# UNIVERSIDAD CATÓLICA LOS ÁNGELES DE CHIMBOTE
# FACULTAD DE INGENIERÍA
# ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

## EVALUACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO 27001:2013, EN LA MUNICIPALIDAD DISTRITAL DE JOSÉ CRESPO Y CASTILLO -AUCAYACU; 2018.

**TESIS PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS**


AUTOR

**DAVILA VILLANUEVA, MIGUEL AUGUSTO**

ASESORA

**SUXE RAMÍREZ, MARÍA ALICIA**


**CHIMBOTE – PERÚ**

**2018**

**JURADO EVALUADOR DE TESIS Y ASESOR**

DR. ING. CIP. VÍCTOR ÁNGEL ANCAJIMA MIÑÁN
PRESIDENTE

MGTR. ING. CIP. ANDRÉS DAVID EPIFANÍA HUERTAS
MIEMBRO

MGTR. ING. CIP. JOSÉ ALBERTO CASTRO CURAY
MIEMBRO

MGTR. ING. MARÍA ALICIA SUXE RAMÍREZ
ASESORA

## DEDICATORIA

A mí querida madre que en paz descanse y a mí querido padre, porque siempre me apoyaron en todo momento de mi vida, por creer en mí y por todo el amor que me tienen y tuvieron. Gracias Dios por los Padres que me distes.

Mis hermanos y amigos de clases y labores, por estar conmigo y apoyarme siempre, los estimo mucho, con ustedes paso un gran porcentaje de mi vida.

Finalmente, a mis maestros, aquellos que marcaron cada etapa de mi camino universitario, que me ayudaron a despejar mis dudas presentadas en la elaboración de la tesis.

***Miguel Augusto Dávila Villanueva***

# AGRADECIMIENTO

El presente trabajo de investigación fue realizado bajo la supervisión Mgtr. Ing. María Alicia Suxe Ramírez, a quien expreso mis sinceras felicitaciones, por hacer posible la realización del presente estudio de Investigación. Además, quiero agradecer su paciencia que tuvo para culminar de manera exitosa el Taller de Tesis.

Agradezco a la Universidad Católica los Ángeles de Chimbote por darme la oportunidad de estudiar y ser un profesional, a cada uno de mis maestros por sus enseñanzas que hicieron posible el logro de mis objetivos, a mis compañeros de clase por su amistad y sanos consejos.

Agradezco a la Municipalidad Distrital de José Crespo y Castillo de Aucayacu por darme la oportunidad de realizar mi trabajo de investigación y a cada uno de mis compañeros de trabajo por haberme facilitado siempre los medios suficientes para llevar a cabo todas las actividades propuestas durante el desarrollo de esta tesis. Muchas gracias

***Miguel Augusto Dávila Villanueva***

## RESUMEN

Este trabajo de tesis se presentó bajo la línea de investigación: Implementación de las Tecnologías de Información y Comunicación para la mejora continua de la calidad en las Organizaciones del Perú, en la Escuela Profesional de Ingeniería de Sistemas de la Universidad Católica los Ángeles de Chimbote; tuvo como objetivo Evaluar la implementación del sistema de gestión de seguridad de la información en la Municipalidad Distrital de José Crespo y Castillo, basado en la norma ISO 27001:2013 - Aucayacu; 2018. La investigación realizada fue de nivel cuantitativo, de diseño no experimental de tipo descriptiva. La población estuvo conformada por 198 trabajadores y la muestra de 30 colaboradores de manera Selectiva se realizó recolección de datos con el uso del instrumento del cuestionario a través de la técnica de la encuesta, en la cual se obtuvo los siguientes resultados: En la dimensión 01: "Situación actual del

Sistema de Gestión de la Seguridad de la información", se encontró el siguiente resultado el 85.50% manifiesta que no cuenta con un sistema de gestión de seguridad de la información, el mismo resultado se encontró en la dimisión 02: "Necesidad de Implementar el Sistema de Gestión de la Seguridad de la Información".

El Sistema de Gestión de Seguridad de la Información (SGSI), se encuentra fundamentado en la norma ISO-27001, que sigue el enfoque basado en procesos que usan el ciclo de Deming o el ciclo de mejora continua, consistente en Planificar-HacerVerificar-Actuar (PHVA), conocido con las siglas en inglés PDCA.



**Palabras Claves:** ISO 27001, MPT, SGSI, seguridad de información, TIC.

## ABSTRACT

This thesis work was presented under the line of research: Implementation of Information and Communication Technologies for the continuous improvement of quality in the Organizations of Peru, in the Professional School of Systems Engineering of the Catholic University Los Angeles de Chimbote; Its objective was to evaluate the implementation of the information security management system in the District Municipality of José Crespo y Castillo, based on ISO 27001: 2013 - Aucayacu; 2018. The research carried out was of a quantitative level, of non-experimental design of a descriptive type. The population was made up of 198 and sample 30 Selectively collected data was made with the use of the questionnaire instrument through the survey technique, in which the following results were obtained: In dimension 01: "Situation of the Information Security Management System ", the following result was found: 85.50% state that they do not have an information security management system, the same result was found in the resignation 02:" Need to Implement the Information Security Management System ".

The Information Security Management System (ISMS) is based on the ISO-27001 standard, which follows the approach based on processes that use the Deming cycle or the continuous improvement cycle, consisting of Plan-Do-Check -Actuar (PHVA), known by the acronym in English PDCA.



Keywords: ISO 27001, MPT, SGSI, information security, TIC.

## ÍNDICE DE CONTENIDO

## ÍNDICE DE TABLAS

## ÍNDICE DE GRÁFICOS

# I. INTRODUCCIÓN

En la actualidad vivimos en la era de la información donde los datos están disponibles para todo el mundo y la información puede ser analizada y tratada por las diversas áreas de la organización y así mismo pueden ser requeridos por las diversas instituciones de acuerdo al grado de influencia gubernamental. La información se ha convertido para las empresas en uno de los recursos intangibles más importantes para la toma de decisiones, las mismas que responde al cumplimiento de la visión, misión, valores y principios que inspiran la continuidad de las empresas. Hoy en día las empresas e instituciones que no cuentan con tecnologías y metodologías para el tratamiento de la información corren el riesgo de perder pocesionamiento en el mundo de los negocios, ya que estas cada día son globalizados a través de las Tecnologías de información y comunicación (1).

La información es un activo intangible muy valioso, la cual se tiene que proteger, pero muchas compañías no saben cómo; con la gran revolución tecnológica que hemos vividos los últimos años, han hecho que las empresas incorporen tecnologías de información y comunicación en sus principales procesos y áreas que mueven su negocio, pero no tienen un plan que asegure su información, esto ha llevado a descuidar los principios básicos de la seguridad de la información que es la confidencialidad, integridad y disponibilidad; estas actividades estimulan el desarrollo sostenible de la compañías por ello muchas empresas para hacer frente a estos retos que enfrentan día a día tienen que desarrollar procesos y estándares que midan y cumplan con dichos propósitos que ajusten todos los principios de negocio Gestión.

Hoy en día son pocas las municipalidades que han implementado Sistema de Gestión de la Seguridad de la Información – SGSI, que les permita controlar de manera adecuada la infraestructura tecnológica a fin de salvaguardar la información y activos ante dificultades internas y externas. El estándar internacional ISO 27001,

pretende lograr la implantación del Sistema de Gestión de Seguridad de Información - SGSI, a fin de tener un plan de control sobre las Tecnologías y la información. (2).

La información es uno de los bienes más importantes, por lo tanto, es de vital importancia salvaguardar la infraestructura tecnológica mediante estándares internacionales sustentados en política de seguridad de información; su contribución a la seguridad del sistema de gestión de seguridad de la información, envolviendo los beneficios de un excelente desempeño de la seguridad de la información; y las implicancias de no tener conformidad con los requisitos del sistema de gestión de seguridad de la información (3).

La Municipalidad Distrital de José Crespo y Castillo – Aucayacu; tiene serios problemas respecto a la seguridad de la información, en muchos casos la información ha sido vulnerada y otras cosas han sido sustraídas, estas dificultades llevan como alternativas de solución mejorar la problemática que existe en las diversas áreas de la Municipalidad a fin de garantizar la fiabilidad, confiabilidad, seguridad y disponibilidad de los datos en todo momento.

De acuerdo a lo planteado surge la siguiente pregunta: ¿De qué manera el Sistema de Gestión de Seguridad de la Información en la Municipalidad Distrital de José Crespo y Castillo, basado en la norma ISO 27001:2013 - Aucayacu; 2018, ayudara a mejorar la administración de la seguridad de la información?

A fin de dar solución a la preguntada formulada se planteó el siguiente objetivo General: Evaluar la implementación del sistema de gestión de seguridad de la información en la Municipalidad Distrital de José Crespo y Castillo, basado en la norma ISO 27001:2013 - Aucayacu; 2018.

Para dar cumplimiento al objetivo general, se plantearon los siguientes objetivos específicos.

1. Analizar la inseguridad de la seguridad de la información, en la actual de la Municipalidad Distrital de José Crespo y Castillo.

2. Evaluar los marcos de referencias que ayuden a mejorar la seguridad de la información en la Municipalidad Distrital de José Crespo y Castillo.
3. Proponer la aplicación de la Norma ISO / IEC 27001, para asegurar mejorar la seguridad de la información.

La presente investigación las siguientes justificaciones:

**Justificación Académica:** Plasmar todo el conocimiento adquiridos a través de todos los años de estudio y formación profesional en la escuela de Ingeniería de Sistemas de la Universidad Católica los ángeles de Chimbote, lo misma que a través de los diversos cursos nos formaron y nos enseñaron acerca de la gestión de las TIC en las organizaciones.

**Justificación Operativa:** Se basa en los objetivos específicos de la presente investigación, la misma que permitirá que la Municipalidad Distrital de José Crespo y Castillo, tenga una mejor gestión en la seguridad de la información, organización de las TIC y gestión de activos.

**Justificación Económica:** Tiene como finalidad ahorrar tiempo y dinero con respecto a la seguridad de la información, la cual hoy en días no solo es importante para la Municipalidad Distrital de José Crespo y Castillo, sino también para las universidades y organizaciones en general.

**Justificación Tecnológica:** En la Municipalidad Distrital de José Crespo y Castillo, se diferencia de las demás municipalidades en la mejora de la gestión de las TIC.

**Justificación Institucional:** Otorgará a la Municipalidad Distrital de José Crespo y Castillo, asegurar la viabilidad, confiabilidad y seguridad de la información.

**Alcance de la Investigación:** La investigación abarca todas las áreas de Municipalidad Distrital de José Crespo y Castillo, centrándose en la infraestructura tecnológica que soporta los procesos de la información.

# II. REVISIÓN LITERARIA.

## 2.1 Antecedentes.

### 2.1.1 Antecedentes a Nivel Internacional.

Según el autor Guamán J. (4), en el año 2015, menciona en su tesis titulada "Diseño de un sistema de gestión de seguridad de la información para instituciones militares", realizado en la Escuela Politécnica Nacional ubicado en la ciudad de Quito - Ecuador, la metodología de la investigación fue sustentada por el autor en tres fases fundamentales: la primera el estudio diagnóstico, la segunda la factibilidad y la tercera el diseño de un sistema de gestión de seguridad de la información para instituciones militares, tomando como referencia la norma ISO 27001:2005 y usando una combinación de metodologías para la evaluación de los riegos que ayude a la toma de decisión sobre las opciones de tratamiento de riesgo adecuado.

Según el autor Pallas G. (5), en el año 2009, menciona en su tesis titulada "Metodología de Implantación de un SGSI en un grupo empresarial jerárquico", realizado en la Universidad de la República ubicado en la ciudad de Montevideo - Uruguay, en la investigación se analizan diferentes enfoques de estos estándares, con el fin de proponer una metodología de implementación, gestión y mejora de un SGSI en un grupo empresarial jerárquico, luego de haber analizado todo el marco teórico que el autor describe concluye que Un grupo empresarial, con una estructura de relación jerárquica o de subordinación, requiere de una metodología que permita gestionar la seguridad de la información atendiendo este aspecto estructural y jerárquico, con criterios alineados a la estrategia empresarial.

Según el autor Suarez S. (6), en el año 2009 menciona en su tesis titulada "Análisis y diseño de un sistema de gestión de seguridad informática en la empresa aseguradora Suárez Padilla & CÍA. Ltda., que brinde una adecuada protección en seguridad informática de la infraestructura tecnológica de la organización", realizado en la Universidad Nacional Abierta y a Distancia ubicada en la ciudad de Bogotá - Colombia, la investigación será ejecutado tomando como referencia una metodología de trabajo que permita en un futuro la implementación del Sistema de Gestión de Seguridad de la Información (SGSI), bajo el estándar ISO 27001, el resultado de la investigación tuvo como fin identificar el estado actual de la organización en cuanto a la Seguridad de la Información se realizaron entrevistas con los responsables de los procesos, solicitando información y verificación de la documentación existente en cuanto a seguridad de la información.

### 2.1.2 Antecedentes a Nivel Nacional.

Según el autor Seclén J. (7), en el año 2016, menciona en su tesis titulada "Factores que afectan la implementación del sistema de gestión de seguridad de la información en las entidades públicas peruanas de acuerdo a la NTP-ISO/IEC 27001", realizado en la Universidad Nacional Mayor de San Marcos ubicado en la ciudad de lima - Perú, la investigación tuvo una metodología cualitativo, ya que tiene como objetivo la indagación descriptiva de los factores que afectan la implementación del Sistema de Gestión de Seguridad de la Información en las Entidades de la Administración Pública según la NTP-ISO/IEC 27001, la investigación es inductiva, ya que pretende obtener conclusiones generales a partir de los resultados obtenidos en el levantamiento de información de las entidades públicas.

Según el autor Alcántara J. (8), en el año 2015, menciona en su tesis titulada "Guía de implementación de la seguridad basado en la norma ISO/IEC 27001, para apoyar la seguridad en los sistemas informáticos de la comisaria del norte P.N.P en la ciudad de Chiclayo", realizada en la Universidad Católica Santo Toribio de Mogrovejo ubicada en la ciudad de Chiclayo – Perú, la metodología de la investigación según el nivel de conocimiento que se pretende alcanzar el diseño de la investigación es el de una Investigación Cuasi-Experimental, la población de la presente investigación lo constituirá los 30 trabajadores de la Comisaria del Norte de la PNP de la ciudad de Chiclayo, debido a que la población es muy pequeña (n<=30) se tomarán a los 30 trabajadores, de acuerdo a lo obtenido en los resultados de la tesis el 10% de los encuestados señaló que se debería mejorar el proceso.

Según el autor Espinoza H. (9), en el año 2013, menciona en su tesis titulada "Análisis y diseño de un sistema de gestión de seguridad de información basado en la norma ISO/IEC 27001:2005 para una empresa de producción y comercialización de productos de consumo masivo.", realizado en la universidad Pontificia Universidad Católica del Perú, ubicada en la ciudad de Lima-Perú, se usó como metodología base a MAGERIT para realizar el análisis de riesgos de los procesos que abarco el alcance del SGSI, el autor concluye Debe tenerse en cuenta que el diseño de SGSI presentado se adapta a los objetivos actuales del proceso de producción, en el cual se ha basado el proyecto, y que este diseño podría variar ya que los objetivos estratégicos y de gobierno de le empresa pueden cambiar y por ello algunos sub procesos que forman parte del alcance del proyecto.

### 2.1.3 Antecedentes a Nivel Regional.

Según el autor Olaya J. (10), en el año 2016, menciona en su tesis titulada "Gestión del Sistema de Seguridad de Información bajo el enfoque de ISO 27001 en la Municipalidad Provincial de Tumbes;
2016", realizado en la Universidad Católica Los Ángeles de Chimbote, ubicado en la ciudad de Piura-Perú, la metodología de la investigación es no experimental debido a que no hay manipulación alguna de la variable, y tampoco se busca hacer algún cambio al fenómeno estudiado durante la investigación, tiene una población de 480 trabajadores y una muestra de 30 trabajadores, obteniendo como resultado que los trabajadores encuestados expresaron la situación actual del Sistema de gestión de la seguridad de la información, no se encuentra implementado obteniendo como resultado en la cual después de realizar el análisis y gestión de riesgos, proponemos un Sistema de Gestión de seguridad con enfoque mixto.

Según el autor Castillo R. (11), en el año 2016, menciona en su tesis titulada "Sistema de Gestión de Seguridad de la Información en la Municipalidad Distrital de Pira aplicando la norma ISO/IEC 27001:2013", realizado en la Universidad Católica Los Ángeles de Chimbote ubicado en la ciudad de Lima - Perú, el autor define la metodología de investigación por el grado de cuantificación reúne las condiciones de una investigación cuantitativa, el investigador para la presente investigación, se tomó como población a todo el personal administrativo que consta de 16 trabajadores que labora en la oficina matriz de la Municipalidad Distrital de Pira, que son aquellos involucrados directamente en los procesos, para cada una de las variables en estudio sobre sistemas de gestión de seguridad de la información, al finalizar el proceso de evaluación.

## 2.2 Bases Teóricas.

### 2.2.1 Las Municipalidades:

Las municipalidades en el Perú se dividen en Provinciales, Distritales y de Centros poblados, están ultimas creadas con ordenanzas Municipales y esta sujetas a régimen determinadas por el estado. Entre sus funciones principales se encuentran la administración de los terrenos y los predios de su localidad, la limpieza de las calles, hacer campañas de salud y recolectar la basura, protección y conservación del medio ambiente, seguridad ciudadana, cuidar el patrimonio cultural, histórico y paisajístico de su localidad, promover el desarrollo económico de su localidad, Promover la participación vecinal, sobre todo en el uso y control de los recursos, organizar servicios sociales para proteger a la población de menores recursos, luchar contra la comercialización y consumo de drogas. (12).

Son organismos gubernamentales que, en el Perú, reciben el nombre de Municipalidades, tiene como hito de partida cabildo, instancia de administración local creada durante el virreynato, Actualmente existen un aproximado de 1855 municipalidades entre Distritales y Provinciales. Las Municipalidades se encuentran dentro de la organización territorial del Estado y canales inmediatos de participación vecinal en los asuntos públicos que se encargan de gestionar con autonomía los intereses propios de su comunidad; siendo elementos esenciales del gobierno local, el territorio, la población y la organización. La estructura orgánica de las municipalidades está compuesta por el concejo municipal y la alcaldía. Los Municipios cuentas características de autonomía política, económica y administrativa en los asuntos de su competencia. (12).

### 2.2.2 Municipalidad Distrital José Crespo y Castillo - Aucayacu.

#### 2.2.2.1 Descripción General.

El Distrito de José Crespo y Castillo está situado en la parte Nor Este de la Provincia Leoncio Prado y forma parte central de la selva amazónica. Su nivel altitudinal alcanza los 540 msnm, con un clima característico que es el trópico de altura; con temperatura media anuales de 23.8° C, siendo la máxima de 30.9° C y la mínima de 18.6° C. (13).

#### 2.2.2.2 Historia y Creación.

Se formó por Ley N° 14777 de 26 de diciembre de 1963, con su capital Aucayacu, se cristalizó en el gobierno del Presidente de la República Fernando Belaúnde Terry. El nombre de Aucayacu deriva de dos voces compuestas de Auca: que es el nombre de una tribu semi salvaje que residía a orillas del río Huallaga; y Yacu: voz quechua que significa agua. De la unión de ambas palabras, tenemos que Aucayacu significa "Guerreros de Agua". Actualmente tiene una población de 25,259 habitantes, está formado por los siguientes pueblos: Caimito,

Pacae, Pueblo Nuevo, Santo Domingo de Anda, Los Milagros, Cotomonillo, La Roca, Aspuzana Nueva, Vieja Aspuzana, Micaela Bastidas, Pucayacu, Saipai, Santa Lucía, Cotomono, Pucate (13).

Tiene una extensión superficial de 2,829.67 km2, de los cuales 600,000 has. están destinados para el desarrollo agrícola, ganadero y forestal, ya que abunda gran variedad de vegetación propia de las zonas tropicales y que forma parte de la riqueza natural de la zona y de la región en general. (13).

Gráfico Nro. 1: Frontis de la Municipalidad.


Fuente: Inforegión (14)

### 2.2.2.3 Visión – Misión.

**Visión.**

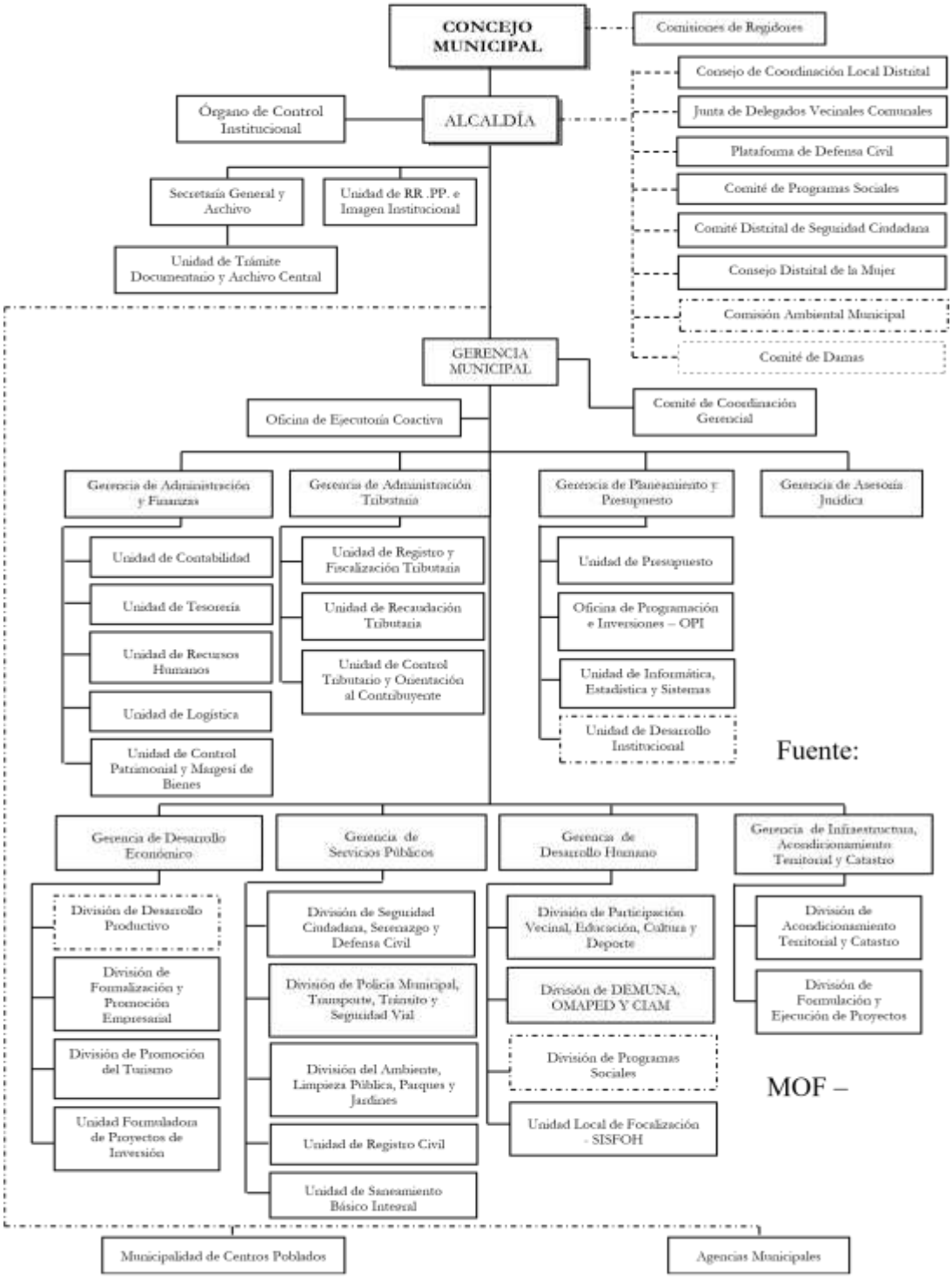
Ser una Institución moderna, concertadora, transparente y solidaria, con gestión eficaz y eficiente, que promueve el desarrollo económico, social, ambiental e Institucional para mejorar la calidad de vida de la población del Distrito de José Crespo y Castillo. (15)

**Misión.**

Somos una entidad pública edil que promueve el desarrollo humano sostenible, a través del uso eficiente de los recursos públicos, para lograr una mejor calidad de vida de la población. (15)

### 2.2.2.4 Organigrama.

Gráfico Nro. 2: Organigrama Funcional




Municipalidad Distrital

**2.2.2.5. Infraestructura Tecnológica de la Municipalidad Distrital.**

**Equipos de Hardware.**

Tabla Nro.1: Hardware

| Nº | MARCA | MODELO | CARACTERISTICAS GENERALES |
|---|---|---|---|
| 1 | Servidor IBM | System x3550 M4 | Intel XEON E5-260 2.30 Ghz, Memoria RAM 8 Gb DDR3 800/1066/1333 (Máx. 384 Gb), RAID ( SATA-600 / SAS 2.0 ) ( ServeRAID H1115 ) / RAID 0, RAID 1, RAID 10, Red: 4 x Gigabit Ethernet Intel I350-AM4, Fuente de Poder y Refigeración: 550 vatios / CA 120/230 V ( 50/60 Hz ), Disco Duro de 1.5 Tb. |
| 2 | 49 computadoras Intel Core | Intel Core | Core i5 3.20 Ghz, Memoria RAM 4 GB, Monitor LG LED 19 M38A-B, Ethertnet 10/100 Mbps, Disco Duro de 1 TB, Case ATX Micronics, Lector/Grabador Multi LG, Teclado USB Multimedia 104, Mouse USB Optico Genius |
| 3 | 11 computadoras HP | HP Elitedesk 800 G1TWR | Core i7 3.40 Ghz, Memoria RAM 8 Gb, Monitor LG 19", Ethertnet 10/100 Mbps, Disco Duro 1 Tb, Case HP ATX, Lector/Grabador DVD, Teclado USB Multimedia y Mouse USB Óptico |
| 4 | 3 laptop Toshiba | Satellite Core i7-4510U | Intel Core i7 2.00 Ghz, Memoria RAM 12,288 MB, Disco Duro 500 Gb, Teclado Numérico |

| | | | |
|---|---|---|---|
| 5 | 2 laptop HP | DesignJet T120 | |
| 6 | 18 impresoras HP | HP LaserJet | |
| 7 | 4 impresoras Canon | PRO MFP | |
| 8 | 3 impresoras Epson | L355 | |
| 9 | 2 fotocopiadoras Ricoh | MP 5001 9250/MP | |
| 10 | 4 fotocopiadoras Konica Minolta | bizhub 363 | |
| 11 | 3 Switch Linksys | LGS308 | Ethernet 10/100 Mbps 8 Puertos RJ-45 |
| 12 | Central Telefónica Hipacth | Hipacth 1150 | Usa 2 líneas externas y 10 líneas internas en su configuración inicial, pudiendo extenderse en su capacidad máxima hasta 10,16 o 17 líneas externas y 40, 46 o 50 líneas internas, |

| | | | |
|---|---|---|---|
| | | | dependiendo de su configuración |
| 13 | Router TPLink | TL-WL941HP | 2.4 Ghz 450 Mbps |
| 14 | Modem Router ADSL | Nucom R5000UNv2 | Con 3G, Puesrto USB, Conector a corriente transformador AC/DC, Cable RJ11 / RJ45, 04 Puertos RJ45 y 01 Puerto ADSL. |
| 15 | 24 unidades Switch DLink | DGS-1024D | Ethernet 10/100 Mbps, Auto MDI/MDIX, 24 Puertos RJ-45 |
| 16 | Rack SATRA | 38RU | Rack de Piso de 38RU 6 pies 1.80 mts Acero Laminado al Frio |
| 17 | Canon | Lide 110 | |

Fuente: Inventario Tecnológico de la Municipalidad.

**Equipos de Software.**

Tabla Nro. 2: Software

| Nº | Aplicativos | CARACTERISTICAS GENERALES |
|---|---|---|
| 1 | Sistema de información financiera (SIAF) | El SIAF es el Sistema Integrado de Administración Financiera, asimismo es un sistema informático que permite administrar, mejorar y supervisar las operaciones de ingresos y gastos de las Entidades del Estado, además de permitir la integración de los procesos presupuestarios, contables y de tesorería de cada entidad. |
| 2 | **S**istema de recaudación tributaria municipal del MEF | Con la finalidad de integrar y facilitar a los Gobiernos Locales un adecuado control y registro de la información de su recaudación tributaria, el Ministerio de Economía y Finanzas a diseñado el Sistema de Recaudación Tributaria Municipal – SRTM, comenzando, en Base de Datos Oracle. |
| 3 | SISFOH - Sistema de focalización de hogares - RUBENS | El SISFOH es un sistema que tiene a cargo el proceso de determinación de la clasificación socioeconómica, requisito que es exigido para acceder a las intervenciones públicas focalizadas como Pensión 65, Juntos, Beca 18 así como el SIS. |

| | | |
|---|---|---|
| 4 | Control patrimonial de bienes estatales - SIMI | Sirve para operar un sistema de registro y control de bienes muebles e inmuebles, que permita conocer e identificar todos |
| | | aquellos bienes que integran el patrimonio de la entidad y de programas especiales, así como contar con los registros actualizados. |
| 5 | Programa de declaración telemática - PDT | El Programa de Declaración Telemática-PDT, es un sistema informático desarrollado por la Superintendencia Nacional de Administración Tributaria (SUNAT) con la finalidad de facilitar la elaboración de las declaraciones juradas bajo condiciones de seguridad del registro de la información. |
| 6 | INDECI (SINPAD – Sistema Nacional para la Prevención y Atención de Desastres) | El Sistema Nacional de Información para la Prevención y Atención de Desastres - SINPAD, está soportada por un sistema informático bajo la plataforma Internet, el mismo que está compuesto por una serie de servicios informáticos con miras a que la información de la Prevención y atención de Desastres en toda su amplitud, sea registrada, mantenida, consultada y utilizada por todas las Instituciones sean éstas Públicas o Privadas |

| | | |
|---|---|---|
| 7 | Sistema de abastecimiento y almacén - GESMUN | Algunas Municipalidades todavía elaboran sus Órdenes de Compra y Ordenes de Servicio en forma manual o en Excel, lo cual no permite llevar un control detallado de la cartera de sus proveedores, ni control de las Órdenes de Compra o Servicio ni control de |
| | | existencias. Por lo que, pensado en la mejora de las labores del área de Abastecimiento o Logística, la empresa Systemas Gerenciales S.A.C. |
| 8 | **S**istema de operaciones contables y financieras MELISSA | Es un Sistema de consulta y generador de reportes gerenciales para toma de decisión que se conecta a la base de datos del SIAF-GL para realizar reportes contables, tesorería. Adicionalmente contiene datos de ejecución presupuestal para efectos de conciliación. |

Fuente: Inventario Tecnológico de la Municipalidad.

**2.2.3 Las Tecnologías de Información y Comunicaciones (TIC).** La revista electrónica TECHTARGET menciona que el término tecnología de la información fue acuñado por Harvard Business Review, con el fin de hacer una distinción entre máquinas diseñadas especialmente para realizar un alcance limitado de funciones y máquinas de computación de propósito general que podrían programarse para diversas tareas. A medida que la industria de TI evolucionó desde mediados del siglo XX, abarcó transistores y circuitos integrados: la capacidad de computación

avanzó mientras que los costos de los dispositivos y el consumo de energía cayeron, un ciclo que continúa en la actualidad cuando surgen nuevas tecnologías. (16).

Gil P., en su artículo de investigación escrito para la Universitat Oberta de Catalunya y publicada por la misma universidad nos dice que las tecnologías de información y comunicación comprenden aplicaciones, sistemas, herramientas, técnicas y metodologías asociadas a la digitalización de señales analógicas, sonidos, textos e imágenes, manejables en tiempo real. Asimismo, se relaciona con equipos de computación, software, telecomunicaciones, redes y bases de datos, lo que permite destacar que la evolución del proceso humano de recibir información y comunicarse, está estrechamente relacionada con la evolución tecnológica, pues trae consigo transformaciones a nivel comercial, educativo, cultural, social y económico, por su carácter global, accesible y universal. (17).

#### 2.2.3.1 Evolución de las TIC.

> La Universidad Internacional de Valencia, en su portal web menciona que los cambios que nuestra sociedad ha experimentado en los últimos años han sido enormes. Nos explica como la evolución de las TICs ha revolucionado no sólo las empresas sino también nuestra vida en general. Nuestra sociedad, nuestras escuelas, nuestros hábitos, y todo lo que nos rodea en general ha experimentado una gran evolución. (18).
>
> Nos habla que en la actualidad volvemos a contactar con personas de las que no sabíamos nada desde hace años y conocemos a otras nuevas que si no hubiera sido por la

evolución de las TICs jamás las habríamos conocido. Las redes sociales públicas como Facebook o Twitter y otras privadas que se utilizan para relacionarse han ayudado en todo esto. (18).

Nuestras compras y la forma en cómo hacemos negocios también ha cambiado. Las TICs han influenciado en nuestros gustos, en nuestras aficiones y en nuestros hábitos de consumo (18).

La Unión Internacional de Telecomunicaciones (ITU), que es el organismo especializado en telecomunicaciones de la Organización de las Naciones Unidas, encargado de regular las telecomunicaciones a nivel internacional en su investigación publicado en su página web titulado Evolución de las TIC a escala mundial nos habla que son numerosos los cambios que afronta en el mundo digital actual el sector de las tecnologías de la información y la comunicación (TIC), desde los avances de las tecnologías hasta la presencia de nuevos agentes, el desplazamiento de los ingresos y el nacimiento de diferentes modelos de actividad económica. (19).

También menciona el crecimiento del tráfico en las telecomunicaciones, ya no son privilegio exclusivo de los seres humanos. La Internet de las Cosas se está haciendo rápidamente realidad y, en un futuro próximo, está previsto que las comunicaciones de máquina a máquina (M2M) aumentarán de manera importante, lo que añadirá más presión

a las redes. Y el futuro crecimiento del tráfico IP parece no tener límites. Este ingente volumen obedece al aumento del número de personas y dispositivos conectados, así como a la creciente disponibilidad de contenidos en línea abundante, diversificada y, en la mayoría de casos, gratuitos
(19).

#### 2.2.3.2 Ventajas de las TIC.

La UNESCO, en su investigación publicada en su página web alude que ventajas de las tecnologías de la información y la comunicación (TIC) pueden ayudar a mejorar el acceso universal a la educación, la igualdad en la instrucción, el ejercicio de la enseñanza y el aprendizaje de calidad y el desarrollo profesional de los docentes, así como a la gestión dirección y administración más eficientes del sistema educativo. (20).

Para la revista Virtual EDUCREA, lo diferencia las ventajas en cualidades, citaremos algunas de esas cualidades, como por ejemplo:

- Motivación. De acuerdo a lo descrito en la revista nos dice que el estudiante se verá más motivado haciendo uso de las herramientas TICs puesto que le permite formarse en la materia de forma más atrayente, amena, divertida, investigando de una forma sencilla.
- Interés. EDUCREA habla que el interés por la materia es algo que a los docentes nos puede costar más de la cuenta dependiendo simplemente por el título de la misma, y a través de las TIC aumenta el interés del alumnado indiferentemente de la materia. Los recursos de animaciones, vídeos, audio, gráficos, textos y ejercicios

interactivos que refuerzan la comprensión multimedia presentes en Internet aumentan el interés del alumnado complementando la oferta de contenidos tradicionales.

- Cooperación. Las TICs posibilitan la realización de experiencias, trabajos o proyectos en común. Es más fácil trabajar juntos, aprender juntos, e incluso enseñar juntos, si hablamos del papel de los docentes pueden colaborar con otros docentes, utilizar recursos que han funcionado bien en determinadas áreas de las que el estudiante será el principal beneficiario.
- Iniciativa y Creatividad. El desarrollo de la iniciativa del estudiante, el desarrollo de su imaginación y el aprendizaje por sí mismo. (21).

### 2.2.4 Conceptos Sistema de Gestión de Seguridad de la Información.

#### 2.2.4.1 ¿Qué es Sistema de Gestión de Seguridad de la Información?

La Organización Internacional para la Estandarización (ISO), define a los SGSI como un enfoque sistemático para administrar la información sensible de la compañía para que permanezca segura. Incluye personas, procesos y sistemas de TI mediante la aplicación de un proceso de gestión de riesgos. Puede ayudar a las pequeñas, medianas y grandes empresas en cualquier sector a mantener seguros los activos de información (22).

#### 2.2.4.2 ISO / IEC 27001: 2013

27001 Academy especialista a nivel mundial en brindar apoyo a las organizaciones para implementar las ISO nos dice que la revisión más reciente de esta norma fue publicada en

2013 y ahora su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2 (23).

ISO / IEC 27001: 2013 es una norma internacional emitida por la Organización Internacional de Normalización (ISO), y especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de la seguridad de la información dentro del contexto de la organización. También incluye requisitos para la evaluación y el tratamiento de riesgos de seguridad de la información adaptados a las necesidades de la organización (24).

#### 2.2.4.3 Encuesta ISO 2016.

27001:2013 se ha transformado en la primordial norma a nivel mundial para la seguridad de la información y muchas compañías han certificado su cumplimiento; aquí se puede ver la cantidad de certificados en los dos últimos años:

Tabla Nro. 3: La Encuesta ISO de Sistema de Gestión Certificaciones Estándar 2016.

| **Estándar** | **Números de certificados en el 2016** | **Números de certificados en el 2016** | **Cambio** | **Cambio en %** |
|---|---|---|---|---|
| ISO 9001** | 1106356 | 1034180 | 72176 | +7% |
| ISO 14001*** | 346189 | 319496 | 26693 | +8% |
| ISO 50001 | 20216 | 11985 | 8231 | +69% |
| ISO 27001 | 33290 | 27536 | 5754 | +21% |
| ISO 22000 | 32139 | 32061 | 78 | 0 |

| | | | | |
|---|---|---|---|---|
| ISO/TS 16949 | 67358 | 62944 | 4414 | +7% |
| ISO 13485 | 29585 | 26255 | 3330 | +13% |
| ISO 22301 | 3853 | 3133 | 720 | +23% |
| ISO 20000-1 | 4537 | 2778 | 1759 | +63% |
| ISO 28000 | 356 | | | |
| ISO 39001 | 478 | | | |
| TOTAL | 1,644,357 | 1,520,368 | | +8% |

Fuente: Resumen ejecutivo de la encuesta ISO 2016 (25).

Los estándares ISO e IEC para seguridad de la información, ISO / IEC 27001 experimentan el mismo crecimiento anual de 20% de incremento anual que el año pasado a 33,290 certificados en todo el mundo (25).

Se registraron un total de 1 643 523 certificados válidos en nueve estándares, en comparación con 1 520 368 en 2015, un aumento del 8%, con otros 834 certificados en dos nuevas incorporaciones a la encuesta que elevan el total de 2016 a 1 644 357 (26).

#### 2.2.4.4 Beneficios de ISO 27001

Para 27001 Academy especialistas en brindar asesoramiento mencionan 4 ventajas comerciales fundamentales que una empresa puede obtener con la implementación de esta norma para la seguridad de la información:

- Cumplir con los requerimientos legales.
- Obtener una ventaja comercial.
- Menores costos.
- Una mejor organización.

La seguridad de la información es parte de la gestión global del riesgo en una empresa. (27), en el siguiente grafico observamos que áreas interviene:

Gráfico Nro. 3: Áreas en las que interviene SGSI.


Fuente: Informe realizado por 27001Academy (27).

### 2.2.4.5 Actualización de la ISO 27001:2005 a ISO 27001:2013.

Tabla Nro. 4: Dominios de Seguridad ISO/IEC 27001.

| ISO 27001 – 2005 (11 Dominios: 133 Controles | | ISO 27001 – 2013 (14 Dominios: 133 Controles | |
|---|---|---|---|
| A5 | Política de Seguridad. | A5 | Política de Seguridad. |
| A6 | Organización de la seguridad de la información. | A6 | Organización de la seguridad de la información. |
| A7 | Gestión de Activos. | A7 | Seguridad de los RRHH. |
| A8 | Seguridad de los RRHH. | A8 | Gestión de Activos. |
| A9 | Seguridad física y del ambiente. | A9 | Control de accesos. |
| A10 | Gestión de comunicación y operaciones. | A10 | Criptografía. |
| A11 | Control de accesos. | A11 | Seguridad física y ambiental. |
| A12 | Adquisición, desarrollo y mantenimiento de sistemas de información. | A12 | Gestión en las operaciones. |
| A13 | Gestión de incidentes de seguridad de la información. | A13 | Transferencia de la información. |
| A14 | Gestión de la continuidad del negocio. | A14 | Adquisición de sistemas, desarrollo y mantenimiento. |
| A15 | Cumplimiento. | A15 | Relación con Proveedores. |
| | | A16 | Gestión de los incidentes de seguridad. |
| | | A17 | Continuidad del negocio. |

| | | | |
|---|---|---|---|
| | | A18 | Cumplimiento con requerimientos legales y contractuales. |

Fuente: Implementación efectiva de un SGSI ISO 27001 (28).

### 2.2.4.6 Dominios, Objetivos de Control y Controles de ISO 27001:2013.

Tabla Nro. 5: ISO/IEC 27001:2013.

| Dominio | Objetivos de Control | Controles |
|---|---|---|
| 5. POLÍTICAS DE SEGURIDAD. | 5.1 Directrices de la Dirección en seguridad de la información. | 5.1.1 Conjunto de políticas para la seguridad de la información. |
| | | 5.1.2 Revisión de las políticas para la seguridad de la información. |
| 6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN. | 6.1 Organización interna. | 6.1.1 Asignación de responsabilidades para la seguridad de la información. |
| | | 6.1.2 Segregación de tareas. |
| | | 6.1.3 Contacto con las autoridades. |
| | | 6.1.4 Contacto con grupos de interés especial. |
| | | 6.1.5 Seguridad de la información en la gestión de proyectos. |

| | | |
|---|---|---|
| | 6.2 Dispositivos para movilidad y teletrabajo. | 6.2.1 Política de uso de dispositivos para movilidad. |
| | | 6.2.2 Teletrabajo. |
| 7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS. | 7.1 Antes de la contratación. | 7.1.1 Investigación de antecedentes. |
| | | 7.1.2 Términos y condiciones de contratación. |
| | 7.2 Durante la | 7.2.1 |

| | | |
|---|---|---|
| | contratación. | Responsabilidades de gestión. |
| | | 7.2.2 Concienciación, educación y capacitación en seguridad de la información. |
| | | 7.2.3 Proceso disciplinario. |
| | 7.3 Cese o cambio de puesto de trabajo. | 7.3.1 Cese o cambio de puesto de trabajo. |
| 8. GESTIÓN DE ACTIVOS. | 8.1 Responsabilidad sobre los activos. | 8.1.1 Inventario de activos. |
| | | 8.1.2 Propiedad de los activos. |
| | | 8.1.3 Uso aceptable de los activos. |
| | | 8.1.4 Devolución de activos. |
| | 8.2 | 8.2.1 Directrices de clasificación. |

| | | |
|---|---|---|
| | Clasificación de la información. | 8.2.2 Etiquetado y manipulado de la información. |
| | | 8.2.3 Manipulación de activos. |
| | 8.3 Manejo de los soportes de almacenamiento. | 8.3.1 Gestión de soportes extraíbles. |
| | | 8.3.2 Eliminación de soportes. |
| | | 8.3.3 Soportes físicos en tránsito. |
| 9. CONTROL DE ACCESOS. | 9.1 Requisitos de negocio para el control de accesos. | 9.1.1 Política de control de accesos. |
| | | 9.1.2 Control de acceso a las redes y servicios |

| | | |
|---|---|---|
| | | asociados. |
| | 9.2 Gestión de acceso de usuario. | 9.2.1 Gestión de altas/bajas en el registro de usuarios. |
| | | 9.2.2 Gestión de los derechos de acceso asignados a usuarios. |
| | | 9.2.3 Gestión de los derechos de acceso con privilegios especiales. |
| | | 9.2.4 Gestión de información confidencial de autenticación de usuarios. |

| | | |
|---|---|---|
| | | 9.2.5 Revisión de los derechos de acceso de los usuarios. |
| | | 9.2.6 Retirada o adaptación de los derechos de acceso. |
| | 9.3 Responsabilidades del usuario. | 9.3.1 Uso de información confidencial para la autenticación. |
| | 9.4 Control de acceso a sistemas y aplicaciones. | 9.4.1 Restricción del acceso a la información. |
| | | 9.4.2 Procedimientos seguros de inicio de sesión. |
| | | 9.4.3 Gestión de contraseñas de usuario. |
| | | 9.4.4 Uso de herramientas de administración de sistemas. |
| | | 9.4.5 Control de acceso al código fuente de los programas. |
| 10. CIFRADO. | 10.1 Controles criptográficos. | 10.1.1 Política de uso de los controles criptográficos. |
| | | 10.1.2 Gestión de claves. |
| 11. SEGURIDAD FÍSICA Y AMBIENTAL. | 11.1 Áreas seguras. | 11.1.1 Perímetro de seguridad física. |

| | | |
|---|---|---|
| | | 11.1.2 Controles físicos de entrada. |
| | | 11.1.3 Seguridad de oficinas, despachos y recursos. |
| | | 11.1.4 Protección contra las amenazas externas y ambientales. |
| | | 11.1.5 El trabajo en áreas seguras. |
| | | 11.1.6 Áreas de acceso público, carga y descarga. |
| | 11.2 Seguridad de los equipos. | 11.2.1 Emplazamiento y protección de equipos. |
| | | 11.2.2 Instalaciones de suministro. |
| | | 11.2.3 Seguridad del cableado. |
| | | 11.2.4 Mantenimiento de los equipos. |
| | | 11.2.5 Salida de activos fuera de las dependencias |

| | | |
|---|---|---|
| | | de la empresa. |
| | | 11.2.6 Seguridad de los equipos y activos fuera de las instalaciones. |
| | | 11.2.7 Reutilización o retirada segura de |

| | | |
|---|---|---|
| | | dispositivos de almacenamiento. |
| | | 11.2.8 Equipo informático de usuario desatendido. |
| | | 11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla. |
| 12. SEGURIDAD EN LA OPERATIVA. | 12.1 Responsabilidades y procedimientos de operación. | 12.1.1 Documentación de procedimientos de operación. |
| | | 12.1.2 Gestión de cambios. |
| | | 12.1.3 Gestión de capacidades. |
| | | 12.1.4 Separación de entornos de desarrollo, prueba y producción. |
| | 12.2 Protección contra código malicioso. | 12.2.1 Controles contra el código malicioso. |
| | 12.3 Copias de seguridad. | 12.3.1 Copias de seguridad de la información. |
| | 12.4 Registro de actividad y supervisión. | 12.4.1 Registro y gestión de eventos de actividad. |
| | | 12.4.2 Protección de los registros de información. |
| | | 12.4.3 Registros |

| | | |
|---|---|---|
| | | de actividad del administrador y operador del sistema. |
| | | 12.4.4 Sincronización de relojes. |
| | 12.5 Control del software en explotación. | 12.5.1 Instalación del software en sistemas en producción. |
| | 12.6 Gestión de la vulnerabilidad técnica. | 12.6.1 Gestión de las vulnerabilidades técnicas. |
| | | 12.6.2 Restricciones en la instalación de software. |
| | 12.7 Consideraciones de las auditorías de los sistemas de información. | 12.7.1 Controles de auditoría de los sistemas de información. |
| 13. SEGURIDAD EN LAS TELECOMUNICACIONES. | 13.1 Gestión de la seguridad en las redes. | 13.1.1 Controles de red. |
| | | 13.1.2 Mecanismos de seguridad asociados a servicios en red. |
| | | 13.1.3 Segregación de redes. |
| | 13.2 Intercambio de información con partes externas. | 13.2.1 Políticas y procedimientos de intercambio de información. |
| | | 13.2.2 Acuerdos de intercambio. |

| | | |
|---|---|---|
| | | 13.2.3 Mensajería electrónica. |
| | | 13.2.4 Acuerdos |

| | | |
|---|---|---|
| | | de confidencialidad y secreto. |
| 14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN. | 14.1 Requisitos de seguridad de los sistemas de información. | 14.1.1 Análisis y especificación de los requisitos de seguridad. |
| | | 14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas. |
| | | 14.1.3 Protección de las transacciones por redes telemáticas. |
| | 14.2 Seguridad en los procesos de desarrollo y soporte. | 14.2.1 Política de desarrollo seguro de software. |
| | | 14.2.2 Procedimientos de control de cambios en los sistemas. |
| | | 14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo. |
| | | 14.2.4 Restricciones a los cambios en los paquetes de software. |

| | | |
|---|---|---|
| | | 14.2.5 Uso de principios de ingeniería en protección de sistemas. |
| | | 14.2.6 Seguridad en entornos de desarrollo. |
| | | 14.2.7 Externalización del desarrollo de software. |
| | | 14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas. |
| | | 14.2.9 Pruebas de aceptación. |
| | 14.3 Datos de prueba. | 14.3.1 Protección de los datos utilizados en pruebas. |
| 15. RELACIONES CON SUMINISTRADORES. | 15.1 Seguridad de la información en las relaciones con suministradores. | 15.1.1 Política de seguridad de la información para suministradores. |
| | | 15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores. |
| | | 15.1.3 Cadena de suministro en tecnologías de la información y Comunicaciones. |

| | | |
|---|---|---|
| | 15.2 Gestión de la prestación del servicio por suministradores. | 15.2.1 Supervisión y revisión de los servicios prestados por terceros. |
| | | 15.2.2 Gestión de cambios en los servicios prestados por terceros. |
| 16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN. | 16.1 Gestión de incidentes de seguridad de la información y mejoras. | 16.1.1 Responsabilidades y procedimientos. |
| | | 16.1.2 Notificación de los eventos de seguridad de la información. |
| | | 16.1.3 Notificación de puntos débiles de la seguridad. |
| | | 16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones. |
| | | 16.1.5 Respuesta a los incidentes de seguridad. |
| | | 16.1.6 Aprendizaje de los incidentes de seguridad de la información. |
| | | 16.1.7 Recopilación de evidencias. |

| | | |
|---|---|---|
| 17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO. | 17.1 Continuidad de la seguridad de la información. | 17.1.1 Planificación de la continuidad de la seguridad de la información. |
| | | 17.1.2 Implantación de la continuidad de la seguridad de la información. |
| | | 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información. |
| | 17.2 Redundancias. | 17.2.1 Disponibilidad de instalaciones para |
| | | el procesamiento de la información. |
| 18. CUMPLIMIENTO. | 18.1 Cumplimiento de los requisitos legales y contractuales. | 18.1.1 Identificación de la legislación aplicable. |
| | | 18.1.2 Derechos de propiedad intelectual (DPI). |
| | | 18.1.3 Protección de los registros de la organización. |
| | | 18.1.4 Protección de datos y privacidad de la información personal. |
| | | 18.1.5 Regulación de los controles criptográficos. |

| | | |
|---|---|---|
| | 18.2 Revisiones de la seguridad de la información. | 18.2.1 Revisión independiente de la seguridad de la información. |
| | | 18.2.2 Cumplimiento de las políticas y normas de seguridad. |
| | | 18.2.3 Comprobación del cumplimiento. |

Fuente: Documento didáctico de Iso27001.es (29).

La ISO/IEC 27001:2013; Describe los dominios, objetivos de control y controles recomendables en cuanto a seguridad de la información con 14 dominios, 35 objetivos de control y 114 controles.

A pesar de que la misma ISO en su página web nos dice que no es obligatoria la implementación de todos los controles, se debe argumentar la no aplicabilidad de los controles no implementados.

Recomienda el uso del ciclo Plan – Do – Check – Act para el diseño de un SGSI. (29).

### 2.2.4.7 Aplicación del Ciclo de Deming (PHVA) para a la norma ISO/IEC 27001.

Para plasmar con el estándar, es preciso la existencia de unos factores y condiciones que garanticen el éxito para Mirian del Carmen Benavides Ruano, cita en su artículo científico a Corti, Betarte & De la Fuente que establecen en su artículo denominado "Hacia una implementación exitosa de un SGSI", un mapeo de las etapas del ciclo de Deming y los productos o entregables exigidos por la norma. (30), el siguiente cuadro especifica los principales procesos que indica la norma mapeados con las etapas del ciclo PHVA.

Tabla Nro. 6: Ciclo de Deming (PHVA) para a la norma ISO/IEC 27001.

| Ciclo PHVA | Procesos |
|---|---|
| Planear<br>(Plan) | Establecer el contexto.<br>Alcance y Limites.<br>Definir Política del SGSI.<br>Definir Enfoque de Evaluación de Riesgos.<br>Identificación de riesgos.<br>Análisis y Evaluación de riesgos.<br>Evaluar alternativas para el Plan de tratamiento de riesgos. Aceptación de riesgos.<br>Declaración de Aplicabilidad |
| Hacer<br>(Do) | Implementar plan de tratamiento de riesgos.<br>Implementar los controles seleccionados.<br>Definir las métricas.<br>Implementar programas de formación y sensibilización.<br>Gestionar la operación del SGSI. |
| | Gestionar recursos.<br>Implementar procedimientos y controles para la gestión de incidentes de seguridad. |

| | |
|---|---|
| Verificar (Check) | Ejecutar procedimientos de seguimiento y revisión de controles.<br>Realizar revisiones regulares de cumplimiento y eficacia de los controles y del SGSI. Medir la eficacia de los controles y verificación de satisfacción de los requerimientos de seguridad.<br>Revisión de la evaluación de riesgos periódicamente.<br>Realizar auditorías internas.<br>Revisión de alcance y líneas de mejoras del SGSI por la Dirección.<br>Actualizar los planes de seguridad.<br>Registrar acciones que podrían impactar la eficacia y/o eficiencia del SGSI. |
| Actuar<br>(Act) | Implementar las mejoras identificadas para el SGSI.<br>Implementar las acciones correctivas y preventivas pertinentes.<br>Comunicar acciones y mejoras a todas las partes involucradas.<br>Asegurarse que las mejoras logren los objetivos previstos. |

Fuente: Articulo de la revista ESPOL Vol. 28 (30).

# III. HIPÓTESIS

## 3.1 Hipótesis General

La evaluación de implementación del sistema de gestión de seguridad de la información en la Municipalidad Distrital de José Crespo y Castillo aplicando la norma ISO 27001:2013 - Aucayacu; 2018, permitirá mejorar los procesos con respecto a la políticas, seguridad, organización y evaluación de las TIC.

## 3.2 Hipótesis específicas

1. El análisis de la seguridad de la información permitirá conocer la situación actual de la Municipalidad Distrital de José Crespo y Castillo.
2. La Determinación de los objetivos de control de seguridad de la información, basado en la norma ISO / IEC 27001 permitirá administrar los activos de información bajo estándares internacionales.
3. La Propuesta de la aplicación de la Norma ISO/IEC 27001, asegurara una mejor seguridad de la información en la Municipalidad Distrital de José Crespo y Castillo.

# IV. METODOLOGÍA

## 4.1. Tipo y nivel de la investigación

La investigación cuantitativa, conlleva a la estructuración, a través de la recopilación y análisis de datos, las cuales son obtenidos de distintas fuentes. Este tipo de investigación implica el uso de herramientas informáticas, estadísticas, y matemáticas para obtener resultados. Es concluyente en su propósito ya que permite cuantificar el problema y entender qué tan

generalizado está mediante la búsqueda de resultados proyectables a una población mayor. (31).

La investigación descriptiva, permite conseguir, conocimiento y comprensión de diferentes situaciones, actitudes y costumbres que predominan en una organización, por lo cual requiere del uso de palabras correctas que describan exactamente las actividades, procesos y personas involucradas. La investigación descriptiva es un método científico que implica observar y describir el comportamiento o situación actual en que se encuentra la empresa investigada, para definir un análisis y procesos de estudio de las variables obtenidas (31).

## 4.2. Diseño de la investigación

Investigación no experimental, se ejecuta sin manipular deliberadamente las variables. Se fundamenta en la observación de fenómenos tal y como se dan en su contexto natural para analizarlos con posterioridad. En este tipo de investigación no hay condiciones ni estímulos a los cuales se expongan los sujetos del estudio. Los sujetos son observados en su ambiente natural. (32).

Transversal:
La investigación transversal es un método no experimental para recoger y analizar datos en un momento determinado. Se basa en la recolección de información para ser analizar en el estado en que se encuentran las variables de estudio en un único tiempo determinado (32).

El diseño de la investigación fue no experimental, porque el investigador observa lo que ocurre de forma natural, sin intervenir de manera alguna y se

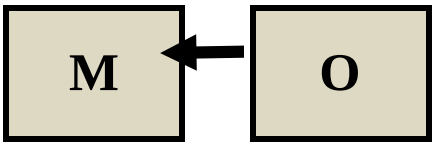
realizó sin manipular deliberadamente las variables, es decir se observó los fenómenos tal y como se dan en su contexto natural para después analizarlos (33).

El diseño de la investigación tiene la siguiente estructura:

Donde:

M = Muestra.

O = Observación.




Por las características de la investigación reúne las condiciones de una investigación cuantitativa, porque permite examinar los datos de manera numérica, para tratar de conocer los hechos, procesos, estructuras y personas en su totalidad, y no a través de la medición de algunos de sus elementos (34).

La metodología cuantitativa es una forma estructurada de recopilar y analizar datos obtenidos de distintas fuentes, esto implica el uso de herramientas informáticas, estadísticas, y matemáticas para obtener resultados. Es concluyente en su propósito ya que trata de cuantificar el problema y entender qué tan generalizado está mediante la búsqueda de resultados proyectables a una población mayor (35).

El tipo de investigación fue descriptiva, porque el objetivo de la investigación es llegar a conocer la situación, costumbres y actitudes predominantes a través de la descripción exacta de las actividades, objetos, procesos y personas, y que no se limita a la recolección de datos. En esta investigación se examinan y describen las variables de estudio. Por las características de su ejecución la investigación es de corte trasversal, las mediciones se hacen en una sola ocasión, por lo que no existen períodos de seguimiento. En otras palabras, con

este diseño, se efectúa el estudio de variables en un momento determinado (36).

.

## 4.3. Población y Muestra.

### La Población.

Actualmente la Municipalidad Distrital de José Crespo y Castillo, cuenta con 198 Trabajadores.

### La Muestra.

El portal de la educación de chile educarchile (37), nos dice "llamamos muestra a un subconjunto de la población que se supone representativa del total de la población y cuyo estudio debería entregar información aplicable a todos los individuos de la población". Siendo 30, tal como se muestra en el Anexo

## 4.4. Definición de Operacionalización de Variables

Tabla Nro. 7: Matriz de operacionalización de la variable adquisición e implementación.

| Variable | Definición conceptual | Dimensiones | Indicadores | Escala de medición | Definición operacional |
|---|---|---|---|---|---|
| Sistema de gestión de seguridad de la información (SGSI), basado en la norma ISO / IEC 27001:2013. | -Estandarización (ISO), define a los SGSI como un enfoque sistemático para administrar la información sensible de la compañía para que permanezca segura. Incluye personas, procesos y sistemas de TI mediante la aplicación de un proceso de gestión de riesgos. (22) | Situación actual del SGSI en Municipalidad Distrital de José Crespo y Castillo | - Políticas de seguridad.<br>- Aspectos organizativos de la seguridad de la información.<br>- Seguridad ligada a los recursos humanos.<br>- Gestión de activos.<br>- Control de accesos.<br>- Cifrado de seguridad.<br>- Seguridad física y ambiental.<br>- Seguridad en la operatividad.<br>- Seguridad en la Telecomunicaciones.<br>- Adquisición, desarrollo y mantenimiento de los sistemas de información. | Ordinal | - Si. -<br>No. |

| | | | | | |
|---|---|---|---|---|---|
| | -ISO / IEC 27001: 2013 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de la seguridad de la información dentro del contexto de la organización. (24), | -Necesidad de Implementar el sistema de gestión de seguridad de información. | - Políticas de seguridad.<br>- Aspectos organizativos de la seguridad de la información.<br>- Seguridad física y ambiental.<br>- Seguridad en la operatividad.<br>- Seguridad en la Telecomunicaciones.<br>- Adquisición, desarrollo y mantenimiento de los sistemas de información.<br>- Relación con suministradores.<br>- Gestión de los incidentes en la seguridad de la información.<br>- Aspectos de la seguridad de la información en la gestión de la continuidad del negocio.<br>- Cumplimiento. | | - Si. -<br>No. |

Fuente: Elaboración propia.

## 4.5. Técnicas e instrumentos.

### 4.5.1. Procedimientos de la recolección de datos.

En la realización de la investigación, se utilizó la técnica de la encuesta, la cual es un estudio observacional, es una técnica de recogida de datos mediante la aplicación de un cuestionario a una muestra de individuos. A través de las encuestas se pueden conocer las opiniones, las actitudes y los comportamientos de los ciudadanos.

Según la investigación de Osmar S., en una encuesta se realizan una serie de preguntas sobre uno o varios temas a una muestra de personas seleccionadas, siguiendo una serie de reglas científicas que hacen que esa muestra sea, en su conjunto, representativa de la población general de la que procede (38).

## 4.6. Plan de análisis

Los datos obtenidos fueron codificados y luego ingresados en una hoja de cálculo del programa Microsoft Excel 2013. Además, se procedió a la tabulación de los mismos. Se realizó el análisis de datos que sirvió para establecer las frecuencias y realizar el análisis de distribución de dichas frecuencias.

### 4.7. Matriz de consistencia.

Tabla Nro. 8: Matriz de Consistencia.

| Problema | Objetivos | Hipótesis | Variables | Metodología |
|---|---|---|---|---|
| ¿De qué manera el Sistema de Gestión de Seguridad de la Información en la Municipalidad Distrital de José Crespo y Castillo, basado en la norma ISO 27001:2013 - Aucayacu; 2018, ayudara a mejorar la administración de la seguridad de la información? | Evaluar la implementación del sistema de gestión de seguridad de la información en la Municipalidad Distrital de José Crespo y Castillo, basado en la norma ISO 27001:2013 - Aucayacu; 2018. | La evaluación de implementación del sistema de gestión de seguridad de la información en la Municipalidad Distrital de José Crespo y Castillo aplicando la norma ISO 27001:2013 - Aucayacu; 2018, permitirá mejorar los procesos con respecto a la políticas, seguridad, organización y evaluación de las TIC. | Sistema Gestión de Seguridad de la información, basado en la norma ISO 27001: 2013. | Tipo: descriptiva<br>Nivel: Cuantitativo<br>Diseño: No experimental y de corte transversal |
| | **Objetivos Específicos** | **Hipótesis Especificas** | | |
| | **1.** Analizar la inseguridad de la seguridad de la información, en la actual de la Municipalidad Distrital de José Crespo y Castillo. | 1. El análisis de la seguridad de la información permitirá conocer la situación actual de la Municipalidad Distrital de José Crespo y Castillo. | | |

| | | | | |
|---|---|---|---|---|
| | | | | |
| | 2. Evaluar los marcos de referencias que ayuden a mejorar la seguridad de la información en la Municipalidad Distrital de José Crespo y Castillo. | 2. La Determinación de los objetivos de control de seguridad de la información, basado en la norma ISO / IEC 27001 permitirá administrar los activos de información bajo estándares internacionales.<br>. | | |
| | 3. Proponer la aplicación de la Norma ISO / IEC 27001, para asegurar mejorar la seguridad de la información. | 3. La Propuesta de la aplicación de la Norma ISO/IEC 27001, asegurara una mejor seguridad de la información en la Municipalidad Distrital de José Crespo y Castillo. | | |

Fuente: Elaboración Propia.

## 4.8. Principios éticos

Durante el desarrollo de la presente investigación denominada "Evaluación de un sistema de gestión de seguridad de la información basado en la norma ISO 27001:2013, en la Municipalidad Distrital de José Crespo y Castillo - Aucayacu; 2018. Hemos considerado en forma estricta el cumplimiento de los principios éticos que permitan asegurar la originalidad de la Investigación. Asimismo, se han respetado los derechos de propiedad intelectual de los libros de texto y de las fuentes electrónicas consultadas, necesarias para estructurar el marco teórico. Los principios éticos establecen las fuentes, del conocimiento y progreso de trabajos científicos y propiedad intelectual (39).

# V. RESULTADOS.

## 5.1 Resultados.

### 5.1.1 Dimensión 1: Situación actual del SGSI en la Municipalidad Distrital de José Crespo y Castillo - Aucayacu; 2018.

Tabla Nro. 9: Documentación de las Políticas de seguridad de la Información.

Distribución de porcentaje y frecuencias de trabajadores relacionadas con La documentación de las Políticas de seguridad de la Información, respecto a las TIC en la Municipalidad Distrital de José Crespo y Castillo - Aucayacu; 2018.

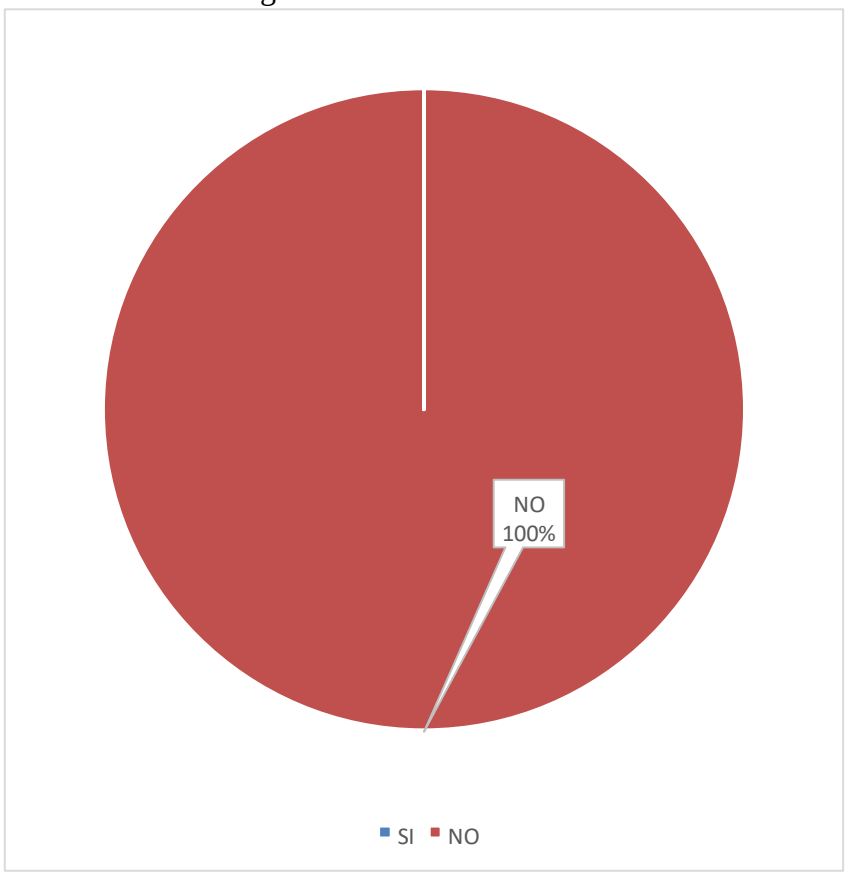
| Alternativas | n | % |
|---|---|---|
| Si | - | - |
| No | 30 | 100 |
| Total | 30 | 100 |

Fuente: Origen del instrumento aplicado a los trabajadores de la Municipalidad Distrital de José Crespo y Castillo, para responder a la pregunta: ¿Considera usted que las políticas de la seguridad de seguridad de la información, se encuentran documentadas?

Aplicado por: Dávila, M; 2018.

En la Tabla Nro. 9, se observa que el 100 % de los encuestados manifestaron que NO conocen sobre las políticas de Seguridad de la Información, no se encuentran documentadas.

Gráfico Nro. 4: Porcentaje sobre la Documentación de las Políticas de seguridad de la Información.




Fuente: Tabla Nro. 9: Documentación de las Políticas de seguridad de la Información.

Tabla Nro. 10: Aspectos Organizativos de la Información.

Porcentajes y frecuencias relacionadas con el análisis de los aspectos organizativos de la información en la Municipalidad Distrital de José Crespo y Castillo - Aucayacu; 2018.

| Alternativas | n | % |
|---|---|---|
| Si | 6 | 20 |
| No | 24 | 80 |

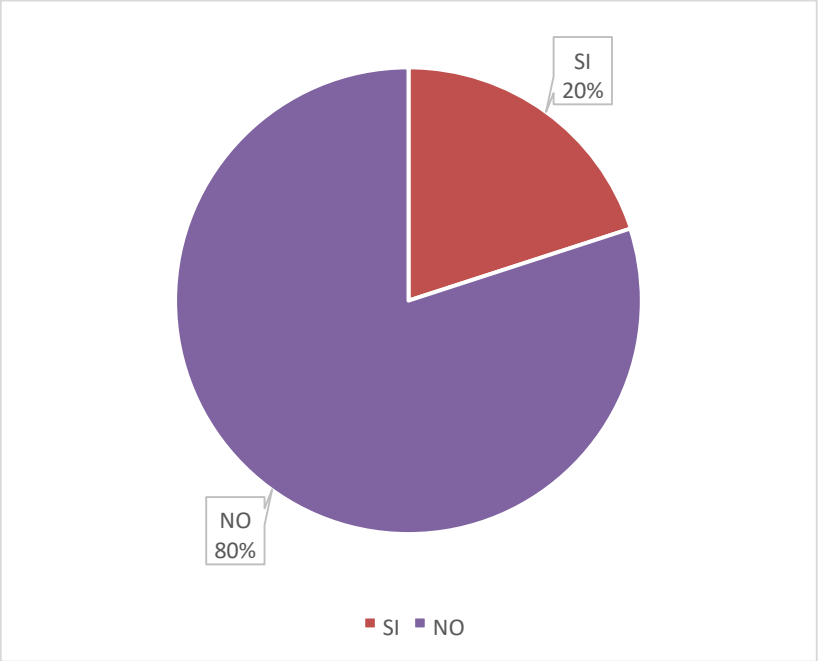
| | | |
|---|---|---|
| Total | 30 | 100 |

Fuente: Origen del instrumento aplicado a los trabajadores de Municipalidad Distrital de José Crespo y Castillo; para responder a la pregunta: ¿Existen procesos establecidos en la organización de la seguridad de la información?

Aplicado por: Dávila, M; 2018.

En la Tabla Nro. 10, se observa que el 80% de los encuestados manifestaron que NO existen aspectos organizativos en la seguridad de la información, mientras que el 20% indica que SI existen.

Gráfico Nro. 5: Porcentajes de los aspectos organizativos de la seguridad de la información.




Fuente: Tabla Nro.  10: Control de los equipos Informáticos.

Tabla Nro.  11: Roles y Responsabilidades del Personal de TI.

Distribución de frecuencias y porcentajes relacionadas con la Seguridad de los recursos humanos, respecto los procesos documentados de responsabilidades y funciones que tiene a cargo el equipo de TI en cantos roles en el área de TI; Municipalidad Distrital de José Crespo y Castillo - Aucayacu; 2018.

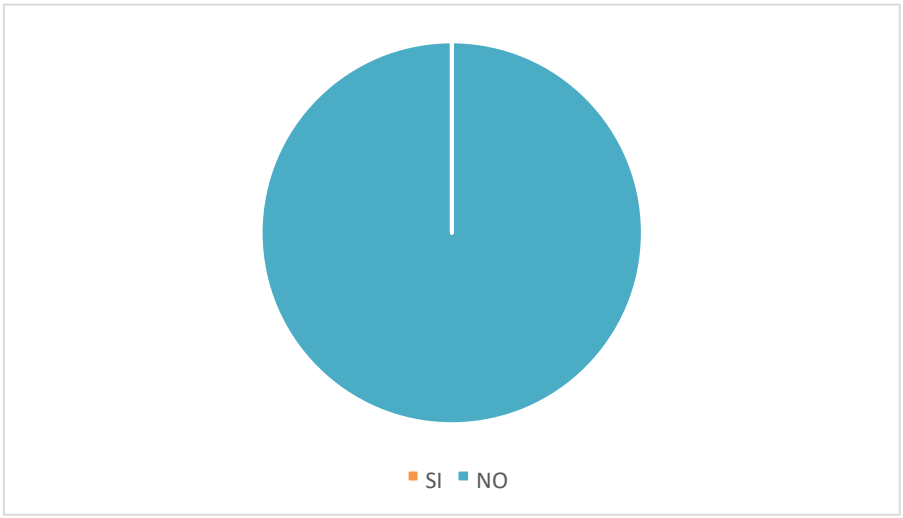
| Alternativas | n | % |
|---|---|---|
| Si | - | - |
| No | 30 | 100 |
| Total | 30 | 100 |

Fuente: Origen del instrumento aplicado a los trabajadores de la Municipalidad Distrital de José Crespo y Castillo; para responder a la pregunta: ¿Existen procesos documentados, respecto a las responsabilidades y roles del personal de TI?

Aplicado por: Dávila, M; 2018.

En la Tabla Nro. 11, se observa que el 100% de los encuestados manifestaron que, NO existen procesos documentados respecto a los roles y responsabilidades.

Gráfico Nro. 6: Porcentaje sobre Roles y Responsabilidades del Personal de TI.




Fuente: Tabla Nro.  11: Roles y Responsabilidades del Personal de TI.

Tabla Nro. 12: Evaluación de la seguridad física y ambiental.

Distribuciones de frecuencias y porcentajes relacionadas con la Verificación de la seguridad física y ambiental; en la Municipalidad Distrital de José Crespo y Castillo - Aucayacu; 2018. Para evaluar si los equipos se encuentran protegidos ante las dificultades medio ambientales.

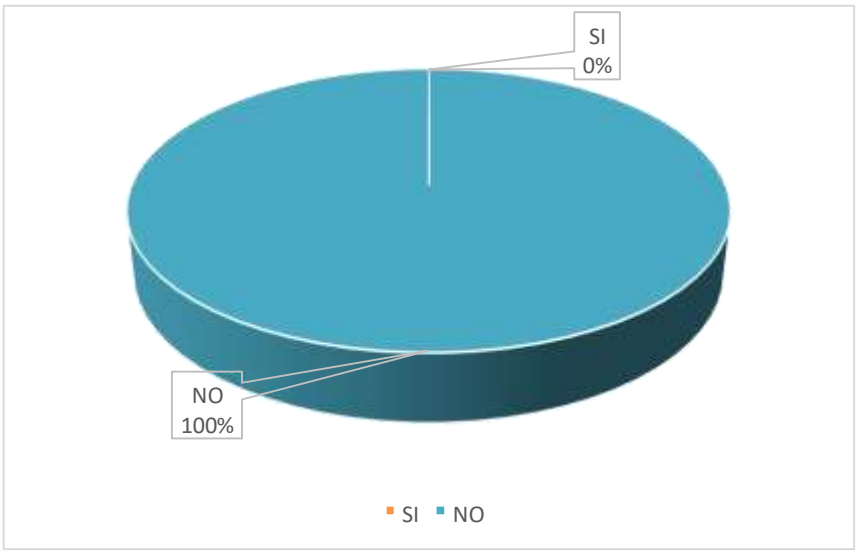
| Alternativas | n | % |
|---|---|---|
| Si | - | - |
| No | 30 | 100 |
| Total | 30 | 100 |

Fuente: Origen del instrumento aplicado a los trabajadores de la Municipalidad Distrital de José Crespo y Castillo; para responder a la pregunta: ¿Existe un proceso documentado, respecto a velar o salvaguardar los equipos de TI, ante problemas medio ambientales?

Aplicado por: Dávila, M; 2018.

En la Tabla Nro. 12, se observa que el 100 % de los encuestados manifestaron que, NO existe un proceso establecido para salvaguardar los equipos en relación a los problemas medio ambientales u otro similares.

Gráfico Nro. 7: Porcentaje sobre la evaluación de la seguridad física y ambiental.




Fuente: Tabla Nro.  12: Evaluación de la seguridad física y ambiental.

Tabla Nro.  13: Proceso de gestión y operación de las comunicaciones.

Distribuciones de frecuencias y porcentajes relacionadas con la evaluación de la gestión y operación de las comunicaciones; en la Municipalidad Distrital de José Crespo y Castillo - Aucayacu; 2018.

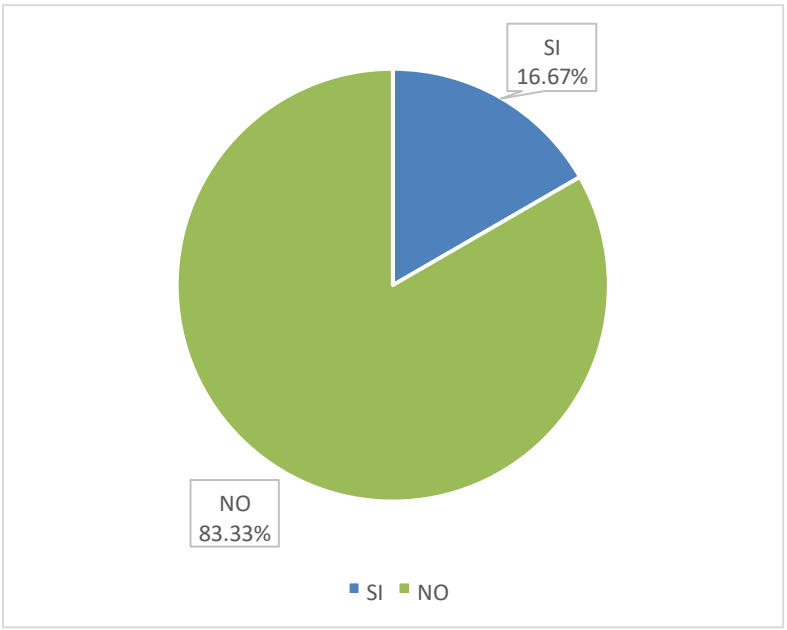
| Alternativas | n | % |
|---|---|---|
| Si | 5 | 16.67 |
| No | 25 | 83.33 |
| Total | 30 | 100 |

Fuente: Origen del instrumento aplicado a los trabajadores de Municipalidad Distrital de José Crespo y Castillo. Para responder a la pregunta: ¿Existen proceso documentados para evaluar la gestión y operación de las comunicaciones?

Aplicado por: Dávila, M; 2018.

En la Tabla Nro. 13, se observa que el 16,67% de los encuestados manifestaron que, SI están satisfechos con respecto a la gestión de operación y comunicaciones, mientras que el 83,33% de los trabajadores expresan que NO existe un proceso establecido respecto a la gestión de operación y comunicaciones.

Gráfico Nro. 8: Porcentaje sobre proceso de gestión y operación de las comunicaciones.




Fuente: Tabla Nro. 13: Proceso de gestión y operación de las comunicaciones.

Tabla Nro. 14: Evaluación del control de accesos.

Distribuciones de frecuencias y porcentajes relacionadas con la evaluación de los procesos de control de accesos; en la Municipalidad Distrital de José Crespo y Castillo - Aucayacu; 2018.

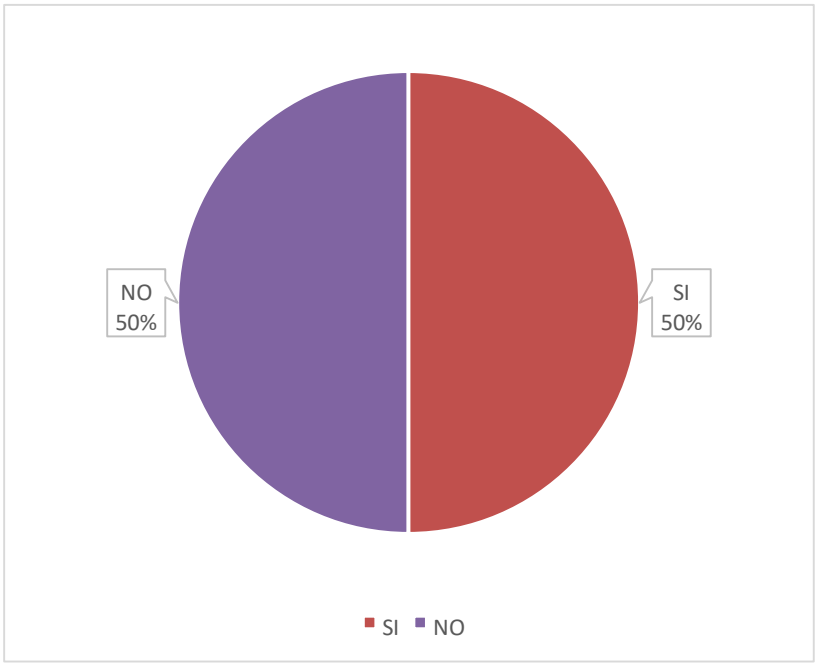
| Alternativas | n | % |
|---|---|---|
| Si | 15 | 50 |
| No | 15 | 50 |
| Total | 30 | 100 |

Fuente: Origen del instrumento aplicado a los trabajadores de Municipalidad Distrital de José Crespo y Castillo; para responder a la pregunta: ¿Los procesos de control de accesos son gestionados y evaluados?

Aplicado por: Dávila M; 2018.

En la Tabla Nro. 14, se observa que el 50% de los encuestados manifestaron que, SI existen un proceso de control y gestión de accesos a usuarios, mientras que el 50% de los trabajadores expresan que NO existen.

Gráfico Nro. 9: Porcentaje sobre evaluación del control de accesos.




Fuente: Tabla Nro.14: Evaluación del control de accesos.

Tabla Nro. 15: Existencia de la seguridad física y ambiental.

Distribuciones de frecuencias y porcentajes relacionadas con la evaluación de existencia de seguridad física y ambiental; en la Municipalidad Distrital de José Crespo y Castillo - Aucayacu; 2018.

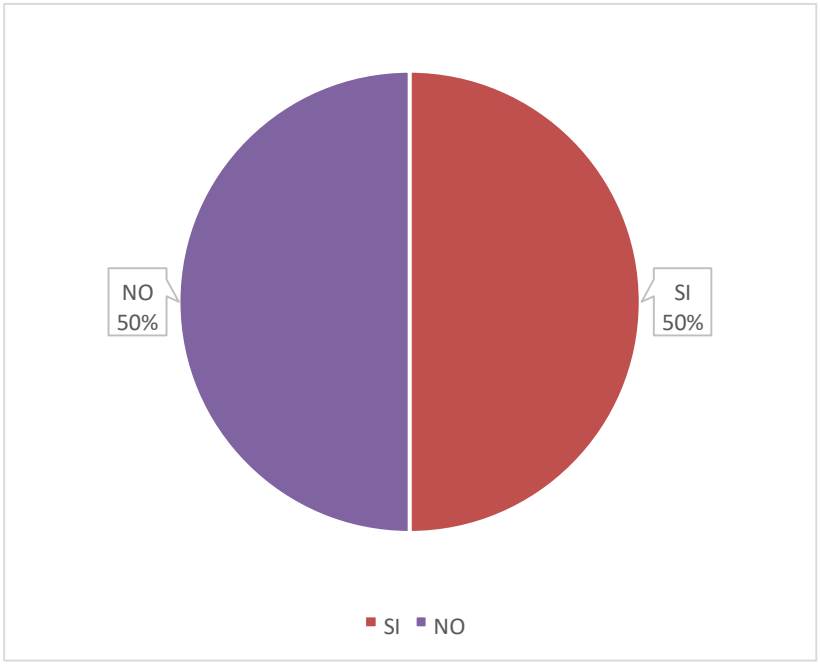
| Alternativas | n | % |
|---|---|---|
| Si | 15 | 50 |
| No | 15 | 50 |
| Total | 30 | 100 |

Fuente: Origen del instrumento aplicado a los trabajadores de Municipalidad Distrital de José Crespo y Castillo; para responder a la pregunta: ¿Existen procesos de seguridad física y ambiental, para salvaguardar la información?

Aplicado por: Dávila M; 2018.

En la Tabla Nro. 15, se observa que el 50% de los encuestados manifestaron que, SI debe mejorar los procesos de existencia de evaluación física y ambiental, mientras que el 50% de los trabajadores expresan que NO existen procesos de seguridad física y ambiental, para salvaguardar la información.

Gráfico Nro.  10: Porcentaje sobre evaluación del control de accesos.




Fuente: Tabla Nro.15: Existencia de la seguridad física y ambiental.

Tabla Nro. 16: Procesos de los sistemas de información.

Distribuciones de frecuencias y porcentajes relacionadas con los procesos de los sistemas de información; en la Municipalidad Distrital de José Crespo y Castillo - Aucayacu; 2018.

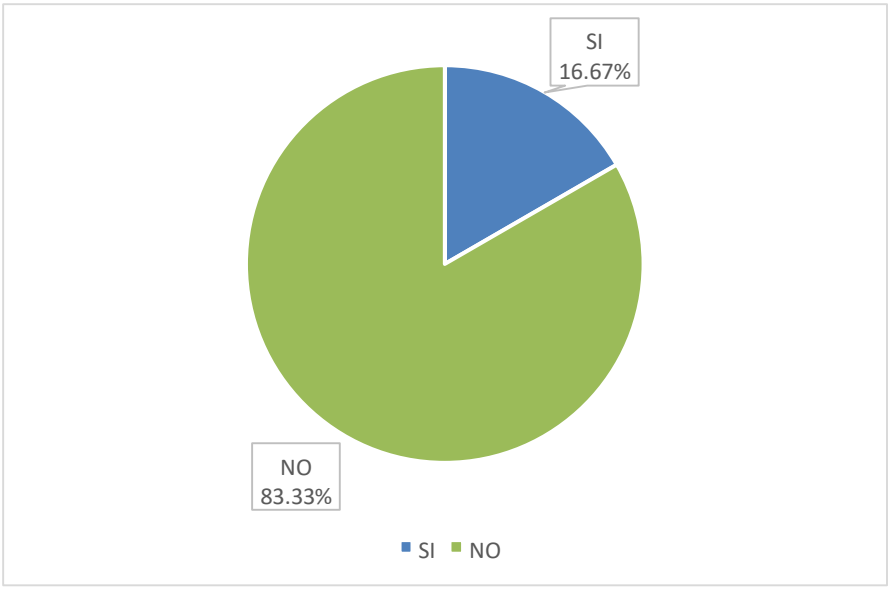
| Alternativas | n | % |
|---|---|---|
| Si | 5 | 16.67 |
| No | 25 | 83.33 |
| Total | 30 | 100 |

Fuente: Origen del instrumento aplicado a los trabajadores de Municipalidad Distrital de José Crespo y Castillo. Para responder a la pregunta: ¿Los procesos operativos de los Sistemas de información son seguros?

Aplicado por: Dávila, M; 2018.

En la Tabla Nro. 16, se observa que el 16,67% de los encuestados manifestaron que, SI están satisfechos de los procesos operativos de la seguridad de la información, mientras que el 83,33% de los trabajadores expresan que NO existe un proceso seguro con respecto a la operatividad de los sistemas de información.

Gráfico Nro. 11: Porcentaje de los procesos operativos de los sistemas de información.




Fuente: Tabla Nro. 16: Procesos de los sistemas de información.

Tabla Nro. 17: Políticas de seguridad de las telecomunicaciones.

Porcentajes y frecuencias relacionadas con a la seguridad de las Telecomunicaciones; en la Municipalidad Distrital de José Crespo y Castillo - Aucayacu; 2018.

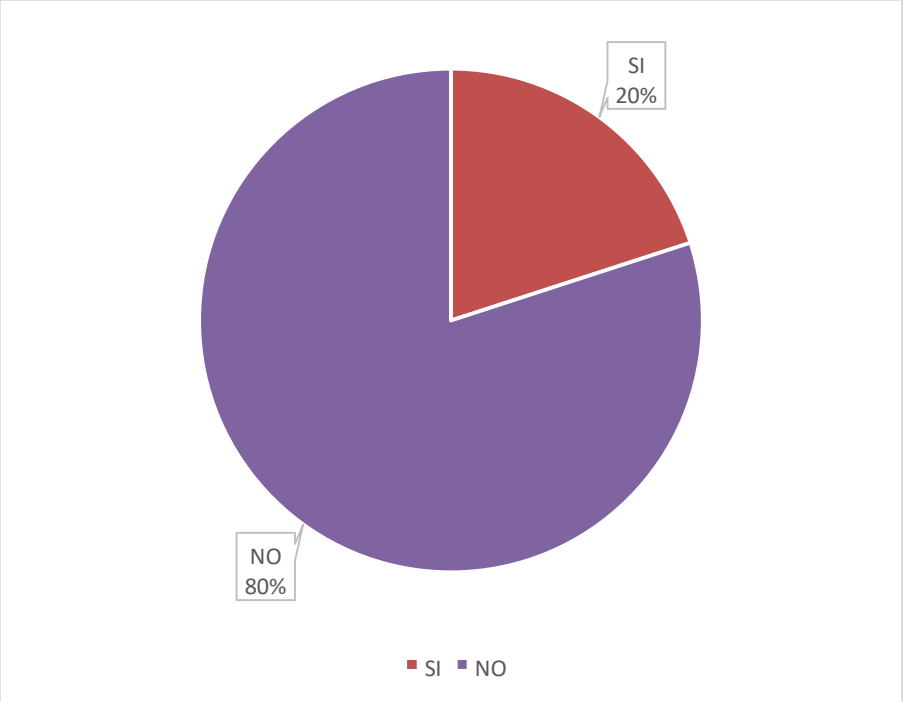
| Alternativas | n | % |
|---|---|---|
| Si | 6 | 20 |
| No | 24 | 80 |
| Total | 30 | 100 |

Fuente: Origen del instrumento aplicado a los trabajadores de Municipalidad Distrital de José Crespo y Castillo; para responder a la pregunta: ¿Existen políticas para la seguridad de las telecomunicaciones?

Aplicado por: Dávila, M; 2018.

En la Tabla Nro. 17, se observa que el 80% de los encuestados manifestaron que NO existen revisiones periódicas de las políticas de seguridad de la información, mientras que el 20% indica que SI existen revisiones periódicas.

Gráfico Nro. 12: Porcentajes de políticas de seguridad de telecomunicaciones.




Fuente: Tabla Nro. 17: Políticas de seguridad de las telecomunicaciones.

### 5.1.2 Dimensión 2: Necesidad de Implementar el Sistema de Gestión de la Seguridad de la Información.

Tabla Nro. 18: Evaluación de las políticas de seguridad de la información.

Distribuciones de frecuencias y porcentajes relacionadas con la importancia de evaluar las políticas de seguridad de la información; en la Municipalidad Distrital de José Crespo y Castillo - Aucayacu; 2018.

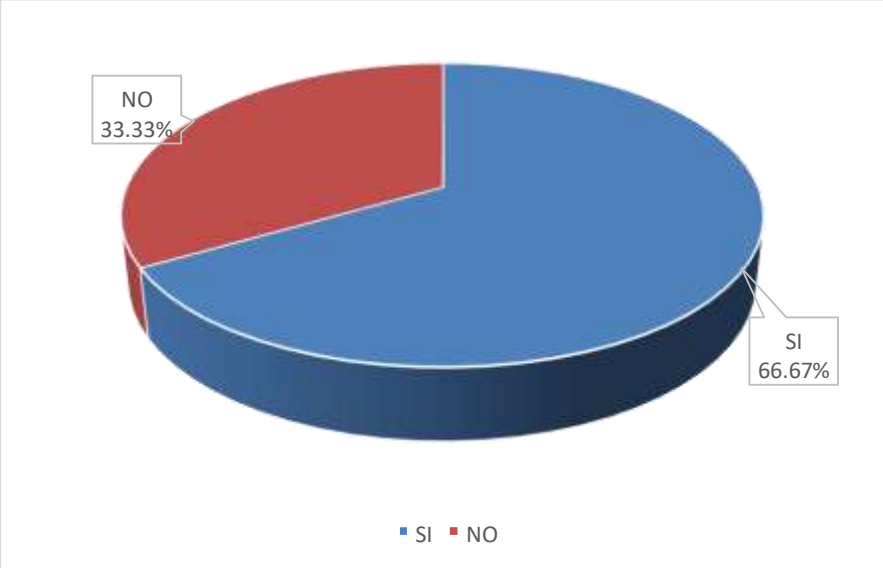
| Alternativas | n | % |
|---|---|---|
| Si | 20 | 50 |
| No | 10 | 50 |
| Total | 30 | 100 |

Fuente: Origen del instrumento aplicado a los trabajadores de la Municipalidad Distrital de José Crespo y Castillo; para responder a la pregunta: ¿Es necesario evaluar las políticas de seguridad de la información?

Aplicado por: Dávila, M; 2018.

En la Tabla Nro. 18, Se puede observar que el 66.67% de los trabajadores encuestados expresaron que, SI están de acuerdo en que se realice una evaluación de las políticas de seguridad de la información, a fin de mejorar este proceso, mientras que 33.33% de los encuestados indicó que NO es necesario la evaluación de las políticas de seguridad de la información.

Gráfico Nro. 13: Porcentaje sobre evaluación de las políticas de seguridad de la información.




Fuente: Tabla Nro. 18: Evaluación de las políticas de seguridad de la información.

Tabla Nro. 19: Plan de gestión de cambios.

Distribución de frecuencias y porcentajes relacionadas con elaboración de un plan de gestión de cambios en los procesos de TI; en la Municipalidad Distrital de José Crespo y Castillo - Aucayacu; 2018.

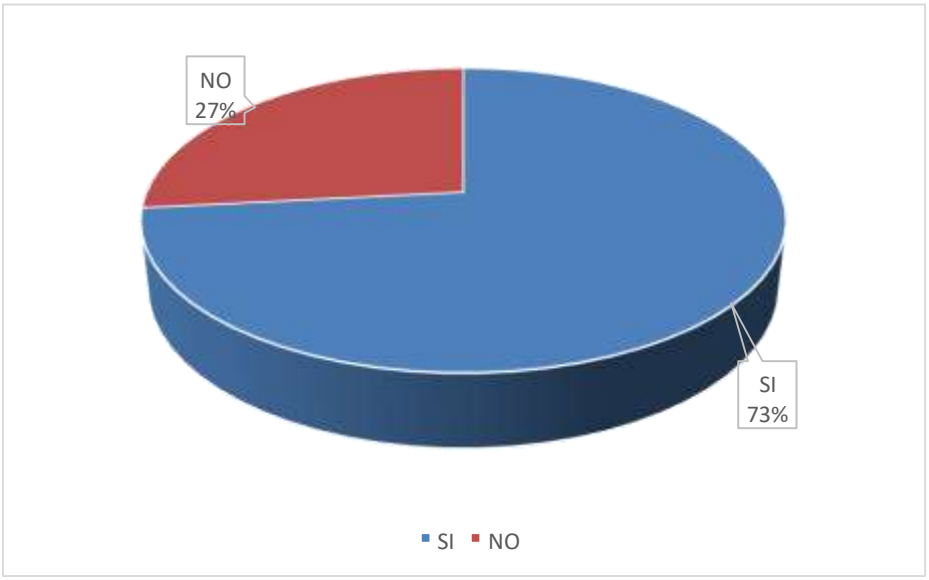
| Alternativas | n | % |
|---|---|---|
| Si | 22 | 50 |
| No | 8 | 50 |
| Total | 30 | 100 |

Fuente: Origen del instrumento aplicado a los trabajadores de la Municipalidad Distrital de José Crespo y Castillo; para responder a la pregunta: ¿Es importante elaborar un plan de gestión de cambios?

Aplicado por: Dávila, M; 2018.

En la Tabla Nro. 19, Se puede observar que el 73.33% de los trabajadores encuestados expresaron que, SI es necesario realizar un plan de gestión de cambios, mientras que el 26.67% de los encuestados indicó que NO.

Gráfico Nro. 14: Porcentaje de implementar plan de gestión de




Fuente: Tabla Nro.  19: Plan de gestión de cambios.

Tabla Nro. 20: Documentación roles y funciones de TI.

Distribución de frecuencias y porcentajes relacionadas al proceso de Documentar los roles y funciones en el personal de TI; en la Municipalidad Distrital de José Crespo y Castillo - Aucayacu; 2018.

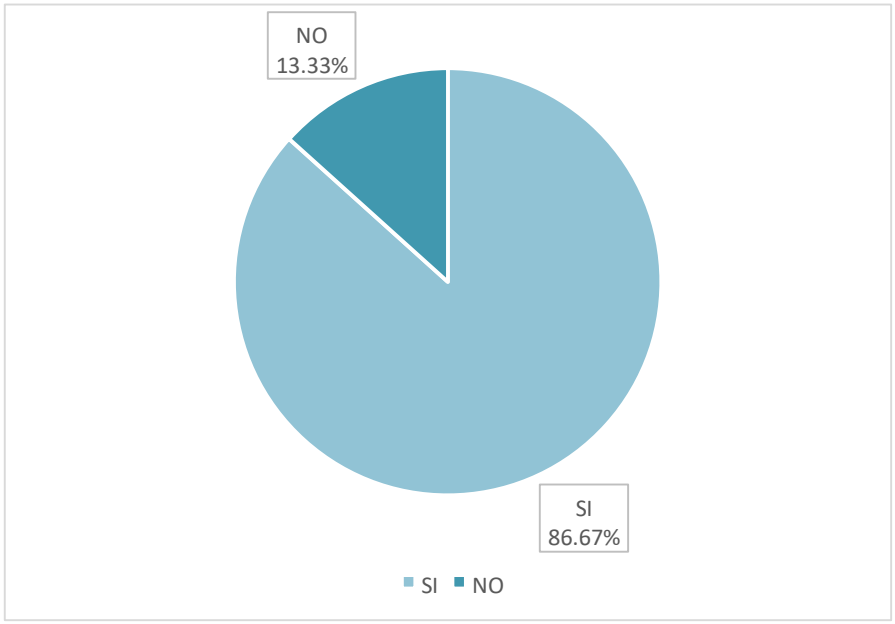
| Alternativas | n | % |
|---|---|---|
| Si | 26 | 86.67 |
| No | 4 | 13.33 |
| Total | 30 | 100 |

Fuente: Origen del instrumento aplicado a los trabajadores de la Municipalidad Distrital de José Crespo y Castillo; para responder a la pregunta: ¿Es necesario documentar los roles y funciones del personal de TI y usuarios que utilizan las TI?

Aplicado por: Dávila, M; 2018.

En la Tabla Nro. 20, Se puede observar que el 86.67 % de los trabajadores encuestados, expresaron que, SI es necesario documentar los procesos de roles y funciones relacionados a las TI, mientras que el 13.33 % de los encuestados indicó que NO es tan necesario.

Gráfico Nro. 15: Porcentaje de documentar roles y funciones de TI.




Fuente: Tabla Nro.  20: Documentación roles y funciones de TI.

Tabla Nro.  21: Documentar procesos para la seguridad física y ambiental.

Distribución de frecuencias y porcentajes relacionadas con mejorar los procesos de seguridad física y ambiental; en la Municipalidad Distrital de José Crespo y Castillo - Aucayacu; 2018.

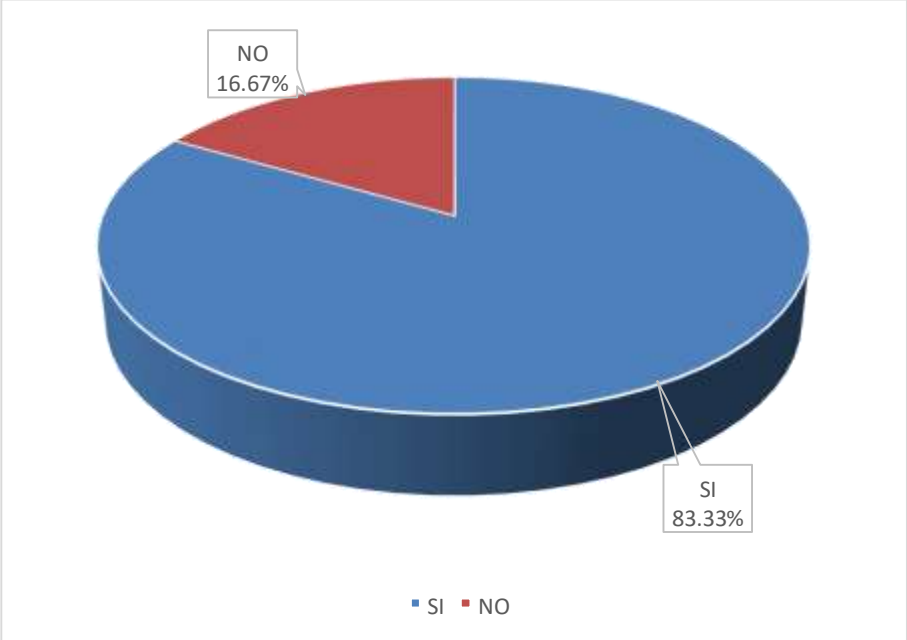
| Alternativas | n | % |
|---|---|---|
| Si | 25 | 83.33 |
| No | 5 | 16.67 |
| Total | 30 | 100 |

Fuente: Origen del instrumento aplicado a los trabajadores de la Municipalidad Distrital de José Crespo y Castillo - Aucayacu; para responder a la pregunta: ¿Es necesario establecer procesos de mejorar la seguridad física y ambiental?

Aplicado por: Dávila, M; 2018.

En la Tabla Nro. 21, Se observa en los resultados, que el 83.33 % del personal de la Municipalidad considera que es necesario, mientras que el 16.67 %, NO creen que no es necesario.

Gráfico Nro. 16: Porcentaje de documentar procesos para la seguridad física y ambiental.




Fuente: Tabla Nro. 21: Documentar procesos para la seguridad física y ambiental.

Tabla Nro. 22: Procesos para la gestión de las comunicaciones y operaciones.

Distribución de frecuencias y respuestas relacionadas a la facilidad de implantar procesos para la gestión de las comunicaciones y operaciones de

TI; en la Municipalidad Distrital de José Crespo y Castillo - Aucayacu; 2018.

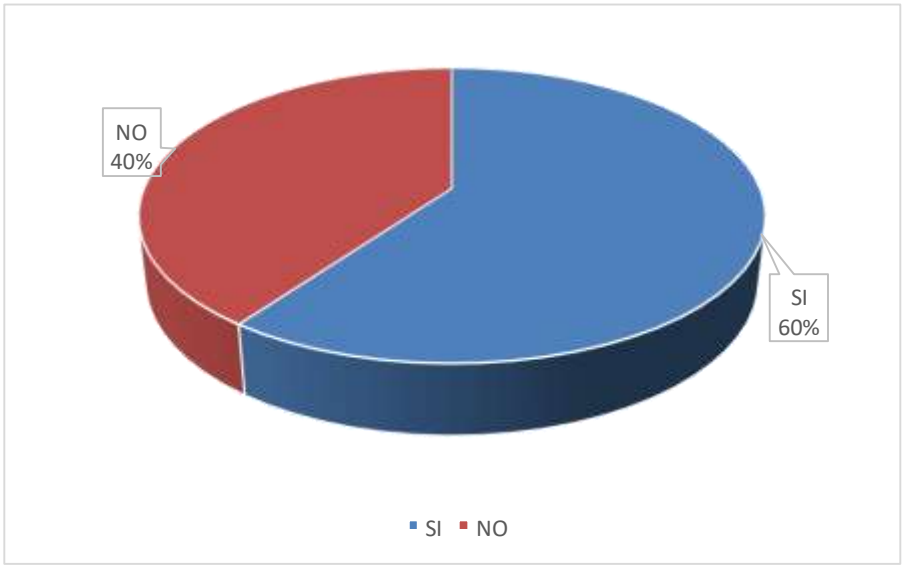
| Alternativas | n | % |
|---|---|---|
| Si | 18 | 60 |
| No | 12 | 40 |
| Total | 30 | 100 |

Fuente: Origen del instrumento aplicado a los trabajadores de la Municipalidad Distrital de José Crespo y Castillo - Aucayacu; 2018; para responder a la pregunta: ¿Es necesario implementar procesos, para mejorar la gestión de comunicaciones y operaciones?

Aplicado por: Dávila, M; 2018.

En la Tabla Nro. 22, Se puede observar que el 60.00% del personal encuestado, considera que es necesario implementar procesos que consoliden las mejoras de las comunicaciones y operaciones, mientras que el 40 % de los encuestados indicó que NO.

Gráfico Nro. 17: Porcentaje de procesos para la gestión de las comunicaciones y operaciones.




Fuente: Tabla Nro.  22: Procesos para la gestión de las comunicaciones y operaciones.

Tabla Nro.  23: Procesos para la evaluación de control de accesos.

Distribución de frecuencias y respuestas relacionadas a la implementación de procesos de evaluación de control de accesos; en la Municipalidad Distrital de José Crespo y Castillo - Aucayacu; 2018.

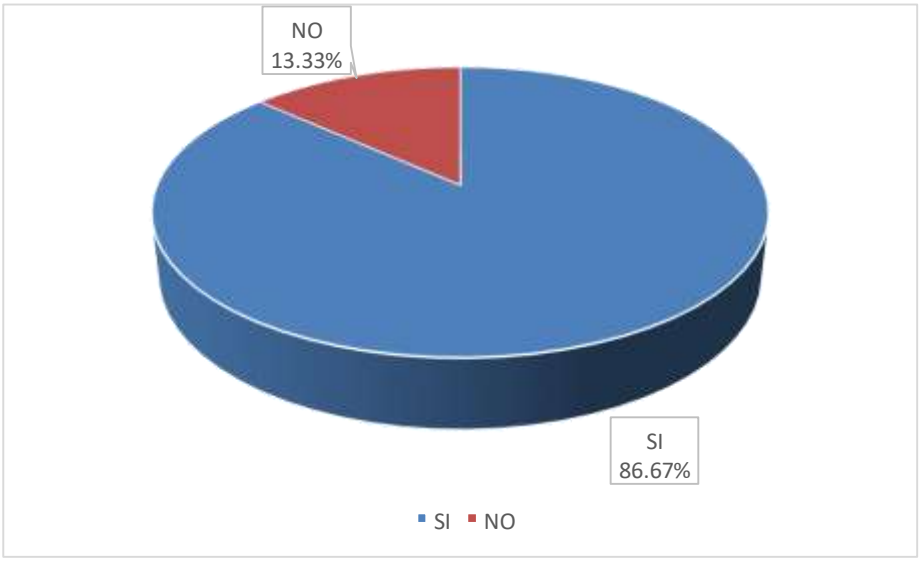
| Alternativas | n | % |
|---|---|---|
| Si | 26 | 86.67 |
| No | 4 | 13.33 |
| Total | 30 | 100.00 |

Fuente: Origen del instrumento aplicado a los trabajadores de la Municipalidad Distrital de José Crespo y Castillo; para responder a la pregunta: ¿Considera necesario implementar procesos de evaluación y control de accesos?

Aplicado por: Dávila M; 2018.

En la Tabla Nro. 23, Se puede observar que el 86.67% de los trabajadores encuestados expresaron que, SI es necesario evaluar los procesos de accesos, mientras que el 13.33 % de los encuestados indicó que NO creen que el control de accesos ayudara a mejorar la seguridad de los sistemas de información.

Gráfico Nro. 18: Porcentaje Procesos para la evaluación de control de accesos.




Fuente: Tabla Nro. 23: Procesos para la evaluación de control de accesos.

### 5.1.3 Resumen de la Dimensión 1: Situación actual del SGSI en Municipalidad Distrital de José Crespo y Castillo - Aucayacu; 2018.

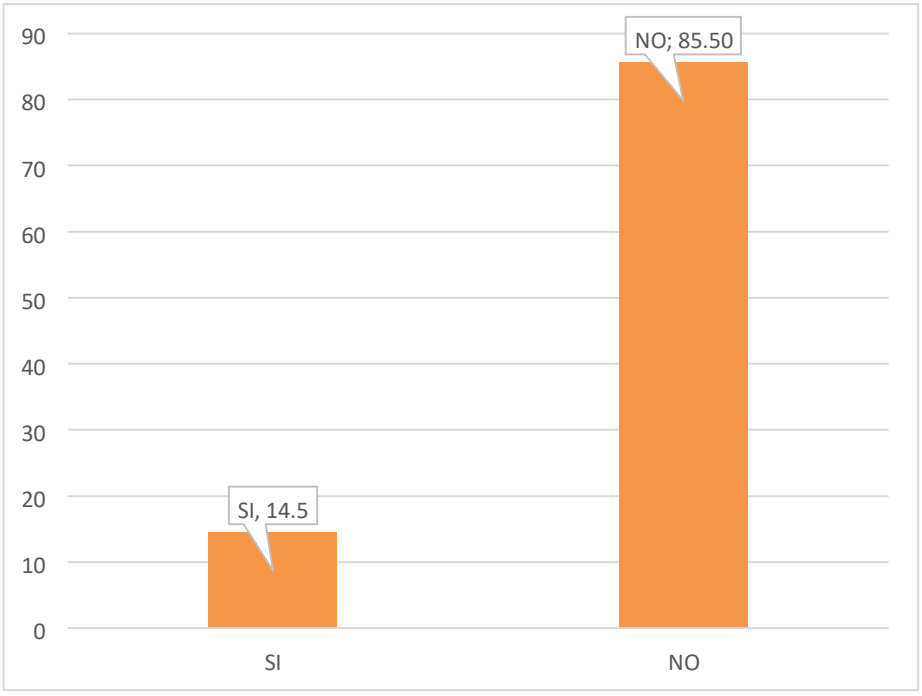
Tabla Nro. 24: Dimensión Situación actual del Sistema de Gestión de la Seguridad de la información.

Que de acuerdo a la evaluación realizada según los criterios que se muestran en la tabla, la situación actual del Sistema de Gestión de la Seguridad de la información no es la adecuada.

| **Dimensión 01: Situación actual del Sistema de Gestión de la Seguridad de la información.** | **SI** | **NO** |
|---|---|---|
| Evaluación de las políticas de seguridad de la información. | - | 100 |
| Analizar la gestión de cambios. | 20 | 80 |
| Revisar las funciones del recurso humano, relacionado a las TIC. | - | 100 |
| Verificar la seguridad física y ambiental, donde se encuentran los equipos informáticos. | - | 100 |
| Evaluar la gestión de las comunicaciones y operaciones. | 16.7 | 83.7 |
| Proceso de gestión y operación de las comunicaciones. | 16.67 | 83.33 |

| | | |
|---|---|---|
| Existencia de la seguridad física y ambiental. | 50 | 50 |
| Evaluación del control de accesos. | 50 | 50 |
| Políticas de seguridad de las telecomunicaciones. | 20 | 80 |
| Procesos de los sistemas de información. | 16.67 | 83.33 |
| Promedio Dimisión 01 | 14.50 | 85.50 |

Gráfico Nro. 19: Situación actual del Sistema de Gestión de la Seguridad de la información.




Fuente: Tabla Nro. 24: Dimensión Situación actual del Sistema de Gestión de la Seguridad de la información.

Se puede observar que el 85.50% de los trabajadores encuestados expresaron la situación actual del Sistema de gestión de la seguridad de la información no se encuentra implementado, mientras que un 14.5%, señalo que si existen procesos implementados.

### 5.1.4 Resumen de la Dimensión 2: Necesidad del SGSI en Municipalidad Distrital de José Crespo y Castillo - Aucayacu; 2018.

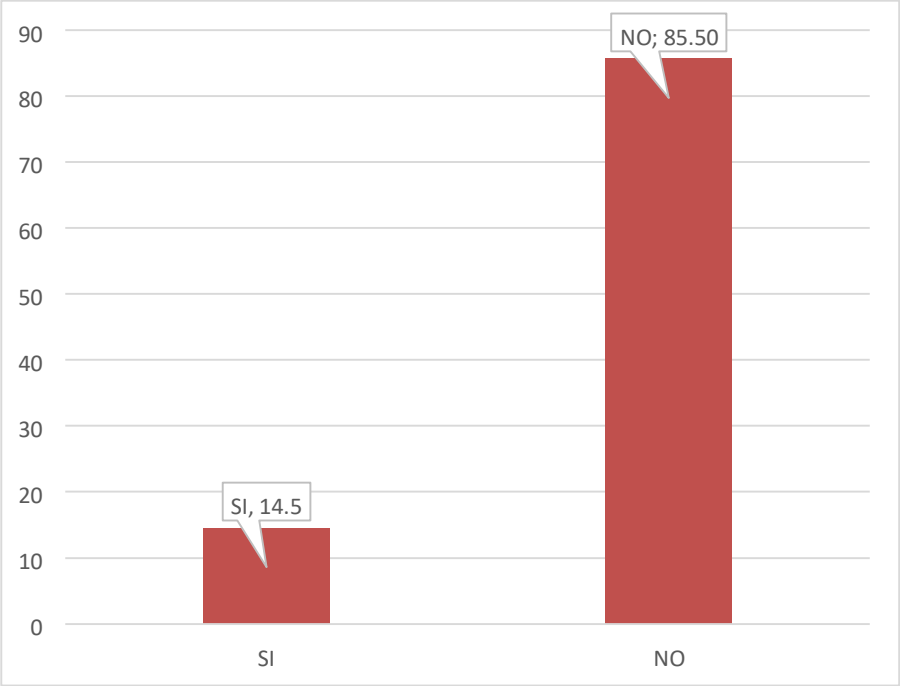
Tabla Nro. 25: Dimensión Necesidad de Implementar el Sistema de Gestión de la Seguridad de la Información.

Necesidad de Implementar el Sistema de Gestión de la Seguridad de la Información. Que de acuerdo a la evaluación realizada según los criterios que se muestran en la tabla, existe la necesidad de implementar el Sistema de Gestión de Seguridad de la Información a fin de mejorar los procesos de TI que se realizan Municipalidad Distrital de José Crespo y Castillo.

| **Dimensión 02: Necesidad de Implementar el Sistema de Gestión de la Seguridad de la Información.** | **SI** | **NO** |
|---|---|---|
| Considera que es necesario evaluar las políticas de seguridad de la información. | - | 100 |
| Elaborar plan de gestión de cambios. | 20 | 80 |
| Documentar los roles y funciones en el personal de TI | - | 100 |
| Establecer procesos para mejorar la seguridad física y ambiental. | - | 100 |
| Implementar procesos para la gestión de las comunicaciones y operaciones. | 16.7 | 83.7 |
| Implementar procesos de evaluación los procesos de control de accesos. | 50 | 50 |
| Reorganizar la seguridad física y ambiental de los equipos informáticos | 50 | 50 |
| Establecer perfiles para mejorar la operatividad | 30 | 70 |
| Regular las telecomunicaciones | 25 | 75 |
| Protocolos para mantenimiento de Software | 20 | 80 |

| | | |
|---|---|---|
| Promedio Dimisión 02 | 14.5 | 85.5 |

Gráfico Nro. 20: Necesidad de implementar el Sistema de Gestión de la Seguridad de la información.




Fuente: Tabla Nro. 26: Dimensión Necesidad de Implementar el Sistema de Gestión de la Seguridad de la Información.

Se puede observar que el 85.50% de los trabajadores encuestados expresaron que, si es necesario la implementación de un Sistema de Gestión de la Seguridad de la Información, mientras que un 14.5 %, señalo que si existen procesos implementados por lo que no es necesario implementar un SGSI.

## 5.2 Análisis de resultados

La presente investigación tuvo como objetivo general, evaluar la gestión de las TI en Municipalidad Distrital José Crespo y Castillo, mediante el sistema de seguridad de la información, aplicando el enfoque ISO 27001:2013. Para poder realizar una posterior aplicación de la norma ISO 27001:2013, se ha realizado un auto evaluación, que consiste en dos dimensiones, que describimos a continuación.

Dimensión 01; Situación actual del Sistema de Gestión de la Seguridad de la información, de acuerdo a los datos procesados mediante cuestionario se ha podido determinar que el 85.50%, considera que es necesario que la Municipalidad cuente con un Sistema de Gestión de la información y comunicación, basada en un marco internacional como es la norma ISO / IEC 27001, este resultado se asemeja a la investigación de Pallas M. (5), en su tesis titulado: "Metodología de Implantación de un SGSI en un grupo empresarial jerárquico", en donde se tuvo como resultados de la dimensión 01, está compuesto por los siguientes datos: El 83.33 % opinaron que los procesos de gestión y operación de las comunicaciones deben emplear criterios de políticas de seguridad, a fin de garantizar la confidencialidad, integridad, confiabilidad y disponibilidad de la información. Los resultados de la Dimensión Nro.01:

"Situación actual del Sistema de Gestión de Seguridad de la Información", ha permitido ver que los procesos se realizan de manera intuitiva, sin seguir protocolos o estándares que aseguren el funcionamiento y seguridad de la información en la Municipalidad Distrital José Crespo y Castillo; según la Organización Internacional para la estandarización (ISO), indica que los SGSI es

un enfoque sistemático que permiten administrar la información sensible de la compañía para que permanezca segura, incluye personas, procesos y sistemas de TI mediante la aplicación de un proceso de gestión de riesgo (22); por lo que concluyo que, establecer objetivos de control de seguridad a través de la norma ISO 27001:2013, mejorará la gestión de las TI en la Municipalidad Distrital de José Crespo y Castillo.

## 5.3 Propuesta de mejora

Habiéndose realizado el análisis de los datos recogidos a través de la evaluación de las dimensiones: Situación Actual del Sistema de Gestión de la seguridad de la información, se ha detectado que no existen planes de acción y contingencias para mitigar los riesgos y vulnerabilidades de la seguridad de la información. Al no existir un plan adecuado no solo se ve afectado, los procesos documentados, sino también los sistemas de información que se encargan de soportar toda la información, el cual es un activo de mucho valor para la Municipalidad Distrital José Crespo y Castillo, la evaluación ha permitido ver que también existe riesgos en las tecnologías que soporta la Información.

Gráfico Nro. 21: Cadena de Activos de Información.


Fuente: Elaboración Propia.

De acuerdo a nuestra investigación se ha seleccionado la Norma ISO 27001:2013, nos muestra que existe la necesidad de mejorar el sistema de gestión de la seguridad de la información, por lo cual se propone los siguientes procesos:

Tabla Nro. 26 Procesos Actuales de la Municipalidad Distrital de José Crespo y Castillo.

| Nro. | Procesos Actuales de la Municipalidad Distrital de José Crespo y Castillo |
|---|---|
| 1 | No existen políticas de seguridad para adquisición de TI. |
| 2 | La Unidad de Estadística e Informática no cuenta con el soporte técnico, no cuenta con un manual de procedimientos para la gestión de las TI. |
| 3 | No existen procesos de seguridad de la información. |
| 4 | Muchos operadores y usuarios de las TI manejan los mismos usuarios y contraseñas. |
| 5 | Se contratan servicios de desarrollo de software sin un control adecuado. |
| 6 | No existen controles de altas y bajas de las TI. |
| 7 | No existe un control de perfiles de responsables y usuarios de las TI. |
| 8 | No existen roles del Personal de TI. |
| 9 | No existe un manual de funciones de manejo de las TI. |
| 10 | No se cuenta con un plan de capacitaciones y entrenamiento al personal que utilizan las TI. |
| 11 | No existen procedimientos de sanciones por el uso indebido de la información. |
| 12 | El servidor y las redes no cuentan con una adecuada seguridad ambiental y la integridad física se ve amenazada por el uso indebido de programas informáticos no verificados. |
| 13 | No existen procesos de operaciones y transacciones de TI. |
| 14 | No cuenta con procesos para solicitudes y atención de soporte de TI. |

Fuente: Elaboración Propia

Tabla Nro. 27: Propuesta de mejora

| Nro. | Procesos propuestos para mejorar Aplicando la ISO/IEC 27001:2013 |
|---|---|
| 1 | Establecer políticas de seguridad, con respecto a la adquisición, distribución y uso de las TI en la Municipalidad Distrital José Crespo y Castillo. |
| 2 | Que la unidad de informática, muestre compromiso con las innovaciones tecnológicas que soportan los procesos de la Municipalidad. |
| 3 | Determinar procesos que aseguren la Seguridad de la información en la Municipalidad Distrital José Crespo y Castillo. |
| 4 | Establecer procedimientos que aseguren la confidencialidad de la información en la Municipalidad Distrital José Crespo y Castillo. |
| 5 | Establecer políticas que aseguren la factibilidad y protección de brindar información a terceros |
| 6 | Definir procesos documentados para el registro de inventarios de activos de TI en la Municipalidad Distrital José Crespo y Castillo. |
| 7 | Realizar el registro automatizado de la asignación de responsables de activos de TI en la Municipalidad Distrital José Crespo y Castillo. |
| 8 | Determinar los roles y responsabilidades del personal de TI en la Municipalidad Distrital José Crespo y Castillo. |
| 9 | Establecer las responsabilidades de los usuarios que hacen uso de las TI de acuerdo a las funciones establecidas en la Municipalidad Distrital José Crespo y Castillo. |
| 10 | Planificar capacitaciones y entrenamientos al personal que utiliza las TI en la Municipalidad Distrital José Crespo y Castillo. |
| 11 | Documentar las políticas para sanciones por uso indebido de los sistemas de información |
| 12 | Definir los procesos de seguridad de ambientes físicos y ambientales para los activos de TI en la Municipalidad Distrital José Crespo y Castillo. |
| 13 | Determinar los procesos para operaciones y transacciones de TI que realiza las unidades operativas de la Municipalidad Distrital José Crespo y Castillo. |
| 14 | Definir los procesos para solicitudes y atención de soporte de TI en la Municipalidad Distrital José Crespo y Castillo. |

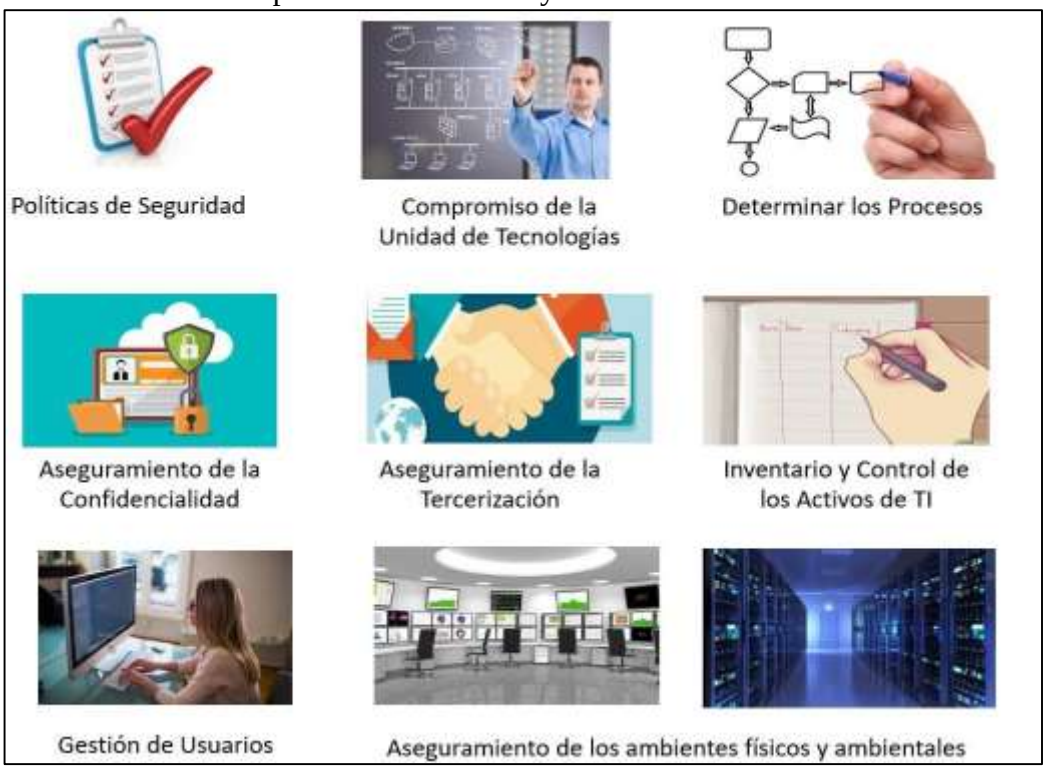
Fuente: Elaboración Propia

La incorporación de los presentes objetos de control, permitirá calcular el nivel de riesgo que considere y las metodologías de otras. No obstante, aquí veremos una fórmula sencilla y rápida de entender, basada en 2 parámetros fundamentales en gestión de riesgos: Probabilidades y Amenazas.

El Plan de Tratamiento de Riesgos tiene que contener una serie de información básica: Responsable del control: Persona que se responsabiliza de la correcta implantación del control, Recursos: Personas, técnicos, empresas externas o materiales que se utilizarán para la implantación del control, Acciones a llevar a cabo: Acciones que serán necesarias, para la implantación del control, Prioridad: Todos los controles no tienen la misma prioridad, ya que por una parte el nivel de riesgo no será el mismo, ni tampoco el valor de cada activo para la Organización, Por tanto es necesario establecer prioridades, las cuales pueden venir determinada por la fecha de implantación de cada control.

Una propuesta efectiva de hacer una adecuada implementación de la Norma ISO 27001: 2013, es analizar las fortalezas y debilidades de los elementos claves que propones en la imagen del grafico Nro. 22

Gráfico Nro. 22: Propuesta de Fortalezas y Debilidades de TI.




Fuente: Elaboración Propia.

## VI. CONCLUSIONES.

Teniendo en cuenta los resultados obtenidos en el presente trabajo de investigación se evidencia la necesidad de implementar un Sistema de Gestión de Seguridad de la Información, bajo el enfoque de la norma ISO / IEC 27001, la misma que permitirá mejorar los procesos de seguridad, confiabilidad y disponibilidad de la información en Municipalidad Distrital José Crespo y Castillo. La misma que guarda concordancia con la hipótesis general.

Asimismo, se presenta los resultados obtenidos por dimensiones de acuerdo a lo planteado en la investigación, se llega a las siguientes conclusiones:

1. Se puede observar que el 85.50% de los trabajadores encuestados expresaron la situación actual del Sistema de gestión de la seguridad de la información, no se encuentra implementado, mientras que un 14.5 %, señalo que si existen procesos implementados.

2. Se puede observar que el 85.50% de los trabajadores encuestados expresaron la necesidad de implementar un Sistema de gestión de la seguridad de la información, motivo a que no se encuentra implementado, mientras que un 14.5%, señalo que si existen procesos implementados.

3. Por lo descrito en la presente tesis ayudara a mejorar la gestión de los activos reduciendo las probabilidades de riesgos y mitigando los impactos que se podrían generar por una mala gestión de activos, los activos soportan los sistemas de información y estos son de vital importancia para el crecimiento empresarial.

4. Es importante resaltar que cada vez que se incorpora una nueva herramienta o procesos de actividades de TIC a la entidad se debe actualizar el análisis de riesgos para poder mitigar de forma responsable los riesgos y por supuesto, considerando la regla básica de Riesgo de TIC en Municipalidad Distrital José Crespo y Castillo.

## VII. RECOMENDACIONES.

1. Implementar el Sistema de Gestión de seguridad de la información para asegurar la confiabilidad, Disponibilidad y Seguridad de la Información en la Municipalidad Distrital José Crespo y Castillo que consolide los procesos tecnológicos.

2. Auto evaluar de manera periódica la seguridad de la información, utilizando los objetivos de control de la norma ISO 27001, en la Municipalidad Distrital José Crespo y Castillo. a fin de garantizar la aplicación de procesos preventivos que ayuden a la continuidad de los servicios y de esta manera la Municipalidad se fortalezca en su reputación a través del uso de los sistemas de información.

3. Capacitaciones constantes al personal de TI en metodologías y procesos de seguridad de la información y comunicaciones de la Municipalidad Distrital José Crespo y Castillo a fin de mejora sus competencias y actualización en nuevas metodologías y herramientas de aplicación de la seguridad de la información.

4. La Unidad Técnica de Informática y estadística, deberá proponer se realice la gestión para la Certificación de la norma ISO / IEC 27001 a fin de garantizar la implementación de acuerdo a las normas y protocolos establecidos por la empresa certificadora.

## REFERENCIAS BIBLIOGRAFÍAS

1. The Free Encyclopedia. La Era De La Informacion. [Online].; 2011 [cited 2018 Junio 13. Available from: http://misecundaria.com/Main/LaEraDeLaInformacion.
2. Business EGSO. La Implantación del Sistema de Gestión de Seguridad de Información Óptica ISO 27001:2013. [Online].; 2014 [cited 2017 Diciembre 07. Available from: https://www.esan.edu.pe/programa/gestion-seguridad-iso-27001/.
3. Gómez Morales G. Método para implementar un SGSI según el ISO/IEC 27001:2013. [Online].; 2017 [cited 2017 Diciembre 07. Available from: https://es.linkedin.com/pulse/m%C3%A9todo-para-implementar-un-sgsiseg%C3%BAn-el-isoiec-g%C3%B3mez-morales.
4. Guamán Seis JA. Diseño de un sistema de gestión de seguridad de la información para instituciones militares. Tesis. Quito: Escuela politécnica nacional, Ecuador; 2015.
5. Pallas Mega G. Metodología de Implantación de un GSI en un grupo empresarial jerárquico. Tesis. Montevideo: Universidad de la República de Uruguay, Uruguay; 2009.
6. Suarez Padilla SY. Análisis y diseño de un sistema de gestión de seguridad informática en la empresa aseguradora Suarez Padilla & Cía. LTDA, que brinda una adecuada protección en seguridad informática de la infraestructura tecnológica de la organización. Tesis. Colombia: Universidad Nacional Abierta y a Distancia de Colombia, Colombia; 2009.
7. Seclén Arana JA. Factores que afectan la implementación del sistema de gestión de seguridad de la información en las entidades públicas peruanas de acuerdo a la NTPISO/IEC 27001. Tesis. Lima: Universidad Nacional Mayor de San Marcos, Perú; 2016.
8. Alcántara Flores JC. Guía de implementación de la seguridad basado en la norma ISO/IEC 27001, para apoyar la seguridad en los sistemas informáticos de la comisaria del norte P.N.P en la ciudad de Chiclayo. Tesis. Chiclayo: Universidad Católica Santo Toribio De Mogrovejo, Lambayeque; 2015.

9. Espinoza Aguinaga HR. Análisis y diseño de un sistema de gestión de seguridad de información basado en la norma ISO/IEC 27001:2005 para una empresa de producción y comercialización de productos de consumo masivo. Tesis. Lima: Pontificia Universidad Católica del Perú, Perú; 2013.
10. Olaya Córdova JS. (1) GESTIÓN DEL SISTEMA DE SEGURIDAD DE INFORMACIÓN BAJO EL ENFOQUE DE ISO 27001 EN LA MUNICIPALIDAD PROVINCIAL DE TUMBES; 2016. Tesis. Piura: Universidad Católica los Ángeles de Chimbote, Piura; 2016.
11. castillo collazos re. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN LA MUNICIPALIDAD DISTRITAL DE PIRA APLICANDO LA NORMA ISO/IEC 27001:2013. Tesis. Huaraz: Universidad Católica Los Ángeles de Chimbote, Computación e Informatica; 2013.
12. Presidencia del Consejo de Ministros. Municipios al Día. [Online].; 2014 [cited 2018 Julio 15. Available from: https://municipioaldia.com/municipalidades-delperu/.
13. Municipalidad Distrital de José Crespo y Castillo. Municipalidad Distrital de José Crespo y Castillo. [Online].; 2015 [cited 2018 Junio 10. Available from: http://www.muniaucayacu.gob.pe/index.php.
14. Agencia de Prensa Ambiental. Inforegión. [Online].; 2009 [cited 2018 Mayo 15. Available from: http://www.inforegion.pe/30769/conformaran-red-de-comites-devigilancia-escolar-en-la-provincia-de-leoncio-prado/.
15. Muniipalidad Distrital De José Crespo Castillo. MOF. 2018..
16. Rouse M. Tecnología de la Información (TI). [Online].; 2000 [cited 2017 Mayo 16. Available from: http://searchdatacenter.techtarget.com/.
17. Gil Rodríguez EP. Identidad y nuevas tecnologías: repensando las posibilidades de intervención para la transformación social. [Online].; 2002 [cited 2017 Noviembre 20. Available from: http://www.uoc.edu/web/esp/art/uoc/gil0902/gil0902.html.
18. Valencia UId. La evolución de las TICs desde el ábaco al Smartphone. [Online].; 2016 [cited 2017 Noviembre 29. Available from: https://www.universidadviu.es/laevolucion-las-tics-desde-abaco-al-smartphone/.

19. (ITU) UIdT. Evolución de las TIC a escala mundial. [Online].; 2014 [cited 2017 Noviembre 20. Available from: http://itunews.itu.int/es/5089-Evolucion-de-las-TICa-escala-mundial-.note.aspx.
20. UNESCO. Las tecnologías de la información y la comunicación (TIC) en la educación. [Online].; 2017 [cited 2017 Mayo 16. Available from: http://www.unesco.org/new/es/unesco/themes/icts/.
21. EDUCREA. Las TICS en el ámbito educativo. [Online]. [cited 2017 Noviembre 29. Available from: https://educrea.cl/las-tics-en-el-ambito-educativo/.
22. ISO. ISO/IEC 27000 family - Information security management systems. [Online].; 2013 [cited 2017 Noviembre 20. Available from: https://www.iso.org/isoiec-27001information-security.html.
23. 27001Academy. ¿Qué es norma ISO 27001? [Online].; 2017 [cited 2017 Noviembre 5. Available from: https://advisera.com/27001academy/es/que-es-iso-27001/.
24. ISO. ISO/IEC 27001:2013. [Online].; 2013 [cited 2017 Noviembre 20. Available from: https://www.iso.org/standard/54534.html.
25. ISO. The ISO Survey of Management System Standard Certifications 2016. [Online].; 2017 [cited 2017 Noviembre 22. Available from: http://isotc.iso.org/livelink/livelink/fetch/-8853493/8853511/8853520/18808772/00._Executive_summary_2016_Survey.pdf?nodeid=19208898&vernum=-2.
26. ISO. Encuesta ISO. [Online].; 2017 [cited 2017 Noviembre 25. Available from: https://www.iso.org/the-iso-survey.html.
27. 27001Academy. ¿Por qué ISO 27001 es importante para su empresa? [Online].; 2017 [cited 2017 Noviembre 26. Available from: https://advisera.com/27001academy/es/que-es-iso-27001/.
28. Baldecchi Q. R. Implementación efectiva de un SGSI ISO 27001. 2014th ed. CIGRAS , editor. Chile: CIGRAS; 2014.

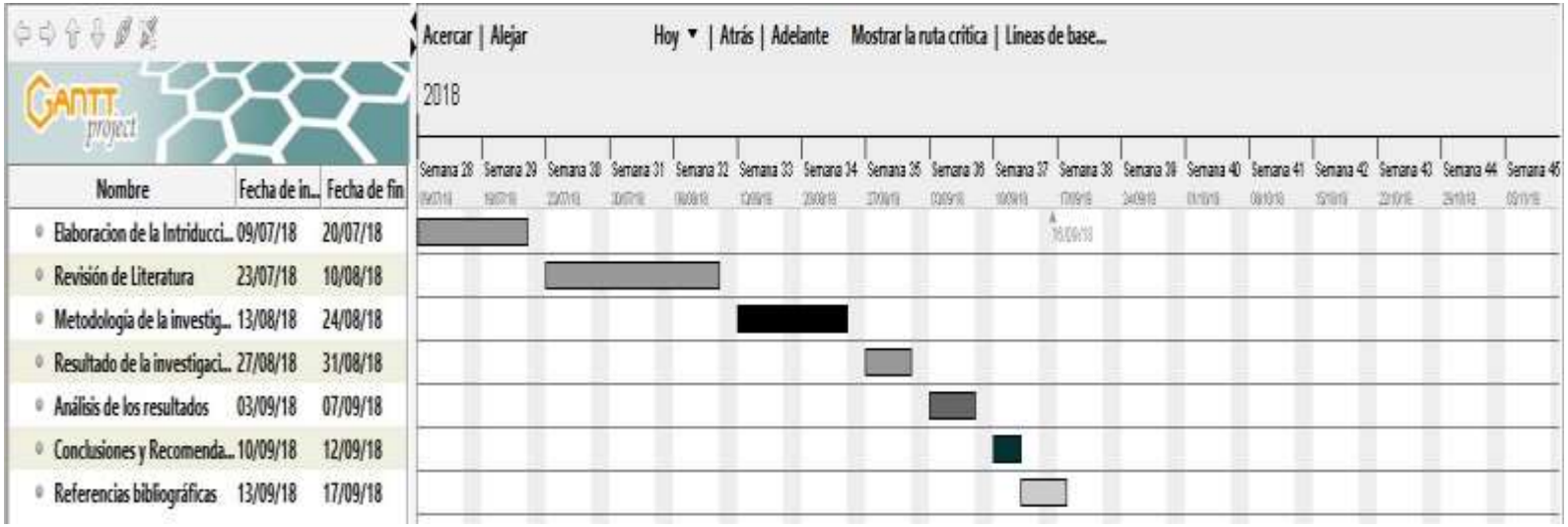
29. Iso27000.es. ISO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES. Iso27000.es. 2012 Octubre.
30. Solarte Solarte F, Enriquez Rosero ER, Benavides Ruano MdC. Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. Revista Tecnológica ESPOL. 2015 Diciembre; 28(5).
31. Hernández Sampieri R, Fernández Collado C, Baptista Lucio MdP. Metodologia de la Investigacion. Quinta ed. Chacón JM, editor. Mexico D.C.: McGraw-Hill; 2010.
32. Gómez MM. Introducción a la metodología de la investigación científica. Primera ed. Cordoba: Editorial Brujas; 2006.
33. D. Sousa V, Driessnack M, Costa Mendes IA. REVISIÓN DE DISEÑOS DE INVESTIGACIÓN RESALTANTES PARA ENFERMERÍA. PARTE 1: DISEÑOS DE INVESTIGACIÓN CUANTITATIVA. Revista Latino-Americana. 2007 Mayo.
34. Maimone GDS. Metodología de la Investigación Características cualitativa. [Online]. [cited 2017 Noviembre 25. Available from: https://sites.google.com/site/51300008metodologia/caracteristicas-cualitativacuantitativa.
35. Research SI. ¿Qué es la investigación cuantitativa? [Online].; 2017 [cited 2017 Noviembre 25. Available from: https://www.sisinternational.com/que-es-lainvestigacion-cuantitativa/.
36. Manterola C, Otzen T. Estudios Observacionales. Los Diseños Utilizados con Mayor Frecuencia en Investigación Clínica. International Journal of Morphology. 2014 Junio; 32(2).
37. educarchile. educarchile. [Online].; 2012 [cited 2017 Diciembre 15. Available from: http://www.educarchile.cl/ech/pro/app/detalle?ID=206980.
38. Horacio Saldaño. Encuesta – instrumento de recolección de datos Lima - Peru; 2009.
39. Ética y Psicología. Ética y Psicología. [Online].; 2014 [cited 2018 Agosto 11. Available from:

http://eticapsicologica.org/index.php/documentos/articulos/item/16que-son-los-principios-eticos.

40. Valencia Duque FJ, Orozco Alzate M. Metodología para la implementación de un Sistema Manizales - Colombia: Revista lbérica de Sistemas y Tecnologías de Información; 2017.
41. SUNEDU. Superintendencia Nacional de Educación Superior Universitaria. [Online].; 2016 [cited 2017 Julio 12. Available from: https://www.sunedu.gob.pe/historia/.
42. Uladech Católica. Universidad Católica los Ángeles de Chimbote. [Online].; 2016 [cited 2017 Junio 02. Available from: http://www.uladech.edu.pe/index.php/uladech-catolica/la-universidad/historia.html.
43. Uladech Católica. Reglamento de Organización y Funciones Uladech R, editor. Chimbote: Uladech; 2017.
44. Caro L. 7 Técnicas e Instrumentos para la Recolección de Datos. [Online]. [cited 2017 Noviembre 14. Available from: https://www.lifeder.com/tecnicasinstrumentos-recoleccion-datos/.
45. Tamayo y Tamayo M. El cuestionario: entrevista de datos Venezuela; 2013.

# ANEXOS

## ANEXO NRO. 1: CRONOGRAMA DE ACTIVIDADES




Fuente: Elaboración propia.

## ANEXO NRO. 2: PRESUPUESTO

TITULO: Evaluación de un sistema de gestión de seguridad de la información basado en la norma ISO 27001:2013, en la Municipalidad Distrital de José Crespo y Castillo - Aucayacu; 2018.

TESISTA: Miguel Augusto Dávila Villanueva.

INVERSIÓN: S/. 321.00.

FINANCIAMIENTO: Recursos Propios.

| DESCRIPCIÓN | CANTIDAD | COSTO UNITARIO | TOTAL PARCIAL | TOTAL |
|---|---|---|---|---|
| **1. BIENES DE CONSUMO** | | | | |
| **1.1. Lapiceros** | 2 | 0.50 | 1.00 | |
| **2.1. Lápices** | 2 | 1.00 | 2.00 | |
| | | | 3.00 | 3.00 |
| **2. SERVICIOS** | | | | |
| **2.1. Fotocopias** | 30 hoja | 0.10 | 3.00 | |
| **2.2. Servicios de Internet** | 80hrs | 1.00 | 80.00 | |
| **2.3. Pasajes locales** | -- | -- | 235.00 | |
| | | | 318.00 | 318.00 |
| **TOTAL** | | | | **321.00** |

Fuente: Elaboración Propia

## ANEXO NRO. 3: CUESTIONARIO

TITULO: Evaluación de un sistema de gestión de seguridad de la información basado en la norma ISO 27001:2013, en la Municipalidad Distrital de José Crespo y Castillo – Aucayacu; 2018.

TESISTA: Miguel Augusto Dávila Villanueva.

PRESENTACIÓN:

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

INSTRUCCIONES:

A continuación, se le presenta una lista de preguntas, agrupadas por dimensión, que se solicita se responda, marcando una sola alternativa con un aspa (“X”) en el recuadro correspondiente (SI o NO) según considere su alternativa.

| **DIMENSIÓN 01: SITUACIÓN ACTUAL DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.** | | | |
|---|---|---|---|
| **NRO** | **PREGUNTA** | **SI** | **NO** |
| 1 | ¿Considera usted que las políticas de la seguridad de la información, se encuentran documentadas? | | |
| 2 | ¿Existen procesos establecidos para el control de activos de TI? | | |
| 3 | ¿Existen procesos documentados, respecto a las responsabilidades y roles del personal de TI? | | |
| 4 | ¿Existe un proceso documentado, respecto a velar o salvaguardar los equipos de TI, ante problemas medio ambientales? | | |
| 5 | ¿Existen proceso documentados para evaluar la gestión y operación de las comunicaciones? | | |

| | | | |
|---|---|---|---|
| 6 | ¿Los procesos de control de accesos son gestionados y evaluados? | | |
| 7 | ¿Existen procesos de seguridad física y ambiental, para salvaguardar la información? | | |
| 8 | ¿Los procesos operativos de los Sistemas de información son seguros? | | |
| 9 | ¿Existen políticas para la seguridad de las telecomunicaciones? | | |
| 10 | ¿Existen protocolos para el mantenimiento del Software? | | |

Fuente: Elaboración Propia

| **DIMENSIÓN 02: NECESIDAD DE IMPLEMENTAR EL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.** | | | |
|---|---|---|---|
| **NRO** | **PREGUNTA** | **SI** | **NO** |
| 1 | ¿Es necesario evaluar las políticas de seguridad de la información? | | |
| 2 | ¿Es importante elaborar un plan de gestión de cambios? | | |
| 3 | ¿Es necesario documentar los roles y funciones del personal de TI y usuarios utilizan las TI? | | |
| 4 | ¿Es necesario establecer procesos de mejorar la seguridad física y ambiental? | | |
| 5 | ¿Es necesario implementar procesos, para mejorar la gestión de comunicaciones y operaciones? | | |
| 6 | ¿Considera necesario implementar procesos de evaluación y control de accesos? | | |
| 7 | ¿Cree que es importante re organizar la seguridad física y ambiental de los equipos informáticos? | | |
| 8 | ¿Considera que se deben establecer perfiles para mejorar la operatividad de los sistemas de información? | | |

| | | | |
|---|---|---|---|
| 9 | ¿Establecer política de seguridad, contribuirá a regular las telecomunicaciones? | | |
| 10 | ¿Los protocolos de seguridad mejoraran los procesos de mantenimiento de Software? | | |

Fuente: Elaboración Propia

**ANEXO NRO. 4: POBLACIÓN DE ENCUESTADOS.**

| AREAS DE LA MUNICIPALIDAD | Nº DE PERSONAS |
|---|---|
| Unidad de Estadística e Informática | 2 |
| Unidad de Recursos Humanos | 2 |
| Unidad de Logística | 3 |
| Unidad de Control Patrimonial y Bienes | 2 |
| Gerencia de Administración y Finanzas | 2 |
| Gerencia de Planeamiento y Presupuesto | 3 |
| Gerencia de Desarrollo Económico | 3 |
| Gerencia de Servicios Públicos | 5 |
| Gerencia de Desarrollo Humano | 4 |
| Gerencia de Infraestructura, Acondicionamiento Territorial y Catastro | 4 |
| **TOTAL** | **30** |

Fuente: Elaboración Propia