el impacto e identificar los riesgos a los que se encuentra expuestos las organizaciones para luego elaborar controles de seguridad para mitigar los riesgos permitiendo establecer métricas que ayuden a medir la eficacia y eficiencia de un sistema de gestión de seguridad de la información .

(Quispe Barreto, 2018), en la Ciudad de Ancash (Perú), en su tesis "Declaración de aplicabilidad mediante la NTP ISO/IEC 27001:2014 para mitigar los siniestros de la información en la sub dirección de licencias de conducir de la Dirección Regional de Transporte y Comunicación de Ancash, concluyo que las organizaciones tanto externas como internas deben tratar de hacer lo más llevadero posible las tareas operativas del sistema SGSI, en beneficio de las partes interesadas, para lo cual necesitan la ayuda de herramientas tecnológicas que automaticen ciertas tareas y así mitigar los siniestros de información mediante el contexto de la organización por lo que la NTP-ISO/IEC 27001:2014 indica que el contexto de la organización, lo Primero son los aspectos externos e internos referidos a comprender la organización y su contexto, segundo los requisitos referidos a comprender las necesidades y expectativas de las partes interesadas y por último identificar las interfaces y dependencias entre actividades realizadas por la organización y las que son realizadas por otras organizaciones .

2.1.3. Antecedentes internacionales.

(Guzmán Silva, 2015), en la Ciudad de Bogotá (Colombia),en su trabajo de investigación "Diseño de un sistema de gestión de seguridad de la información para una entidad financiera de segundo piso, concluyó que el diseño de un sistema de gestión de seguridad de la información basado en un modelo de mejoras prácticas y lineamientos de seguridad, como es la norma ISO/IEC 27001:2013, es una herramienta útil que permite identificar los diferentes factores que se deben tener en cuenta cuando las organizaciones deciden establecer un modelo de seguridad de la información, puesto que si las organizaciones logran cumplir al pie de la letra lo establecido en la norma ISO/IEC 27001:2013, pueden llegar a forjar en el tiempo un adecuado y sostenible SGSI, aunque dicha labor depende del tamaño y naturaleza de la organizacion y de la cultura de la misma en relacion a la seguridad de la información. Por otro

lado, menciona que es indispensable contar con el apoyo del alta dirección, para poder concebir un modelo de seguridad de la información que realmente refleje la misión y visión de la organización; y es fundamental contar con este apoyo antes de comenzar a diseñar un SGSI, ya que, si esto no se logra conseguir, es casi seguro que cualquier iniciativa de seguridad no alcancen los resultados que se esperan .

(Sandoval Vargas, 2014), en la Ciudad de Guayaquil (Ecuador), en su tesis "Análisis de la norma ISO/IEC 27001. Diseño de Implementación en la red de una empresa, concluyó que: la implementación de un SGSI basado en la norma ISO/IEC 27001 garantiza la ejecución de un conjunto de procesos que gestionen la accesibilidad de la información en la organización, asimismo señala que realizar esta implementación siguiendo las cuatro fases fundamentales del Ciclo de Deming (Planificar, Hacer Verificar y Actuar), nos permite desarrollar una metodología de trabajo clara y estructurada, y que la revisión periódica de los controles seleccionados e implementados reduce los riesgos de pérdida, robo o corrupción de la información en la organización .

(Suárez Padilla, 2013), en la Ciudad de Guayaquil (Ecuador), en su tesis "Estudio de la seguridad de la información aplicado a Recursos Humanos, Adquisiciones y Cómputo para empresas del Sector Pesquero, concluyó que la importancia que posee el área de seguridad en las tecnologías de información, radica en que las empresas están en la obligación, incluso de aspecto legal, mantener las mejores prácticas ofrecidas en las Normas Internacionales, estipuladas en la ISO 27000, ISO 27001, cuyos estándares permitirán, después de su correcta implementación y puesta en marcha de controles minuciosos y continuos, que la empresa u organización desarrolladora obtenga un agregado de confianza y solidez .

2.2. Bases teórico - científicas

2.2.1. Información.

Es un activo con valor para la organización, que requiere una protección adecuada frente a la constante exposición a distintas amenazas y vulnerabilidades. La información acoge múltiples formas. Puede estar impresa o escrita en papel, almacenada en repositorios electrónicos, transmitida a través de las redes y por servicios de mensajería, mostrada en video o hablada en conversación. Sea cual sea la forma que tome la información, o medio en

que se almacene o comparta, siempre tiene que estar apropiadamente protegida (INDECOPI, 2014) .

Según (Chiavenato, 2006) Son un conjunto de datos con significado, esto quiere decir que reduce la incertidumbre o que aumenta el conocimiento de algo. En verdad, la información es un mensaje con significado en un determinado contexto, que está disponible para un uso inmediato y que proporciona orientación a las acciones por el hecho de reducir el margen de incertidumbre en nuestras decisiones .

2.2.2. Seguridad.

Según (Peso Navarro & Remos Gonzalez, 2004) Debe entenderse como el proceso de resguardo de los activos frente a ejercicios o escenarios perjudiciales y no deseados, mediante la implementación de políticas, acciones y controles, emanadas por normativas correspondientes, lo que supone un incremento en los presupuestos de las organizaciones. Todo ello se lleva a cabo en las entidades con el objetivo de proteger los intereses de los accionistas, de los empleados, de los clientes, de los proveedores y de los ciudadanos afectados según el sector .

2.2.3. Seguridad de la información.

Para (INDECOPI, 2014), la seguridad de la información es el resguardo de las dimensiones de confidencialidad, integridad y disponibilidad de la información; es decir, que la información solo esté dispuesta y accesible para el personal correcto y autorizado, la información también debe ser integra y correcta sin alteraciones de ninguna naturaleza y que esté disponible a los usuarios cuando lo requieran. Así también puede involucrar otras propiedades como la autenticidad, no repudio y confiabilidad .

Podría entenderse por seguridad de la información a todas aquellas medidas reactivas y preventivas del hombre, de las organizaciones y de los sistemas tecnológicos que permitan resguardar y proteger la información con la finalidad de mantener la confidencialidad, la autenticidad e Integridad de la misma. Marcando diferencia entre el concepto de seguridad de la información con el de seguridad informática, en el que la seguridad informática sólo se encarga de la seguridad en el medio informático (Fitzgerald, 2007).

2.2.3.1. Principios básicos de la seguridad de la información.

De acuerdo a Mendillo, los principios básicos de la seguridad de la información, son: (Mendillo, 2009)

Confidencialidad. Mediante la cual se refiere a que la información no sea vista, leída o escuchada por parte de personas extrañas o no autorizadas por la organización.

Integridad. Esta referida a que los datos enviados lleguen correctamente, es decir que no se hayan dañado por errores de transmisión o interferencia y que no hayan sido dañados o alterados intencionalmente.

Disponibilidad. Esta referido a que la información y los recursos informáticos no sean negados a los usuarios autorizados cuando requieran su uso y que se pueda restablecer prontamente y eficiente el servicio en caso de fallas .

2.2.4. Seguridad informática.

2.2.4.1. Sistema de gestión de la seguridad de la información.

Mediante el sistema de gestión de seguridad de la información se produce la implementación de un conjunto de procesos que permiten, implementar, mantener y mejorar de manera continua la seguridad de la información, sobre la base de los riesgos a los que se enfrenta la organización. Así mismo mencionan que la implementación de un SGSI supone el establecimiento de procesos formales y una clara definición de responsabilidades en base a una serie de políticas, planes y procedimientos que deberán constar como información documentada (Gómez Fernández & Fernández Rivero , 2015)

Es fundamental que el sistema de gestión de la seguridad de la información este integrado con los procesos de la organización y la estructura de gestión general y que la seguridad de la información se considere en el diseño de procesos, sistemas y controles de la información. Se espera que la implementación de un sistema de gestión de seguridad de la información crezca en relación con las necesidades de la organización o empresa (INDECOPI, 2014).

2.2.5. Política de seguridad.

La política de seguridad es la información documentada en la que se reflejan, en términos generales, los objetivos y metas de la organización y las principales líneas de acción que permiten proteger la información frente a pérdidas de confidencialidad, integridad y disponibilidad. La definición de esta política debe tener en cuenta los requisitos del negocio,

contractuales, legales y estatutarios, los cuales quedarán reflejados en la misma. Asimismo, este documento debe ser comunicado a todas las partes interesadas del SGSI (Gómez Fernández & Fernández Rivero , 2015).

(Peltier, Peltier, & Blackley, 2005) considera a la política de seguridad de información como la piedra angular de una efectiva arquitectura de seguridad de la información, ya que de ella nacen otros documentos importantes tales como directivas, estándares, procedimientos y guías y nos mencionan que estas cumplen con 2 roles importantes, un rol interno y otro externo .

Rol Interno: pues se menciona a cada uno de los miembros de la organización, qué se espera que realicen y cómo se evaluará el trabajo realizado (Peltier, Peltier, & Blackley, 2005).

Rol Externo: sirve para mostrarle al mundo externo como es que se trabaja dentro de la organización, que somos conscientes de la necesidad de proteger nuestra información y la de los clientes y que estamos trabajando para realizarlo (Peltier, Peltier, & Blackley, 2005).

2.2.6. Riesgo

El riesgo es cualquier ocurrencia o suceso que de llegar a ocurrir amenazaria los objetivos y metas de una organización, todo riesgo tiene una posibilidad de ocurrencia por lo que se miden como la multiplicidad del impacto por probabilidad

(Halvorson, 2008) explica tres naturalezas del riesgo, estos son: los riesgos estratégicos, tácticos y operacionales:

- Los riesgos estratégicos están relacionados directamente con la seguridad de la información; sin embargo, las orientaciones de estos riesgos están en las ganancias y reputación de la organización, ya que se derivan de decisiones estratégicas que han sido tomadas o serán tomadas en la organización.
- Los riesgos tácticos están relacionados a los sistemas de control y monitoreo de los riesgos que afectan a la información, son aquellos que afectan indirectamente a la información.
- Los riesgos operacionales son los relacionados a aquellos activos que pueden afectar los objetivos de una empresa (tales como presupuestos, cronogramas y tecnologías) .

(MARGERIT, 2012) Señala que el riesgo se debe definir como la estimación del grado o nivel de exposición de que una amenaza se produzca sobre uno o más activos causando daños

o perjuicios a la organización. Es decir, lo que le podría pasar a los activos si no se protegieran adecuadamente. Es importante saber qué características son de interés en cada activo, así como saber en qué medida cada una de estas características están en peligro, es decir, analizar el sistema para poder protegerlo adecuadamente .

2.2.7. Análisis y evaluación de riesgos

Se puede decir que el análisis de riesgos es "un proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una Organización (MARGERIT, 2012). En ese sentido, sabiendo lo que podría pasar, se deben de tomar decisiones para tratar y prevenir estos riesgos.

El análisis y gestión de riesgos de los sistemas de información es la parte fundamental de las actuaciones relacionadas con el análisis, la evaluación y la gestión del riesgo. En ese sentido, siguiendo una metodología de gestión de riesgos se puede analizar los riesgos, identificar las amenazas y su impacto, y gestionar el riesgo basado en:

a) Elementos (activos, amenazas, vulnerabilidades, riesgos, impactos, salvaguardas).
b) Eventos (estáticos, dinámicos organizativos, dinámicos físicos)
c) Procesos (planificación, análisis de riesgos, gestión de riesgos, selección de salvaguardas) (MARGERIT, 2012).

2.2.8. Control.

Son aquellos medios para manejar el riesgo; entre ellos están: las políticas, los procedimientos, los lineamientos, las prácticas o estructuras organizacionales, las cuales pueden ser administrativas, técnicas, de gestión o de naturaleza legal. El control también puede ser definido como sinónimo de salvaguarda o contramedida (MARGERIT, 2012).

Una clasificación generalizada de los controles puede ser:

- Preventivos: Ya que reducen las vulnerabilidades.
- Detectivos: En vista de que descubren amenazas o escenarios previos a ellas permitiendo activar otros controles necesarios.
- Correctivos: Corrigen o contrarrestan el impacto de la ocurrencia de una amenaza.
- Disuasivos: Reducen la probabilidad de ocurrencia de las amenazas.

2.2.9. Normas de seguridad de la información.

2.2.9.1. Serie de Normas ISO/IEC 27000

La Seguridad de la Información tiene asignada la serie 27000 dentro de los estándares ISO/IEC, siendo un conjunto de estándares desarrollados por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission) y que proporcionan un marco de gestión de la seguridad de la información que puede ser utilizado por cualquier tipo de organización, ya sea pública o privada, grande o pequeña. Las distintas normas que componen la serie ISO 27000 son:

ISO/IEC 27000: Contiene términos y definiciones empleados en toda la serie 27000.

ISO/IEC 27001: Sistemas de Gestión de la Seguridad de la Información (SGSI). Es el estándar principal de la familia, especifica los requisitos necesarios para establecer, emplementar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información. Es certificable.

ISO/IEC 27002: (antes ISO17799). Guía de mejores prácticas que describe los objetivos de control y controles aconsejables en cuanto a seguridad de la información con 14 dominios, 35 objetivos de control y 114 controles. Otorga recomendaciones de las mejores prácticas en la prevención de la confidencialidad, integridad y disponibilidad. Para ello, la norma se estructura en dominios que cubren la gestión de la seguridad de la información.

ISO/IEC 27003: Es una guía que se centra en los aspectos críticos indispensables para el diseño e implementación con éxito de un SGSI de acuerdo con la ISO/IEC 27001. Describe el proceso de especificación y diseño desde la concepción hasta la puesta en marcha de planes de implementación, así como el proceso de obtención de aprobación por la dirección para implementar un SGSI

ISO/IEC 27004: Es una guía para el desarrollo y utilización de métricas y técnicas de medida que pueden ser aplicadas para determinar la eficacia de un SGSI y de los controles o grupos de controles implementados según ISO/IEC 27001

ISO 27005: Proporciona directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC 27001:2013 y está diseñada para ayudar a la aplicación eficiente de la seguridad de la información basada en un enfoque de gestión de riesgos

ISO 27006: Especifica los requisitos para acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información (SGSI).

ISO/IEC 27007: Provee una guía para conducir una auditoria de un SGSI, así como las competencias necesarias de los auditores de sistemas de gestión de seguridad complementando la ISO/IEC 19011.

ISO/IEC TR 27008: Es un reporte técnico que brinda una guía para la revisión de la implementación de los controles del SGSI.

ISO/IEC 27010: Provee una guía para gestionar la seguridad de la información en caso la organización intercambie o comparta información importante, ya sea que pertenezca al sector público o privado, que lo haga nacional o internacionalmente, o en el mismo sector u otros sectores del mercado en el que opera.

ISO/IEC 27011: Provee una guía para apoyar la implementación de un SGSI en una empresa de telecomunicaciones.

ISO/IEC 27013: Brinda una guía para la implementación integrada del ISO/IEC 27001 y el ISO/IEC 20000 (gestión de servicios de TI), que pueden ser implementados al mismo tiempo o uno después de otro.

ISO/IEC 27014: Brinda una guía para conocer los principios y procesos del gobierno de la seguridad de la información, que busca que las organizaciones puedan evaluar, dirigir y monitorear la gestión de la seguridad de la información.

ISO/IEC TR 27015: Sirve como complemento a las normas de la familia ISO/IEC 27000 para la implementación, mantenimiento y mejora del SGSI en empresas que provean servicios financieros.

ISO/IEC TR 27016: Es un reporte técnico que brinda una metodología que permite a las organizaciones saber cómo valorar de manera correcta los activos de información identificados, los riesgos potenciales a los activos, apreciar el valor de los controles que protegen a estos activos y determinar el nivel óptimo de recursos que deben ser usados para asegurarlos.

ISO/IEC 27799:2008: Brinda una guía para apoyar la implementación de un SGSI en las empresas de salud con la adaptación del ISO/IEC 27002 según los requerimientos de este sector (ISO 27000, s.f.)

2.2.9.2. Norma técnica peruana NTP-ISO/IEC 27001:2014

"Es una adaptación de la ISO/IEC 27001. La Presidencia del Consejo de Ministros a través de la Oficina Nacional de Gobierno Electrónico, hoy en día Secretaría de Gobierno Digital (SeGDi), dispone el uso obligatorio de la Norma Técnica Peruana "NTP–ISO/IEC

27001:2014 EDI, Tecnología de la Información. Técnicas de seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos (ISO 27000, s.f.)

En esencia esta Norma Técnica Peruana ha sido pensada y elaborada para facilitar los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información (SGSI). Asimismo, la adopción de un SGSI es una decisión estratégica para una organización. El establecimiento e implementación de un SGSI de la organización está directamente vinculada por las necesidades y objetivos de la organización, los requisitos de seguridad, los procesos organizativos utilizados y el tamaño y estructura de la organización (INDECOPI, 2014).

Estructura de la NTP-ISO/IEC 27001:2014

La norma ISO 27001:2013 (en el Perú NTP-ISO/IEC 27001:2014) no sólo establece cambios en el contenido (respecto a la ISO 2001:2005) sino también en la estructura, lo que verá reflejado en otros documentos que forman parte de la familia ISO 27000. La norma ISO 27001:2013 ha sido desarrollada con base al Anexo SL, en la que se proporciona un formato y un conjunto de lineamientos que siguen el desarrollo documental de un sistema de gestión sin tomar en cuenta el enfoque empresarial, se seleccionan bajo la misma estructura todos los documentos que se relacionan con el sistema de gestión de seguridad de la información y así se evitan problemas de integración con otros marcos de referencia (Excellence, 2015)

La estructura de la norma queda así:

1. Introducción.
2. Objeto y campo de aplicación.
3. Referencias Normativas.
4. Términos y definiciones.
5. Contexto de la organización.
6. Liderazgo.
7. Planificación.
8. Soporte.
9. Operación.
10. Evaluación.
11. Mejora.
12. Lista de controles .

Cuando una organización quiere cumplir los requisitos de la NTP-ISO/IEC 27001, debe demostrar la efectiva implantación de los apartados 4 al 10, que son los que conforman el cuerpo principal de la norma. Asimismo, el SGSI debe contar con información documentada en varios niveles (ver Figura 1):

- Las políticas son las que proporcionan las líneas generales de actuación en cada caso.
- La información documentada sobre procesos (generalmente denominadas procedimientos), que proporcionan todas las actividades a ejecutar.
- La información documentada sobre evidencias (anteriormente denominados registros), que permite acreditar que se han llevado las actividades previstas (Gómez Fernández & Fernández Rivero , 2015).

Figura 1. Niveles de Información Documentada
Fuente: Cómo implementar un SGSI según UNE-ISO/IEC 27001:2014 y su aplicación en el Esquema Nacional de Seguridad, p. 18, (Gómez Fernández & Fernández Rivero , 2015)

1. Contexto de la organización. En este punto es importante conocer la organización y su contexto, de manera que el Plan de Seguridad tenga en cuenta los propios objetivos del negocio de la organización con los que deberá alinearse el PSI. Este conocimiento implica comprender tanto los aspectos internos y externos de la organización, así como las necesidades y expectativas de las partes interesadas.

Se trata de identificar aquellos procesos sobre los que el SGSI va a actuar, no siendo necesario aplicarlo sobre toda la actividad de la organización. Asimismo, a la hora de definir el alcance se deben tener en cuenta los recursos de los que se dispone, siendo generalmente más práctico limitarlo a aquellos procesos o servicios más importantes para la organización, y en posteriores ciclos de mejora continua, ir incorporando el resto (Gómez et al., 2015). Cabe mencionar que el alcance debe estar disponible como información documentada.

2. Liderazgo. El proceso de implementación de un SGSI sería imposible de lograr sin la implicación constante de la dirección. Entre otras cosas, la dirección deberá demostrar su compromiso, aportando los recursos necesarios (tanto económicos como humanos), estableciendo la política y objetivos de seguridad de la información acorde a los objetivos estratégicos de la organización, comunicando la importancia de gestionar efectivamente la seguridad de la información, promoviendo la mejora continua, entre otras actividades (Gómez Fernández & Fernández Rivero , 2015).

Asimismo, también se contempla el establecimiento de roles, responsabilidades y autoridades organizacionales para asegurar que el SGSI esté conforme a los requisitos de la NTP ISO 27001:2014 y reportar sobre el desempeño del mismo a la alta dirección.

3. Planificación. Teniendo en cuenta el contexto de la organización y las necesidades y expectativas de las partes interesadas, la organización debe establecer acciones para tratar los riesgos y oportunidades; para esto se debe definir y aplicar un proceso de valoración de riesgos de seguridad de la información que:

- Determine cuales son los criterios de aceptación de riesgo y la metodología para llevar a cabo la evaluación del riesgo.
- Identifique cuales son los riesgos de seguridad de la información, asociados a la pérdida de confidencialidad, integridad y disponibilidad de la información. La identificación de riesgos debe ser lo más exhaustiva posible para poder ser evaluado y tratado, además se debe de identificar también al propietario del riesgo, que deberá aprobar los niveles de riesgo y los planes de tratamiento.
- Analice los riesgos, valorando las consecuencias y probabilidades de materialización de los riesgos identificados en la fase anterior, obteniendo de este modo los niveles de riesgo.
- Evalúe cuales los riesgos de seguridad de la información. Comparando los resultados obtenidos en la anterior fase con los criterios de aceptación de riesgos para determinar las medidas de tratamiento y su prioridad (Gómez Fernández & Fernández Rivero , 2015)

En este apartado también se debe elaborar un documento denominado Declaración de Aplicabilidad, que contenga los controles necesarios y la justificación de su implementación o exclusión en comparación a los controles definidos. Además, se debe formular un plan de

tratamiento de riesgos de seguridad de la información, que debe ser aprobado por los propietarios del riesgo.

Otro punto a tener en cuenta es el establecimiento de los objetivos de seguridad de información, los cuales deben ser consistente con la política de seguridad de la información, ser medibles (si es práctico), ser comunicados y actualizados.

4. Soporte. En este requisito la NTP-ISO/IEC 27001 la norma contempla:

- La gestión de recursos, que sirve para el establecimiento, implementación, mantenimiento y mejora del SGSI.
- La competencia, ya que la organización debe determinar y asegurar la competencia necesaria de todo el personal implicado en el SGSI.
- La concientización de todo del personal que trabaja en la organización y demás partes interesadas.
- La comunicación, que debe incluir: qué es, cuándo, quién y a quién se debe comunicar y los procesos por los que debe efectuarse la comunicación.
- La información documentada. "Establece el proceso de documentar, mantener, controlar y conservar toda la documentación que corresponde al Sistema de Gestión de Seguridad de la Información (Excellence, 2015).

5. Operación. señala todos los requisitos para medir el funcionamiento del PSI. Es así que, tras obtener la aprobación, por parte de la dirección, del plan de tratamiento de riesgos y de los procesos definidos en las fases anteriores, es el momento de ponerlos en práctica.

Esta aprobación implica la provisión de los recursos necesarios para llevarlos a cabo y que deberían haberse identificado en el plan de tratamiento de riesgos.

Debe hacerse un seguimiento de las acciones previstas, ajustando aquellos aspectos que se detecten como necesarios y actualizando en su caso los planes de tratamientos de riesgos, procedimientos, etc., siempre bajo la supervisión del responsable de seguridad (Gómez Fernández & Fernández Rivero , 2015).

6. Evaluación. Consiste en el monitoreo, medición, análisis y evaluación, del desempeño de la seguridad de la información y la efectividad del SGSI. Las auditorías internas y externas constituyen la base para poder realizar la identificación y la medición de la eficiencia y el desempeño que realiza el PSI.

Se debe de considerar el estado en el que se encuentran los planes de acción para poder atender las no conformidades como es debido, además se debe establecer la necesidad de definir quién y cuándo realiza las evaluaciones, además de quien tiene que analizar la información que se ha recolectado (Excellence, 2015).

7. ***Mejora.*** Los principales elementos de mejora son las no conformidades identificadas, las cuales deben de contabilizarse y compararse con las accione correctivas para asegurarse de que no se repitan y que las acciones correctoras que se realicen sean realmente efectivas. Es decir, la organización debe mejorar continuamente su SGSI (Excellence, 2015).

2.2.10. Ciclo de mejora continua.

La versión 2014 de la norma ISO 27001 no considera el ciclo PDCA (Plan-Do-Check-Act) como marco obligatorio para la gestión de la mejora continua del SGSI, pero en su apartado 10.2 la norma ISO 27001:2014 menciona que la organización debe mejorar continuamente la conveniencia, adecuación y efectividad del PSI. Es decir, el ciclo PDCA está implícito en la propia estructura de la norma y es importante conocerla.

- Según (Gómez et al., 2015) El modelo PDCA consta de un conjunto de fases o etapas, que permiten establecer un modelo comparable a lo largo del tiempo, de manera que se pueda medir el grado de mejora alcanzado:
- Plan. En esta etapa se da la planificación de la implantación de SGSI. Es decir, se determina el contexto de la organización, se definen los objetivos y las políticas que permitirán alcanzarlos.
- Do. En esta etapa se implementa y pone en funcionamiento el SGSI. Y se ponen en práctica las políticas y los controles que, de acuerdo al análisis de riesgos, se han seleccionado para cumplirlas. Para ello debe de disponer de procedimientos en los que se identifique quién debe hacer qué tareas, asegurando que se realice una capacitación necesaria para ello.
- Check. En esta fase se realiza el monitoreo y revisión del SGSI. Se controla que los procesos se ejecuten de la manera prevista y que además permiten alcanzar los objetivos de la manera más eficiente.
- Act. En esta fase se mantiene y mejora el SGSI, definiendo y ejecutando las acciones correctivas necesarias para rectificar los fallos detectados en la anterior etapa (Gómez et al., 2015).

En la figura 2 se muestra la alineación del modelo PDCA en la ISO 27001:2013.

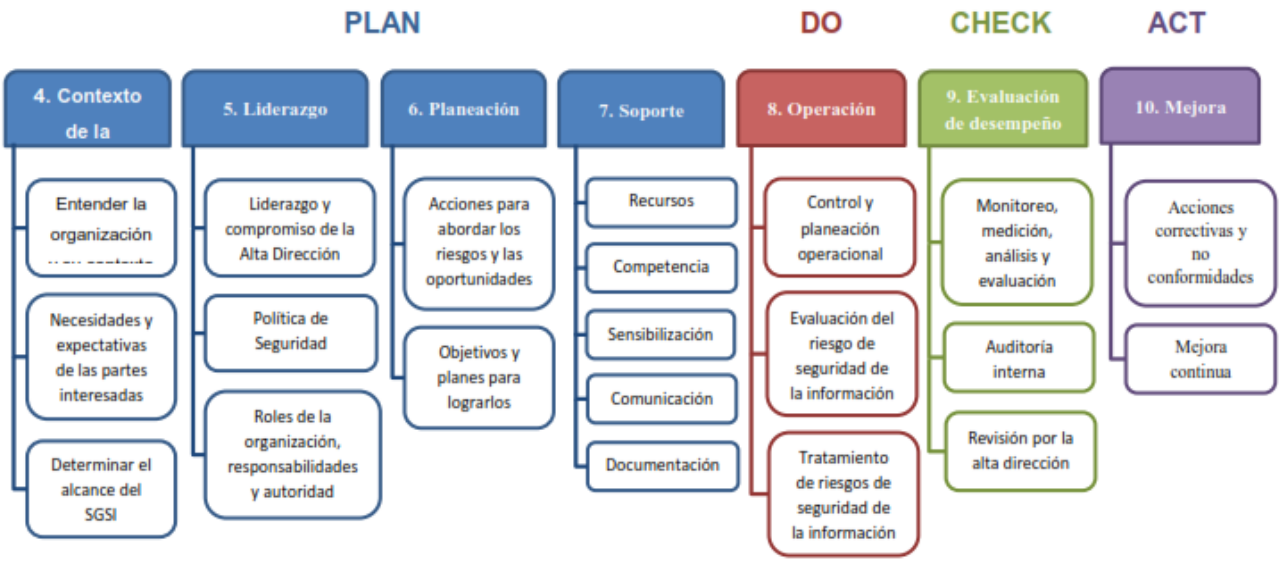

Figura 2. Ciclo PDCA en ISO/IEC 27001:2014

Fuente: ONGEI, taller de transición de la norma ISO/IEC 27001:2005 a la ISO/IEC 27001:2013

2.2.11. Metodologías de análisis y gestión de riesgos de la información.

Existen muchas metodologías de análisis y gestión de riesgos de la información, en el presente trabajo se describe dos de estas, por ser las más utilizadas.

2.2.11.1. Margerit V.3

MAGERIT es la metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica de España, que estima que la gestión de los riesgos es una piedra angular en las guías de buen gobierno (Portal de Administración Electrónica, 2016).

En ese sentido, siguiendo la terminología de la normativa ISO 31000, MAGERIT responde a lo que se denomina “Proceso de Gestión de los Riesgos”, sección 4.4 (“Implementación de la Gestión de los Riesgos”) dentro del “Marco de Gestión de Riesgos”. En otras palabras, MAGERIT permite implementar el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones siempre teniendo en cuenta los riesgos derivados del uso de tecnologías de la información. MAGERIT persigue los siguientes objetivos (MARGERIT, 2012):

Directos:

- Formar conciencia en los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos.
- Permite ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC).
- Permite ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos en control (MARGERIT, 2012).

Indirectos:

- Permite preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso (MARGERIT, 2012)

MARGERIT divide la gestión de riesgos en dos subprocesos, estos son:

1. **Análisis de riesgos:**

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

- Determinar cuáles son los activos relevantes para la organización, su interrelación y su valor, en el sentido de qué perjuicio (coste) supondría su degradación.
- Determinar las amenazas a las que están expuestos aquellos activos.
- Determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo.
- Estimar cual es el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza.
- Estimar el riesgo, definido como el impacto por probabilidad (MARGERIT, 2012).

La Figura 3 recoge los elementos del análisis de riesgos contemplados en MARGERIT.

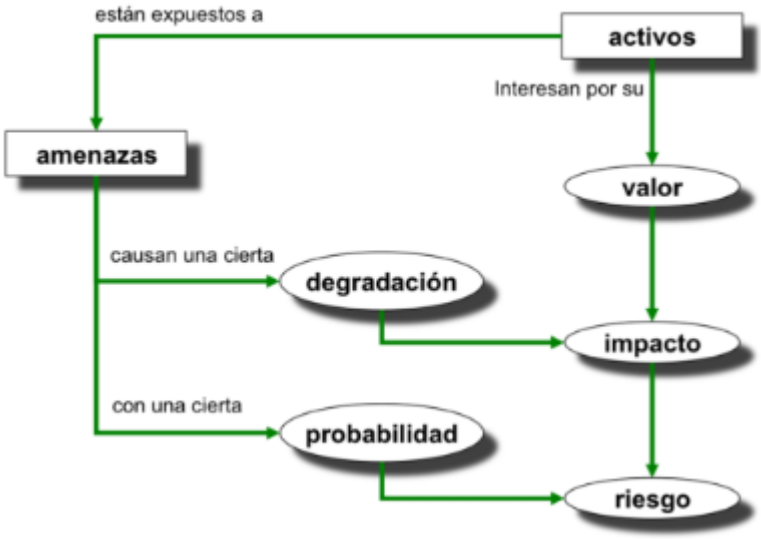

Figura 3. Elementos del análisis de riesgos potenciales
Fuente: MARGERIT V.3 – Libro I, p.22

En la Figura 4 se muestran las tareas propuestas por MARGERIT para llevar a cabo el análisis de los riesgos.

MAR – Método de Análisis de Riesgos
MAR.1 – Caracterización de los activos
MAR.11 – Identificación de los activos
MAR.12 – Dependencias entre activos
MAR.13 – Valoración de los activos
MAR.2 – Caracterización de las amenazas
MAR.21 – Identificación de las amenazas
MAR.22 – Valoración de las amenazas
MAR.3 – Caracterización de las salvaguardas
MAR.31 – Identificación de las salvaguardas pertinentes
MAR.32 – Valoración de las salvaguardas
MAR.4 – Estimación del estado de riesgo
MAR.41 – Estimación del impacto
MAR.42 – Estimación del riesgo

Figura 4. Tareas para llevar a cabo el análisis de riesgos
Fuente: (MARGERIT, 2012)

2. Tratamiento de riesgos:

Nos permite organizar una defensa concienzuda y prudente, para que de esta manera la organización pueda sobrevivir a los incidentes de seguridad y seguir operando en las mejores condiciones. Sin embargo, se dice que el riesgo se reduce a un nivel residual que la dirección asume (MARGERIT, 2012).

Se puede decir que la gestión de la seguridad de un sistema de información es la gestión de sus riesgos y que el análisis permite racionalizar dicha gestión (MARGERIT, 2012).

De esta manera MAGERIT busca no solo formar conciencia en los responsables del gobierno de TI de la existencia de riesgos, sino que ayuda a descubrir y planificar un tratamiento oportuno para mantener a estos riesgos bajo control (MARGERIT, 2012).

Capítulo 3 – Fases del Plan de Seguridad Informática

El desarrollo del presente Plan de Seguridad Informática (PSI), basado en la NTP-ISO/IEC 27001:2014, está organizado en 3 Fases:

- Fase I: Diagnóstico Situacional de la Municipalidad del Centro Poblado de Salcedo Puno, en Relación a la NTP-ISO/IEC 27001:2014.
- Fase II: Preparación del Plan de Seguridad Informática.
- Fase II: Plan de Seguridad Informática

3.1. Fase I: Diagnóstico situacional de la municipalidad del centro poblado de salcedo en relación a la NTP-ISO/IEC 27001:2014

Para la realización del diagnóstico situacional de la Municipalidad del Centro Poblado de Salcedo Puno, se elaboró un instrumentos de recopilación de información llamada encuesta (ver ANEXO A), que permitió el levantamiento de información y realizar la evaluación situacional de la Municipalidad del Centro Poblado de Salcedo Puno con respecto a los requisitos de la NTP-ISO/IEC 27001:2014, que se presentan a continuación, se harán en dos formas: Describiendo los hallazgos de la evaluación y mostrándolos cuantitativamente en base a una escala de Likert, como se ve en la siguiente tabla 1:

Tabla 1
Criterios de evaluación con respecto a los requisitos de la NTP ISO/IEC 27001:2014

Criterio de Calificación	Descripción	Valoración
No Diseñado	Los hallazgos muestran que el requisito no lo tienen diseñado.	0 – 20 %
Parcialmente Diseñado	Los hallazgos muestran que si se tiene el requisito parcialmente diseñado y además no se ajusta específicamente al requisito de la NTP ISO/IEC 27001:2014.	21 – 40 %
Diseñado	Los hallazgos muestran que si se tiene el requisito de la NTP ISO/IEC 27001:2014, diseñado, pero sin	41 – 60 %

	evidencias de aplicación.	
Parcialmente Implementado	Los hallazgos muestran la conformidad del diseño con el requisito de la NTP ISO/IEC 27001:2014, pero con escasas evidencias de aplicación.	61 – 80 %
Implementado	Los hallazgos muestran que el diseño si se implementó en base al requisito de la NTP ISO/IEC 27001:2014, y si se cuenta con evidencias de aplicación permanentes.	81- 100%

Fuente: Adaptado de "Propuesta para la implementación del sistema de gestión de calidad basado en la norma ISO 9001:2008 en una empresa del sector construcción" (Tesis), p. 37, Medina Bocanegra. 2013.

Los resultados que se obtuvieron al diagnosticar la situación actual de la Municipalidad del Centro Poblado de Salcedo Puno, con respecto a los requisitos de la NTP ISO/IEC 27001:2014 se muestra en la tabla siguiente 2:

Tabla 2

Resultados de la Evaluación de los Requisitos de la NTP ISO/IEC 27001:2014

Sección	Requisito de la NTP ISO/ IEC 27001:2014	Estado	Evidencia/Sugerencia	Valoración
1	**Contexto de la Organización**	No Diseñado	De acuerdo a los hallazgos encontrados, se recomienda la realización del análisis del contexto de la Municipalidad del Centro Poblado de Salcedo Puno, para entender los aspectos internos y externos, y, requisitos relevantes para el Plan de Seguridad Informática (PSI).	6%
2	**Liderazgo**	No Diseñado	Las autoridades de la Entidad, deben mostrar liderazgo y compromiso respecto al PSI. La	1%

			asignación de los roles con respecto a la seguridad información deben estar pensadas para asegurar la responsabilidad y su autoridad. Elaborar un PSI y establecer los las metas de Seguridad de la Información en concordancia a las metas organizacionales.	
3	**Planificación**	No Diseñado	Planificar el procedimiento de gestión y valoración de riesgos en seguridad de la información.	0%
4	**Soporte**	No Diseñado		7%
5	**Operación**	No Diseñado		0%
6	**Evaluación del Desempeño**	Parcial mente Diseñado	Implementar el PSI y elaborar un cronograma para evaluar periódicamente su funcionamiento y garantizar que el sistema se mantiene eficaz a lo largo del tiempo. Asimismo documentar dichas evaluaciones.	21%
7	**Mejoras**	No Diseñado	Implantar el PSI y elaborar un plan de mejora continua para actualizar el PSI de acuerdo a los cambios y novedades de la organización, las tecnologías, las amenazas, etc., tratando de mantener los riesgos controlados en todo momento.	0%
Valoración Total de los Requisitos de la NTP ISO/IEC 27001:2014				5%

Fuente: Elaboración del Estudio.

De acuerdo al diagnóstico de la Municipalidad del Centro Poblado de Salcedo Puno, en relación a los requisitos de la NTP ISO/IEC 27001:2014, se puede señalar que el Sistema de Gestión de Seguridad en la Información, se encuentra en una etapa inicial y precaria, como se

puede apreciar en la tabla 2, la Municipalidad del Centro Poblado de Salcedo Puno solo obtuvo un 5% en el cumplimiento de los requisitos de la NTP ISO/IEC 27001:2014, de un total de 100%.Este resultado indica que los hallazgos evidenciados muestran que no se tiene muchos de los requisitos y/o ni si quiera se han bosquejado su implementación.

3.1.1. Resultados de la encuesta realizada

En la presente sección se muestran los resultados obtenidos de la encuesta realizada al personal del Área de Informática y Elaboración de Datos de la Oficina de Administración y Finanzas de la Municipalidad del Centro Poblado de Salcedo Puno. La encuesta consta de 16 preguntas que permitieron realizar el diagnostico situacional de la seguridad informática.

Los resultados se muestran gráficamente con su respectivo análisis del hallazgo encontrado al encuestar a 4 trabajadores del Área de Informática y Elaboración de Datos de la Oficina de Administración y Finanzas de la Municipalidad del Centro Poblado de Salcedo Puno:

- Al Jefe de la Oficina de Administración y Finanzas.
- Al Jefe del Área de Informática y Elaboración de Datos.
- A 2 Auxiliares del Área de Informática y Elaboración de Datos.

Los criterios de inclusión que se tomaron en cuenta para el personal al cual se le elaboro la encuesta fue:

- El personal tiene conocimiento sobre seguridad de la información.
- El personal es responsable de los activos en relación a las tecnologías de información.
- El personal pertenece al área de Informática y Elaboración de Datos.

Los criterios de exclusión que se tomaron en cuenta para el personal al cual se le elaboro la encuesta fue:

- El personal no tiene conocimiento alguno sobre seguridad de la información por lo que la información recopilada no sería de mucho aporte para el trabajo de investigación.
- El perteneces a diferentes áreas que no tiene relación con el área Informática y Elaboración de Datos .

Pregunta 1: ¿Considera Ud. que en su área de trabajo existe información que debe ser protegida?

Tabla 3

Resultados de la Pregunta 1

N° DE PREGUNTA	CONTEO DE RESPUESTAS		PORCENTAJE	
	SI	NO	SI	NO
Pregunta 1	4	0	100%	0%

Fuente: Elaboración del Estudio

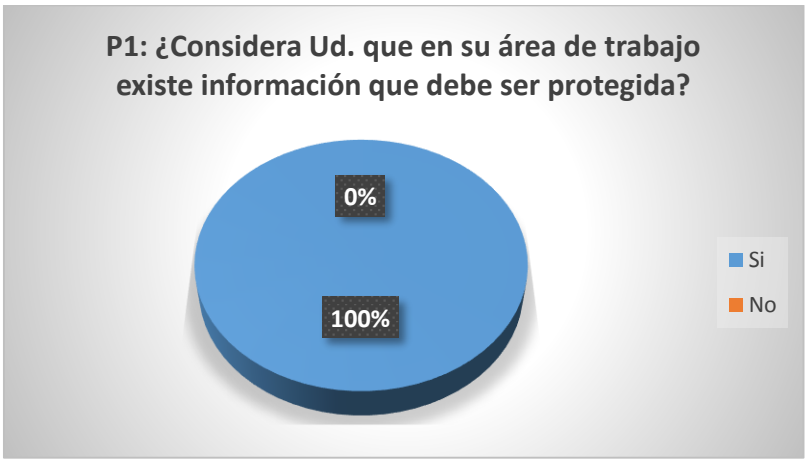

Figura 5. Resultados Gráficos para la Pregunta 1.
Fuente: Elaboración del Estudio.

Análisis de resultados: El 100% de encuestados creen que en su área de trabajo existe información que debe ser protegido. Se evidencia la preocupación por el tema de seguridad de la información y la importancia que hoy en día tiene en las empresas el contar con un Plan de Seguridad Informática (PSI).

Pregunta 2: ¿En su área de trabajo se ha categorizado la información de acuerdo al grado de importancia que tienen para la Municipalidad del Centro Poblado de Salcedo Puno?

Tabla 4

Resultados de la Pregunta 2

N° DE PREGUNTA	CONTEO DE RESPUESTAS		PORCENTAJE	
	SI	NO	SI	NO
Pregunta 2	0	4	0%	100%

Fuente: Elaboración del Estudio

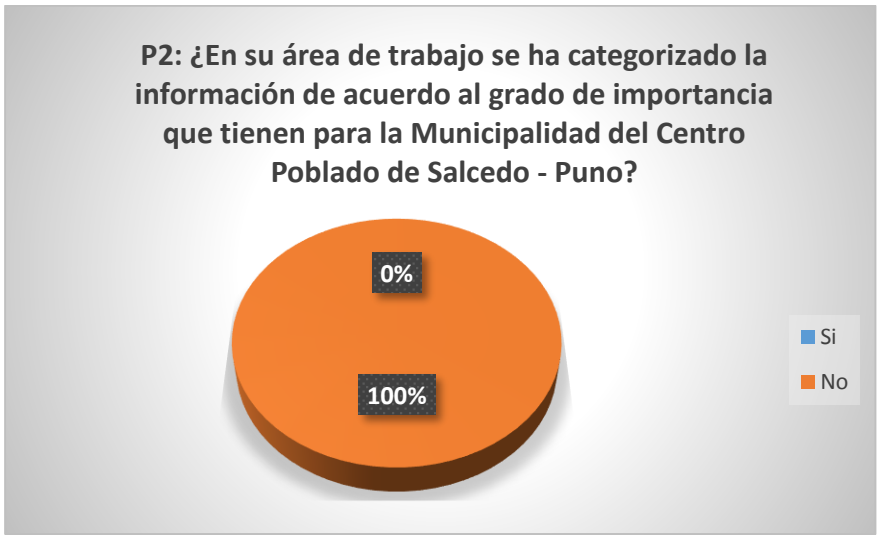

Figura 6. Resultados Gráficos para la pregunta 2.
Fuente: Elaboración del Estudio.

Análisis de Resultados: El 100% de los encuestados indicaron que la información no está categorizada de acuerdo al grado de importancia, aunque sí se sabe que se tiene información confidencial. La categorización de la información de acuerdo a su nivel de importancia es valiosa ya que la información se considera como el activo más importante y requiere un adecuado tratamiento en su seguridad.

Pregunta 3: ¿Ha recibido Ud. capacitación sobre seguridad de la información de acuerdo a su función laboral?

Tabla 5

Resultados de la Pregunta 3

N° DE PREGUNTA	CONTEO DE RESPUESTAS		PORCENTAJE	
	SI	NO	SI	NO
Pregunta 3	0	4	0%	100%

Fuente: Elaboración del Estudio

Figura 7. Resultados Gráficos para la pregunta 3.
Fuente: Elaboración del Estudio.

Análisis de Resultados: De los resultados se puede inferir que el 100% de los encuestados nunca recibieron capacitación sobre seguridad de la información. Este factor es muy peligroso ya que el personal de administra y gestiona la información en la Municipalidad del Centro Poblado de Salcedo Puno deberían estar a la vanguardia en este tema, por ser prioridad el resguardo de la información como activo.

Pregunta 4: ¿Su contrato contempla ítems que estipulen responsabilidades con respecto a la seguridad de la información?

Tabla 6

Resultados de la Pregunta 4

N° DE PREGUNTA	CONTEO DE RESPUESTAS		PORCENTAJE	
	SI	NO	SI	NO
Pregunta 4	1	3	25%	75%

Fuente: Elaboración del Estudio

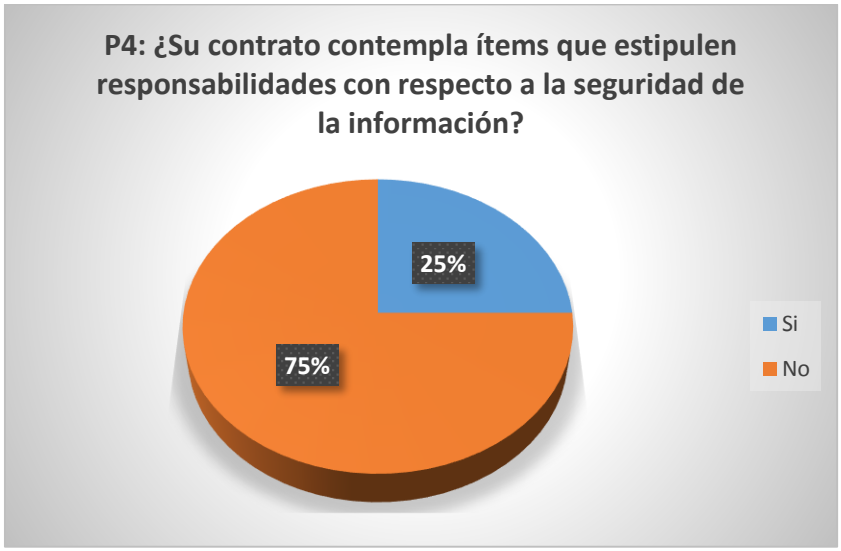

Figura 8. Resultados Gráficos para la pregunta 4.
Fuente: Elaboración del Estudio.

Análisis de Resultados: El 75% de los encuestados indicaron que no está estipulado nada al respecto de la responsabilidad de su cargo con la seguridad de la información, solo el Jefe del Departamento de Informática y Elaboración de Datos, indico que en su contrato si se estipula esa responsabilidad, es por ello que se requiere la formulación del Plan de Seguridad Informática.

Pregunta 5: Dentro de su área de trabajo ¿se considera la seguridad de información cuando se gestiona un proyecto?

Tabla 7

Resultados de la Pregunta 5

N° DE PREGUNTA	CONTEO DE RESPUESTAS		PORCENTAJE	
	SI	NO	SI	NO
Pregunta 5	0	4	0%	100%

Fuente: Elaboración del Estudio

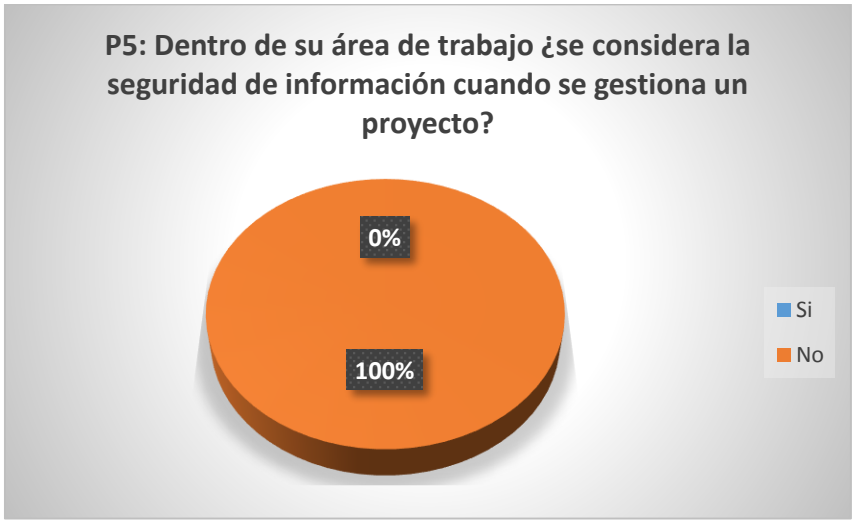

Figura 9. Resultados Gráficos para la pregunta 5.
Fuente: Elaboración del Estudio.

Análisis de Resultados: Se observa que hasta el momento no se han considerado temas de seguridad de la información en la gestión de los proyectos en la Municipalidad, razón por la cual el 100% indicaron que no se considera la seguridad de la información. También factor de riesgo, ya que la información de los proyectos es sensible, valiosa e importante.

Pregunta 6: ¿Cuenta Ud. con un computador/laptop para realizar sus funciones? (Si la respuesta es No pasar a la pregunta 9)

Tabla 8

Resultados de la Pregunta 6

N° DE PREGUNTA	CONTEO DE RESPUESTAS		PORCENTAJE	
	SI	NO	SI	NO
Pregunta 6	4	0	100%	0%

Fuente: Elaboración del Estudio

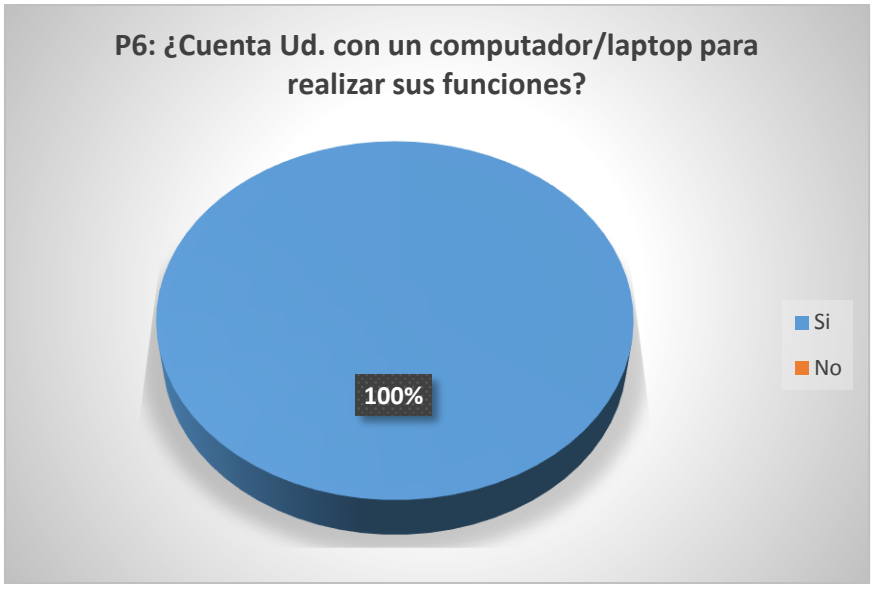

Figura 10. Resultados Gráficos para la pregunta 6.
Fuente: Elaboración del Estudio.

Análisis de Resultados: El 100% manifestó que cuentan con un equipo de cómputo para realizar su trabajo.

Pregunta 7: ¿Cuenta Ud. con una clave de acceso para ingresar a su computador y/o laptop?

Tabla 9

Resultados de la Pregunta 7

N° DE PREGUNTA	CONTEO DE RESPUESTAS		PORCENTAJE	
	SI	NO	SI	NO
Pregunta 7	1	3	25%	75%

Fuente: Elaboración del Estudio

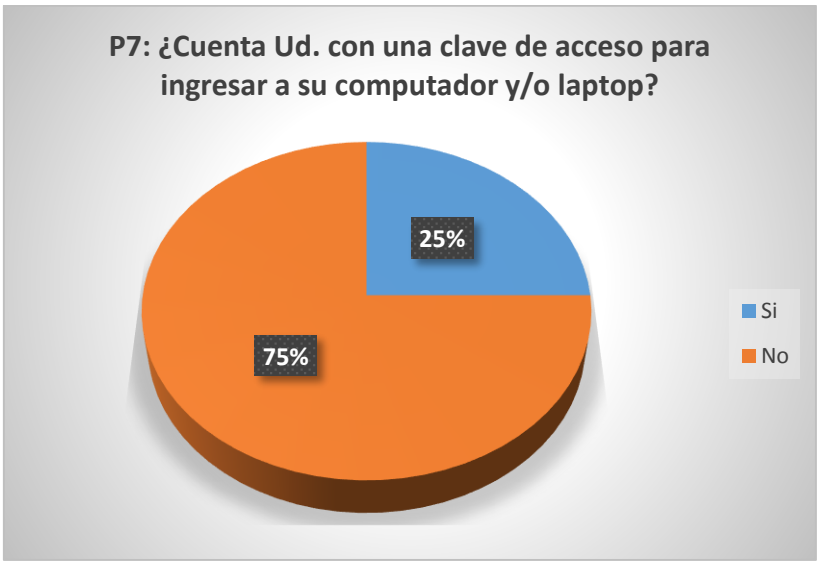

Figura 11. Resultados Gráficos para la pregunta 7.
Fuente: Elaboración del Estudio.

Análisis de Resultados: El 75% de los encuestados indican que no cuentan con clave de acceso para ingresar a la computadora que se les asigno para realizar su trabajo. Este hecho es sumamente peligroso y genera mucho riesgo porque se afecta directamente a la confidencialidad e integridad de la información de la organizacion.

Pregunta 8: Cuando su computador está desatendido ¿Se activa el bloqueo de pantalla con contraseña para proteger la información?

Tabla 10

Resultados de la Pregunta 8

N° DE PREGUNTA	CONTEO DE RESPUESTAS		PORCENTAJE	
	SI	NO	SI	NO
Pregunta 8	1	3	25%	75%

Fuente: Elaboración del Estudio

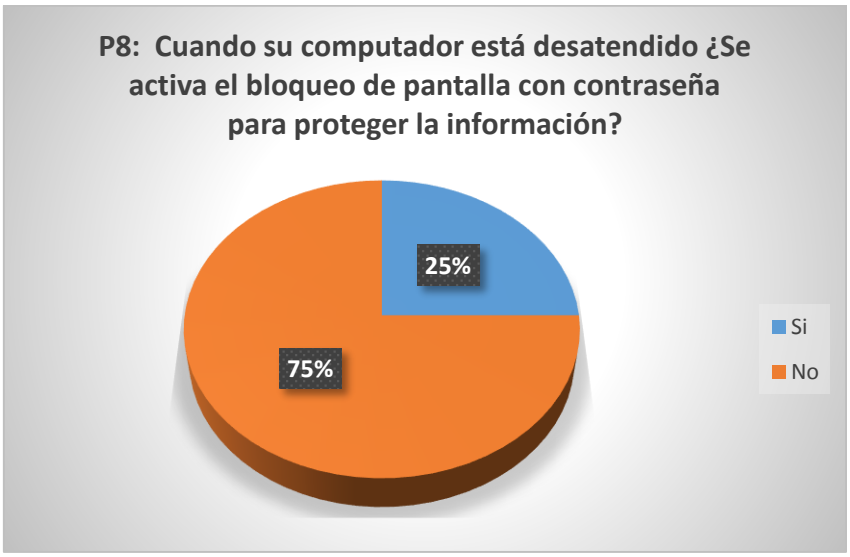

Figura 12. Resultados Gráficos para la pregunta 8.
Fuente: Elaboración del Estudio.

Análisis de Resultados: El 75% de los encuestados indican que no está configurada a la opción de loqueo de pantalla cuando el computador esta sin uso por un instante de tiempo pertinente. Este hecho también de suma importancia porque se afecta directamente a la confidencialidad de la información.

Pregunta 9: ¿En lo que va del año ha sufrido modificación o pérdida de información ya sea por virus, acceso de personas no autorizadas, deterioro, tras papeleo, etc.?

Tabla 11

Resultados de la Pregunta 9

N° DE PREGUNTA	CONTEO DE RESPUESTAS		PORCENTAJE	
	SI	NO	SI	NO
Pregunta 9	4	0	100%	0%

Fuente: Elaboración del Estudio

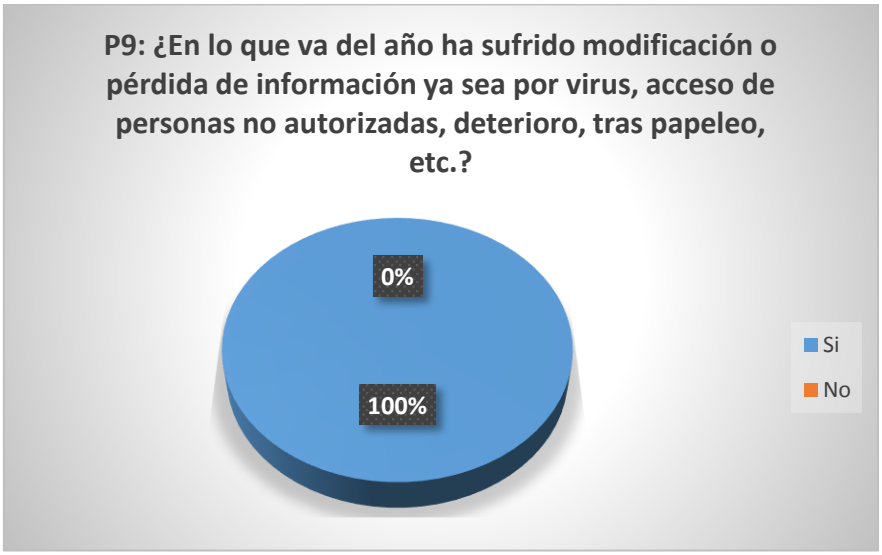

Figura 13. Resultados Gráficos para la pregunta 9.
Fuente: Elaboración del Estudio.

Análisis de Resultados: El 100% indica que si ha sufrido alguna modificación o perdida de información en lo que va del año, por distintos factores mencionados en la pregunta. Este factor es sumamente peligroso, ya que afecta directamente en la integridad y disponibilidad de la información.

Pregunta 10: ¿En lo que va del año se ha divulgado información sensible para la Municipalidad del Centro Poblado de Salcedo Puno sin su autorización o conocimiento?

Tabla 12

Resultados de la Pregunta 10

N° DE PREGUNTA	CONTEO DE RESPUESTAS		PORCENTAJE	
	SI	NO	SI	NO
Pregunta 10	4	0	100%	0%

Fuente: Elaboración del Estudio

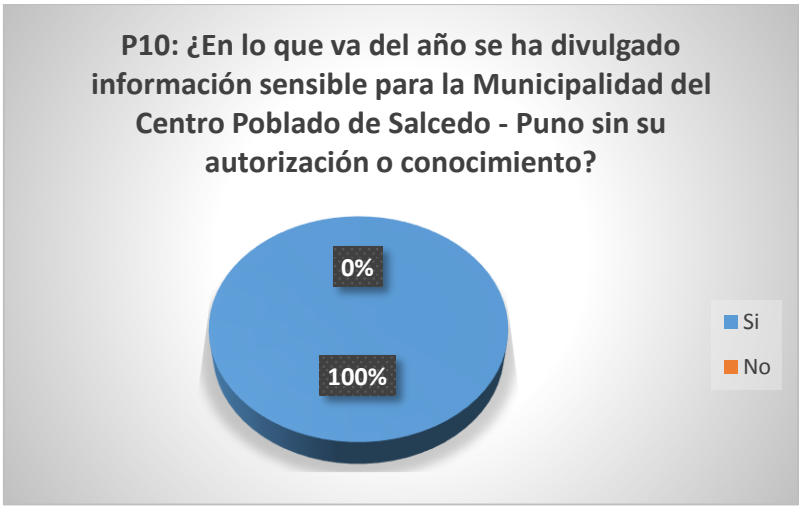

Figura 14. Resultados Gráficos para la pregunta 10.
Fuente: Elaboración del Estudio.

Análisis de Resultados: El 100% manifiesta que, si se ha divulgado información sensible de la Municipalidad del Centro Poblado de Salcedo Puno, inclusive se ha visto que se han modificado datos en la base de datos de contabilidad, acto que se viene investigando actualmente. Es factor si es de preocupación, es por ello que en la Municipalidad del Centro Poblado de Salcedo Puno se está priorizando la elaboración de un Plan de Seguridad Informática que permita contrarrestar y saber actuar ante incidentes de ataques a los sistemas que manejan la información.

Pregunta 11: ¿En su área de trabajo se han realizado evaluación de riesgos relacionados con la información?

Tabla 13

Resultados de la Pregunta 11

N° DE PREGUNTA	CONTEO DE RESPUESTAS		PORCENTAJE	
	SI	NO	SI	NO
Pregunta 11	1	3	25%	75%

Fuente: Elaboración del Estudio

Figura 15. Resultados Gráficos para la pregunta 11.
Fuente: Elaboración del Estudio.

Análisis de Resultados: El 75% indica que nunca se ha realizado una evaluación de riesgos, recién actualmente se viene planificando una evaluación de riesgos de toda la infraestructura y servicios tecnológicos de la Municipalidad del Centro Poblado de Salcedo Puno.

Pregunta 12: ¿En su área de trabajo se han realizado una evaluación de vulnerabilidades de la red?

Tabla 14

Resultados de la Pregunta 12

N° DE PREGUNTA	CONTEO DE RESPUESTAS		PORCENTAJE	
	SI	NO	SI	NO
Pregunta 12	1	3	25%	75%

Fuente: Elaboración del Estudio

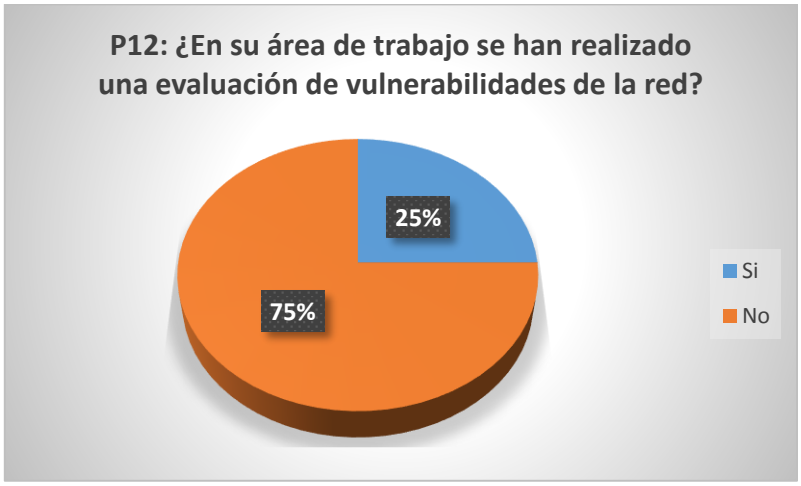

Figura 16. Resultados Gráficos para la pregunta 12.
Fuente: Elaboración del Estudio.

Análisis de Resultados: EL 75% de los encuestado indica que no se ha realizado dicha evaluación, 25% indica que si se realizó una evaluación de las vulnerabilidades de los sistemas de red con los que cuenta su área. Se puede indicar al respecto que no es suficiente una evaluación empírica sin considerar estándares de seguridad informática.

Pregunta 13: ¿Su área de trabajo cuenta con software antivirus actualizado?

Tabla 15

Resultados de la Pregunta 13

N° DE PREGUNTA	CONTEO DE RESPUESTAS		PORCENTAJE	
	SI	NO	SI	NO
Pregunta 13	3	1	75%	25%

Fuente: Elaboración del Estudio

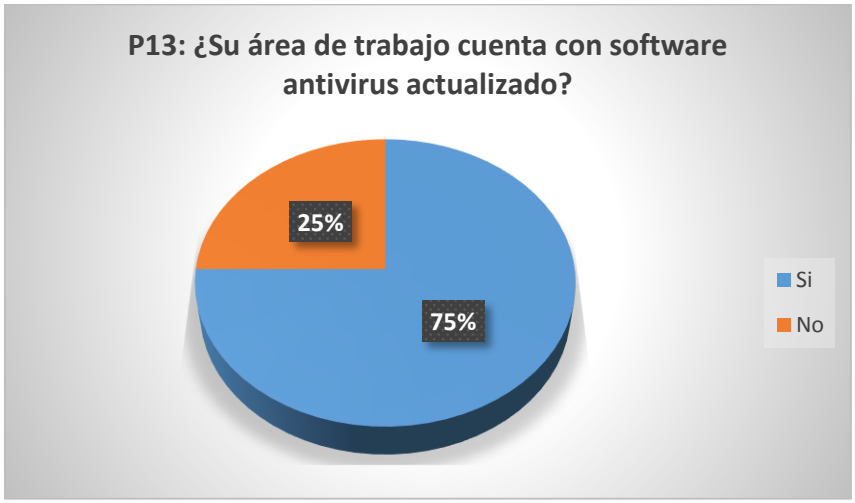

Figura 17. Resultados Gráficos para la pregunta 13.
Fuente: Elaboración del Estudio.

Análisis de Resultados: El 75% indica que, si cuentan con software antivirus, el detalle que los procesos y mecanismo de actualización no se cumplen, lo que ocasiona que por algún tiempo los sistemas estén desprotegidos y a expensas de cualquier ataque.

Pregunta 14: ¿Realiza Ud. copias de seguridad para proteger su información?

Tabla 16

Resultados de la Pregunta 14

N° DE PREGUNTA	CONTEO DE RESPUESTAS		PORCENTAJE	
	SI	NO	SI	NO
Pregunta 14	2	2	50%	50%

Fuente: Elaboración del Estudio

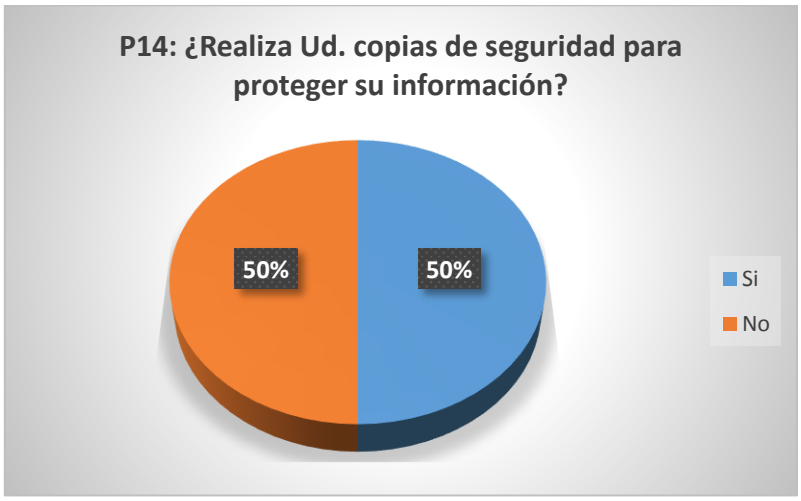

Figura 18. Resultados Gráficos para la pregunta 14.
Fuente: Elaboración del Estudio.

Análisis de Resultados: El 50% manifestó que se realizan copias de seguridad y respaldo de la información que gestiona su área y las demás áreas también, el detalle es que sus sistemas de respaldo son poco convencionales para la cantidad y calidad de la información que generan.

Pregunta 15: ¿Considera que su oficina está protegida contra amenazas externas o ambientales que ocasionen pérdidas de información?

Tabla 17

Resultados de la Pregunta 15

N° DE PREGUNTA	CONTEO DE RESPUESTAS		PORCENTAJE	
	SI	NO	SI	NO
Pregunta 15	1	3	25%	75%

Fuente: Elaboración del Estudio

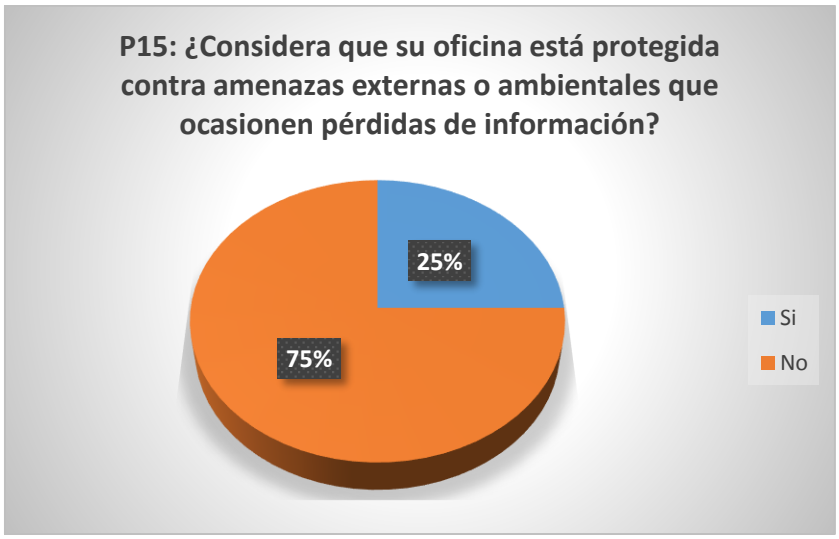

Figura 19. Resultados Gráficos para la pregunta 15.
Fuente: Elaboración del Estudio.

Análisis de Resultados: El 75% indica que las instalaciones de su oficina no están protegidas contra amenazas externas o ambientales, ya que la infraestructura tecnológica no está en los ambientes ni las formas correctas de instalación.

Pregunta 16: ¿Sabe Ud. si dentro de la Municipalidad del Centro Poblado de Salcedo Puno existe un Plan de Seguridad Informática?

Tabla 18

Resultados de la Pregunta 16

N° DE PREGUNTA	CONTEO DE RESPUESTAS		PORCENTAJE	
	SI	NO	SI	NO
Pregunta 16	0	4	0%	100%

Fuente: Elaboración del Estudio

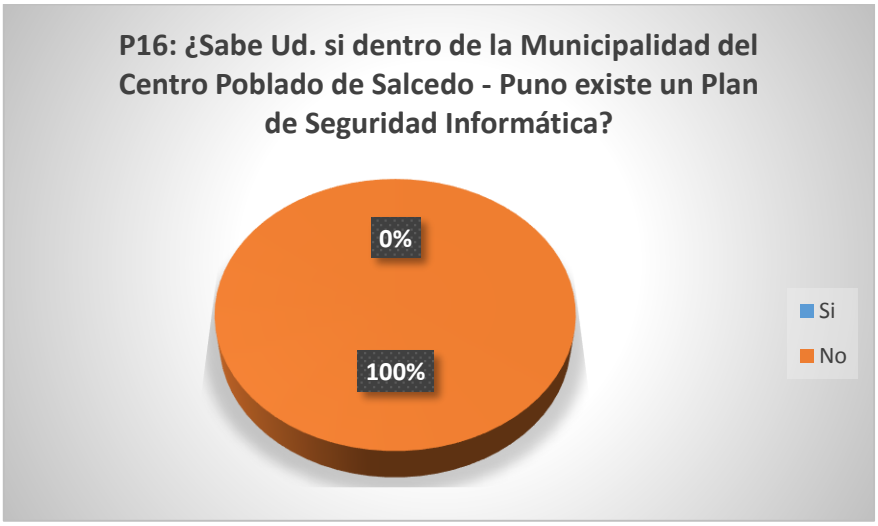

Figura 20. Resultados Gráficos para la pregunta 16.
Fuente: Elaboración del Estudio.

Análisis de Resultados: El 100% indica que no se tiene un Sistema de Gestión de la Seguridad de la Información, pero concluyen que hoy en día es un sistema con el que deben contar todas las empresas públicas o privadas, por el enorme riesgo que se corre por no contar con un PSI.

3.2. Fase II: Preparación del Plan de Seguridad Informática.

Se desarrolla esta fase del Plan de Seguridad Informática con el propósito de alcanzar las siguientes metas u objetivos:

- Se desea definir el alcance del Plan de Seguridad Informática de la Municipalidad del Centro Poblado de Salcedo Puno.

- Identificar cuáles son los requisitos legales, para el Plan de Seguridad Informática.
- Elaborar cuales son las políticas de seguridad.
- Proponer el Plan de seguridad a la Oficina de Administración y Finanzas de la Municipalidad del Centro Poblado de Salcedo Puno para su posterior aplicación.

Para el logro de los objetivos trazados en esta fase del Plan de Seguridad Informática se realizó un análisis interno y externo del contexto de la Municipalidad del Centro Poblado de Salcedo Puno.

3.2.1. Contexto de la Municipalidad del Centro Poblado de Salcedo Puno

La NTP ISO/IEC 27001:2014, indica como contexto de la Municipalidad del Centro Poblado de Salcedo Puno, la importancia de comprender la organización y su contexto, esto es, comprender los aspectos internos y externos, y la importancia de estos para el establecimiento del Plan de Seguridad Informática, así como para entender las necesidades y expectativas de las partes interesadas y determinar el alcance del Plan de Seguridad Informática.

3.2.1.1. Contexto Externo

El análisis de los factores externos de la Municipalidad del Centro Poblado de Salcedo Puno se desarrolló teniendo en consideración factores como: (Políticos-Legales, Económicos, Socio-Culturales y Tecnológicos), a continuación, se muestra el resultado del análisis:

Factor Político-Legal:

- Interés del estado por la seguridad de la información a nivel de todas las entidades públicas (la PCM a través de la Secretaría de Gobierno Digital (SeGDi).
- Desarrollo y fortalecimiento del Gobierno Electronico.
- Marco regulatorio sobre seguridad de la información.
- Soporte de la Secretaría de Gobierno Digital (SeGDi) para el establecimiento del SGSI.

Factor Económico:

- Costos muy elevados para la contrata de consultores para establecer un PSI.
- Presupuesto limitado por parte del estado, para la formulación e implementación del PSI.

Socio-Cultural:

- Más hogares con acceso a internet y dispuestos a realizar trámites online.

- Cada vez más se cierran las brechas en el uso de tecnologías.
- Las sociedades de hoy cada vez más tecnológicas y móviles, y la peruana no es ajena este avance.
- Hoy en día las sociedades se preocupan por la seguridad de su información.

Tecnológico:

- Aparición de nueva tecnología de información, que el estado las está adaptando para su uso.
- Aparición de nuevas necesidades de implementación tecnológica. Existencia de una fuerte oferta tecnológica en los mercados.
- La Red Dorsal Nacional de Fibra Óptica (RDNFO, que permitirá mejorar la velocidad de acceso a la información.
- Vulnerabilidades y riesgos en la seguridad informática.

Es importante tener claro el contexto externo de la Municipalidad del Centro Poblado de Salcedo Puno, para tener claro los criterios de riesgo y amenazas.

3.2.1.2. Contexto interno

Con el propósito de alinear con la cultura y comportamiento organizacional, los procesos de negocio y la estrategia de la organización, se desarrolla el presente análisis del contexto interno de la Municipalidad del Centro Poblado de Salcedo Puno.

A. Naturaleza de la Entidad. La Municipalidad del Centro Poblado de Salcedo Puno, como órgano de gobierno local tiene personería jurídica de derecho, con autonomía económica y administrativa en asuntos de su competencia, aplicando la normatividad y la legislación de forma general de conformidad con la Constitución Política del Perú.

B. Finalidad.

- Promover el desarrollo socio-económico sostenible y armónico del distrito de Salcedo - Puno, teniendo en consideración el manejo de riesgos naturales con un enfoque transversal.
- Fomentar el bien común de los ciudadanos mediante a adecuada prestación de los servicios públicos locales que satisfagan sus necesidades vitales, tales como: de salubridad, vivienda, abastecimiento, seguridad, cultura, recreación, transporte y comunicaciones.

- Desarrollar programas sociales garantizando el ejercicio pleno de los derechos de los ciudadanos, así como la igualdad de oportunidades.
- Promover el desarrollo económico de sus habitantes, mediante el impulso y dinamización de la actividad empresarial de la Micro y Pequeña Empresa.

C. Misión. La Municipalidad del Centro Poblado de Salcedo Puno, es un órgano de Gobierno Local que goza de provisión de bienes y servicios de calidad para todas y todos los ciudadanos del Centro Poblado de Salcedo buscando contribuir al desarrollo sostenible del mismo, de modo que impacte en su bienestar general.

D. Visión. La Municipalidad del Centro Poblado de Salcedo Puno busca ser un gobierno distrital, para lograr resultados que beneficien a la población generando mayores oportunidades de emprendimiento para la nueva generación con una buena distribución de los recursos humanos y económicos en equidad de géneros, buscando ser la primera Municipalidad del Centro Poblado de Salcedo Puno en ser un distrito seguro, ordenado, saludable, moderno, turístico y sostenible, con habitantes que gozan de calidad de vida.

E. Líneas Estratégicas. Las líneas estratégicas son:

- Línea estratégica 1: INSTITUCIONALIDAD Y GOBERNABILIDAD, mediante la cual las instituciones públicas, privadas y organizaciones sociales pertenecientes a la jurisdicción de la Municipalidad, participan de forma activa y democráticamente en la gestión del desarrollo y se identifican con la problemática del centro poblado.
- Línea estratégica 2: DESARROLLO HUMANO, EDUCACION, SALUD, CULTURA E IDENTIDAD. Mediante la cual la Municipalidad promueve el desarrollo humano e integral de sus vecinos: calidad de vida, promoción de la salud, educación de calidad, fomento a la cultura e identidad y una política inclusiva y de acceso universal.
- Línea estratégica 3: DESARROLLO FÍSICO Y MEDIO AMBIENTAL. Mediante la articulación con las comunidades y sectores de manera ordenada, así como zonificando económica y ecológicamente, mediante el uso racional y gestión eficiente de los recursos naturales.
- Línea estratégica 4: DESARROLLO ECONÓMICO PRODUCTIVO. La Municipalidad fortalece y genera el incremento de las economías familiares a través de cadenas productivas y corredores económicos articulados al mercado local, regional, nacional e internacional.

F. Objetivos estratégicos.

- Fortalecer a las instituciones y organizaciones sociales del Centro Poblado para la gestión integral del desarrollo con gobernabilidad, democracia y participación
- Promover el desarrollo humano integral de los habitantes, basado en valores, con acceso oportuno y adecuado a los derechos de salud, educación, cultura e identidad cultural.
- Fomentar el desarrollo del Centro Poblado articulando e integrando a la zona urbana con las comunidades y sectores de manera ordenada, zonificado económica y ecológicamente, mediante el uso racional y gestión eficiente de los recursos naturales.
- Promover la actividad ganadera, turística, forestal, artesanal y gastronómica, a través cadenas productivas, corredores económicos, articulando al mercado.

G. Proceso de gestión de la infraestructura tecnológica

Este objetivo tiene como finalidad planear, organizar, dirigir, ejecutar y supervisar el diseño, implementación y mantenimiento de la infraestructura tecnológica de la Municipalidad del Centro Poblado de Salcedo Puno, mediante el uso de protocolos de comunicación, gestionando los recursos tecnológicos, y, garantizando los niveles adecuados de confidencialidad, integridad y disponibilidad de los sistemas de información, de los datos y de las comunicaciones de la Municipalidad del Centro Poblado de Salcedo Puno. Esto inicia con la concepción del Plan Operativo Informático (POI), su ejecución y adecuada prestación de servicios a los usuarios (internos y externos); estableciendo el monitoreo, la evaluación continua y los planes de contingencia,

El proceso de gestión de la infraestructura tecnológica tiene los siguientes sub procesos:

- Gestión de la infraestructura y plataforma de procesamiento de datos.
- Administrar la operatividad de los sistemas de información, equipos.
- Informáticos y de comunicaciones de la entidad.
- Gestión de soporte técnico.
- Gestión de cambios de tecnologías de información.
- Gestión de la seguridad de la información.
- Gestión de la página web y servicios online.
- Gestión del ciclo de vida del desarrollo de software de la entidad.
- Gestión de plan de contingencia informática y de comunicaciones.
- Administrar el inventario de equipos de cómputo.
- Mejora de los sistemas estadísticos de la Municipalidad.
- Gestión de proyección social tecnológico para la Municipalidad.

- Asesorar a los usuarios internos en sus requerimientos informáticos.

Se garantiza la confidencialidad, integridad y disponibilidad de la información con el proceso de gestión de infraestructura tecnológica en la Municipalidad, con este proceso se logra administrar los recursos tecnológicos a través de los cuales se gestiona y controla el intercambio seguro de la información de los demás procesos que fluyen en la Municipalidad, por esta razón es imperiosa la necesidad de Planificar la seguridad informática en la Municipalidad del Centro Poblado de Salcedo Puno.

Se aclara que para la definición del presente proceso se desarrollaron reuniones constantes con los responsables del Área de Informática y Elaboración de Datos, además de ajustar la propuesta al ROF de la Municipalidad del Centro Poblado de Salcedo Puno.

H. Aspectos Técnicos

- La Municipalidad del Centro Poblado de Salcedo Puno, cuenta con una red de área local (LAN), constituida por 30 estaciones de trabajo, 15 portátiles y 2 servidores (1 servidor de aplicación y 1 servidor de bases de datos).
- La Municipalidad del Centro Poblado de Salcedo Puno cuenta con un Data Center, con los servidores y además una centralita telefónica que maneja las comunicaciones y anexos de la Municipalidad.
- Se centraliza toda la información en el servidor de base de datos necesaria para el funcionamiento de los diferentes sistemas de la Municipalidad del Centro Poblado de Salcedo Puno.
- Se cuenta con un sistema de alimentación ininterrumpida UPS.
- Se cuentan también con 2 líneas de Internet, para la salida de los sistemas de información de la Municipalidad del Centro Poblado de Salcedo Puno.
- Asimismo, se cuenta con un firewall para controlar el acceso a la red.
- Diariamente se realizan copias de seguridad y se almacenan en un disco duro externo ubicado en el Data Center. Un consolidado de Backups se guarda mensualmente en DVDs y se almacenan en un estante con llave.

I. Servicios en línea de la Municipalidad del Centro Poblado de Salcedo Puno

Para usuarios externos:

Hasta el momento no se ha implementado ningún servicio, la página Web del Municipio solo es de presentación e informativa.

Para Usuarios Internos:

- Sistema de trámite documentario.

- Sistema de Patrimonio.
- Sistema de Rentas.
- Sistema New Gestión de Logística.
- SIAF.
- Todos los Sistemas de Información Web del Estado.

Esta relación se extrae de las reuniones que se tuvieron con los responsables del Área de Informática y Procesamiento de Datos de la Municipalidad del Centro Poblado de Salcedo Puno.

3.2.1.3. Matriz FODA

Tabla 19

Matriz FODA

Fortalezas	Oportunidades
• La predisposición del personal de la Municipalidad y especialmente del Área de Informática y Procesamiento de datos, para la implementación del Plan de Seguridad Informática. • Las buenas relaciones del Área de informática y procesamiento de datos, con las demás áreas y gerencias de la Municipalidad.	• Soporte del estado a través de la Secretaría de Gobierno Digital (SeGDi) en relación a la seguridad de la información. • Tecnología nueva de Información y Comunicación.
Debilidades	**Amenazas**
• No se tiene al personal dedicado a la seguridad de la información. • No cuentan con licencias de Software para S.O y aplicaciones. • Se cuenta con un sólo proveedor de internet para la salida de todos los sistemas de información. • No existe un plan de capacitación para	• Falta de Presupuesto para implementación de Infraestructura y servicios. • Consultores en TIC muy caros. • Constante cambio de tecnología. • Uso incorrecto de las tecnologías por parte de la sociedad.

el personal en temas de seguridad. • No tienen actualizados los sistemas de antivirus.

Fuente: Elaboración del Estudio.

3.2.2. Políticas de seguridad informática

Las políticas de seguridad informática deben ser aprobadas por los órganos de gobierno de la Municipalidad del Centro Poblado de Salcedo Puno de acuerdo a los requisitos de la NTP ISO/IEC 27001:2014). Dicha revisión se llevará al final de cada año.

Después de aprobar las políticas de seguridad informática, estas se deben darse a conocer a todos los involucrados en la gestión de la información, socializando dichas políticas con todas las partes interesadas y miembros de la organización. Dentro de las políticas que se definieron están:

- Que la responsabilidad por la seguridad de la información no sólo corresponde a las áreas de seguridad informática, sino que también le corresponde a cada funcionario de la Municipalidad del Centro Poblado de Salcedo Puno.
- Los mecanismos de acceso que les sean otorgados a los funcionarios son responsabilidad exclusiva de cada uno de ellos por lo que no deben ser divulgados a terceros, a menos que exista un requerimiento sustentado u obedezca a una orden de la alta dirección.
- Todo funcionario que utilice los recursos de los sistemas tiene la responsabilidad de velar por la confidencialidad, integridad y disponibilidad de la información que maneje o a la que acceda.
- Toda información sensible o confidencial debe estar encriptado, ya sea que se encuentre al interior de la Municipalidad del Centro Poblado de Salcedo Puno o externamente, mediante el uso de cualquier medio de almacenamiento, transporte o transmisión.
- Toda información confidencial debe tener un proceso periódico de respaldo; Asimismo, tener asignado un período de retención determinado, la fecha de la última modificación y la fecha en que deja de ser sensible o se degrada. Sin embargo, dicha información no se debe guardar de forma indefinida por lo cual se debe determinar un período máximo de retención.
- Es política de la Municipalidad del Centro Poblado de Salcedo Puno, resguardar y proteger la información que se maneje buscando mantener la confidencialidad, así como la disponibilidad e integridad.

- Todos los usuarios de los sistemas de información deberán cumplir con la normativa y los requisitos legales relacionados a la seguridad informática.
- El Municipio debe fortalecer la cultura de seguridad de la información en sus funcionarios.
- Se debe garantizar la continuidad de los servicios y procesos de la Municipalidad del Centro Poblado de Salcedo Puno.
- Se debe implementar, mantener y realizar seguimiento al Plan de Seguridad Informática.

3.2.3. Alcance del Plan de Seguridad Informática

El alcance del Plan de Seguridad Informática, está orientado a cubrir todo lo referente al proceso de gestión de la infraestructura tecnológica, sub proceso de gestión de la seguridad de la información, dentro de los sistemas de información que sustentan los procesos de negocio.

Se tienen en cuenta los activos de información considerados como relevantes dentro del alcance.

3.2.4. Objetivos de la seguridad informática

- Asegurar la confidencialidad de la información de los ciudadanos almacenados en los sistemas de información de la Municipalidad del Centro Poblado de Salcedo Puno.
- Asegurar la confidencialidad, integridad y disponibilidad de la información sensible de la Municipalidad del Centro Poblado de Salcedo Puno.
- Maximizar la disponibilidad y calidad de los servicios prestados a los ciudadanos.
- Garantizar que nuestras operaciones y procesos actuales y futuros cumplan con la legislación y normatividad vigente en materia de seguridad de la información.
- Reducir los riesgos de seguridad de la información a un nivel aceptable para la Municipalidad del Centro Poblado de Salcedo Puno.
- Difundir la Política de seguridad a través de cada uno de los responsables de área.
- Evaluar la efectividad del Plan de Seguridad Informática y llevar a cabo la mejora continua.

3.2.5. Requisitos legales

El requisito fundamental que se debe de cumplir para implementar un Plan de Seguridad Informática, es el de cumplir con la legislación vigente en el Perú. Su cumplimento protege a la Municipalidad del Centro Poblado de Salcedo Puno de amenazas externas e internas,

además permite respetar los derechos de los ciudadanos y proveedores y evitará infracciones involuntarias con sus respectivos costes.

A continuación, se hace mención de algunas leyes y normas relacionadas con seguridad de la información que afectan a la Municipalidad del Centro Poblado de Salcedo Puno:

3.2.5.1. Norma de control interno de las entidades del estado

Esta Norma fue aprobada con Resolución de Contraloría General Nº 320-2006-CG, de fecha 30 de octubre del 2006. Según las normas básicas para las actividades de control gerencial, en su punto 3.10. Controles para las Tecnologías de Información y Comunicaciones (TIC) se define que la información de la entidad es provista mediante el uso de Tecnologías de la Información y Comunicaciones (TIC).

Las TIC abarcan datos, sistemas de información, tecnología asociada, instalaciones y personal. Las actividades de control de las TIC incluyen controles que garantizan el procesamiento de la información para el cumplimiento de la misión y de los objetivos de la entidad, debiendo estar diseñados para prevenir, detectar y corregir errores e irregularidades mientras la información fluye a través de los sistemas. Asimismo, la citada norma señala:

Comentario 01.- estos controles generales están conformados la estructura, políticas y procedimientos que se aplican a las TIC de la entidad y que van a contribuir a asegurar su correcta operatividad. Los principales controles deben establecerse en:

- Sistemas de seguridad de planificación y gestión de la entidad en los cuales los controles de los sistemas de información deben aplicarse en las secciones de desarrollo, producción y soporte técnico.
- La segregación de funciones.
- Controles de acceso general, mediante la seguridad física y lógica de los equipos centrales.
- La continuidad en el servicio.

Comentario 02.- Par el funcionamiento de las TIC, la entidad debe diseñar controles en las siguientes etapas:

i. Definición de los recursos
ii. Planificación y organización
iii. Requerimiento y salida de datos o información
iv. Adquisición e implementación
v. Servicios y soporte

vi. Seguimiento y monitoreo.

Comentario 07.- Para el adecuado ambiente de control en los sistemas informáticos, es necesario que éstos sean preparados y programados con anticipación para mantener la continuidad del servicio. Para ello se debe elaborar, mantener y actualizar de forma periódica un plan de contingencia debidamente autorizado y aprobado por el titular de la organización o funcionario designado por este donde se estipule procedimientos previstos para la recuperación de datos con el fin de afrontar situaciones de emergencia.

Comentario 08.- El programa de planificación y administración de seguridad otorga el marco y establece el ciclo continuo de la administración de riesgos para las TIC, mediante el desarrollo de políticas de seguridad, asignando responsabilidades y realizando el seguimiento de la correcta operación de los controles.

3.2.5.2. Ley N°29733.- Ley de protección de datos personales

Fue promulgada el 2011, y entro en vigencia el 8 de mayo de 2015 y tiene el objeto de garantizar el derecho fundamental a la protección de los datos personales, previsto en el artículo 2 numeral 6 de la Constitución Política del Perú, a través de su adecuado tratamiento, en un marco de respeto de los demás derechos fundamentales que en ella se reconocen.

Mediante la aplicación de esta Ley las empresas y entidades públicas están obligadas a garantizar la protección de los datos con los que cuentan en sus sistemas informáticos evitando el acceso de terceros no autorizados.

3.2.5.3. Ley 30096.- Ley de delitos informáticos

Entró en vigencia el 23 de octubre de 2013. Tiene por objeto prevenir y sancionar las conductas ilícitas que afectan los sistemas y datos informáticos y otros bienes jurídicos de relevancia penal, que sean cometidas mediante la utilización de tecnologías de la información o de la comunicación, con la finalidad de garantizar la lucha eficaz contra la ciberdelincuencia.

3.2.5.4. Ley N° 30171.- ley que modifica la ley 30096, ley de delitos informáticos

Publicada en el diario Oficial el Peruano en el 10 de marzo del 2014. Modificación de los artículos 2, 3, 4, 5, 7, 8 y 10 de la Ley 30096, Ley de Delitos Informáticos, se modificaron los

artículos 2, 3, 4, 5, 7, 8 y 10 de la Ley 30096, en los siguientes términos: Acceso ilícito, atentado a la integridad de datos informáticos, atentado a la integridad de sistemas informáticos, proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos, interceptación de datos informáticos, fraude informático, abuso de mecanismos y dispositivos informáticos.

3.2.5.5. Resolución Ministerial Nº 004-2016-PCM

Publicada el 8 de enero de 20016. Se aprueba 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.

Dicha norma señala que las entidades integrantes del Sistema Nacional de Informática, tendrán un plazo máximo de dos (2) años para la implementación y/o adecuación de la NTP ISO/IEC 27001:2014.

Asimismo, dichas entidades públicas tendrán un plazo de 60 días contados a partir de la fecha de publicación, para la presentación del cronograma de implementación y/o adecuación del sistema de gestión de la Seguridad de la Información, el mismo que deberá ser presentado a la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) de la Presidencia del Consejo de Ministros.

3.2.6. Comité de seguridad de la información

De acuerdo al requisito 5.3 Roles, responsabilidades y autoridades organizacionales de la NTP ISO/IEC 27001:2014 la alta dirección debe asegurar que las responsabilidades y la autoridad para los roles relevantes a la seguridad de la información estén asignadas y comunicadas.

Asimismo, la RM Nº 004-2016-PCM en su artículo 5 establece la creación del comité de gestión de seguridad de la información para dar cumplimiento al requisito 5.3 de la NTP ISO/IEC 27001:2014. Este comité de gestión de seguridad de la Información, estará conformado por:

i. El alcalde.
ii. El gerente municipal.
iii. El responsable de planificación y presupuesto.

iv. Jefe del Área de Informática y Procesamiento de Datos.
v. El responsable de la oficina de asesoría jurídica.
vi. El oficial de seguridad de la información.

3.2.6.1. Alcalde

- Aprobar la política de seguridad de la información y comunicarla a todos los trabajadores de la entidad.
- Definir y establecer los roles y responsabilidades relacionados con la seguridad de la información en niveles directivo y operativo.
- Promover una cultura de seguridad de la información en la entidad.

3.2.6.2. El Gerente Municipal

- Proponer al Alcalde y Concejo Municipal la política de seguridad de la información para la entidad.
- Hacer cumplir la política de seguridad de la información dentro de la entidad.
- Revisar la política de seguridad de la información en intervalos planificados o cuando se produzcan cambios significativos en la normatividad de seguridad.
- Controlar el avance de la seguridad de información dentro de la Municipalidad del Centro Poblado de Salcedo Puno.

3.2.6.3. El responsable de la Oficina de Planificación y Presupuestos

Gestionar y coordinar los medios necesarios para la implementación, ejecución y mantenimiento del PSI.

3.2.6.4. Jefe del Área de Informática y Procesamiento de Datos.

- Garantizar la disponibilidad y operatividad de los sistemas de información, equipos informáticos y de comunicaciones de la entidad.
- Establecer los mecanismos adecuados para la gestión y administración de riesgos, seguridad de la información, velar por la capacitación del personal de la entidad en lo referente a estos temas.
- Informar al gerente municipal sobre aspectos relacionados con el PSI.

- Asegurar la existencia de metodologías para el tratamiento de riesgos y oportunidades, políticas de seguridad de la información, así como la existencia de los documentos exigidos por la NTP ISO/IEC 27001:2014.
- Asegurar el cumplimiento de las políticas y requerimientos de seguridad establecidos para la adquisición, diseño, desarrollo, operación, administración y mantenimiento de infraestructura tecnológica de la entidad.
- Asignar las funciones, roles y responsabilidades de Seguridad, a los trabajadores a su cargo para la operación y administración de la infraestructura tecnológica de la entidad. Dichas funciones, roles y responsabilidades deben encontrarse documentadas y apropiadamente segregadas.
- Aprobar la implementación de los controles y medidas de seguridad.

3.2.6.5. El responsable de la Oficina de Asesoría Jurídica

- Conocer e interpretar las leyes y normatividad vigente relacionada con seguridad de la información y bajo el contexto de la entidad.
- Evaluar el cumplimiento de las leyes y normatividad vigente en temas de seguridad de la información dentro de la entidad.
- Mantener actualizado un archivo de normas legales relacionadas con la seguridad de la información.

3.2.6.6. El oficial de seguridad de la información.

- Diseñar y coordinar la implementación de las políticas, normas y procedimientos de seguridad de la información, con la participación activa de las dependencias de la entidad.
- Identificar los riesgos a los que se encuentran expuestos los activos de información de la Municipalidad del Centro Poblado de Salcedo Puno y gestionar la actualización del mapa de riesgos.
- Definir los controles asociados al Plan de Seguridad Informática Información y evaluarlos periódicamente.
- Establecer un programa periódico de revisión de vulnerabilidades y coordinar los respectivos planes de mitigación.

- Desarrollar de forma periódica, charlas de capacitación y concientización en temas de seguridad de información para el personal de la entidad.
- Atender auditorías internas y externas de aspectos asociados a la Seguridad de Información y, facilitar la información sobre documentos de gestión de seguridad y los controles implementados.

3.3. Fase III: Plan de Seguridad Informática

Con el propósito de alcanzar los objetivos del PSI de la Municipalidad de Centro Poblado de Salcedo Puno, se procedió a evaluar los riesgos de la seguridad informática, para elaborar la lista de controles que permitan mitigar los riesgos identificados.

3.3.1. Evaluación de riesgos

En base a la metodología de análisis y gestión de riesgos que se utilizó (MARGERIT), se precisaron la siguiente taxonomía de activos:

3.3.1.1. Taxonomía de Activos de Información

Tabla 20

Taxonomía de Activos de Información

Tipo de Activo	Tipo de Activo
Dato / Información	Los datos son el core que permite a una organización prestar sus servicios. La información es un activo abstracto que será almacenado en equipos o soportes de información (normalmente agrupado como ficheros o bases de datos) o será transferido de un lugar a otro por los medios de transmisión de datos.
Servicios	Están orientados a satisfacer las necesidades de los usuarios, contempla servicios prestados por el sistema.
Software / Aplicaciones Informáticas	Se refiere a tareas que han sido automatizadas para su desempeño por un equipo informático. Las aplicaciones gestionan, analizan y transforman los datos permitiendo la explotación de la información para la prestación de los servicios.
Equipos Informáticos	Son los medios materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización, siendo pues depositarios

	temporales o permanentes de los datos, soporte de ejecución de las aplicaciones informáticas o responsables del procesado o la transmisión de datos.
Redes de Comunicacion	Incluyendo tanto instalaciones dedicadas como servicios de comunicaciones contratados a terceros; pero siempre centrándose en que son medios de transporte que llevan datos de un sitio a otro.
Soporte de Información	Dispositivos físicos que permiten almacenar información de forma permanente o, al menos, durante largos periodos de tiempo.
Equipamiento Auxiliar	En este epígrafe se consideran otros equipos que sirven de soporte a los sistemas de información.
Instalaciones	En este epígrafe entran los lugares donde se hospedan los sistemas de información y comunicaciones
Personal	Personas relacionadas con los sistemas de información

Fuente: (MARGERIT, 2012)

Luego de verificar la clasificación de activos que nos proporciona margerit tal como se muestra en la tabla 20 se procedio a identificar los activos de información del Municipio del Centro Poblado de Salcedo – Puno, para lo cual se identificaron a través de la ejecución de un cuestionario (ver ANEXO B). En la siguiente tabla se muestra los resultados encontrados al ejecutar dicho cuestionario.

Tabla 21

Inventario de Activos de Información

Fuente: Elaboración del Estudio.

Nombre del activo	Descripción del activo	Tipo de Activo	Ubicación
Datos vitales	Datos que almacenan los diferentes sistemas de información esenciales para el funcionamiento de la Municipalidad	Dato/Información.	Data Center.
Archivos Personales	Documentos personales de los trabajadores de la Municipalidad	Dato/Información.	Computadoras Personales.
Copias de Respaldo	Copias de respaldo de los datos/información que manejan los distintos sistemas de la Municipalidad	Dato/Información.	Data Center/PC Administrador.

Datos de Configuración de los Sistemas de Información	Corresponde a los documentos, manuales y procedimientos relacionados con la administración de los diferentes sistemas de información	Dato/Información.	Archivo físico (estantería).
Datos de Gestión interna	Corresponde a los documentos de la Municipalidad	Dato/Información.	Archivo físico (estantería)/ VPS.
Código fuente de los sistemas de información	Corresponde a los códigos fuente de los distintos sistemas desarrollados en Municipalidad	Dato/Información.	Servidores de Versiones (en la nube).
Servicios online	Corresponde a los servicios de consulta como, por ejemplo: Portal de transparencia, Foro Municipal, consulta de visita a funcionarios.	Servicio.	Página Web de la Municipalidad.
Correo electrónico	Correo electrónico institucional.	Servicio.	Servidor de correo GMAIL
Página Web	Página Web de la entidad	Software/Aplicaciones informática	VPS
Sistema de trámite documentario	Sistema para la gestión de trámite externo e interno, utilizado por la unidad de trámite documentario y archivos.	Software/Aplicaciones informática..	Servidor de aplicaciones Windows
SIAF	Sistema que manejan la oficina de administración y Finanzas y Planeamiento y Presupuesto.	Software/Aplicaciones informática	Servidor SIAF
Sistema Gestor de Base de Datos	Sistema de gestión y administración de las bases de datos de la entidad.	Software/Aplicaciones informática.	PC de los administradores
Aplicaciones Comerciales	Office, sistemas operativos, antivirus, entre otros.	Software/Aplicaciones Informática.	Computadoras Personales
Servidores de aplicaciones de Producción	Servidores de producción que soportan las aplicaciones y sistemas de información.	Equipos informáticos.	Data Center de la Municipalidad
Servidores de Base de datos	Servidores de producción que soportan las aplicaciones y sistemas de información.	Equipos informáticos.	Data Center de la Municipalidad
Computador del Funcionario	Computadores que utilizan los funcionarios de la entidad.	Equipos informáticos.	SG de Sistemas y Tecnología

Fuente: Elaboración del Estudio.

3.3.1.2. Valoración de activos

La valoración de los activos se realizó teniendo en consideración aspectos como: el económico, el legal y la imagen; aspectos que afectan a los activos en sus dimensiones de confidencialidad, integridad y disponibilidad, como se muestra en la siguiente Tabla 22:

Tabla 22

Criterio de Valoración de Activos de Información

Aspectos	Descripción	Criterio de Calificación	Valoración
Económico (E)	**Perdidas Económicas para la Municipalidad**	Pérdidas económicas excepcionalmente elevadas	5
		Causa de pérdidas económicas elevadas	4
		Causa de graves pérdidas económicas	3
		Causa de pérdidas financieras o merma de ingresos	2
		Supondría pérdidas económicas mínimas	1
Legal (L)	**Incumplimiento de Leyes y Normas**	Probablemente cause un incumplimiento excepcionalmente grave de una ley o regulación.	5
		Probablemente cause un incumplimiento grave de una ley o regulación.	4
		Probablemente sea causa de incumplimiento de una ley o regulación.	3
		Probablemente sea causa de incumplimiento leve o técnico de una ley o regulación.	2
		Pudiera causar el incumplimiento leve o técnico de una ley o regulación	1
Imagen (IMG)	**Afecta a la Imagen de la Municipalidad**	Probablemente causaría una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones a con otras organizaciones	5
		Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones	4

	con otras organizaciones	
	Probablemente sea causa una cierta publicidad negativa por afectar negativamente a las relaciones con otras organizaciones	3
	Probablemente afecte negativamente a las relaciones internas de la organización	2
	Pudiera causar una pérdida menor de la confianza dentro de la Organización	1

Fuente: Adaptado de "Diseño de un sistema de gestión de seguridad de la información para una entidad financiera de segundo piso", p.85, (Guzmán Silva, 2015)

Además, se realizaron preguntas con el objeto de determinar la criticidad del activo de información, como se puede apreciar en la siguiente tabla 23:

Tabla 23

Preguntas para determinar la Criticidad del Activo de Información

Parámetro	Aspecto	Pregunta
Confidencialidad	**Económico**	¿Su divulgación no autorizada puede relevar información sensible de la empresa requerida para la toma de decisiones estratégicas y financieras causando pérdida económica?
	Legal	¿Su divulgación no autorizada puede afectar el cumplimiento de leyes o normas impartidas por entes de control?
	Imagen	¿Su divulgación no autorizada puede afectar la imagen de la entidad?
Integridad	**Económico**	¿Si el activo o la información que se gestiona a través de él son alterados sin autorización puede generar pérdidas económicas para la entidad?
	Legal	¿Si el activo o la

		información que se gestiona a través de él son alterados sin autorización puede generar sanciones de entes de control?
	Imagen	¿Si el activo o la información que se gestiona a través de él son alterados sin autorización puede afectar la imagen de la entidad?
Disponibilidad	**Económico**	¿Si el activo o información que se gestiona a través de él no están disponibles puede generar pérdidas económicas para la entidad?
	Legal	¿Si el activo o la información que se gestiona a través de él no están disponibles puede generar sanciones legales de entes de control?
	Imagen	¿Si el activo o la información que se gestiona a través de él no están disponibles puede afectar a la imagen de la entidad?

Fuente: Adaptado de "Diseño de un sistema de gestión de seguridad de la información para una entidad financiera de segundo piso", p.86, (Guzmán Silva, 2015)

Finalmente, para poder determinar adecuadamente el nivel de criticidad del activo valorado, se usó el criterio establecido en la Tabla 24. De esta manera se determinó la importancia de los activos de información dentro del proceso: gestión de la infraestructura tecnológica.

Tabla 24

Nivel de Criticidad de los Activos de Información

Criterio de evaluación	Valor	Nivel
El activo de información compromete en un nivel alto la integridad y/o confidencialidad y/o disponibilidad de la información de la Municipalidad	**3<VF<=5**	**Alto**
El activo de información compromete en un nivel medio la integridad y/o confidencialidad y/o disponibilidad de la información de la Municipalidad.	**VF=3**	**Medio**

El activo de información compromete en un nivel bajo la integridad y/o confidencialidad y/o disponibilidad de la información de la Municipalidad.	**0<VF<3**	**Bajo**

Fuente: Adaptado de "Diseño de un sistema de gestión de seguridad de la información para una entidad financiera de segundo piso", p. 86, Guzmán Silva. 2015.

Para la Municipalidad del Centro Poblado de Salcedo Puno

En la siguiente tabla 25 se muestra la valoración de los activos de información y su nivel de Criticida

Tabla 25

Valoración de Activos de Información y Nivel de Criticidad

Nº	Nombre del activo	Confidencialidad			Integridad			Disponibilidad			VFC	VFI	VFD	VF	Nivel de criticidad
		E	L	IMG	E	L	IMG	E	L	IMG					
1	Copias de Respaldo	5	4	4	4	4	5	4	4	5	4	4	4	4	ALTO
2	Datos de Configuración de los Sistemas de Información	2	3	2	3	2	2	2	2	2	2	2	2	2	BAJO
3	Datos de Gestión interna	5	4	4	4	5	4	5	4	4	4	4	4	4	ALTO
4	Credenciales (contraseñas)	4	5	4	5	5	4	5	4	4	4	5	4	4	ALTO
5	Datos de control de acceso	4	5	5	4	4	4	4	5	4	5	4	4	4	ALTO
6	Log de los sistemas de información	4	3	4	4	3	4	4	4	3	4	4	4	4	ALTO
7	Código fuente de los sistemas de información	5	5	5	5	5	4	5	4	5	5	5	5	5	ALTO
8	Código ejecutable	3	4	3	2	2	1	3	2	3	3	2	3	3	MEDIO
9	Correo electrónico	4	4	4	3	2	2	3	3	4	4	2	3	3	MEDIO
10	Gestión de privilegios	5	4	5	5	5	5	3	3	3	5	5	3	4	ALTO
11	Base de Datos	4	4	4	5	5	5	4	4	4	4	5	4	4	ALTO
12	Página Web	1	1	2	2	1	2	1	3	3	1	2	2	2	BAJO
13	Sistema de trámite documentario	1	4	3	4	3	2	5	3	3	3	3	4	3	MEDIO
14	Sistema de Patrimonio	5	5	5	5	5	4	4	3	4	5	5	4	4	ALTO
15	SIAF	5	5	4	5	5	4	5	5	5	5	5	5	5	ALTO
16	Sistema de Rentas	4	4	5	4	5	5	5	5	5	4	5	5	5	ALTO
17	Sistema New Gestión de Logística	4	5	5	5	4	4	5	5	5	5	4	5	5	ALTO

19	Scripts de Backup	2	3	2	2	2	3	2	3	2	2	2	2	2	BAJO
20	Servidores de aplicaciones	5	5	4	5	5	5	5	4	5	5	5	5	5	ALTO
21	Servidor de Base de Datos	5	5	5	5	5	5	5	5	5	5	5	5	5	ALTO
24	Computador del funcionario	3	4	3	3	4	5	4	5	4	3	4	4	4	ALTO
25	Computadores administradores de SI	4	4	5	5	4	4	4	4	4	4	4	4	4	ALTO
26	Computadores de escritorio usuarios	2	3	3	2	2	3	3	3	3	3	2	3	3	MEDIO
27	Impresoras	1	2	1	2	1	1	2	1	2	1	1	2	1	BAJO
28	Firewall	4	4	4	4	5	3	5	4	4	4	4	4	4	ALTO
29	Soporte de la red	3	1	1	2	2	2	2	2	3	2	2	2	2	BAJO
30	Centralita telefónica	2	3	3	2	2	1	2	3	3	3	2	3	2	BAJO
31	Red inalámbrica	3	2	2	2	3	1	2	1	3	2	2	2	2	BAJO
32	Red local	2	1	2	2	3	1	3	2	3	2	2	3	2	BAJO
33	Internet	1	2	1	2	1	1	3	3	3	1	1	3	2	BAJO

Fuente: Elaboración del Estudio. E=Económico, L=Legal, IMG=Imagen, VFC=Valor final de confiabilidad, VFI=Valor final de integridad, VFD=Valor final de disponibilidad, VF=Valor final del activo de información.

Para aclarar la tabla anterior Tabla 25. Valoración de Activos de Información y Nivel de Criticidad, se especifican algunos datos, que se consignan en la tabla:

- El valor de la columna VFC (Valor Final de Confiabilidad), corresponde al promedio de los valores de los aspectos: económico, legal e imagen, que afectan a la seguridad del activo en su dimensión de confiabilidad. Este mismo criterio se siguió para obtener los valores de VFI (Valor Final de Integridad) y VFD (Valor Final de Disponibilidad) cada uno dentro de la dimensión que le corresponde.
- El valor de VF (Valor Final del activo de información), es el promedio de los valores: VFC, VFI y VFC.

De la tabla anterior se escogen únicamente los activos de información con nivel de criticidad ALTO y MEDIO, y, agruparlos por los activos que los contienen, como se puede apreciar en la siguiente tabla.

Tabla 26

Activos por Contenedor

N°	Nombre del activo	Nivel de criticidad	Contenedor
1	**Sistema New Gestión de Logística**	ALTO	Data Center
2	**Servidores de aplicaciones**	ALTO	
3	**Servidor de Base de Datos**	ALTO	
4	**Firewall**	ALTO	
5	**Código ejecutable**	MEDIO	Servidor de Aplicaciones / SIAF
6	**Sistema de trámite documentario**	MEDIO	
7	**Sistema de Patrimonio**	ALTO	
8	**SIAF**	ALTO	
9	**Sistema de Rentas**	ALTO	
10	**Datos de Gestión interna**	ALTO	Servidor de Base de Datos/Usuario Interno
11	**Datos de control de acceso**	ALTO	Servidor de Base de Datos/Usuario Interno
12	**Base de Datos**	ALTO	Servidor de Base de datos
13	**Copias de Respaldo**	ALTO	Servidores/Disco Duro/PC Administrador
14	**Log de los sistemas de información**	ALTO	Log de Eventos del Servidor
15	**Correo electrónico**	MEDIO	Servidor de Correo Electrónico del Proveedor
16	**Gestión de privilegios**	ALTO	Recursos tecnológicos y aplicaciones
17	**Credenciales (contraseñas)**	ALTO	PC Administrador
18	**Código fuente de los sistemas de información**	ALTO	PC desarrollador/Servidor de Aplicaciones
19	**Computador del funcionario**	ALTO	Local del Municipio
20	**Computadores administradores de SI**	ALTO	
21	**Computadores de escritorio usuarios**	MEDIO	

Fuente: Elaboración del Estudio.

De acuerdo a la tabla anterior, se puede determinar los contenedores de activos de información que serán utilizados para el proceso de valoración de riesgos.

Tabla 27

Contenedores

N°	Contenedor
1	Data Center
2	Servidor de Aplicaciones / SIAF
3	Servidor de Base de Datos/Usuario Interno
4	Servidores/Disco Duro/PC Administrador
5	Log de Eventos del Servidor
6	Servidor de Correo Electrónico del Proveedor
7	Recursos tecnológicos y aplicaciones
8	PC Administrador
9	PC desarrollador/Servidor de Aplicaciones
10	Local del Municipio

Fuente: Elaboración del Estudio.

3.3.1.3. Identificación de Amenazas

Se presenta la lista de las amenazas de acuerdo al catálogo de amenazas contemplado en MARGERIT v.3 (ver ANEXO C). Para la identificación de las amenazas se trabajó coordinadamente con el personal del Área de Informática y Procesamiento de Datos de la Municipalidad del centro Poblado de Salcedo – Puno, quienes, de acuerdo a su experiencia y conocimientos de la Infraestructura tecnológica y los servicios en la Municipalidad, en conjunto se determinaron las amenazas que afectan a los activos de información identificados en la tabla anterior y se estimó una probabilidad de ocurrencia de estas amenazas.

El criterio tomado para la estimación de la probabilidad de ocurrencia de la amenaza se detalla en la tabla siguiente:

Tabla 28

Probabilidad de Ocurrencia de Amenazas

Criterio	Valor	Puntuación
Más de 2 años	Prácticamente Imposible	1
Anual	Poco Probable	2
Trimestral	Posible	3
Mensual	Probable	4
A diario	Muy probable	5

Fuente: Elaboración del Estudio.

En la siguiente tabla se muestra la identificación de las amenazas, la dimensión de su afectación al activo de información y además la probabilidad de ocurrencia de la misma.

Tabla 29

Identificación de Amenazas

Código	Amenaza	Dimensiones Afectadas			Probabilidad de ocurrencia
		C	I	D	
1	Fuego			1	2
2	Tormenta eléctrica, rayos			1	4
3	Error de Usuario	3	1	3	3
4	Errores del administrador	3	3	1	3
5	Errores de configuración		1		3
6	Alteración accidental de la información		1		2
7	Eliminación accidental de Información		1	1	3
8	Fugas de Información			1	4
9	Vulnerabilidades de los programas (software)	3	1	2	2
10	Errores de mantenimiento/actualización de programas (software)		1	2	3
11	Errores de mantenimiento/actualización de equipos (hardware)			1	4
12	Indisponibilidad del personal por enfermedad			1	4
13	Manipulación de los registros de Actividad (log)		1	2	2
14	Suplantación de la identidad del usuario	1	2	1	2
15	Abuso de privilegios de acceso	1	2	2	4
16	Difusión de software dañino	2	2	1	4
17	Acceso no autorizado	1	2		2
18	Destrucción deliberada de Información		1	1	2
19	Manipulación de programas	2	1	2	3
20	Caída del sistema por agotamiento de recursos			1	4
21	Robo de Equipos	2		1	2
22	Indisponibilidad del personal por huelga			1	2

23	Ejecución de ingeniería social	1	2	3	**3**
24	Corte del suministro eléctrico			1	**4**
25	Condiciones inadecuadas de temperatura o humedad			1	**3**
26	Degradación de los soportes de almacenamiento de la información			1	**2**
27	Instalación de software no autorizado	1	2		**4**
28	Inestabilidad de la línea de internet			1	**4**

Fuente: Elaboración del Estudio.

Nota: Las amenazas pueden afectar a los activos de información en uno, dos, o sus tres dimensiones de seguridad. Para efectos de esta investigación, se muestra la(s) dimensión(es) de seguridad afectada en orden de relevancia, donde 1 es muy relevante, 2 medianamente relevante y 3 poco relevante.

Debe estar claro que no todas las amenazas afectan a todos los activos de información, es por esta razón que se clasificaron las amenazas por activo de información. Finalmente se valoró la degradación del activo de información de acuerdo al criterio mostrado en la siguiente tabla:

Tabla 30

Criterio para valorar la Degradación del Activo de Información

Criterio	Valor
Sin degradación(SD)	1
Degradación baja (B)	2
Degradación media(M)	3
Degradación alta (A)	4

Fuente: Elaboración del Estudio.

Tabla 31

Degradación de los activos: Data Center y SIAF

DATA CENTER				
Amenazas	**Probabilidad**	**Degradación Confidencialidad**	**Degradación Integridad**	**Degradación Disponibilidad**
Fuego	2	1	1	4
Tormenta eléctrica, rayos	4	1	1	4
Errores del administrador	2	1	2	4
Suplantación de la identidad del usuario	2	4	2	3
Abuso de privilegios de acceso	4	3	3	1
Acceso no autorizado	2	4	2	1
Robo de Equipos	2	2	1	4
Corte del suministro eléctrico	4	1	4	4
Condiciones inadecuadas de temperatura o humedad	3	1	4	4

SIAF				
Amenazas	**Probabilidad**	**Degradación Confidencialidad**	**Degradación Integridad**	**Degradación Disponibilidad**
Error de Usuario	3	3	3	1
Errores del administrador	3	1	2	4
Errores de configuración	3	1	4	1
Errores de mantenimiento/actualización de programas	4	1	3	1

(software)				
Indisponibilidad del personal por enfermedad	4	1	1	3
Suplantación de la identidad del usuario	2	4	1	3
Abuso de privilegios de acceso	4	4	2	1
Acceso no autorizado	2	4	3	1
Caída del sistema por agotamiento de recursos	4	1	1	4
Corte del suministro eléctrico	4	1	1	4

Fuente: Elaboración del Estudio

3.3.1.4. Calculo del Impacto

En este ítem, se calculó el impacto, que viene dado en función del valor del activo y la degradación que producirá la amenaza en caso de materializarse. Para ello se estableció el siguiente criterio:

Tabla 32

Criterios para calcular el Impacto

Degradación de la amenaza	Valor del activo				
	1	2	3	4	5
1 (Sin degradación)	1	1	1	1	1
2 (Degradación baja)	1	2	2	3	4
3 (degradación media)	1	2	3	4	4
4 (degradación alta)	1	3	4	4	5

Fuente: Elaboración del Estudio.

Tabla 33

Valor del Impacto

Valor	Descripción
1	Insignificante
2	Menor
3	Medio
4	Crítico
5	Catastrófico

Fuente: Elaboración del Estudio.

3.3.1.5. Calculo del Riesgo

Se calcula el riesgo en función del impacto que se producirá sobre el activo de información en el caso de materializarse y de la probabilidad de materialización.

El riesgo crece con el impacto y con la probabilidad, pudiendo distinguirse una serie de zonas a tener en cuenta en el tratamiento del riesgo. Para la presente investigación se elaboró la siguiente matriz de evaluación de riesgos:

Tabla 33

Matriz de evaluación de riesgos

Impacto		Matriz de evaluación de riesgos				
Catastrófico	5	15	19	22	24	25
Crítico	4	10	14	18	21	23
Medio	3	6	9	13	17	20
Menor	2	3	5	8	12	16
Insignificante	1	1	2	4	7	11
		1	2	3	4	5
		Prácticamente imposible	**Poco probable**	**Posible**	**Probable**	**Muy Probable**
		PROBABILIDAD (DE LA AMENAZA) = FUTURO				

Fuente: Elaboración del Estudio.

Los niveles de riesgo fueron asignados de acuerdo al siguiente criterio:

Tabla 34

Niveles de Riesgo

Criterio	Nivel
17<Nivel de riesgo<=25	Alto
8<Nivel de riesgo<=17	Medio
0<Nivel de riesgo<=8	Bajo

Fuente: Elaboración del Estudio.

A continuación, se muestra el resultado de la valoración de riesgos para los activos Data Center y SIAF.

Tabla 35

Impacto y riesgo para el Data Center y SIAF

DATA CENTER										
Amenazas		**Degradación**			**Impacto**			**Estimación del Riesgo**		
	Probabilidad	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Confidencialidad**	**Integridad**	**Disponibilidad**
Fuego	2	1	1	4	Insignificante	Insignificante	Crítico	Bajo	Bajo	Medio
Tormenta eléctrica, rayos	4	1	1	4	Insignificante	Insignificante	Crítico	Bajo	Bajo	Alto
Errores del administrador	2	1	2	4	Insignificante	Menor	Crítico	Bajo	Medio	Alto
Suplantación de la identidad del usuario	2	4	2	3	Crítico	Menor	Medio	Alto	Medio	Medio
Abuso de privilegios de acceso	4	3	3	1	Medio	Medio	Insignificante	Medio	Medio	Bajo
Acceso no autorizado	2	4	2	1	Crítico	Menor	Insignificante	Medio	Medio	Bajo
Robo de Equipos	2	2	1	4	Menor	Insignificante	Crítico	Bajo	Bajo	Alto
Corte del suministro eléctrico	4	1	4	4	Insignificante	Crítico	Crítico	Bajo	Alto	Alto
Condiciones inadecuadas de temperatura o humedad	3	1	4	4	Insignificante	Crítico	Crítico	Bajo	Alto	Alto
SIAF										

Error de Usuario	3	3	3	1	Medio	Medio	Insignificante	Medio	Bajo	Bajo
Errores del administrador	3	1	2	4	Insignificante	Menor	Crítico	Bajo	Bajo	Medio
Errores de configuración	3	1	4	1	Insignificante	Crítico	Insignificante	Bajo	Alto	Bajo
Errores de mantenimiento/actualización de programas (software)	4	1	3	1	Insignificante	Medio	Insignificante	Bajo	Medio	Bajo
Indisponibilidad del personal por enfermedad	4	1	1	3	Insignificante	Insignificante	Medio	Bajo	Bajo	Medio
Suplantación de la identidad del usuario	2	4	1	3	Crítico	Insignificante	Medio	Medio	Bajo	Medio
Abuso de privilegios de acceso	4	4	2	1	Crítico	Menor	Insignificante	Alto	Medio	Bajo
Acceso no autorizado	2	4	3	1	Crítico	Medio	Insignificante	Medio	Medio	Bajo
Caída del sistema por agotamiento de recursos	4	1	1	4	Insignificante	Insignificante	Crítico	Bajo	Bajo	Alto
Corte del suministro eléctrico	4	1	1	4	Insignificante	Insignificante	Crítico	Bajo	Bajo	Alto

Fuente: Elaboración del Estudio

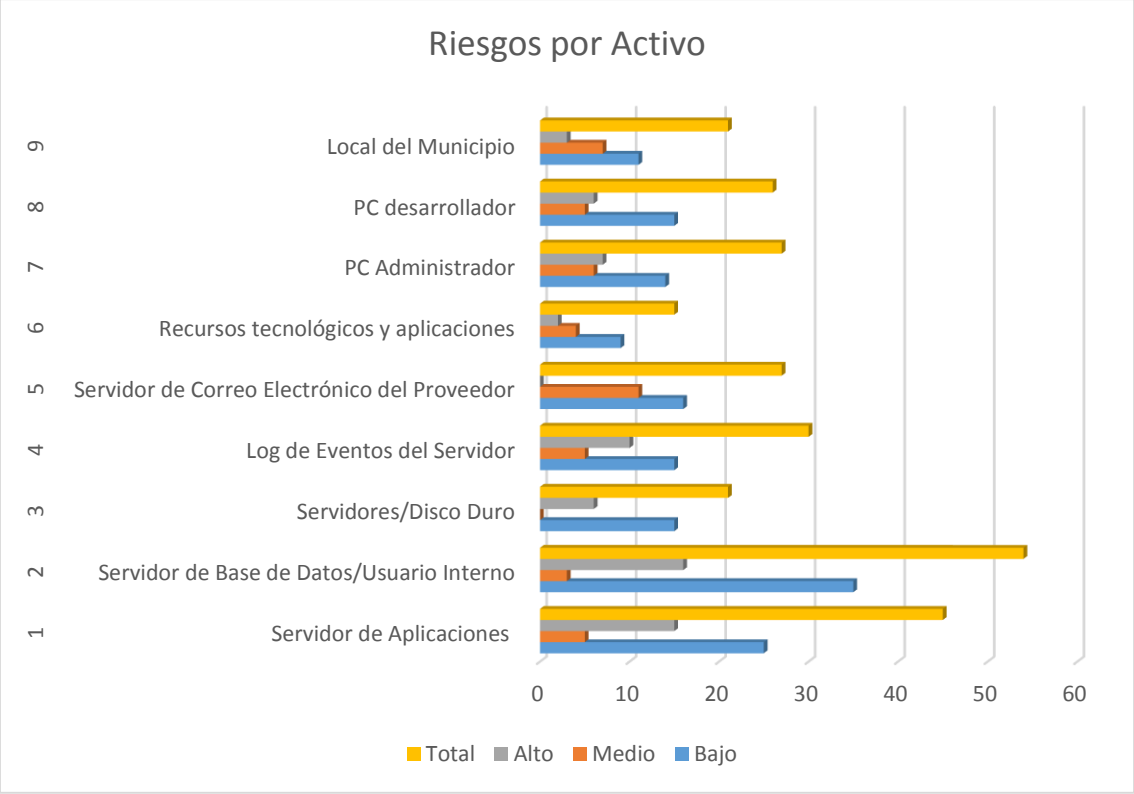

Figura 21. Riesgos por Activo
Fuente: Elaboración del Estudio.

Como se puede apreciar en la figura anterior, es que los activos de información con mayores probabilidades de riesgo son: El servidor de Base de Datos y el Servidor de Aplicaciones.

3.3.1.6. Tratamiento del Riesgo

Las opciones que se tienen para tratar de acuerdo a la naturaleza del riesgo son:

Tabla 36

Jerarquía de Controles

Tratamiento	Descripción
Eliminar	Una de las alternativas más difíciles de implementar y más costosas ya que puede implicar la eliminación de un activo, proceso o del área del negocio que es fuente de riesgo.

Transferir	El riesgo fuera del apetito del riesgo se comparte con una o varias partes, pueden ser agentes externos.
Mitigar	Reducir el riesgo cuando se encuentra fuera del apetito del riesgo, se puede cambiar la probabilidad de ocurrencia o cambiar las consecuencias.
Asumir	En este escenario se decide aceptar el riesgo cuando no es posible mitigarlo y se debe continuar la actividad que lo originó.

Fuente: Adaptado de "Diseño de un sistema de gestión de seguridad de información para una empresa inmobiliaria alineado a la norma ISO/IEC 27001:2013", p.50, (Justino Salinas, 2015)

Se aclara que, para los riesgos de nivel medio y alto, se aplicaran controles, que ayuden a reducir el riesgo producido por las amenazas a un nivel aceptable, en las dimensiones afectadas y para los riesgos de nivel bajo, se establecerá como máximo riesgo asumible. Los riesgos de nivel alto serán priorizados y se aplicarán con urgencia todas las medidas de seguridad posibles.

A continuación, se muestra los controles para reducir los riesgos de los activos con mayor probabilidad de riesgos como son: Servidor de Base de Datos, Data Center y Servidor de Aplicaciones. Cabe mencionar que en funciona a las amenazas identificadas se proponen los controles que ayudarán a reducir los riesgos a un nivel aceptable.

Tabla 37

Controles para el tratamiento de riesgos del Servidor de Base de Datos

Activo y valoración				Amenaza, vulnerabilidad y riesgo		Análisis y evaluación del riesgo			Tratamiento del riesgo			
						Estimación del Riesgo						
Nombre del Activo	Confidencialidad	Integridad	Disponibilidad	Amenaza	Vulnerabilidad	Confidencialidad	Integridad	Disponibilidad	Jerarquía de Control	Control alineado a la NTP ISO/IEC 27001:2014	Control Específico	Responsable
Servidores de Bases de Datos	5	5	5	Errores del administrador	No existe un plan/manual de las BDs que se manejan y sus requerimientos técnicos, ausencia de procedimientos de control de cambios, desmotivación	Bajo	Bajo	Alto	Mitigar	A.8.2 Clasificación de la información. A.12.4.3 Registros del administrador y del operador.	Manual de sistemas y requerimientos técnicos. Elaboración de un procedimiento formal de control de cambios. Elaboración de un procedimiento formal de manejo de servidores Capacitación en temas de seguridad.	Area de Informática y Procesamiento de Datos
				Errores de configuración	Inexistencia de plan de configuración y manejo de log	Bajo	Alto	Bajo	Mitigar	A.12.4.3 Registros del administrador y del operador. A.12.4.1 Registro de eventos.	Elaboración del manual de configuración de servidores. Actualización de log de eventos.	Area de Informática y Procesamiento de Datos

Alteración accidental de la información	Inexistencia de normas de seguridad, mala configuración de roles y permisos.	Bajo	Bajo	Alto	Mitigar	A.8.2 Clasificación de la información. A.12.4.3 Registros del administrador y del operador.	Control de versiones del software.	Area de Informática y Procesamiento de Datos
						A.12.4.3 Registros del administrador y del operador.	Procedimiento formal de control de cambios.	
						A.12.4.1 Registro de eventos.	Verificación de roles y permisos.	
Eliminación accidental de Información	Inexistencia de normas de seguridad y plan de contingencia.	Bajo	Alto	Bajo	Mitigar	A.8.2 Clasificación de la información.	Control de versiones del software.	Area de Informática y Procesamiento de Datos
						A.12.4.3 Registros del administrador y del operador.	Procedimiento formal de control de cambios.	
						A.12.4.1 Registro de eventos.	Verificación de roles y permisos.	
Fugas de Información	Inadecuada administración de seguridad, contraseñas no seguras, inexistencia de los de eventos de seguridad.	Alto	Bajo	Bajo	Mitigar	A. 12.4.3 Registros del administrador y del operador.	Establecimiento de métodos de cifrado y Backup.	Area de Informática y Procesamiento de Datos
						A.7.2.3 Proceso disciplinario.	Gestión de Permisos. Procedimientos disciplinarios establecidos en los contratos.	
Vulnerabilidades de los programas (software)	Falta de licencia, inexistencia de monitorización de software/versiones.	Bajo	Alto	Bajo	Mitigar	A.14.2.4 Restricción sobre cambios a los paquetes software.	Adquisición de licencia de programas y/o evaluación del uso de software libre. Gestión de vulnerabilidades	Area de Informática y Procesamiento de Datos
						A.16.6.1 Gestión de vulnerabilidades técnicas.		
Errores de mantenimiento/actualización de programas (software)	Falta de licencia, inexistencia de plan de mantenimiento y vigilancia tecnológica.	Bajo	Alto	Bajo	Mitigar	A.16.6.1 Gestión de vulnerabilidades técnicas.	Elaboración de un plan de mantenimiento y actualización de software. Elaboración de un plan de contingencia.	Area de Informática y Procesamiento de Datos

Errores de mantenimiento/actualización de equipos (hardware)	Inexistencia de plan de mantenimiento y vigilancia tecnológica, falta de equipos de contingencia, ausencia de un sistema de continuidad del negocio.	Bajo	Bajo	Alto	Mitigar	A.11.2.4 Mantenimiento de equipos. A.16.6.1 Gestión de vulnerabilidades técnicas	Elaboración de un Plan de contingencia – Equipos de contingencia. Plan de mantenimiento de hardware	Area de Informática y Procesamiento de Datos
Manipulación de los registros de Actividad (log)	Inexistencia de auditorías a las cuentas de usuario, inexistencia de mecanismos de cifrado.	Bajo	Medio	Bajo	Mitigar	A.12.4.2 Protección de información de registros.	Establecer controles para evitar accesos no autorizados la información de los registros. Mecanismos de cifrado.	Area de Informática y Procesamiento de Datos
Abuso de privilegios de acceso	Falta de políticas de acceso y auditorías internas. (cuentas de usuario sin auditar)	Alto	Bajo	Bajo	Mitigar	A.7.2.3 Proceso disciplinario. A.9.4.1 Restricción de acceso a la información.	Elaboración de políticas de acceso. Diseñar esquemas de seguridad basado en roles y permisos Diseñar un esquema de privilegios sobre el fileserver.	Area de Informática y Procesamiento de Datos/ Jefe de RR.HH.
Difusión de software dañino	Falta de monitoreo del estado y reglas del firewall y antivirus, inadecuada asignación de roles y permisos, no existe políticas de seguridad.	Bajo	Alto	Alto	Mitigar	A.12.2.2 Controles contra códigos maliciosos. A.16.6.2 Restricción sobre la instalación de software.	Plataforma de seguridad perimetral. Control de la red. Control de instalación de software.	Area de Informática y Procesamiento de Datos

							Actualización de antivirus (monitorización)	
Acceso no autorizado	Falta de monitoreo del estado y reglas del firewall,	Medio	Bajo	Bajo	Mitigar	A.14.2.8 Pruebas de seguridad del sistema.	Diseñar esquemas de seguridad basado en roles y permisos Diseñar un esquema de privilegios sobre el Fileserver. Plataforma de seguridad perimetral.	Área de Informática y Procesamiento de Datos
Destrucción deliberada de Información	Administradores de plataformas descontentos inexistencia de un sistema de continuidad del negocio, falta de seguridad en los soportes de red.	Bajo	Bajo	Medio	Mitigar	A.7.2.3 Proceso disciplinario.	Establecimiento de métodos de cifrado y Backup.	Área de Informática y Procesamiento de Datos/ jefe de RR. HH
							Procedimientos disciplinarios establecidos en los contratos	
Caída del sistema por agotamiento de recursos	No existe un monitoreo de consumo de recursos hardware de los sistemas, falta de mantenimiento de equipos.	Bajo	Bajo	Alto	Mitigar	A.11.2.3 Seguridad del cableado.	Plataforma de seguridad perimetral.	Área de Informática y Procesamiento de Datos
						A.13.1.3 Segregación en redes.	Elaboración de un Plan de contingencia – monitoreo preventivo de consumo de recursos Hardware de los sistemas.	Área de Informática y Procesamiento de Datos
Corte del suministro eléctrico	Susceptibilidad a las variaciones de tensión.	Bajo	Bajo	Alto	Mitigar	A.11.2.2 Servicios de suministro.	Contar con sistema de alimentación ininterrumpida.	Área de Informática y Procesamiento de Datos

							Mantenimiento de sistema de alimentación ininterrumpida.	
Condiciones inadecuadas de temperatura o humedad	Susceptibilidad a humedad, recalentamiento, polvo y suciedad	Bajo	Bajo	Alto	Mitigar	A.11.2.1 Emplazamiento y protección de los equipos.	Ubicación adecuada de equipos según estándares internacionales.	Área de Informática y Procesamiento de Datos
						A.11.2.4 Mantenimiento de equipos.	Plan de mantenimiento de equipos.	
Degradación de los soportes de almacenamiento de la información	Equipos/dispositivos susceptibles a cambios de temperatura y humedad, falta de esquemas de reemplazo.	Bajo	Bajo	Alto	Mitigar	A.11.2.4 Mantenimiento de equipos.	Plan de mantenimiento de soportes de información. Inventario de activos y monitoreo del funcionamiento y tiempo de vida.	Área de Informática y Procesamiento de Datos

	Inestabilidad de la linea de internet	Un solo proveedor de servicios de comunicaciones, gestión inadecuada de la red.	Bajo	Bajo	Alto	Mitigar	A.13.1.2 Seguridad de servicios de red.	Plan de contingencia- Uso de varias lineas dedicadas y redundancia de servicios con diversos proveedores del servicio. – balanceo de carga. Acuerdos de nivel de servicio con el(los) proveedor(es) de comunicaciones.	Area de Informática y Procesamiento de Datos

Fuente: Elaboración del Estudio.

Tabla 38

Controles para el tratamiento de riesgos del Data Center

Activo y valoración				Amenaza, vulnerabilidad y riesgo		Análisis y evaluación del riesgo			Tratamiento del riesgo			
						Estimación del Riesgo						
Nombre del Activo	Confidencialidad	Integridad	Disponibilidad	Amenaza	Vulnerabilidad	Confidencialidad	Integridad	Disponibilidad	Jerarquía de Control	Control alineado a la NTP ISO/IEC 27001:2014	Control Específico	Responsable
Data Center	5	5	5	Fuego	Extintores vencidos. Falta de capacitación en uso de extintores, ausencia de un sistema de continuidad del negocio, falta de mecanismos de respaldo de información.	Bajo	Bajo	Medio	Mitigar	A.11.1.4 Protección contra amenazas externas y ambientales.	Uso de estándar para el diseño de un Data Center Compra de extintores y capacitación al personal. Instalación de detectores de humo. Plan de contingencia.	Área de Informática y Procesamiento de Datos
				Tormenta eléctrica, rayos	Ausencia de un sistema de continuidad de negocio.	Bajo	Bajo	Alto	Mitigar	A.11.1.4 Protección contra amenazas externas y ambientales.	Uso de estándar para el diseño de un Data Center Pozo a tierra, pararrayos. UPS para dispositivos críticos. Mantenimiento de grupos electrógenos.	Área de Informática y Procesamiento de Datos
				Errores del administrador	Falta de capacitación. Mala segregación de funciones, desmotivación del personal.	Bajo	Medio	Alto	Mitigar	A.11.1.2 Controles de ingreso físico. A.11.1.5 Trabajo en áreas seguras.	Elaborar un plan de seguridad. Capacitaciones en temas de seguridad. Verificación de funciones.	Área de Informática y Procesamiento de Datos

	Suplantación de la identidad del usuario	Usuarios confiados, no hay un registro de quién entra y qué hace en el Data Center.	Alto	Medio	Bajo	Mitigar	A.9.3.1 Uso de información de autentificación secreta. A.11.1.2 Controles de ingreso físico.	Buenas prácticas en el uso de información de autentificación secreta. Implementar control de acceso restringido y controlar las tareas que se realizan dentro del Data Center.	Área de Informática y Procesamiento de Datos
	Abuso de privilegios de acceso	Mala segregación de funciones, administradores descontentos.	Alto	Alto	Bajo	Mitigar	A.7.2.3 Proceso disciplinario A.11.1.2 Controles de ingreso físico.	Correcta segregación de funciones. Términos y condiciones de contrato claros en temas de seguridad.	Jefe de Recursos Humanos
	Acceso no autorizado	Usuarios confiados, no hay un registro de quién entra y qué hace en el Data Center.	Medio	Medio	Bajo	Mitigar	A.11.1.2 Controles de ingreso físico. A.11.1.3 Asegurar oficinas, áreas e instalaciones.	Instalación de cámaras de video vigilancia. Implementación de un control de acceso seguro (biométrico, etc.)	Área de Informática y Procesamiento de Datos
	Robo de Equipos	No hay un registro de quién entra y qué hace en el Data Center, no existe inventario de activos, ausencia o inadecuada plataforma de vigilancia.	Medio	Bajo	Bajo	Mitigar	A.11.1.3 Asegurar oficinas, áreas e instalaciones.	Instalación de cámaras de video vigilancia. Inventario de activos de información del Data Center.	Área de Informática y Procesamiento de Datos
	Corte del suministro eléctrico	Falta de algunos UPS.	Bajo	Bajo	Alto	Mitigar	A.11.1.4 Protección contra amenazas externas y ambientales.	Adquisición de equipos alimentación ininterrumpida para equipos críticos del Data Center. Mantenimiento de equipos de alimentación ininterrumpida. Acuerdos de niveles de	Área de Informática y Procesamiento de Datos

	Condiciones inadecuadas de temperatura o humedad	No se monitoriza las condiciones de temperatura y humedad	Bajo	Bajo	Alto	Mitigar	A.11.1.4 Protección contra amenazas externas y ambientales.	servicio con Electrocentro. Monitoreo constante de temperatura del Data Center	Área de Informática y Procesamiento de Datos

Fuente: Elaboración del Estudio.

Tabla 39

Controles para el tratamiento de riesgos del Servidor de Aplicaciones

Activo y valoración				Amenaza, vulnerabilidad y riesgo		Análisis y evaluación del riesgo			Tratamiento del riesgo			
						Estimación del Riesgo						
Nombre del Activo	Confidencialidad	Integridad	Disponibilidad	Amenaza	Vulnerabilidad	Confidencialidad	Integridad	Disponibilidad	Jerarquía de Control	Control alineado a la NTP ISO/IEC 27001:2014	Control Específico	Responsable
Servidores de Aplicación	4	4	5	Errores de configuración	No existe un manual del administrador	Bajo	Medio	Bajo	Mitigar	A.12.3.1 Respaldo de la información A.12.4.3 Registros del administrador y del operador	Elaboración de un manual de administrador. Revisar log de eventos.	Área de Informática y Procesamiento de Datos
				Fugas de Información	Poca fidelización trabajadores, no existe un registro de acceso y manejo de backup	Alto	Bajo	Bajo	Mitigar	A.12.3.1 Respaldo de la información A.12.4.3 Registros del administrador y del operador	Establecimiento de métodos de cifrado. Prevención de la exposición de backups. Almacenamiento en lugares seguros y control de acceso a backups.	Área de Informática y Procesamiento de Datos

Destrucción deliberada de Información	Poca fidelización trabajadores, no existe un registro de acceso y manejo de backup, falta de un plan de contingencia, Ausencia de un sistema de continuidad del negocio	Bajo	Bajo	Medio	Mitigar	A.12.3.1 Respaldo de la información A.12.4.1 Registro de eventos.	Almacenamiento en lugares seguros y control de acceso a backups. evisar log de eventos. Elaboración del plan de contingencia. Elaboración del plan de contingencia.	Área de Informática y Procesamiento de Datos
Errores del administrador	No existe un plan/manual de los sistemas que se manejan y sus requerimientos técnicos, ausencia de procedimientos de control de cambios, desmotivación	Bajo	Medio	Alto	Mitigar	A.8.2 Clasificación de la información A.12.4.3 Registros del administrador y del operador	Manual de sistemas y requerimientos técnicos. Elaboración de un procedimiento formal de control de cambios. Elaboración de un procedimiento formal de manejo de servidores Capacitación en temas de seguridad.	Área de Informática y Procesamiento de Datos
Errores de configuración	Inexistencia de plan de configuración y manejo de log	Bajo	Medio	Bajo	Mitigar	A.12.4.3 Registros del administrador y del operador. A.12.4.1 Registro de eventos.	Elaboración del manual de configuración de servidores. Actualización de log de eventos.	Área de Informática y Procesamiento de Datos
Alteración accidental de la información	Inexistencia de normas de seguridad.	Bajo	Bajo	Alto	Mitigar	A.8.2 Clasificación de la información A.12.4.3 Registros del administrador y del operador. A.12.4.1 Registro de eventos.	Control de versiones del software. Procedimiento formal de control de cambios. Verificación de roles y permisos.	Área de Informática y Procesamiento de Datos

	Eliminación accidental de Información	Inexistencia de normas de seguridad y plan de contingencia.	Bajo	Alto	Bajo	Mitigar	A.8.2 Clasificación de la información A.12.4.3 Registros del administrador y del operador. A.12.4.1 Registro de eventos. de eventos.	Control de versiones del software. Procedimiento formal de control de cambios. Verificación de roles y permisos.	Área de Informática y Procesamiento de Datos
	Vulnerabilidades de los programas (software)	Falta de licencia	Bajo	Alto	Alto	Mitigar	A.14.2.4 Restricción sobre cambios a los paquetes software. A.16.6.1 Gestión de vulnerabilidades técnicas.	Adquisición de licencia de programas y/o evaluación del uso de software libre. Gestión de vulnerabilidades	Área de Informática y Procesamiento de Datos
	Errores de mantenimiento/actualización de programas (software)	Falta de licencia, inexistencia de plan de mantenimiento y vigilancia tecnológica.	Bajo	Alto	Bajo	Mitigar	A.16.6.1 Gestión de vulnerabilidades técnicas	Elaboración de un plan de mantenimiento y actualización de software. Elaboración de un plan de contingencia.	Área de Informática y Procesamiento de Datos
	Errores de mantenimiento/actualización de equipos (hardware)	Inexistencia de plan de mantenimiento y vigilancia tecnológica, falta de equipos de contingencia, ausencia de un sistema de continuidad del negocio.	Bajo	Bajo	Alto	Mitigar	A.11.2.4 Mantenimiento de equipos A.16.6.1 Gestión de vulnerabilidades técnicas	Elaboración de un Plan de contingencia – Equipos de contingencia. Plan de mantenimiento de hardware	Área de Informática y Procesamiento de Datos

Fuente: Elaboración del Estudio.

Capítulo 4 – Resultados y Discusión

4.1. Comprobación de la Prospectiva.

El radio de acción del presente Plan de Seguridad Informática basada en la NTP ISO/IEC 27001:2014, se centra en el Área de Informática y Procesamiento de datos de la Municipalidad del Centro Poblado de Salcedo Puno. En base a la metodología MARGERIT, se ha seguido todo el procedimiento y aplicado la normativa para elaborar el PSI

Uno de los pasos más importantes fue la clasificación de los activos de información que posee la Municipalidad del Centro Poblado de Salcedo Puno, de acuerdo a lo que propone MARGERIT. Seguidamente estos activos de información fueron valorados, para determinar el nivel de criticidad de los mismos, ya que es importante determinar el nivel de importancia que tiene cada activo en los procesos del negocio de la Municipalidad del Centro Poblado de Salcedo Puno.

La identificación de las amenazas es otro proceso valioso para la elaboración del PSI, ya que gracias a estos datos se pudo hacer el cálculo del impacto y del riesgo respectivamente, para que se tenga asegurada el tratamiento del riesgo identificado para cada activo de información. El tratamiento consta de ajustar los controles que te provee la norma para reducir al mínimo el riesgo y sobre todo su impacto que podría ser perjudicial al dejar desencadenarse en los activos de información de la Municipalidad del Centro Poblado de Salcedo Puno.

Las políticas expresadas en este PSI y los controles seleccionados para mitigar los riesgos, son de obligatorio cumplimiento para todo el personal de la Municipalidad del Centro Poblado de Salcedo Puno.

4.2. Cumplimiento de Objetivos.

Se diseñó un Plan de Seguridad Informática basado en la NTP-ISO/IEC 27001:2014, para que con su aplicación se pueda mitigar o disminuir el impacto de los riesgos a los que están expuestos los activos de información de la Municipalidad del Centro Poblado de Salcedo Puno. Tener Políticas claras y controles adecuados para las amenazas y riesgos es fundamental hoy en día en las organizaciones.

Se analizaron las áreas funcionales de la Municipalidad del Centro Poblado de Salcedo Puno, así como se definió claramente el alcance del diseño del Plan de Seguridad Informática, que permitió definir el radio de acción del PSI.

La evaluación de los riegos a los que están expuestos los activos de información en la Municipalidad del Centro Poblado de Salcedo Puno, se desarrolló teniendo en consideración la metodología MARGERIT v.3. Esta evaluación permitió dimensionar la probabilidad de ocurrencia del riesgo y sobre todo las acciones a seguir en base a los controles seleccionados de la NTP-ISO/IEC 27001:2014.

Se elaboró la lista de controles de seguridad para mitigar los riesgos identificados en el diseño del Plan de Seguridad Informática para la Municipalidad del Centro Poblado de Salcedo Puno.

4.3. Contribuciones (Impacto).

El Plan de Seguridad Informática constituye el documento importante para el control y la seguridad en la explotación de las tecnologías informáticas de la Municipalidad del Centro Poblado de Salcedo Puno. Como ya se indicó las medidas que se establecen en el presente Plan de Seguridad Informática son de obligatorio cumplimiento para todo el personal que haga uso de las tecnologías informáticas instaladas en la Municipalidad del Centro Poblado de Salcedo Puno.

Se comparte la conclusión a la que llego (Guzmán Silva, 2015), en su trabajo de investigación “Diseño de un sistema de gestión de seguridad de la información para una entidad financiera de segundo piso”, que el diseño de un sistema de gestión de seguridad de la información basado en un modelo de mejoras prácticas y lineamientos de seguridad, como es la norma ISO/IEC 27001:2013, es una herramienta de gran ayuda que permite identificar los diferentes aspectos que se deben tener en cuenta cuando las organizaciones deciden establecer un modelo de seguridad de la información, ya que si las organizaciones logran cumplir al pie de la letra lo establecido en la norma ISO/IEC 27001:2013, pueden llegar a forjar en el tiempo un adecuado y sostenible PSI, aunque dicha labor depende del tamaño y naturaleza de la entidad y de la cultura de la misma en torno a la seguridad de la información.

Otro factor de importancia al diseñar un Plan de Seguridad Informática, es el compromiso de la alta dirección de las organizaciones, para llevar a cabo dicho Plan e imprescindible para la implementación, como lo señala en sus conclusiones (Justino Salinas, 2015), en su tesis “Diseño de un sistema de gestión de seguridad de información para una empresa inmobiliaria alineado a la NORMA ISO/IEC 27001.2013”. Coincido también con la importancia de establecer políticas de seguridad de información que contenga los lineamientos para una eficiente administración de la información con el fin de garantizar la seguridad de los sistemas

y mantener la integridad de la información, de la infraestructura de procesamiento y minimizar el impacto de vulnerabilidades e incidentes de seguridad.

Finalmente, también se está de acuerdo con la conclusión a la que llega (Suárez Padilla, 2013), es su tesis "Estudio de la seguridad de la información aplicado a Recursos Humanos, Adquisiciones y Cómputo para empresas del Sector Pesquero", que indica que las empresas están en la obligación de certificarse y mantener las mejores prácticas ofrecidas en las Normas Internacionales, estipuladas en la ISO 27000 y 27001.

CONCLUSIONES

1. Se diseñó un Plan de Seguridad Informática basado en la NTP-ISO/IEC 27001:2014, para que con su aplicación se pueda mitigar o disminuir el impacto de los riesgos a los que están expuestos los activos de información de la Municipalidad del Centro Poblado de Salcedo Puno. Tener Políticas claras y controles adecuados para las amenazas y riesgos es fundamental hoy en día en las organizaciones. Además, se menciona en esta conclusión el compromiso de los directivos de la Municipalidad del Centro Poblado de Salcedo Puno por llevar a cabo la implementación del PSI propuesto.
2. Se analizaron las áreas funcionales de la Municipalidad del Centro Poblado de Salcedo Puno, para identificar como alcance del Plan de Seguridad Informática el Área de Informática y Procesamiento de Datos, dependiente de la Oficina de Administración y Finanzas de la Municipalidad del Centro Poblado de Salcedo Puno.
3. La evaluación de los riegos a los que están expuestos los activos de información en la Municipalidad del Centro Poblado de Salcedo Puno, se desarrolló teniendo en consideración la metodología MARGERIT v.3. Esta evaluación permitió dimensionar la probabilidad de ocurrencia del riesgo y sobre todo las acciones a seguir en base a los controles seleccionados de la NTP-ISO/IEC 27001:2014.
4. Considerando los riesgos identificados, se elaboró la lista de controles de seguridad para mitigar los riesgos altos y medios identificados en el diseño del Plan de Seguridad Informática para la Municipalidad del Centro Poblado de Salcedo Puno

RECOMENDACIONES

1. El procedimiento seguido en el presente trabajo puede ser usado para diseñar PSI en otras instituciones similares a la Municipalidad del Centro Poblado de Salcedo Puno.
2. Todas las organizaciones deberían adoptar los lineamientos propuestos por la NTP ISO/IEC 27001:2014, para gestionar la seguridad de su información, especialmente a las entidades públicas, por tener hoy en día carácter de obligatoriedad.
3. La implementación del Plan de Seguridad Informática debería estar supervisada por un experto que garantice el éxito de su implementación, es por ellos que se recomienda contratar los servicios de un consultor en temas de seguridad de la información.
4. En el Área de Informática y Procesamiento de Datos de la Municipalidad del Centro Poblado de Salcedo Puno, el personal muchas veces toma el rol de Oficial de Seguridad de la Información, pero por su carga laboral también se ocupa de otras funciones y tareas. Se recomienda definir las tareas y funciones del Oficial de Seguridad de la Información, además de disponer un personal dedicado exclusivamente a cumplir dicho rol.
5. Se recomienda programar capacitaciones permanentes sobre los temas de seguridad de la información, para generar conciencia al respecto en los funcionarios y trabajadores del Municipio del Centro Poblado de Salcedo – Puno.

REFERENCIAS

Areitio, J. (2008). *Seguridad de la Información, Redes, Informática y Sistemas de Información.* Madrid: Paraninfo.

Ariasca Suma, F., & Quispe Borda, S. (2017). *Desarrollo de una Propuesta de Implementacion de la NTP ISO/IEC 27001:2014, Sistema de Gestion de Seguridad de la Informacion, para la Oficina Funcional de Informatica del Gobierno Regional del Cusco.* Cusco: Universidad Nacional Andina del Cusco.

Carnegie Mellon, U. (2007). *Introducing OCTAVE ALlegro: Improving the Information Security Risk Assessment Process*. Obtenido de http://resources.sei.cmu.edu/asset_files/TechnicalReport/2007_005_001_148 85.pdf

Ccesa Quincho, M. (2017). *Diseño De Un Sistema De Gestión De Seguridad De La Información Bajo La Ntp Iso/Iec 27001:2014 Para La Municipalidad Provincial De Huamanga.* Huamanga: Universidad Nacional de San Cristobal de Huamanga.

Chiavenato, I. (2006). *Introducción a la teoría general de la administración.* Mexico: McGraw Hill.

CISCO. (27 de Setiembre de 2018). *Lo que usted necesita saber sobre seguridad de la red*. Obtenido de http://www.cisco.com/web/LA/soluciones/la/information_security/index.html

Endler, D. (2007). *HAcking Exposed VoIP: Voice Over IP Security Secret & Solutions.* Osborne: MacGraw-Hill.

Estandarización, O. I. (2005). *Estándar de Seguridad ISO 27000.*

Excellence, I. (18 de 08 de 2015). *La norrma ISO 27001:2013 ¿Cuál es su estructura?* . Obtenido de http://www.prng-ssi.com/2015/08/norma-iso-27001-2013-estructura/

Fitzgerald, T. (2007). Information Security Governance. En H. Tipton, & M. Krause, *Information Security Management Handbook* (págs. 15-34). USA: Auerbach.

Garcia-Cervigón, A. (2011). *Seguridad Informática.* Madrid: Paraninfo.

Glemser, T. (2015). *Seguridad en la voz sobre IP - Protocolo SIP y RTP*. Hackin9.

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

Gómez López, J. (2008). *VoIP y Asterik.* Almeria: Alfaomega.

Guzman. (s.f.).

Guzmán Silva, C. (2015). *Diseño de un Sistema de Gestión de Seguridad de la Información para una Entidad Financiera de Segundo Piso.* Colombia: Institución Universitaria Politécnico Grancolombiano.

Halvorson, N. (2008). *Information Risk Management: A Process Approach to Risk Diagnosis and Treatment. Information Security Management Handbook.* . USA: Auerbach Publications.

INDECOPI. (2014). *Norma Técnica Peruana NTP-ISO/IEC 27001:2014. Tecnologia de la información. Ténicas de seguridad. Sistema de gestión de seguridad de la información.Requisitos."*. Lima: Segunda Edición.

ISO 27000. (s.f.). *ISO 27000.es*. Obtenido de El Portal de ISO 27001 en Español: http://www.iso27000.es/iso27000.html

ISO/IEC, 1. (2005). *Estándar Internacional ISO/IEC 17799:2005.* Caracas: Seguridad en informática y comunicaciones DVD.

Justino Salinas, Z. (2015). *Diseño de un Sistema de Gestión de Seguridad de Información para una empresa inmobiliaria alineado a la norma ISO/IEC 27001:2013.* Lima: Pontificia Universidad Católica del Perú.

MARGERIT. (2012). *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* Madrid: Ministerio de Hacienda y Administación Pública.

Mendillo, V. (2009). *Auditoria de Seguridad para redes y servicios.* Caracas: Seguridad en informatica y comunicaciones DVD.

Microsoft. (2015). *Academia Latinoamericana de Seguridad.* Caracas: Seguridad en informatica y comunicaciones DVD.

Peltier, T., Peltier, J., & Blackley, J. (2005). *Information Security Fundamentals.* USA: Auerbach Publications.

Peso Navarro, E., & Remos Gonzalez, M. (2004). *El Documento de Seguridad. Análisis técnico y jurídico.* Obtenido de https://books.google.com.pe/books?id=4I2Cdi_8wgcC&printsec=frontcover&hI=esv=onepage&q&f=false/

Quispe Barreto, J. (2018). *Declaración de aplicabilidad mediante la NTP ISO/IEC 27001:2014 para mitigar los siniestros de la información en la sub dirección de licencias de conducir de la Direccion Regional de Tranporte y Comunicacion de Ancash.* Ancash: Universidad Nacional Santiago Antunez de Mayolo.

Ross, J. (2017). *VoIP voz sobre IP.* Rio de Janeiro: Edicoes Tecnicas.

Sandoval Vargas, C. (2014). *Análisis de la Norma ISO/IES 27001. Diseño de Implementación en la red de una Empresa.* Ecuador: Universidad Católica de Santiago de Guayaquil.

Stallings, W. (2004). *Fundamentos de Seguridad en Redes.* Madrid: Pearson Prentice Hall.

Suárez Padilla, G. (2013). *Estudio de la Seguridad de la Información aplicado a los Recursos Humanos, Adquisiciones y Cómputo para empresas del Sector Pesquero.* Ecuador: Universidad de Guayaquil.

Valarino, E. (2010). *Metodología de la Investigación. Paso a Paso.* Mexico DF: Trillas.

ANEXO A. Cuestionario sobre diagnostico situacional

Cuestionario sobre diagnóstico situacional de la seguridad de la información

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

   ☐ Sí ☐ No

2. ¿En su área de trabajo se ha categorizado la información de acuerdo al grado de importancia que tienen para la Municipalidad del Centro Poblado de Salcedo - Puno?

   ☐ Sí ☐ No

3. ¿Ha recibido Ud. capacitación sobre seguridad de la información de acuerdo a su función laboral?

   ☐ Sí ☐ No

4. ¿Su contrato contempla ítems que estipulen responsabilidades con respecto a la seguridad de la información?

   ☐ Sí ☐ No

5. Dentro de su área de trabajo ¿se considera la seguridad de información cuando se gestiona un proyecto?

   ☐ Sí ☐ No

6. ¿Cuenta Ud. con un computador/laptop para realizar sus funciones? (Si la respuesta es No pasar a la pregunta 9)

   ☐ Sí ☐ No

7. ¿Cuenta Ud. con una clave de acceso para ingresar a su computador y/o laptop?

   ☐ Sí ☐ No

8. Cuando su computador está desatendido ¿Se activa el bloqueo de pantalla con contraseña para proteger la información?

   ☐ Sí ☐ No

9. ¿En lo que va del año ha sufrido modificación o pérdida de información ya sea por virus, acceso de personas no autorizadas, deterioro, tras papeleo, etc.?

☐ Sí ☒ No

10. ¿En lo que va del año se ha divulgado información sensible para la Municipalidad del Centro Poblado de Salcedo - Puno sin su autorización o conocimiento?

☐ Sí ☒ No

11. ¿En su área de trabajo se han realizado evaluación de riesgos relacionados con la información?

☐ Sí ☐ No

12. ¿En su área de trabajo se han realizado una evaluación de vulnerabilidades de la red?

☐ Sí ☐ No

13. ¿Su área de trabajo cuenta con software antivirus actualizado?

☐ Sí ☐ No

14. ¿Realiza Ud. copias de seguridad para proteger su información?

☐ Sí ☐ No

15. ¿Considera que su oficina está protegida contra amenazas externas o ambientales que ocasionen pérdidas de información?

☐ Sí ☒ No

16. ¿Sabe Ud. si dentro de la Municipalidad del Centro Poblado de Salcedo - Puno existe un Plan de Seguridad Informática?

☐ Sí ☒ No

ANEXO B. Cuestionario para identificar activos

CUESTIONARIO PARA IDENTIFICAR ACTIVOS

Instrucciones: En cada tabla marque (X) los activos con los que cuenta la dependencia:

TABLA DE RELACIÓN DE ACTIVOS DE TIPO ACTIVOS ESENCIALES
¿Qué activos son fundamentales para que la dependencia consiga sus objetivos y estos estén alineados con los objetivos de la organización?
Marque (X) los activos con los que cuenta la dependencia ( ) Datos de interés para la administración pública ( ) Datos vitales (esencial para el funcionamiento de la organización) ( ) Datos de carácter personal (información concerniente al personal) ( ) Datos clasificados (aquellos sometidos a normatividad específica de la organización y que determina su control de acceso y distribución) ( ) Servicios
Nota: Estos activos esenciales marcan los requisitos de seguridad para todos los demás componentes del sistema.

TABLA DE RELACIÓN DE ACTIVOS DE TIPO DATO/INFORMACIÓN
¿Qué activos de tipo dato/información son fundamentales para que la dependencia consiga sus objetivos y estos estén alineados con los objetivos de la organización?
Marque (X) los activos con los que cuenta la dependencia ( ) Ficheros o bases de datos. ( ) Copias de respaldo. ( ) Datos de configuración de los sistemas de información. ( ) Datos de gestión interna. ( ) Credenciales (Ejem. contraseñas). ( ) Datos de validación de credenciales. ( ) Datos de control de acceso. ( ) Registro de actividad o log de los sistemas de información. ( ) Código fuente de los sistemas de información. ( ) Código ejecutable de los sistemas de información.

TABLA DE RELACIÓN DE ACTIVOS DE TIPO SERVICIO
¿Qué activos de tipo servicio son fundamentales para que la dependencia consiga sus objetivos y estos estén alineados con los objetivos de la organización?
Marque (X) los activos con los que cuenta la dependencia. ( ) Anónimo (sin requerir identificación del usuario). ( ) Al público en general (sin relación contractual) ( ) A usuarios externos (bajo una relación contractual). ( ) Interno (a usuarios de la propia organización). ( ) Internet. ( ) Intranet. ( ) Acceso remoto a cuenta local ( ) Correo Electrónico. ( ) Almacenamiento de ficheros (File Server). ( ) Transferencia de ficheros (FTP). ( ) Intercambio electrónico de datos (EDI). ( ) Servicios de directorio. ( ) Gestión de Identidades (Servicios que permiten altas y bajas de usuarios de los sistemas). ( ) Gestión de privilegios. ( ) PKI - infraestructura de clave pública (Servicios asociados a sistemas de criptografía de clave pública – Gestión de certificados).
Nota: Esta sección contempla servicios prestados por el sistema.

TABLA DE RELACIÓN DE ACTIVOS DE TIPO SOFTWARE/APLICACIONES INFORMÁTICAS
¿Qué activos de tipo software son fundamentales para que la dependencia consiga sus objetivos y estos estén alineados con los objetivos de la organización?

Marque (X) los activos con los que cuenta la dependencia. ( ) Software de desarrollo propio. ( ) Software de desarrollo a medida (subcontratado). ( ) Página Web. ( ) Intranet. ( ) Servidor de presentación ( ) Servidor de aplicaciones (X) ERP. ( ) Cliente de correo electrónico. ( ) Servidor de correo electrónico. ( ) Servidor de ficheros. ( ) Sistema de gestión de bases de datos. ( ) Monitor transaccional. ( ) Ofimática. ( ) Anti virus.
( ) Sistema operativo. ( ) Gestor de máquinas virtuales ( ) Servidor de Terminales. ( ) Sistema de Backup. ( ) Otros._____
Nota: Esta sección contempla servicios prestados por el sistema.

TABLA DE RELACIÓN DE ACTIVOS DE TIPO EQUIPOS INFORMÁTICOS
¿Qué activos de tipo hardware son fundamentales para que la dependencia consiga sus objetivos y estos estén alineados con los objetivos de la organización?

Marque (X) los activos con los que cuenta la dependencia

( ) Grandes equipos.

( ) Equipos medios.

( ) Informática personal.

( ) Informática móvil.

( ) Equipo virtual.

( ) Equipamiento de respaldo.

( ) Medios de impresión (impresoras y servidores de impresión).

( ) Escáneres.

( ) Dispositivos Criptográficos.

( ) Dispositivos de frontera.

( ) Módems.

( ) Concentradores (Hub).

( ) Conmutadores (Swicth).

( ) Encaminadores (Router).

( ) Pasarelas (bridge).

( ) Cortafuegos (Firewall).

( ) Punto de acceso inalámbrico.

( ) Centralita telefónica.

( ) Teléfono IP.

( ) Otros. _____

TABLA DE RELACIÓN DE ACTIVOS DE TIPO REDES DE COMUNICACIONES
¿Qué medios de transporte utiliza la dependencia para transmitir información?
Marque (X) los activos con los que cuenta la dependencia ( ) Red telefónica. ( ) RDSI (red digital). ( ) X25 (red de datos). ( ) ADSL. ( ) punto a punto.

ANEXO C. Cuestionario para identificar amenazas

CUESTIONARIO PARA IDENTIFICAR AMENAZAS Y ESTABLECER PROBABILIDAD DE MATERIALIZACIÓN

Amenaza	Marca (X)	Probabilidad de ocurrencia
Fuego		
Tormenta eléctrica, rayo		
Error de Usuario		
Errores del administrador		
Errores de configuración		
Alteración accidental de la información		
Destrucción de Información		
Fugas de Información		
Vulnerabilidades de los programas (software)		
Errores de mantenimiento / actualización de programas (software)		
Errores de mantenimiento / actualización de equipos (hardware)		
Caída del sistema por agotamiento de recursos (interrupción en los servicios)		
Indisponibilidad del personal		
Manipulación de los registros de Actividad (log)		
Manipulación de la configuración		
Suplantación de la identidad del usuario		
Abuso de privilegios de acceso		
Difusión de software dañino		
Acceso no autorizado		
Modificación deliberada de la información		
Destrucción deliberada de Información		
Divulgación de la Información		
Manipulación de programas		
Manipulación de los equipos		
Denegación del servicio		
Robo de Equipos		
Indisponibilidad deliberada del personal		
Extorsión		
Ejecución de ingeniería social		
Corte del suministro eléctrico		
Condiciones inadecuadas de temperatura o humedad		
Degradación de los soportes de almacenamiento de la información		
Uso inadecuado de las sistemas y/comunicaciones que generan interrupciones		
Hacking no ético		
Instalación de software no autorizado		
Otro:_____		

Fuente: MARGERIT v.3.