UNIVERSIDAD DE HUANUCO

FACULTAD DE INGENIERIA

PROGRAMA ACADÉMICO DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

TESIS

“Auditoría de seguridad de la información aplicando la norma ISO/IEC 27001 en la Municipalidad Distrital de Luyando”

PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS E INFORMÁTICA

AUTOR: Evaristo Cipriano, Albert Elvis

ASESOR: Baldeon Canchaya, Walter Teofilo

HUÁNUCO – PERÚ

2024

U

D

H

TIPO DEL TRABAJO DE INVESTIGACIÓN:

- Tesis (X)
- Trabajo de Suficiencia Profesional( )
- Trabajo de Investigación ( )
- Trabajo Académico ( )

LÍNEAS DE INVESTIGACIÓN: Gestión y Desarrollo de Sistemas de Información

AÑO DE LA LÍNEA DE INVESTIGACIÓN (2020)

CAMPO DE CONOCIMIENTO OCDE:

Área: Ingeniería, Tecnología

Sub área: Ingeniería eléctrica, Ingeniería electrónica

Disciplina: Ingeniería de sistemas y comunicaciones

DATOS DEL PROGRAMA:

Nombre del Grado/Título a recibir: Título Profesional de Ingeniero de sistemas e informática

Código del Programa: P06

Tipo de Financiamiento:

- Propio (X)
- UDH ( )
- Fondos Concursables ( )

DATOS DEL AUTOR:

Documento Nacional de Identidad (DNI): 44308899

DATOS DEL ASESOR:

Documento Nacional de Identidad (DNI): 22512084

Grado/Título: Maestro en ingeniería de sistemas e informática con mención en: gerencia de sistemas y tecnologías de información

Código ORCID: 0000-0002-4270-073X

DATOS DE LOS JURADOS:

N°	APELLIDOS Y NOMBRES	GRADO	DNI	Código ORCID
1	Sulca Correa, Omar Iván	Máster universitario en ingeniería informática	42230320	0000-0002-6442-588X
2	Suarez Paucar, Carlos Enrique	Maestro en ciencias con mencion en ingenieria de sistemas	41836635	0000-0001-5123-2088
3	Espinoza Inocente, German Lenin	Doctor en Administración	22530218	0009-0003-0405-3345

UNIVERSIDAD DE HUANUCO
Facultad de Ingeniería

P. A. DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

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

En la ciudad de Huánuco, siendo las 17:00 horas del día viernes 08 del mes de marzo de año 2024, se lleva a cabo la sustentación presencial en cumplimiento de lo señalado en el Reglamento de Grados y Títulos de la Universidad de Huánuco, quienes se reunieron los **Jurados Calificadores** integrado por los Docentes:

- Mg. Omar Iván Sulca Correa — PRESIDENTE.
- Mg. Carlos Enrique Suarez Paucar — SECRETARIO.
- Mg. German Lenin Espinoza Inocente — VOCAL.

Nombrados mediante la Resolución N° 0471-2024-D-FI-UDH para evaluar la Tesis intitulada: **"AUDITORÍA DE SEGURIDAD DE LA INFORMACIÓN APLICANDO LA NORMA ISO/IEC 27001 EN LA MUNICIPALIDAD DISTRITAL DE LUYANDO"** Presentado por el (la) **Bach: EVARISTO CIPRIANO, ALBERT ELVIS,** para optar el Título Profesional de Ingeniero(a) de Sistemas e Informática.

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

Habiendo absuelto las objeciones que le fueron formuladas por los miembros del Jurado y de conformidad con las respectivas disposiciones reglamentarias, procedieron a deliberar y calificar, declarándolo(a) APROBADO por UNANIMIDAD con el calificativo cuantitativo de 12 y cualitativo de SUFICIENTE según el (Art. 47).

Siendo las 19:44 horas del día 08 del mes de marzo del año 2024, los miembros del Jurado Calificador firman la presente Acta en señal de conformidad.

Mg. Omar Iván Sulca Correa
ORCID: 0000-0002-6442-588X
DNI: 42230320
Presidente

Mg. Carlos Enrique Suarez Paucar
ORCID: 0000-0001-5123-2088
DNI: 41836635
Secretario

Mg. German Lenin Espinoza Inocente
ORCID: 0009-0003-0405-3345
DNI: 22530218
Vocal

UNIVERSIDAD DE HUÁNUCO
FACULTAD DE INGENIERÍA
Programa Académico de Ingeniería de Sistemas e Informática

CONSTANCIA DE ORIGINALIDAD

Yo, BALDEON CANCHAYA, WALTER TEOFILO, asesor del PA Ingeniería de Sistemas e Informática y designado mediante documento: RESOLUCIÓN Nº 977-2022-D-FI-UDH, del bachiller EVARISTO CIPRIANO, ALBERT ELVIS, de la investigación titulada:"**AUDITORÍA DE SEGURIDAD DE LA INFORMACIÓN APLICANDO LA NORMA ISO/IEC 27001 EN LA MUNICIPALIDAD DISTRITAL DE LUYANDO**",

Puedo constar que la misma tiene un índice de similitud del 23% verificable en el reporte final del análisis de originalidad mediante el Software Turnitin. Por lo que concluyo que cada una de las coincidencias detectadas no constituyen plagio y cumple con todas las normas de la Universidad de Huánuco.

Se expide la presente, a solicitud del interesado para los fines que estime conveniente.

Huánuco, 11 de marzo de 2024

Walter Baldeon Canchaya
DNI: 22512084
Código Orcid:0000-0002-4270-073X

2 revision

INFORME DE ORIGINALIDAD

23%	18%	5%	14%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	es.slideshare.net Fuente de Internet	2%
2	repositorio.unife.edu.pe Fuente de Internet	1%
3	Submitted to Universidad del Istmo de Panamá Trabajo del estudiante	1%
4	repository.udistrital.edu.co Fuente de Internet	1%
5	renatiqa.sunedu.gob.pe Fuente de Internet	1%
6	apirepositorio.unh.edu.pe Fuente de Internet	1%
7	Submitted to Fundación Universitaria Católica del Norte Trabajo del estudiante	1%
8	core.ac.uk Fuente de Internet	1%

Walter Baldeon Canchaya

DNI: 22512084

Código Orcid:0000-0002-4270-073X

DEDICATORIA

A mi madre, mi esposa y mis hijos quienes me motivan para poder seguir superándome.

A mi madre, quien es un claro ejemplo de superación personal y académico, quien con su fortaleza, sabiduría y amor incondicional me ha ayudado en cada paso de mi vida.

A mi esposa y compañera por ese apoyo moral que me brinda para ser mejor cada día.

AGRADECIMIENTO

Agradecer a Dios quién me ha guiado y me ha dado la fortaleza para seguir adelante. A mi familia por su paciencia y estímulo constante, además su apoyo incondicional a lo largo de mis estudios. Y a todas las personas que de una y otra forma me apoyaron moralmente.

ÍNDICE

DEDICATORIA II
AGRADECIMIENTO III
ÍNDICE IV
ÍNDICE DE TABLAS VII
ÍNDICE DE FIGURAS IX
RESUMEN XI
ABSTRACT XII
INTRODUCCIÓN XIII
CAPÍTULO I 14
PROBLEMA DE INVESTIGACIÓN 14
1.1. DESCRIPCIÓN DE PROBLEMA 14
1.2. FORMULACIÓN DEL PROBLEMA 16
1.2.1. PROBLEMA GENERAL 16
1.2.2. PROBLEMAS ESPECÍFICOS 16
1.3. OBJETIVOS 16
1.3.1. OBJETIVO GENERAL 16
1.3.2. OBJETIVOS ESPECÍFICOS 16
1.4. JUSTIFICACIÓN DE LA INVESTIGACIÓN 17
1.4.1. JUSTIFICACIÓN TEÓRICA 17
1.4.2. JUSTIFICACIÓN PRÁCTICA 17
1.4.3. JUSTIFICACIÓN METODOLÓGICA 17
1.5. LIMITACIONES DE LA INVESTIGACIÓN 17
1.6. VIABILIDAD DE LA INVESTIGACIÓN 18
1.6.1. VIABILIDAD TÉCNICA 18
1.6.2. VIABILIDAD SOCIOECONÓMICA 18
1.6.3. VIABILIDAD INSTITUCIONAL 18
CAPÍTULO II 19
MARCO TEÓRICO 19
2.1. ANTECEDENTES DE LA INVESTIGACIÓN 19
2.1.1. ANTECEDENTES INTERNACIONALES 19
2.1.2. ANTECEDENTES NACIONALES 22
2.1.3. ANTECEDENTES LOCALES 24

2.2. BASES TEÓRICAS 24
2.2.1. AUDITORIA DE SEGURIDAD 24
2.2.2. CICLO DE DEMING 30
2.3. DEFINICIONES CONCEPTUALES 35
2.4. HIPÓTESIS 36
2.4.1. HIPÓTESIS GENERAL 36
2.4.2. HIPÓTESIS ESPECIFICAS 37
2.5. VARIABLES 37
2.5.1. VARIABLE INDEPENDIENTE 37
2.5.2. VARIABLE DEPENDIENTE 37
2.6. OPERACIONALIZACIÓN DE VARIABLES 38
CAPÍTULO III 39
METODOLOGÍA DE LA INVESTIGACION 39
3.1. TIPO DE INVESTIGACIÓN 39
3.1.1. ENFOQUE 39
3.1.2. ALCANCE O NIVEL 39
3.1.3. DISEÑO 39
3.2. POBLACIÓN Y MUESTRA 40
3.2.1. POBLACIÓN 40
3.2.2. MUESTRA 41
3.3. TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE DATOS . 41
3.3.1. PARA LA RECOLECCIÓN DE DATOS 41
3.3.2. PARA LA PRESENTACIÓN DE DATOS 42
3.3.3. PARA EL ANÁLISIS Y LA ANÁLISIS E INTERPRETACIÓN DE LOS DATOS 42
CAPÍTULO IV 43
RESULTADOS 43
4.1. PROCESAMIENTO DE DATOS 43
4.2. CONTRASTACIÓN DE HIPÓTESIS Y PRUEBA DE HIPÓTESIS ... 73
CAPÍTULO V 93
DISCUSIÓN DE RESULTADOS 93
5.1. CONTRASTACIÓN DE LOS RESULTADOS DEL TRABAJO DE INVESTIGACIÓN 93
CONCLUSIONES 95

RECOMENDACIONES 96
REFERENCIAS BIBLIOGRÁFICAS 97
ANEXOS 99

ÍNDICE DE TABLAS

Tabla 1 Clasificación 30
Tabla 2 Operacionalización de variables 38
Tabla 3 Población 40
Tabla 4 Políticas de seguridad para la gestión de información 43
Tabla 5 Conocimientos de las políticas de seguridad existentes 44
Tabla 6 Responsabilidades para uso de los recursos de la municipalidad .. 45
Tabla 7 Control adecuado del acceso para que personas no autorizadas .. 46
Tabla 8 Existencia de controles de usuarios 47
Tabla 9 Características de contraseñas 48
Tabla 10 Mantenimiento correctivo y preventivo de los equipos 49
Tabla 11 Actividades del departamento de Tecnología de la información ... 50
Tabla 12 Existencia de monitoreo constantemente a los sistemas 51
Tabla 13 Sistema de inventario de recursos informáticos 52
Tabla 14 Conocimientos en seguridad de la información del personal 53
Tabla 15 Políticas de seguridad por departamento 54
Tabla 16 Existencia de política de confidencialidad de la información 55
Tabla 17 Revisión periódicamente el cableado en los departamentos de la municipalidad 56
Tabla 18 Copias de seguridad de la información 57
Tabla 19 Políticas de seguridad para la gestión de información 58
Tabla 20 Conocimientos de las políticas de seguridad existentes 59
Tabla 21 Responsabilidades para uso de los recursos de la municipalidad 60
Tabla 22 Control adecuado del acceso para que personas no autorizadas 61
Tabla 23 Existencia de controles de usuarios 62
Tabla 24 Características de contraseñas 63
Tabla 25 Mantenimiento correctivo y preventivo de los equipos 64
Tabla 26 Actividades del departamento de Tecnología de la información ... 65
Tabla 27 Existencia de monitoreo constantemente a los sistemas 66
Tabla 28 Sistema de inventario de recursos informáticos 67
Tabla 29 Conocimientos en seguridad de la información del personal 68
Tabla 30 Políticas de seguridad por departamento 69
Tabla 31 Existencia de política de confidencialidad de la información 70

Tabla 32 Revisión periódicamente el cableado en los departamentos de la municipalidad 71
Tabla 33 Copias de seguridad de la información 72
Tabla 34 Resumen de procesamiento de casos 74
Tabla 35 Pruebas de normalidad 75
Tabla 36 Estadísticas de muestras emparejadas 76
Tabla 37 Prueba de muestras emparejadas 76

ÍNDICE DE FIGURAS

Figura 1 Políticas de seguridad para la gestión de información 43
Figura 2 Conocimientos de las políticas de seguridad existentes 44
Figura 3 Responsabilidades para uso de los recursos de la municipalidad . 45
Figura 4 Control adecuado del acceso para que personas no autorizadas . 46
Figura 5 Existencia de controles de usuarios 47
Figura 6 Características de contraseñas 48
Figura 7 Mantenimiento correctivo y preventivo de los equipos 49
Figura 8 Actividades del departamento de Tecnología de la información 50
Figura 9 Existencia de monitoreo constantemente a los sistemas 51
Figura 10 Sistema de inventario de recursos informáticos 52
Figura 11 Conocimientos en seguridad de la información del personal 53
Figura 12 Políticas de seguridad por departamento 54
Figura 13 Existencia de política de confidencialidad de la información 55
Figura 14 Revisión periódicamente el cableado en los departamentos de la municipalidad 56
Figura 15 Copias de seguridad de la información 57
Figura 16 Políticas de seguridad para la gestión de información 58
Figura 17 Conocimientos de las políticas de seguridad existentes 59
Figura 18 Responsabilidades para uso de los recursos de la municipalidad? 60
Figura 19 Control adecuado del acceso para que personas no autorizadas 61
Figura 20 Existencia de controles de usuarios 62
Figura 21 Características de contraseñas 63
Figura 22 Mantenimiento correctivo y preventivo de los equipos 64
Figura 23 Actividades del departamento de Tecnología de la información .. 65
Figura 24 Existencia de monitoreo constantemente a los sistemas 66
Figura 25 Sistema de inventario de recursos informáticos 67
Figura 26 Conocimientos en seguridad de la información del personal 68
Figura 27 Políticas de seguridad por departamento 69
Figura 28 Existencia de política de confidencialidad de la información 70
Figura 29 Revisión periódicamente el cableado en los departamentos de la municipalidad 71

Figura 30 Copias de seguridad de la información..... 72

RESUMEN

La presente investigación tuvo como objetivo: Determinar la mejora en la confiabilidad y seguridad de la información en la Municipalidad Distrital de Luyando al realizar una auditoría de seguridad de la información, aplicando la Norma ISO/IEC 27001.

Tuvo un enfoque cuantitativo. El diseño que se adoptó fue el Pre experimental de “pre test” y “post test”, en este caso el test que se utilizó fue el cuestionario de encuesta con un solo grupo de investigación.

Como población se tomó a 32 funcionarios de la municipalidad y como técnica se empleó la encuesta y el cuestionario como instrumento para obtener información sobre cómo mejorar la aplicación de la norma ISO/27001 en la Municipalidad Distrital de Luyando.

El resultado más resaltante que se obtuvo es que la Municipalidad Distrital de Luyando cuenta con políticas de seguridad básicas que no permiten el correcto aseguramiento de la información; razón por la cual es recomendable utilizar una normativa estricta y confiable que garantice la confidencialidad y seguridad de la información.

Para finalizar, se llegaron a las siguientes conclusiones: En la Municipalidad Distrital de Luyando no existe un manual de acciones que se deban tomar en caso ocurran dificultades en el manejo de la información. Además, las instalaciones del cuarto de servidores son reducidas, gran parte de los funcionarios no cierran la sesión de usuario de los sistemas utilizados. Finalmente, no se aplican los controles necesarios en cuanto al manejo y gestión de contraseñas por parte de los funcionarios municipales.

Palabras claves: auditoría de seguridad, políticas de seguridad, Norma ISO/IEC 27001, confiabilidad de la información, seguridad de la información.

ABSTRACT

The objective of this research was: Determine the improvement in the reliability and security of information in the district municipality of Luyando by carrying out an information security audit, applying the ISO/IEC 27001 Standard.

This research had a quantitative approach. The pre-experimental design of “pre test” and “post test” was adopted, in this case the test that will be used is called a SURVEY QUESTIONNAIRE with a single research group.

As a population, 32 municipal officials were taken and as a technique the survey was implemented to obtain information on how and improved the application of the ISO/27001 standard in the District Municipality of Luyando.

The most notable result obtained is that the district municipality of Luyando has basic security policies that do not allow the correct assurance of information; which is why it is advisable to use strict and reliable regulations that guarantee the confidentiality and security of the information.

Finally, the conclusions were reached: In the district municipality of Luyando there is no manual of actions that must be taken in case of difficulties in the management of information. The server room facilities are limited. Many officials do not log out users from the systems used. The necessary controls are not applied regarding the handling and management of passwords by municipal officials.

Keywords: security audit, security policies, ISO/IEC 27001 Standard, information reliability, information security.

INTRODUCCIÓN

Considerando que la seguridad de la información es un tema muy importante que debe ser tomado en cuenta en todas las instituciones, porque pueden ser víctimas de un ataque informático y afectar los recursos de las instituciones, si no se implementan prácticas que permitan mitigar los riesgos que surgen dentro de las instituciones organizaciones.

Sería improbable decir que una instalación tiene un nivel perfecto de seguridad porque siempre hay un índice de inseguridad, pero se puede reducir. Cada unidad procesa información reservada a su organización, por lo que se debe asegurar su integridad y confiabilidad.

Este proyecto se basa en la implementación de estrategias basadas en la norma ISO 27001, con la cual, además de la gestión de los riesgos percibidos, se pueden implementar políticas que permitan la seguridad de los recursos institucionales, logrando así la confianza en cada activo institucional.

La norma ISO 27001 puede ser aplicada en cualquier empresa o institución, independientemente de su actividad o tamaño, su objetivo es proteger la información mediante la creación de prácticas que permitan la gestión.

En este sentido, este estudio consta de seis capítulos. El primer capítulo consta del problema, descripción del problema, objetivos y el significado de la investigación. El segundo capítulo consta del marco teórico y conceptual, el cual consta de los antecedentes de la investigación, fundamentos teóricos, definiciones conceptuales, hipótesis y variables. El tercer capítulo hace referencia al marco metodológico, que incluye el enfoque, nivel y diseño de la investigación, población y muestra, técnicas y herramientas de recolección de datos, y técnicas de procesamiento y análisis de datos. En el cuarto capítulo se presentan los resultados del estudio junto con las correspondientes pruebas de hipótesis. En el capítulo cinco se presenta la discusión de resultados. Luego incluye conclusiones y recomendaciones, así como referencias bibliográficas y anexos.

CAPÍTULO I

PROBLEMA DE INVESTIGACIÓN

1.1. DESCRIPCIÓN DE PROBLEMA

Mesquid et al. (2018), sostienen que en la actualidad, las empresas que manejan grandes y pequeñas cantidades de información a nivel mundial, son blancos fáciles de ataques informáticos debido a que no cuentan con las debidas normas de seguridad, es por eso que los organismos internacionales encargados de la seguridad de la información, mediante la utilización de estándares logran minimizar el riesgo de ataques informáticos, que provocan perdida de información ocasionando así grandes problemas a nivel empresarial; por este motivo es imprescindible que las empresas puedan evaluar los riesgos asociados, para que establezcan las estrategias y controles adecuados y así aseguren una permanente protección para salvaguardar la información, para ello se podría emplear la norma ISO 27001 que detalla los requisitos para establecer, implantar, mantener, supervisar y mejorar la gestión de la seguridad de la información de una organización.

Toda empresa que maneja información ya sea para controlar su personal, ventas, stock, recursos, etc. Han optado por la implantación de sistemas de gestión con el fin de garantizar la eficacia y fiabilidad de su información en procesos de negocio.

Cano (2004), sostiene que la seguridad de la información no es un campo que se haya estudiado a fondo, aunque es un área importante ya que todas las empresas manejan sistemas de información, por este motivo están expuestos a ataques que buscan vulnerar los sistemas y así violentar su información.

En el departamento de Huánuco las diferentes instituciones públicas y privadas que manejan información, tienen intranquilidad por las amenazas que representan los ataques informáticos, las auditorías permiten obtener resultados reales de las falencias con las que cuentan las instituciones.

La Municipalidad Distrital de Luyando, maneja información de recursos humanos (personal, ausentismo, productividad, antigüedad, capacitación, etc.), recursos materiales (localización, estado actual, equipamiento, servicios, valuación, patrimonio artístico y cultural etc.), recursos financieros (relación entre actividad económica y recaudación, distribución espacial de la recaudación, composición y evolución de los recursos, relación entre presupuesto y ejecución, proyección y evolución de disponibilidades, composición y evolución del endeudamiento, etc.), esta información es delicada y valiosa pero que esta manejada por sistemas de información que no están diseñados orientados a seguridad de la información ya que no se diseñaron contemplando alguna política de seguridad además de desarrollarse por distintas personas que desarrollaban la labor de practicantes que lo último que pensaban era en la seguridad de la información que se manejaría en la municipalidad, además el personal que labora en la municipalidad no lleva ningún tipo de procedimiento de acceso a sus correos, páginas de internet y mucho menos contemplan algún tipo de seguridad en sus credenciales de acceso a los sistemas ya que se encontró que en su mayoría empleaban contraseñas demasiado conocidas como lo son 1234, abcd, etc.

Todo lo anteriormente mencionado hace evidente que la municipalidad no cuenta con las mínimas políticas de seguridad de la información, esto hace que toda la información sea vulnerable ante amenazas y al no contar con las debidas políticas de seguridad para proteger su información.

Es por ello que el presente trabajo se enfoca en la seguridad de la información realizando una auditoria completa a la institución evaluando la confiabilidad, integridad y disponibilidad de la seguridad de la información, buscando lograr la confidencialidad y seguridad de la información que maneja la institución.

1.2. FORMULACIÓN DEL PROBLEMA

1.2.1. PROBLEMA GENERAL

¿De qué manera realizar una auditoría de seguridad de la información, aplicando la Norma ISO/IEC 27001 mejorará la confiabilidad y seguridad de la información en la Municipalidad Distrital de Luyando?

1.2.2. PROBLEMAS ESPECÍFICOS

- ¿De qué manera analizar la situación actual del manejo de la información mejorará la seguridad de la información en la Municipalidad Distrital de Luyando?
- ¿De qué manera realizar la auditoria con la norma ISO/IEC 27001 optimizará la confidencialidad y seguridad de la información en la Municipalidad Distrital de Luyando?
- ¿De qué manera generar un manual de políticas de seguridad para el manejo de la información optimizará el uso de los equipos en la Municipalidad Distrital de Luyando?

1.3. OBJETIVOS

1.3.1. OBJETIVO GENERAL

Determinar la mejora en la confiabilidad y seguridad de la información en la Municipalidad Distrital de Luyando al realizar una auditoría de seguridad de la información, aplicando la Norma ISO/IEC 27001.

1.3.2. OBJETIVOS ESPECÍFICOS

- Mejorar la seguridad de la información en la Municipalidad Distrital de Luyando.
- Optimizar la confidencialidad y seguridad de la información en la Municipalidad Distrital de Luyando.

- Optimizar el uso de los equipos en la Municipalidad Distrital de Luyando.

1.4. JUSTIFICACIÓN DE LA INVESTIGACIÓN

1.4.1. JUSTIFICACIÓN TEÓRICA

El presente trabajo de investigación se ejecutó para colaborar con el conocimiento sobre la seguridad de la información. los resultados de esta investigación podrán plasmarse en futuras propuestas a las instituciones, ya que se estaría demostrando que la seguridad es lo primordial para todo tipo de información almacenada.

1.4.2. JUSTIFICACIÓN PRÁCTICA

La calidad del estudio radicó en que al finalizar la investigación se tendrá claro cómo mantener seguridad y confiabilidad de la información en las instituciones.

1.4.3. JUSTIFICACIÓN METODOLÓGICA

Los resultados de la presente investigación se basaron en generar procesos que aseguren la seguridad de la información en las instituciones, una vez culminada estos resultados podrán servir de guía del correcto uso de la seguridad de la información en futuras investigaciones y en otras instituciones.

1.5. LIMITACIONES DE LA INVESTIGACIÓN

La presente investigación no presento limitaciones ya que se contó son todos los recursos humanos, financieros y de acceso a la información necesarios para la culminación del presente trabajo de investigación.

1.6. VIABILIDAD DE LA INVESTIGACIÓN

1.6.1. VIABILIDAD TÉCNICA

El estudio fue viable ya que se dispone de la información referentes al tema del proyecto de investigación.

1.6.2. VIABILIDAD SOCIOECONÓMICA

El estudio fue viable ya que se cuenta con los recursos económicos que se hizo uso en el proyecto.

1.6.3. VIABILIDAD INSTITUCIONAL

El estudio fue viable ya que se cuenta con el respaldo de todo el personal y autoridades de la Municipalidad Distrital de Luyando.

CAPÍTULO II

MARCO TEÓRICO

2.1. ANTECEDENTES DE LA INVESTIGACIÓN

2.1.1. ANTECEDENTES INTERNACIONALES

Lucano (2019), en la tesis titulada “Diagnóstico y diseño de un sistema de gestión de seguridad de la información (SGSI), basado en la norma ISO/IEC 27001:2013, en un banco público”, Universidad Central del Ecuador, Ecuador, este proyecto presenta una investigación sobre la seguridad de la información, el diagnóstico de la realidad actual de los Bancos Públicos y el diseño de un sistema para su gestión, basado en la Norma Internacional ISO 27001 en su versión 2013. Para desarrollar este trabajo, se utilizó la metodología bibliográfica documental, que hizo con la información de varios documentos fundamentales, obtenidos de las diferentes áreas del Banco del Instituto Ecuatoriano de Seguridad Social (BIESS). La adopción de un Sistema de Gestión de Seguridad de la Información (SGSI) es de gran interés en bancos del sector público, debido a la importancia de la información utilizada en sus procesos, con la finalidad de mejorar la gestión de la seguridad de la información y la administración de sus activos de información. Los beneficios brindados por el diagnóstico y diseño del SGSI fueron el establecer el nivel de madurez actual del BIESS con respecto a la Norma en mención, para la disminución de riesgos de los activos y recursos de tecnología de la información manteniendo su integridad, disponibilidad y confidencialidad.

Santos-Olmo (2020), en la tesis titulada “Metodología para el Análisis de Riesgos de Sistemas de Información, usando Meta-Pattern y Adaptabilidad, Universidad de Castilla-La Mancha”, España, Hoy en día, poder proteger de una forma adecuada los activos de información se ha convertido en un factor crítico en el ámbito de la ciberseguridad. La aparición de conceptos como el internet de las cosas, los sistemas

ciberfísicos, las ciudades inteligentes o de la llamada cuarta revolución industrial ha ocasionado la transformación de una sociedad tradicionalmente analógica en una sociedad digital y totalmente conectada. Esta transformación ha sido muy beneficiosa para todos los actores involucrados (gobierno, empresas, ciudadanos), pero con ella también han aparecido nuevos riesgos de gran impacto. Ante este nuevo escenario, la sociedad está demandando soluciones que le permitan implantar medidas de seguridad adecuadas, pero hasta el momento todos los esfuerzos no han redundado en la obtención de soluciones realmente efectivas. La gestión de la seguridad de los sistemas de información ha permitido poner las primeras bases para resolver esta problemática, mediante la aparición de estándares como los de la familia de la ISO/IEC 27000. Esta familia de estándares ha supuesto un cambio de paradigma a la hora de afrontar la seguridad TIC en las empresas y ha posibilitado comenzar a resolver de forma eficiente, aunque aún incompleta, algunos de los problemas existentes. Pero para poder aplicar de forma correcta la gestión de la seguridad, uno de los aspectos principales es la necesidad de analizar los riesgos a los que están sometidos los activos de valor de una compañía, con el objetivo de poder gestionar estos riesgos y tomar medidas adecuadas para su control. Sin embargo, los sistemas actuales de análisis y gestión de riesgos no han terminado de mostrarse útiles para las empresas. Un análisis de las metodologías existentes en este campo ha permitido determinar que las metodologías de análisis y gestión de riesgos actuales tienen algunas carencias que deben ser subsanadas para que puedan ser realmente efectivos y puedan ser utilizadas por cualquier tipo de empresas, con independencia de su tamaño. Para suplir estas carencias, en esta tesis doctoral se propone el desarrollo de una metodología de análisis y gestión de riesgos denominada MARISMA, cuyo objetivo es facilitar la realización de un análisis de riesgos dinámico y su posterior gestión, que supla las carencias detectadas en las metodologías actuales. Esta metodología incluirá un modelo de información que dará soporte a los diferentes esquemas normativos y a las técnicas que permitan su evolución dinámica. Además, se presenta el prototipo de una

herramienta denominada eMarisma que da soporte automatizado para el desarrollo de los diferentes procesos de la metodología MARISMA. Por último, y con el objeto de validar y mejorar la metodología, se ofrece el resultado de su aplicación en un caso de estudio de un sistema real. Este trabajo de investigación se ha desarrollado en el marco de diversos proyectos de investigación, usando los métodos de investigación denominados Revisión sistemática de la literatura e Investigación-Acción.

Gareca (2019), en la tesis titulada “Guía documental de gestión de seguridad aplicando la ISO 27001 E ISO 27002 para el control de acceso a la información en la empresa CONCRETEC”, Bolivia, en el presente trabajo se da respuesta al problema de investigación ¿Cómo aplicar la Gestión de Seguridad de la Información para mejorar el control de acceso físico y lógico a la información de la empresa Concretec?, con el objetivo general: Proponer una Guía de Gestión de Seguridad de la Información, basado en la norma ISO 27001 e ISO 27002, que permita mejorar el control de acceso físico y lógico en el contexto mencionado. Se realiza la sistematización de los aspectos teóricos relacionados con la Gestión de Seguridad de la Información (identificando sus características y la correcta elección de los dominios y controles) y el Control de Acceso a la Información (modelos, técnicas, tipos y métodos), para el control de acceso físico y lógico. Se realiza el diagnóstico de la situación actual de los accesos físicos y lógicos a la información de la empresa Concretec, con la aplicación de los instrumentos de investigación, definiendo los problemas críticos candidatos a resolver en la propuesta de solución. Se estructura una Guía de Gestión de Seguridad de la Información basado en la ISO 27001 e ISO 27002 con un enfoque de sistemas y se definen las políticas y procedimientos para mejorar el control de acceso físico y lógico a la Información de la empresa Concretec. Finalmente, se valida la Guía de Gestión de Seguridad de la Información propuesta, mediante la aplicación de la prueba Chi Cuadrada para la demostración de la hipótesis de investigación

2.1.2. ANTECEDENTES NACIONALES

Agurto (2017), en la investigación titulada “Diagnóstico de los activos de información de los procesos implementados por el estándar ISO 9001 en el área QHSE de la empresa PISER S.A.C Talara, basado en la norma ISO 27001”, generó gran cantidad de información la cual está expuesta a deteriorarse, perderse, ser modificada o llegar a manos de la competencia, ya que para la ISO 27001, en toda empresa, el activo fundamental es su información. Se realizaron constantes reuniones con los colaboradores del área de logística e informática y el área QHSE para identificar y valorar los activos de información de los procesos implementados bajo la norma ISO 27001, se utilizaron cuestionarios y listas de cotejo para cada dimensión según la norma ISO 27001, obteniendo resultados que el 58% de fuga de documentación especializada es de manuales, procedimientos, documentación técnica, por debajo con el 33% otra de la fuga de documentación es por las incidencias en información de carácter personal. En conclusión, luego de realizar dicha investigación se propuso elaborar la propuesta técnica, en la que incluyen los controles de seguridad basada en la norma ISO 27001, acorde con los procesos implementados por el estándar ISO 9001.

Castro (2018), en el proyecto denominado “Implementación de la NTP ISO/IEC 27001:2014, para mejorar la gestión de la seguridad en los sistemas de información de la Autoridad Portuaria Nacional”, la cual estuvo dividido en 3 etapas y tuvo como alcance los procesos de REDENAVES, Gestión de Licencias y Gestión de los Sistemas de Información en su sede central ubicado en el Callao. Los resultados que se obtuvieron permitieron determinar de forma real que, al implementar la Norma Técnica Peruana ISO/IEC 27001:2014, se obtuvo un mayor nivel de uso de documentos tales como procedimientos, política y otros, que favorecieron a la institución para descubrir las irregularidades en la seguridad de la información plasmado en varios métodos de seguridad para resguardarla. Así mismo, el Plan de Tratamiento de Riesgos,

posibilitó la reducción de los niveles de riesgos de los activos de información, respecto a las amenazas y vulnerabilidades en la institución, esto plasmado en una metodología para mitigarlos a través de actividades y poder minimizar los impactos a los activos de información. Finalmente, con el Plan de Capacitación y Concientización se logró incrementar la conciencia en temas relacionados a seguridad de la información y se impulsó al personal a comprometerse a resguardar su información y mitigar riesgos en favor de la institución.

Vásquez y Delgado (2019), en la tesis titulada “Modelo de seguridad informática aplicando la Norma ISO/IEC 27001 para proteger los activos de información en la empresa Berendson Natación S.R.L.”, Universidad de Lambayeque, Lambayeque, el presente informe de tesis desarrolló un modelo de sistema de gestión de seguridad de la información aplicada a las pymes en la ciudad de Chiclayo, basado en la norma ISO 27001. Las Normas ISO no sólo son herramientas al alcance de las grandes empresas, sino que también las medianas o pequeñas empresas pueden conseguir los beneficios que se derivan de su implantación y su mantenimiento. Se trató de adaptar la norma a las pymes, ya que demanda un costo muy elevado implementar el ISO 27001. Para la obtención de la información se consideró conveniente el uso de las técnicas de recolección de datos tales como las encuestas, para su posterior Análisis e Interpretación; y de esta manera medir la realidad problemática apoyado en el uso de la Norma ISO 27001, lográndose identificar las deficiencias para mejorar los niveles de seguridad y confiabilidad en los sistemas de información de la empresa Berendson Natación S.R.L. Se propuso una metodología de implementación de la ISO 27001 para que sea aplicada en un modelo de sistemas de gestión de seguridad de la información en la empresa Berendson Natación S.R.L. Se buscó facilitar las tareas que dificultan a la empresa debido a los recursos limitados con los que cuentan en presupuesto, conocimiento y personal.

2.1.3. ANTECEDENTES LOCALES

Vilca (2017), en la tesis titulada “Sistema de gestión de la seguridad de la información bajo el ISO 27001 para mejorar la seguridad en cuanto al uso de los activos y tecnologías de la información en la empresa Geosurvey de la ciudad de Lima en el año 2016”, Universidad de Huánuco, empleó una metodología bajo el enfoque cuantitativo y de tipo aplicativo; ya que se utilizó la tecnología para la solución de un problema, así mismo se empleó el diseño pre experimental de pre y post test se llevó a cabo un experimento en condiciones controladas. Tanto la población como la muestra estuvo conformada por 33 trabajadores siendo no probabilística, se tomaron en cuenta todos los trabajadores de las diferentes áreas de la empresa. Para la recolección de datos se utilizó el cuestionario como técnica y el cuestionario de encuesta como instrumento para luego los datos sean procesados en el software estadístico SPSS.

2.2. BASES TEÓRICAS

2.2.1. AUDITORIA DE SEGURIDAD

Núñez (2018), sostiene que la auditoría de seguridad sirve para comprobar que las medidas de seguridad y control de los sistemas informáticos se adecúan a la normativa que se ha desarrollado para la protección de los datos; además identifica las deficiencias, y propone medidas correctivas o complementarias.

Al obtener los resultados, se detallan, archivan y reportan a cada uno de los responsables mismos que deberán establecer medidas para prevenir, reforzar y proceder a la corrección, pero siempre siguiendo un proceso secuencial que permita a los administradores la mejora de la seguridad de los sistemas y así se aprende de los errores cometidos.

Al realizar auditorías de seguridad de un Sistema de Información, se llega a conocer en ese momento cuál es la situación exacta de los

activos de la información en cuanto a protección, control y medidas de seguridad.

2.2.1.1. ESTÁNDARES DE SEGURIDAD DE LA INFORMACIÓN

Núñez (2018), sostiene que son aquellos que proporcionan un marco de gestión de seguridad de la información disponible por cualquier tipo de organización, pública o privada, grande o pequeña. Estos estándares contienen excelentes prácticas las cuales son recomendadas en seguridad de la información estas sirven para desarrollar, implementar y mantener especificaciones para los Sistemas de Gestión de la Seguridad de la Información.

2.2.1.2. ISO/IEC 27001

Esta norma específica los requisitos para la creación, implementación, funcionamiento, supervisión, revisión, mantenimiento y mejora de un Sistema de Gestión de Seguridad de la Información (SGSI) documentado, teniendo en cuenta los riesgos empresariales generales de la organización.

Es decir, explica cómo diseñar un SGSI y establecer los controles de seguridad, de acuerdo con las necesidades de una organización o de partes de la misma, pero no aclara mediante qué procedimientos se ponen en práctica. Por ejemplo, uno de los principales requisitos es la realización de un análisis de riesgos con unas determinadas características de objetividad y precisión, pero no aporta indicaciones de cuál es la mejor manera de llevar a cabo dicho análisis.

Puede ejecutarse con una herramienta comercial, con una aplicación diseñada expresamente para la empresa, mediante reuniones, entrevistas, tablas o cualquier otro método que se estime oportuno.

Todos estos recursos servirán para cumplir la norma, siempre y cuando se observen los requisitos de objetividad del método, los resultados sean repetibles y la metodología se documente.

2.2.1.3. SISTEMAS DE INFORMACIÓN

Un sistema de información es el conjunto de elementos o componentes relacionados con la información que interaccionan entre sí para lograr un objetivo: facilitar y/o recuperar información.

Para entender a los sistemas de información hay que estar al tanto de que existen necesidades en las organizaciones y comunidades que deben ser satisfechas, además hay que dominar las complejidades de cómo se maneja la información y cuáles son las potencialidades de los medios que se emplean para organizar y recuperar información. Regularmente el término "sistema de información" es usado de manera errónea, en la mayoría de los casos los recursos materiales de un sistema de información están constituidos casi en su totalidad por sistemas informáticos. Estrictamente, un sistema de información no tiene por qué disponer de dichos recursos. Entonces se podría decir que los sistemas de información informáticos son un subconjunto de los sistemas de información.

2.2.1.4. AMENAZA

Fernández (2019), sostiene que es cualquier cosa que provoque un daño a nuestro activo. Por ejemplo, si un virus corrompe el ordenador en donde el alumno tiene su trabajo final, no podrá acceder al momento de presentarlo y tal vez lo pierda.

2.2.1.5. RIESGO

Fernández (2019), sostiene que es una situación del mundo real, en el cual hay una exposición a la adversidad conformada por un sin número de circunstancias del entorno donde hay posibilidad de pérdidas. Los riesgos informáticos son exposiciones los mismos

que pueden ser atentados y amenazas a los sistemas de información.

2.2.1.6. TIPOS DE RIESGOS

a) Spam

Fernández (2019), sostiene que son aquellos que acarrean virus a la PC cuando abrimos las páginas que son restringidas por ejemplo porno, correos no deseados entre otras, este tipo de páginas provocan que nuestros equipos se infecten.

b) Piratería

Fernández (2019), sostiene que el software ilegal incrementa los riesgos de exposición a virus que pueden destruir los sistemas, también información valiosa para los usuarios. De este modo, puede generar grandes conflictos en los sistemas y por ello causar cuantiosos perjuicios económicos. Altas posibilidades de pérdida total de los datos y no teniendo acceso al servicio de atención al cliente, actualizaciones del software, documentación técnica, formación y solución de errores.

c) Fuga de Información

Fernández (2019), sostiene que al perder información involucra grandes problemas, por ejemplo, cuando se nos encarga una ingeniería social.

d) Ataques Informáticos

Fernández (2019), sostiene que los ataques informáticos aprovechan las debilidades o falla en el software, en el hardware, e incluso, en las personas que forman parte de un ambiente informático; a fin de obtener un beneficio, usualmente de índole económico, causando un efecto negativo en la seguridad del

sistema, que luego se ve repercutido directamente en los activos de la organización.

Para menguar el impacto negativo causado por ataques, existen procedimientos y mejores prácticas que proporcionan la lucha contra las actividades delictivas y reducen notablemente el campo de acción de los ataques. Uno de los pasos más importantes en seguridad, es la educación. Comprender cuáles son las debilidades más comunes que pueden ser aprovechadas y cuáles son sus riesgos asociados, permitirá conocer de qué manera se ataca un sistema informático ayudando a identificar las debilidades y riesgos para luego desplegar de manera inteligente estrategias de seguridad efectivas.

2.2.1.7. ASPECTOS DE SEGURIDAD QUE COMPROMETE UN ATAQUE

Naranjo y Reyes (2017), sostiene que la seguridad Está conformada por tres elementos fundamentales que constituyen los objetivos que los atacantes buscan comprometer. Estos elementos incluyen la confidencialidad, la integridad y la disponibilidad de los recursos. En base a esto, los atacantes tratarán de aprovechar las vulnerabilidades de un sistema o red para encontrar una o más debilidades en alguno de estos tres aspectos de la seguridad.

a) Confidencialidad.

Un atacante podría substraer información sensible como contraseñas u otro tipo de datos que viajan en texto claro a través de redes confiables, quebrantando la confidencialidad al permitir que otra persona, que no es el destinatario, tenga acceso a los datos. Un ejemplo que compromete este elemento es el envenenamiento de la tabla ARP (ARP Poisoning).

b) Integridad.

Mientras la información se trasfiere a través de los protocolos de la comunicación, los atacantes podrían interceptar el mensaje y realizar cambios en determinados bits del texto cifrado con la intención de alterar los datos del criptograma. Este tipo de ataques se denomina Bit-Flipping y son considerados ataques contra la integridad de la información. El ataque no se lleva a cabo de manera directa contra el sistema de cifrado, pero sí en contra de un mensaje o de una serie de mensajes cifrados. En el extremo, esto puede convertirse en un ataque de denegación de servicio contra todos los mensajes en un canal que utiliza cifrado.

c) Disponibilidad.

Los atacantes podrían utilizar los recursos de la organización, como sería el caso del ancho de banda de la conexión DSL para inundar de mensaje el sistema víctima y forzar la caída del mismo, negando así los recursos y servicios a los usuarios legítimos del sistema. Esto se conoce como Denial of Service (DoS) y atenta directamente contra la integridad de la información.

2.2.1.8. VULNERABILIDADES

Cano (2004), sostiene que son las inseguridades que posee el activo tanto por problemas tecnológicos, como problemas de procedimientos. Está demostrado que la gran mayoría de pérdidas de activos son por falta de procedimientos o desconocimiento.

Dichas vulnerabilidades no son más que el producto de los fallos causados por el inadecuado diseño de un software, así como también puede ser provocado por las limitaciones tecnológicas con que fue diseñado.

Hay algunos tipos des de vulnerabilidades. La primera es conocida como vulnerabilidad teórica, y el segundo, que es de interés para el usuario, la vulnerabilidad real, que comúnmente se lo conoce como Exploit.

2.2.1.9. TIPOS DE VULNERABILIDADES EN INFORMÁTICA

Naranjo y Reyes (2017), sostiene que Es crucial no subestimar las vulnerabilidades, ya que pueden representar diversos riesgos, incluso si no estamos manejando información crítica o documentos de importancia. Este asunto es de gran seriedad y es objeto de estudio y clasificación por parte de numerosas empresas y organizaciones.

Su clasificación es básicamente la siguiente:

Tabla 1

Clasificación

CALIFICACIÓN	DEFINICIÓN
Crítica	Este tipo de vulnerabilidad permite la propagación de amenazas sin que sea necesaria la participación del usuario.
Importante	Este tipo de vulnerabilidad es capaz de poner en riesgo la confidencialidad, integridad o disponibilidad de los datos de los usuarios, como así también, la integridad o disponibilidad de los recursos de procesamiento que este disponga.
Moderada	Este es uno de los tipos de vulnerabilidades más sencillas de combatir, ya que el riesgo que presenta se puede disminuir con medidas tales como configuraciones predeterminadas, auditorías y demás. Aparte, las vulnerabilidades moderadas no son aprovechables en todo su potencial ya que no afecta a una gran masa de usuarios.
Baja	Este tipo de vulnerabilidad es realmente muy difícil de aprovechar por un atacante, y su impacto es mínimo, ya que no afecta a una gran masa de usuarios.

2.2.2. CICLO DE DEMING

La norma ISO 27001 incluye el ciclo de Deming, como bien sabemos consiste en Planificar-Hacer-Verificar-Actuar (PHVA) y puede ser aplicado a todos los procesos. La metodología PHVA se puede describir de la siguiente forma:

- **Planificar:** Se establecen los objetivos y los procesos necesarios para conseguir resultados según las necesidades de los clientes y la política de seguridad de la organización.

- **Hacer:** Se implantan los procesos.

- **Verificar:** Se revisan y se evalúan tanto lo servicios como los procesos comprándolos con las políticas, los objetivos y los requisitos de información sobre los resultados.

- **Actuar:** Comienzan a emprender acciones para mejorar el rendimiento del Sistema de Gestión de Seguridad de la Información de forma continua.

Planificación

Se debe realizar una planificación de la implantación y la prestación de la gestión de servicios. El alcance puede venir definido dentro de parte del plan de gestión de servicios. La gestión de servicios tiene que estar planificada. Como mínimo, en dichas planificaciones se debe incluir lo siguiente:

- El alcance de la gestión de los servicios de la empresa.

- Los requisitos y los objetivos que tiene que cumplir la gestión de servicios.

- Los procesos que se deben realizar.

- La infraestructura de las funciones y las responsabilidades de gestión, incluyendo al responsable del proceso y la gestión de proveedores externos a la organización.

- La interfaz entre todos los procesos de gestión de servicios y el modo en el que se tiene que coordinar las actividades llevadas a cabo por la empresa.

- Enfocar lo que se tiene que hacer para poder identificar, evaluar y

gestionar los problemas y los riesgos de llevar a cabo los objetivos que se han definido.

- El intercambio de información con proyectos que ya estén creados o en proceso.
- Los recursos, las instalaciones y el presupuesto necesario para conseguir todos los objetivos que han sido definidos.
- Es la herramienta más adecuada para dar soporte a todos los procesos del Sistema de Gestión de Seguridad de la Información.

Tiene que existir una gestión clara por parte de la dirección y las responsabilidades tienen que estar documentadas, revisadas, autorizadas, comunicadas e implementadas.

En cualquier plan específico de un proceso que se elabore debe ser compatible con el plan de gestión de servicios de la empresa.

Un plan de gestión de servicios tiene que incluir:

- Implementación de gestión de servicios.
- Facilitar los procesos de gestión de servicios.
- Los cambios en los procesos de gestión de servicios.
- Las mejoras en los procesos de gestión de servicios.
- Nuevos servicios.

Hacer

Implantar los objetivos y planificar la gestión de servicios. La empresa tiene que implantar el plan de gestión de servicios para poder gestionar de una forma mucho más segura la información y se debe incluir:

- La asignación de fondos y presupuestos

- Asignación de funciones y responsabilidades
- Documentación y mantenimiento de políticas, procedimientos y definiciones para cada proceso
- Identificar y gestionar los riesgos para el servicio
- Gestionar equipos
- Servicio de atención al cliente y operaciones
- Informe de progreso y coordinación de procesos de gestión de servicios

Verificar

Se tiene que supervisar y verificar todos los objetivos y el plan de gestión de servicios establecido por la organización, para comprobar que se cumplen.

La empresa tiene que realizar una planificación para poder implementar la supervisión y la verificación de los procesos de gestión de servicios y los servicios asociados.

La norma ISO 27001 nos dice que los resultados de la verificación deben ofrecer información sobre el programa de mejora del servicio. Entre todos los elementos que se tienen que supervisar, evaluar y analizar se encuentran:

Los logros respecto de los objetivos del servicio definido.

La satisfacción de los clientes.

- La utilización de recursos.
- Las tendencias.
- Las no conformidades.
- Todos los resultados de los análisis que pueden generar una

mejora.

Las empresas tienen que aplicar los métodos más adecuados para poder supervisar y evaluar los procesos de gestión de servicios en el Sistema de Gestión de Seguridad de la Información.

Todos los métodos tienen que demostrar las capacidades que presentan los procesos para conseguir los resultados planificados.

Actuar

El objetivo que persigue esta fase es mejorar la eficacia de las prestaciones y la gestión de los servicios.

Se debe realizar una política, que sea pública, para mejorar el servicio. Cualquier falta de conformidad con la norma ISO 27001 tiene que ser remediada. Todas las funciones y las responsabilidades que sean necesarias para realizar las actividades de mejora del servicio se tienen que definir de forma clara.

Todas las mejoras de los servicios que propone la organización deben pasar por ser revisadas, registradas, priorizadas y autorizadas. Se puede utilizar un plan de mejora del servicio para poder controlar la actividad.

La empresa tiene que disponer de un proceso que identifique, evalúe y gestione todas las actividades de mejora.

Se tienen que incluir las mejoras del proceso individual para que la persona responsable del proceso pueda implantar los recursos necesarios y las mejoras de toda la empresa.

La empresa puede realizar una serie de actividades con las que recopilar datos para llevar a cabo evaluaciones comparativas de la capacidad de la empresa; identificar, planificar e implementar las mejoras necesarias; consultar a las partes interesadas; generar objetivos para conseguir mejorar la calidad de la seguridad de la información y

disminuir los costes. Se tienen que considerar las aportaciones que se realizan referentemente a las mejoras que se realizan en el Sistema de Gestión de Seguridad de la Información ISO 27001. Se debe revisar la política de seguridad y los procedimientos siempre que sea necesario.

Las mejoras que se realizan en el servicio de más importancia se tienen que gestionar como un proyecto.

2.3. DEFINICIONES CONCEPTUALES

1. SGSI

Es la abreviatura utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información. (Núñez, 2018)

2. CONFIDENCIALIDAD

Confidencialidad es la cualidad de confidencial (que se dice o hace en confianza y con seguridad recíproca entre dos o más individuos). Se trata de una propiedad de la información que pretende garantizar el acceso sólo a las personas autorizadas. (Naranjo y Reyes, 2017)

3. DISPONIBILIDAD

La capacidad de garantizar que tanto el sistema como los datos van a estar disponibles al usuario en todo momento. Pensemos, por ejemplo, en la importancia que tiene este objetivo para una empresa encargada de impartir ciclos formativos a distancia.

Constantemente está recibiendo consultas, descargas a su sitio web, etc., por lo que siempre deberá estar disponible para sus usuarios. (Fernández, 2019)

4. INTEGRIDAD

Integridad deriva del adjetivo integer, que significa intacto, entero, no tocado o no alcanzado por un mal.

Observando las raíces de este adjetivo, este se compone del vocablo in- , que significa no, y otro término de la misma raíz del verbo tangere, que significa tocar o alcanzar, por lo tanto, la integridad es la pureza original y sin contacto o contaminación con un mal o un daño, ya sea físico o moral. (Núñez, 2018)

5. IMPACTO

Impresión o efecto intenso producido en una persona por una acción o suceso. (Naranjo y Reyes, 2017)

6. RIESGO

Es un término proveniente del italiano, idioma que, a su vez, lo adoptó de una palabra del árabe clásico que podría traducirse como “lo que depara la providencia”. El término hace referencia a la proximidad o contingencia de un posible daño. (Fernández, 2019)

7. EVALUACIÓN DEL RIESGO

Es el procedimiento de evaluar riesgos generados del peligro, considerando la adaptación de controles que ya existen y la toma de decisión si el riesgo es o no aceptable. (Núñez, 2018)

2.4. HIPÓTESIS

2.4.1. HIPÓTESIS GENERAL

H_g: realizar una auditoría de seguridad de la información, aplicando la Norma ISO/IEC 27001 mejorará la confiabilidad y seguridad de la información en la Municipalidad Distrital de Luyando.

H_0: realizar una auditoría de seguridad de la información, aplicando la Norma ISO/IEC 27001 no mejorará la confiabilidad y seguridad de la información en la Municipalidad Distrital de Luyando.

2.4.2. HIPÓTESIS ESPECIFICAS

H_1: Analizar la situación actual del manejo de la información mejorará la seguridad de la información en la Municipalidad Distrital de Luyando.

H_0: Analizar la situación actual del manejo de la información no mejorará la seguridad de la información en la Municipalidad Distrital de Luyando.

H_2: Realizar la auditoria con la norma ISO/IEC 27001 optimizará la confidencialidad y seguridad de la información en la Municipalidad Distrital de Luyando.

H_0: Realizar la auditoria con la norma ISO/IEC 27001 no optimizará la confidencialidad y seguridad de la información en la Municipalidad Distrital de Luyando

H_3: Generar un manual de políticas de seguridad para el manejo de la información optimizará el uso de los equipos en la Municipalidad Distrital de Luyando.

H_0: Generar un manual de políticas de seguridad para el manejo de la información no optimizará el uso de los equipos en la Municipalidad Distrital de Luyando.

2.5. VARIABLES

2.5.1. VARIABLE INDEPENDIENTE

Auditoría de seguridad de la información aplicando la norma ISO/IEC 27001

2.5.2. VARIABLE DEPENDIENTE

Seguridad de la información en la Municipalidad Distrital de Luyando

2.6. OPERACIONALIZACIÓN DE VARIABLES

Tabla 2

Operacionalización de variables

VARIABLES	DIMENSIONES	INDICADORES
VARIABLE DEPENDIENTE Seguridad de la información en la Municipalidad Distrital de Luyando	Confidencialidad	• Nivel de confidencialidad de la seguridad de información.
	Integridad	• Nivel de integridad de la seguridad de información
	Disponibilidad	• Nivel de disponibilidad de la seguridad de información.
VARIABLE INDEPENDIENTE Auditoría de seguridad de la información aplicando la norma ISO/IEC 27001	Seguridad	• Gestión del riesgo • Control de la seguridad • Ciclo de vida de los sistemas • Planes de seguridad • Seguridad en Recursos Humanos • Protección física de las oficinas de trabajo • Seguridad en el puesto de trabajo • Control de la información saliente/entrante

CAPÍTULO III

METODOLOGÍA DE LA INVESTIGACION

3.1. TIPO DE INVESTIGACIÓN

Sampieri et al (2010), sostiene que la investigación básica está dirigida a un conocimiento más completo a través de la comprensión de los aspectos fundamentales de los fenómenos, de los hechos observables o de las relaciones que establecen los entes.

Ante lo antes mencionado la presente investigación será del tipo básica

3.1.1. ENFOQUE

Sampieri et al (2010), sostiene que el enfoque cuantitativo se fundamenta en un esquema deductivo y lógico que busca formular preguntas de investigación e hipótesis para posteriormente probarlas.

Ya que en la presente investigación se formuló preguntas e hipótesis la presente investigación fue de enfoque cuantitativo.

3.1.2. ALCANCE O NIVEL

Sampieri et al (2010), sostiene que los estudios explicativos van más allá de la descripción de conceptos o fenómenos o del establecimiento de relaciones entre conceptos; es decir, están dirigidos a responder por las causas de los eventos y fenómenos físicos o sociales.

Ya que en la presente investigación describe la seguridad de la información en la municipalidad la presente investigación fue una investigación explicativa.

3.1.3. DISEÑO

Fiallo et al (2008), sostiene que en la investigación Pre experimental el investigador asume un papel activo, efectúa una acción

a los participantes en un estudio y después observa las consecuencias, es decir, introduce cambios intencionales con el fin de observar los efectos que originan.

Ya que el investigador asume un papel activo en la presente investigación se adoptó la investigación Pre experimental de “pre test” y “post test”, en este caso el test que se utilizó la llamamos cuestionario de encuesta con un solo grupo de investigación, considerando el siguiente esquema:

ESQUEMA

Dónde:

G = Grupo de investigación (Los 32 funcionarios de la municipalidad)
X = Aplicación (Aplicación de la norma ISO/IEC 27001)
O1 = Pre Observación
O2 = Post Observación

3.2. POBLACIÓN Y MUESTRA

3.2.1. POBLACIÓN

Los 32 funcionarios de la municipalidad de quienes se recogió la información sobre la confiabilidad y seguridad de la información en la Municipalidad Distrital de Luyando.

Tabla 3

Población

DEPARTAMENTO	NÚMERO DE FUNCIONARIOS
AGUA POTABLE Y ALCANTARILLADO	4
ALCALDÍA	2
ASESORÍA JURÍDICA	2
DEPARTAMENTO DE CATASTROS Y AVALÚOS	3
DEPARTAMENTO DE DESARROLLO SOCIAL	4
DEPARTAMENTO DE OBRAS PÚBLICAS	4
DEPARTAMENTO DE LOGISTICA	2

DEPARTAMENTO DE SERVICIOS PÚBLICOS	3
DEPARTAMENTO ECONOMÍA	3
REGISTRO DE LA PROPIEDAD	2
TALENTO HUMANO	1
TESORERÍA	2
TOTAL	32

3.2.2. MUESTRA

Se empleó una muestra poblacional que consiste en 32 funcionarios de la Municipalidad Distrital de Luyando.

Además, no se contempla criterios de inclusión y exclusión ya que todos los funcionarios están obligados a participar de la investigación por disposición de las autoridades de la municipalidad.

3.3. TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE DATOS

3.3.1. PARA LA RECOLECCIÓN DE DATOS

- **TÉCNICAS**

Fichaje: Esta técnica sirvió para recopilar y almacenar mediante el registro los aspectos esenciales de los documentos bibliográficos y que consultemos sobre el tema de investigación.

Se emplearon fichas bibliográficas sobre seguridad de la información.

Encuesta: Técnica que permitió obtener información sobre cómo influyó y mejoró la aplicación de la norma ISO/27001 en la Municipalidad Distrital de Luyando, mostrado previa y posteriormente a la aplicación de la investigación.

- **INSTRUMENTO**

Para la presente investigación el test que se utilizó fue el cuestionario de encuesta para medir la confiabilidad y seguridad de la información antes y después de la aplicación de la presente investigación

en la Municipalidad Distrital de Luyando como primordial instrumento de recolección de datos, con la finalidad de obtener toda la información relevante para la resolución del problema planteado.

3.3.2. PARA LA PRESENTACIÓN DE DATOS

Para la presentación de los datos usamos tablas y figuras que nos proporcionó el programa SPSS en su versión 25.

3.3.3. PARA EL ANÁLISIS Y LA ANÁLISIS E INTERPRETACIÓN DE LOS DATOS

Sánchez (2015). Afirma que la prueba t de Student para muestras relacionadas permite comparar las medias de dos series de mediciones realizadas sobre las mismas unidades estadísticas.

En cuanto al análisis e Análisis e Interpretación de los datos de la investigación se hizo uso del programa SPSS en su versión 25 , que nos brindó todas las facilidades para el desarrollo de la presente investigación, para ello se empleó el estadístico “T” de Student para muestras relacionadas.

CAPÍTULO IV

RESULTADOS

4.1. PROCESAMIENTO DE DATOS

PRE TEST APLICADO AL INICIO DE LA INVESTIGACIÓN

Tabla 4

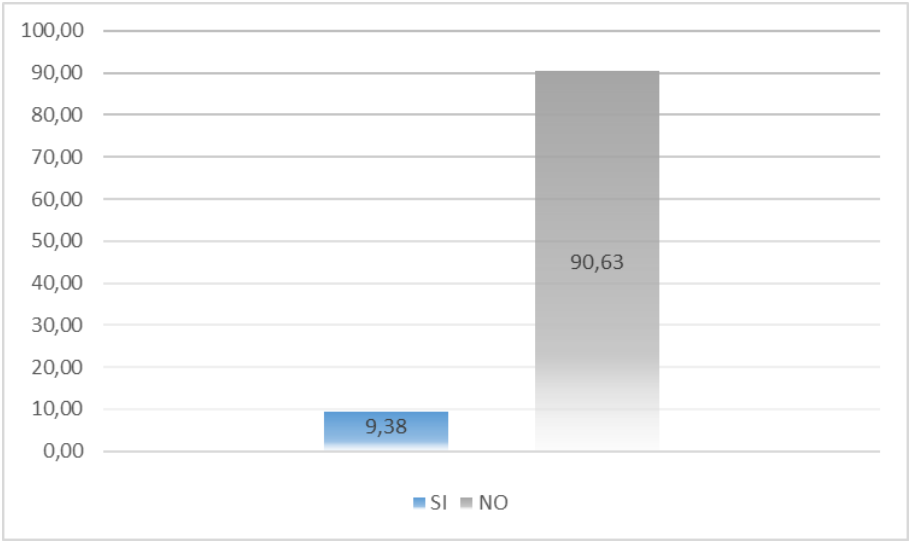
Políticas de seguridad para la gestión de información

¿En la municipalidad se cuenta con políticas de seguridad para la gestión de información?		
	Frecuencia	Porcentaje
SI	3	9,38
NO	29	90,63
Total	32	100,00

Nota: Resultado del programa SPSS

Figura 1

Políticas de seguridad para la gestión de información



Nota: Resultado del programa SPSS

Interpretación:

En la Tabla 4 y Figura 1 se observa que el 9.38% sostiene que la municipalidad si cuenta con políticas de seguridad para la gestión de información y el 90.63% sostiene que la municipalidad no cuenta con políticas de seguridad para la gestión de información.

Tabla 5

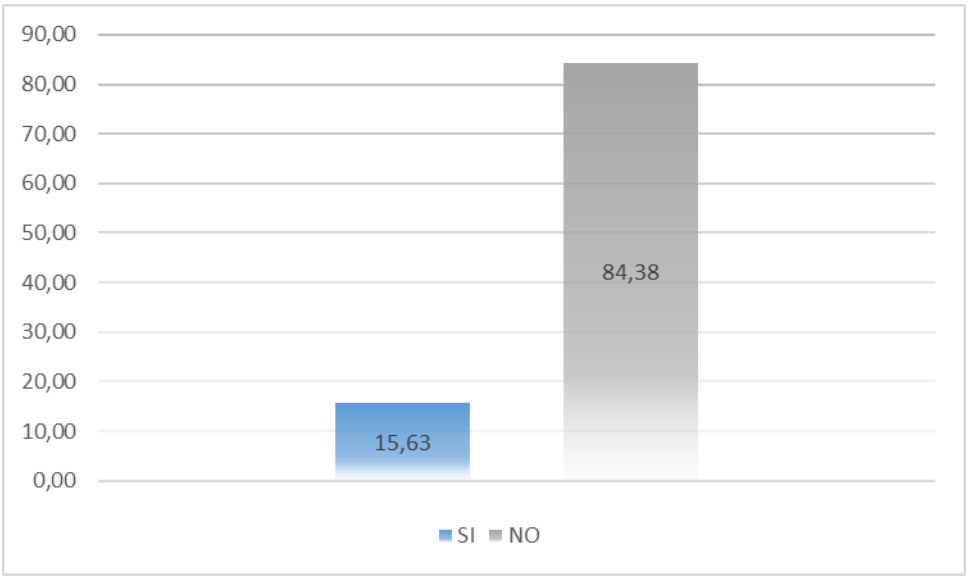
Conocimientos de las políticas de seguridad existentes

¿El personal de la municipalidad tiene conocimientos de las políticas de seguridad existentes?		
	Frecuencia	Porcentaje
SI	5	15,63
NO	27	84,38
Total	32	100,00

Nota: Resultado del programa SPSS

Figura 2

Conocimientos de las políticas de seguridad existentes



Nota: Resultado del programa SPSS

Análisis e Interpretación:

En la Tabla 5 y Figura 2 se observa que el 15.63% sostiene que el personal de la municipalidad si tiene conocimientos de las políticas de seguridad existentes y el 84.38% sostiene que el personal de la municipalidad no tiene conocimientos de las políticas de seguridad existentes.

Tabla 6

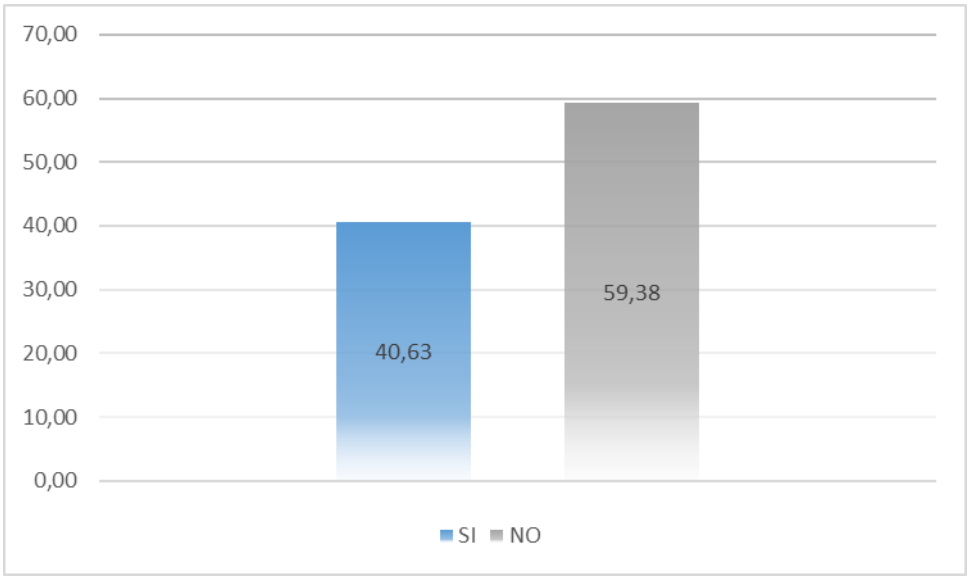
Responsabilidades para uso de los recursos de la municipalidad

¿Cada empleado tiene responsabilidades asignadas del uso de los recursos de la municipalidad?		
	Frecuencia	Porcentaje
SI	13	40,63
NO	19	59,38
Total	32	100,00

Nota: Resultado del programa SPSS

Figura 3

Responsabilidades para uso de los recursos de la municipalidad



Nota: Resultado del programa SPSS

Análisis e Interpretación:

En la Tabla 6 y Figura 3 se observa que el 40.63% sostiene que cada empleado si tiene responsabilidades asignadas del uso de los recursos de la municipalidad y el 59.38% sostiene que cada empleado no tiene responsabilidades asignadas del uso de los recursos de la municipalidad.

Tabla 7

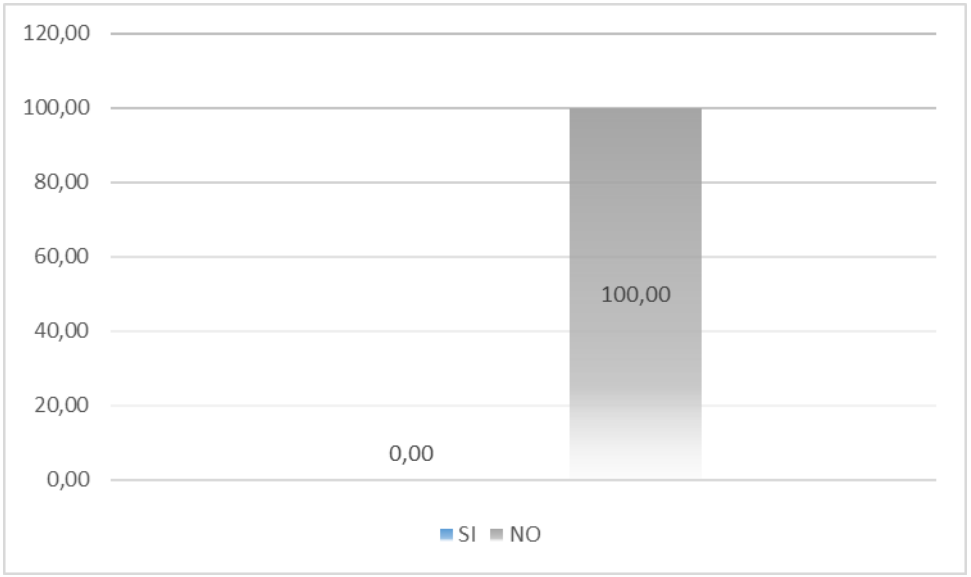
Control adecuado del acceso para que personas no autorizadas

¿Se lleva un control adecuado del acceso del personal para que personas no autorizadas no puedan acceder a los equipos y sistema de la municipalidad?		
	Frecuencia	Porcentaje
SI	0	0,00
NO	32	100,00
Total	32	100,00

Nota: Resultado del programa SPSS

Figura 4

Control adecuado del acceso para que personas no autorizadas



Nota: Resultado del programa SPSS

Análisis e Interpretación:

En la Tabla 7 y Figura 4 se observa el 100% sostiene que no se lleva un control adecuado del acceso del personal para que personas no autorizadas no puedan acceder a los equipos y sistema de la municipalidad.

Tabla 8

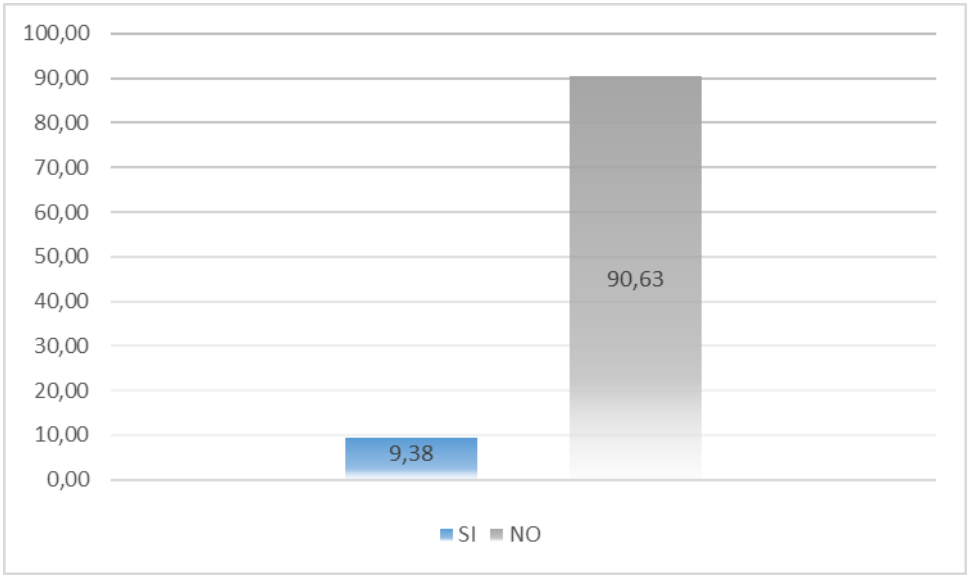
Existencia de controles de usuarios

¿Se tiene establecido los debidos controles de usuarios con las debidas restricciones de acuerdo al perfil de cada uno?		
	Frecuencia	Porcentaje
SI	3	9,38
NO	29	90,63
Total	32	100,00

Nota: Resultado del programa SPSS

Figura 5

Existencia de controles de usuarios



Nota: Resultado del programa SPSS

Análisis e Interpretación:

En la Tabla 8 y Figura 5 se observa que el 9.38% sostiene que si se tiene establecido los debidos controles de usuarios con las debidas restricciones de acuerdo al perfil de cada uno y el 90.63% sostiene que no se tiene establecido los debidos controles de usuarios con las debidas restricciones de acuerdo al perfil de cada uno.

Tabla 9

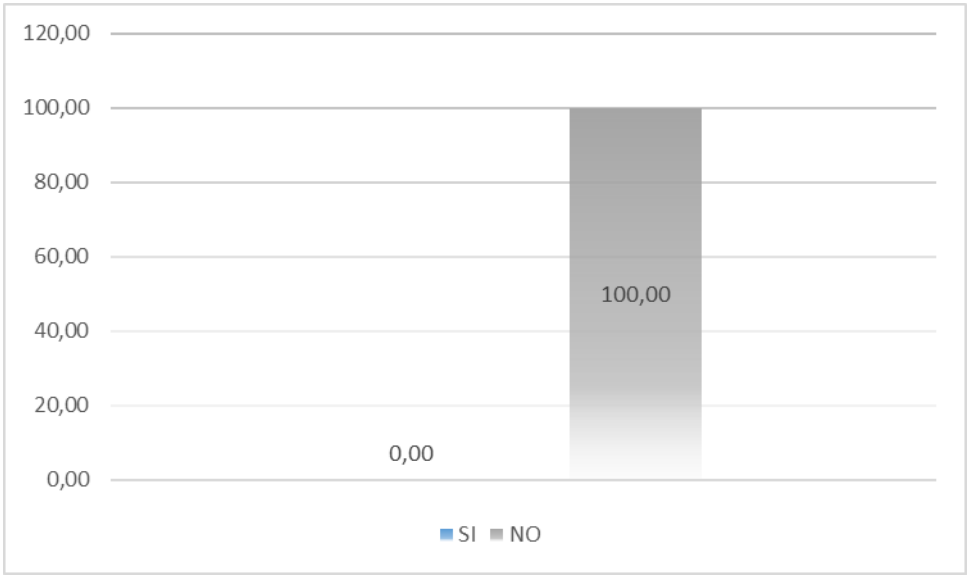
Características de contraseñas

¿Los sistemas al momento de ingresar una contraseña solicita que esta tenga letras números y caracteres especiales?		
	Frecuencia	Porcentaje
SI	0	0,00
NO	32	100,00
Total	32	100,00

Nota: Resultado del programa SPSS

Figura 6

Características de contraseñas



Nota: Resultado del programa SPSS

Análisis e Interpretación:

En la Tabla 9 y Figura 6 se observa el 100% sostiene que los sistemas al momento de ingresar una contraseña no solicitan que esta tenga letras números y caracteres especiales.

Tabla 10

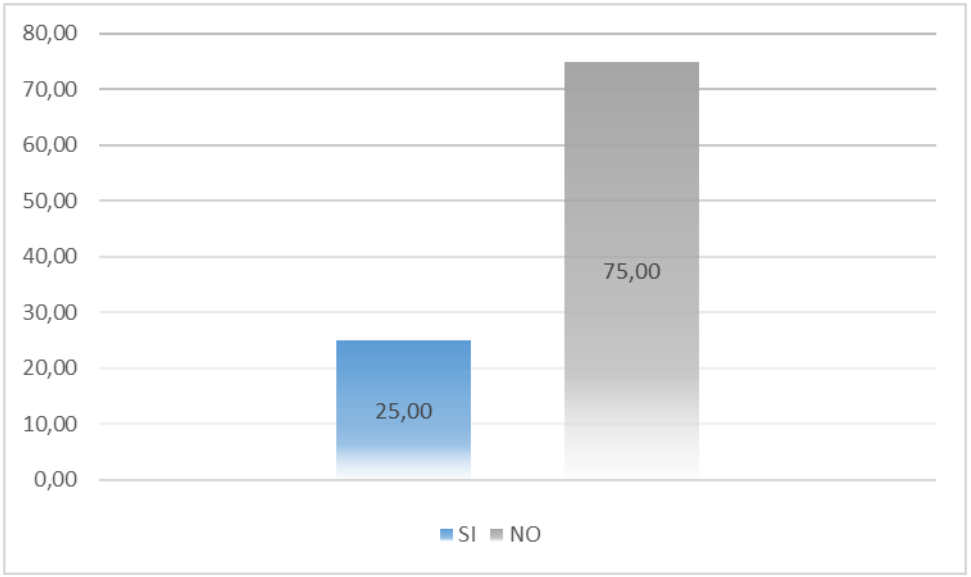
Mantenimiento correctivo y preventivo de los equipos

¿Se lleva a cabo periódicamente el mantenimiento correctivo y preventivo de los equipos de la municipalidad?		
	Frecuencia	Porcentaje
SI	8	25,00
NO	24	75,00
Total	32	100,00

Nota: Resultado del programa SPSS

Figura 7

Mantenimiento correctivo y preventivo de los equipos



Nota: Resultado del programa SPSS

Análisis e Interpretación:

En la Tabla 10 y Figura 7 se observa que el 25.00% sostiene que si se lleva a cabo periódicamente el mantenimiento correctivo y preventivo de los equipos de la municipalidad y el 75.00% sostiene que no se lleva a cabo periódicamente el mantenimiento correctivo y preventivo de los equipos de la municipalidad.

Tabla 11

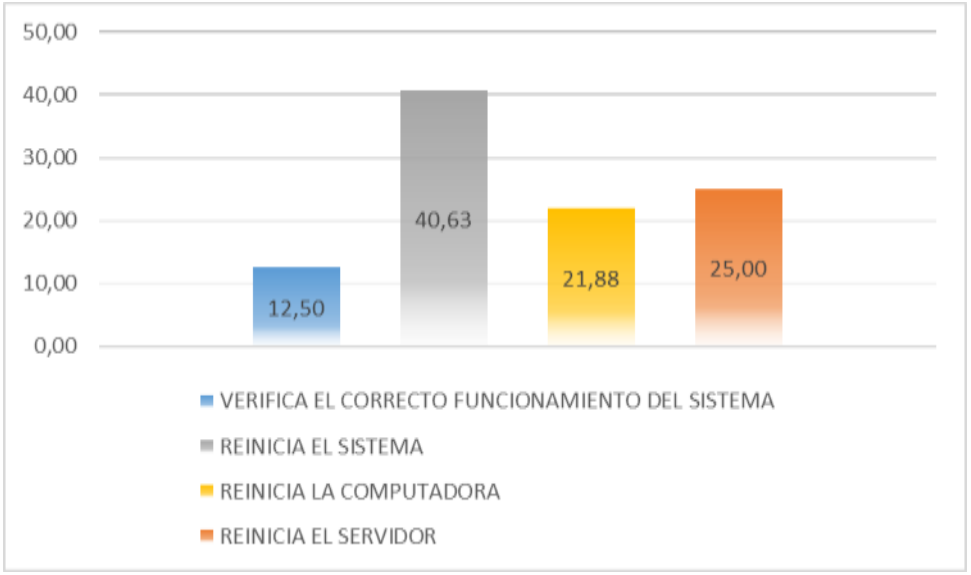
Actividades del departamento de Tecnología de la información

¿Qué hace el departamento de Tecnología de la información cuando el sistema tiene algún fallo?		
	Frecuencia	Porcentaje
VERIFICA EL CORRECTO FUNCIONAMIENTO DEL SISTEMA	4	12,50
REINICIA EL SISTEMA	13	40,63
REINICIA LA COMPUTADORA	7	21,88
REINICIA EL SERVIDOR	8	25,00
Total	32	100,00

Nota: Resultado del programa SPSS

Figura 8

Actividades del departamento de Tecnología de la información



Nota: Resultado del programa SPSS

Análisis e Interpretación:

En la Tabla 11 y Figura 8 se observa que ante la pregunta ¿qué hace el departamento de tecnología de la información cuando el sistema tiene algún fallo? el 12.50% sostiene que verifica el correcto funcionamiento del sistema; el 40.63% sostiene que reinicia el sistema; el 21.88% sostiene que reinicia la computadora; el 25.00% sostiene que reinicia el servidor.

Tabla 12

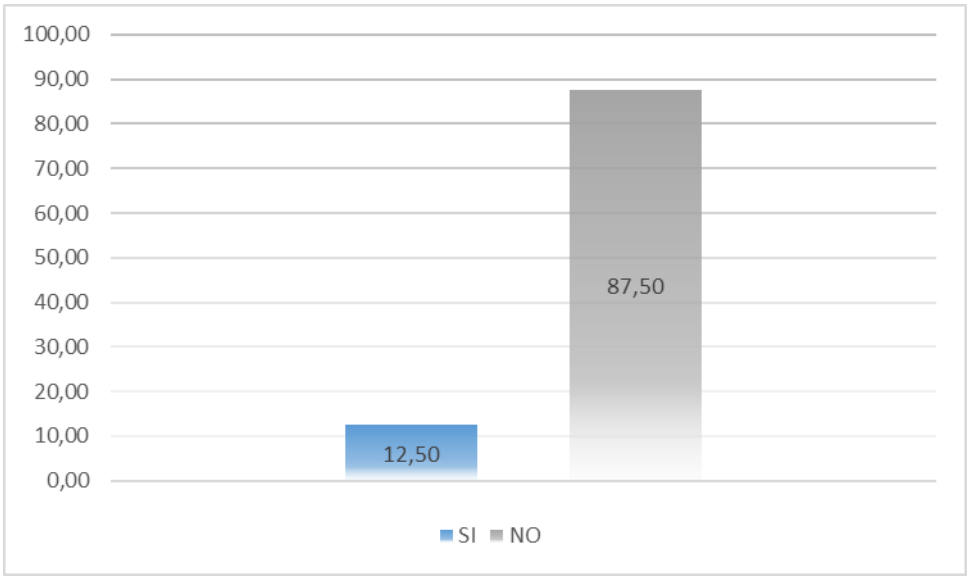
Existencia de monitoreo constantemente a los sistemas

¿Se realizan monitoreo constantemente a los sistemas para evitar cualquier eventualidad?		
	Frecuencia	Porcentaje
SI	4	12,50
NO	28	87,50
Total	32	100,00

Nota: Resultado del programa SPSS

Figura 9

Existencia de monitoreo constantemente a los sistemas



Nota: Resultado del programa SPSS

Análisis e Interpretación:

En la Tabla 12 y Figura 9 se observa que el 12.50% sostiene que si se realizan monitoreo constantemente a los sistemas para evitar cualquier eventualidad y el 87.50% sostiene que no se realizan monitoreo constantemente a los sistemas para evitar cualquier eventualidad.

Tabla 13

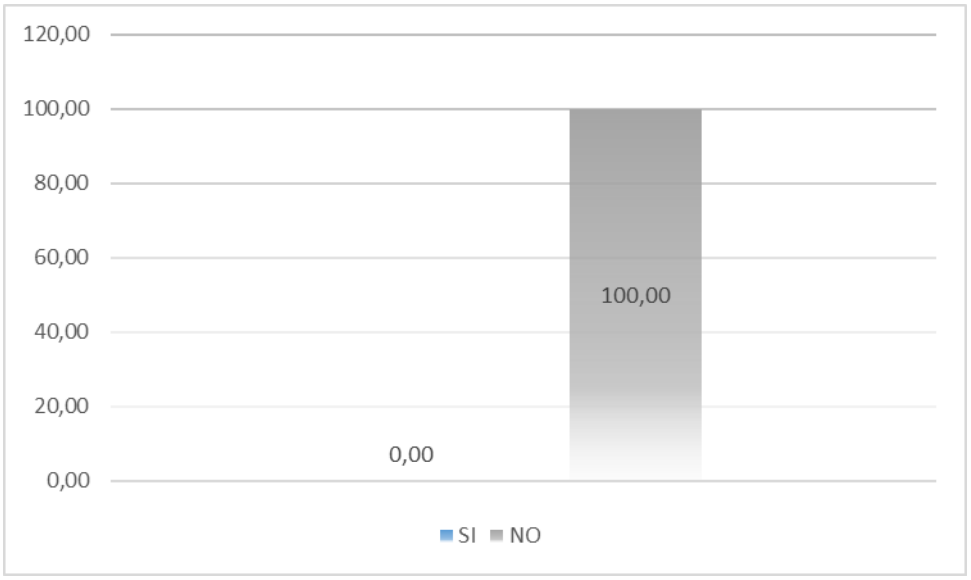
Sistema de inventario de recursos informáticos

¿Cuentan con un sistema de inventario de recursos informáticos de la institución?		
	Frecuencia	Porcentaje
SI	0	0,00
NO	32	100,00
Total	32	100,00

Nota: Resultado del programa SPSS

Figura 10

Sistema de inventario de recursos informáticos



Nota: Resultado del programa SPSS

Análisis e Interpretación:

En la Tabla 13 y Figura 10 se observa que el 100% sostiene que no se cuentan con un sistema de inventario de recursos informáticos de la institución.

Tabla 14

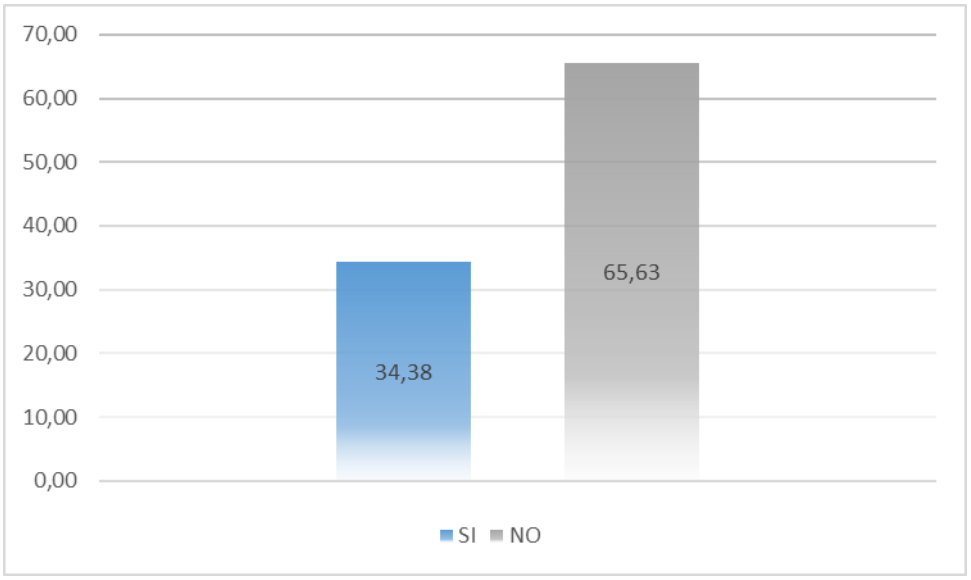
Conocimientos en seguridad de la información del personal

¿El departamento cuenta con personal que tengan amplios conocimientos en seguridad de la información?		
	Frecuencia	Porcentaje
SI	11	34,38
NO	21	65,63
Total	32	100,00

Nota: Resultado del programa SPSS

Figura 11

Conocimientos en seguridad de la información del personal



Nota: Resultado del programa SPSS

Análisis e Interpretación:

En la Tabla 14 y Figura 11 se observa que el 34.38% sostiene que el departamento si cuenta con personal que tengan amplios conocimientos en seguridad de la información y el 65.63% sostiene que el departamento no cuenta con personal que tengan amplios conocimientos en seguridad de la información.

Tabla 15

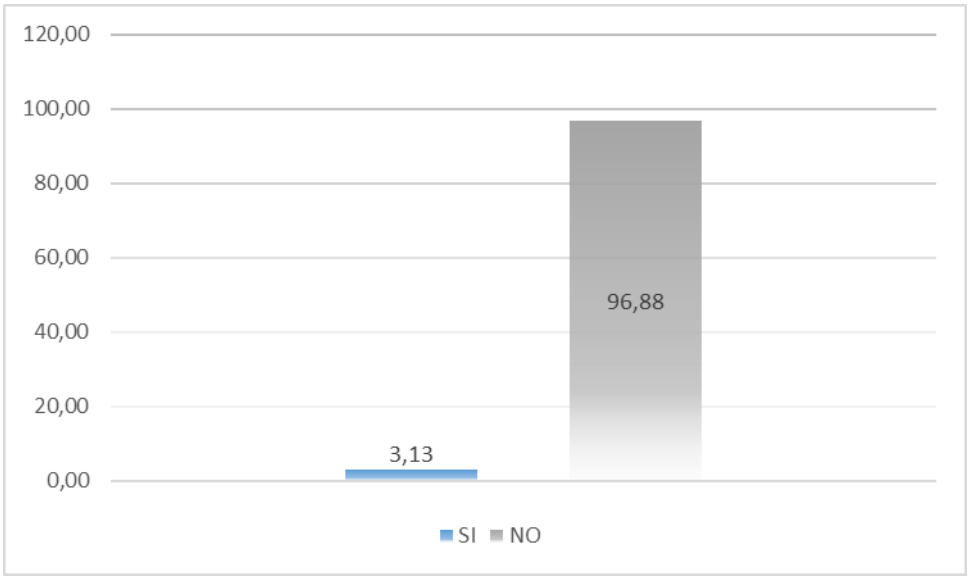
Políticas de seguridad por departamento

¿Cada departamento de la municipalidad tiene asignada políticas de seguridad?		
	Frecuencia	Porcentaje
SI	1	3,13
NO	31	96,88
Total	32	100,00

Nota: Resultado del programa SPSS

Figura 12

Políticas de seguridad por departamento



Nota: Resultado del programa SPSS

Análisis e Interpretación:

En la Tabla 15 y Figura 12 se observa que el 3.13% sostiene que cada departamento de la municipalidad si tiene asignada políticas de seguridad y el 96.88% sostiene que cada departamento de la municipalidad no tiene asignada políticas de seguridad.

Tabla 16

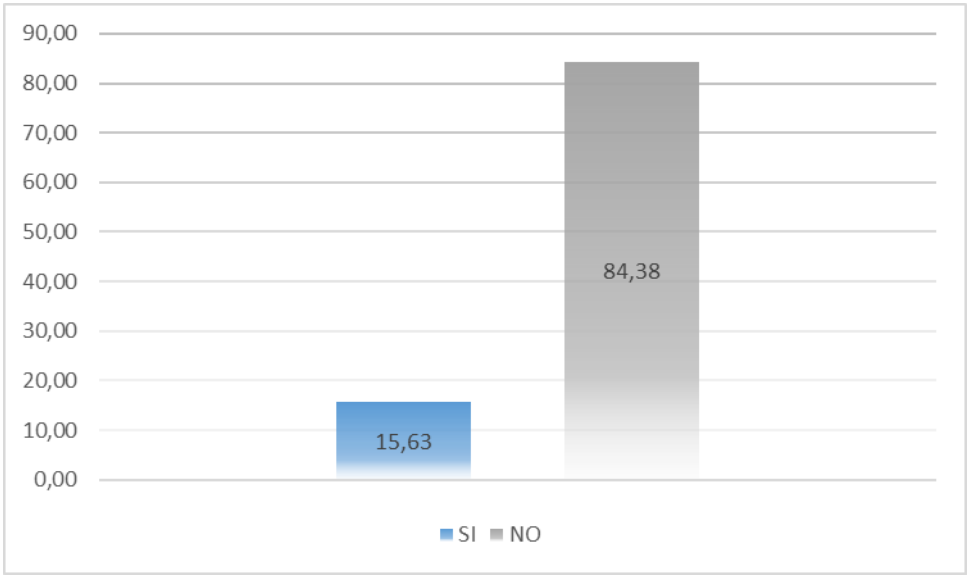
Existencia de política de confidencialidad de la información

¿Cuenta la municipalidad con algún tipo de política de confidencialidad de la información en el caso de que un empleado abandone el cargo se le supriman todos los accesos al sistema?		
	Frecuencia	Porcentaje
SI	5	15,63
NO	27	84,38
Total	32	100,00

Nota: Resultado del programa SPSS

Figura 13

Existencia de política de confidencialidad de la información



Nota: Resultado del programa SPSS

Análisis e Interpretación:

En la Tabla 16 y Figura 13 se observa que el 15.63% sostiene que la municipalidad si cuenta con algún tipo de política de confidencialidad de la información en el caso de que un empleado abandone el cargo se le supriman todos los accesos al sistema y el 84.38% sostiene que la municipalidad no cuenta con algún tipo de política de confidencialidad de la información en el caso de que un empleado abandone el cargo se le supriman todos los accesos al sistema.

Tabla 17

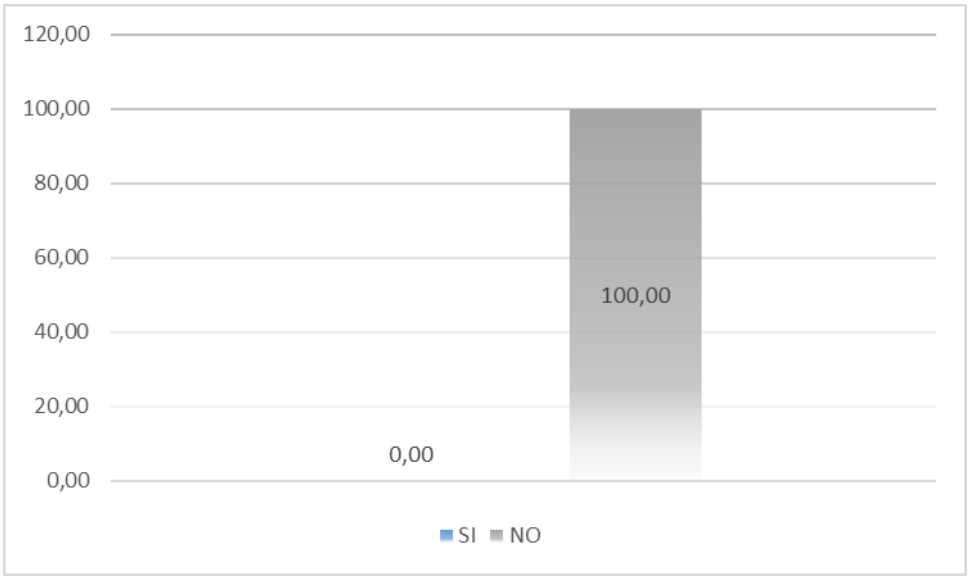
Revisión periódicamente el cableado en los departamentos de la municipalidad

¿Se revisa periódicamente el cableado en todos los departamentos de la municipalidad?		
	Frecuencia	Porcentaje
SI	0	0,00
NO	32	100,00
Total	32	100,00

Nota: Resultado del programa SPSS

Figura 14

Revisión periódicamente el cableado en los departamentos de la municipalidad



Nota: Resultado del programa SPSS

Análisis e Interpretación:

En la Tabla 17 y Figura 14 se observa que el 100% sostiene que no se revisa periódicamente el cableado en todos los departamentos de la municipalidad.

Tabla 18

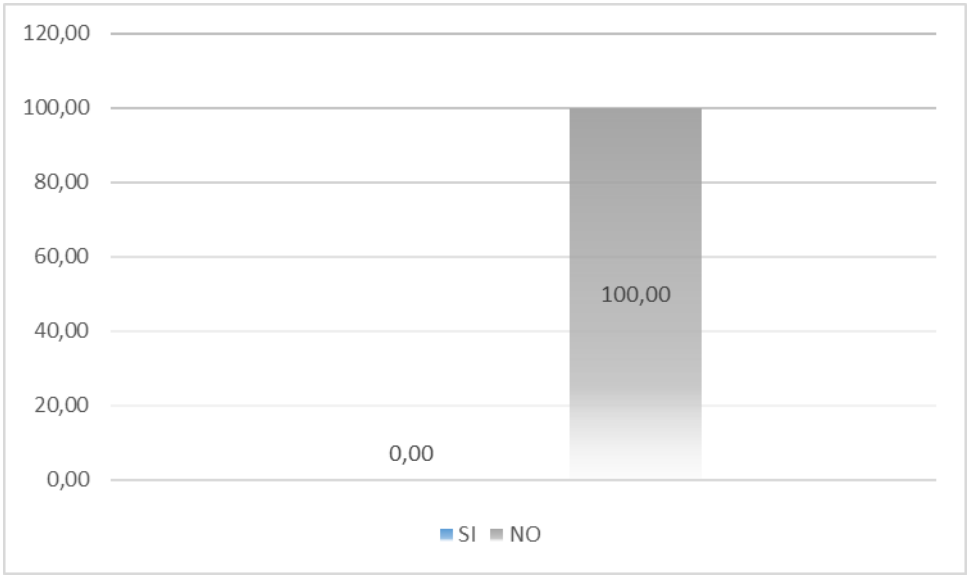
Copias de seguridad de la información

¿Se realizan copias de seguridad de la información?		
	Frecuencia	Porcentaje
SI	0	0,00
NO	32	100,00
Total	32	100,00

Nota: Resultado del programa SPSS

Figura 15

Copias de seguridad de la información



Nota: Resultado del programa SPSS

Análisis e Interpretación:

En la Tabla 18 y Figura 15 se observa que el 100% sostiene que no se realizan copias de seguridad de la información.

POST TEST APLICADO AL INICIO DE LA INVESTIGACIÓN

Tabla 19

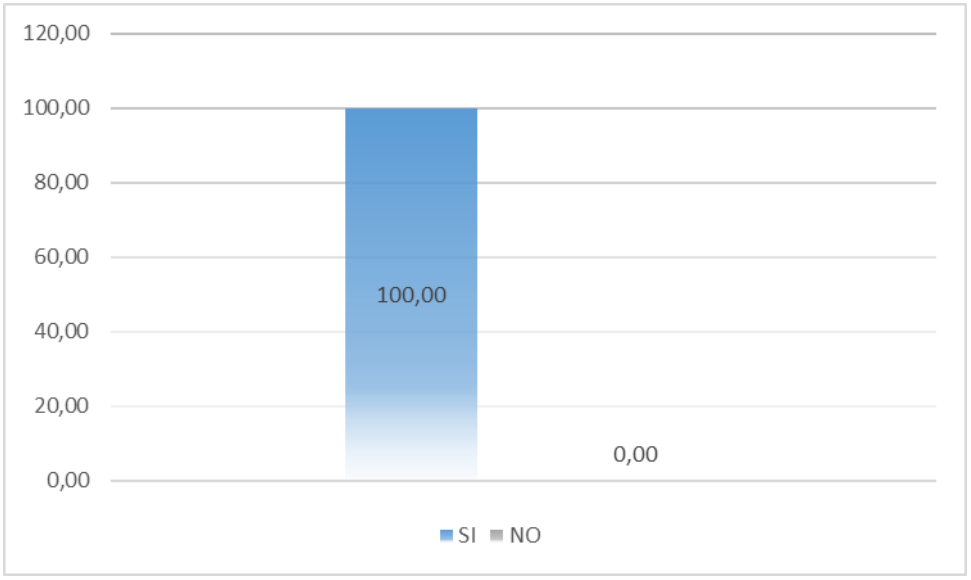
Políticas de seguridad para la gestión de información

¿En la municipalidad se cuenta con políticas de seguridad para la gestión de información?		
	Frecuencia	Porcentaje
SI	32	100,00
NO	0	0,00
Total	32	100,00

Nota: Resultado del programa SPSS

Figura 16

Políticas de seguridad para la gestión de información



Nota: Resultado del programa SPSS

Análisis e Interpretación:

En la Tabla 19 y Figura 16 se observa que el 100% sostiene que la municipalidad si cuenta con políticas de seguridad para la gestión de información.

Tabla 20

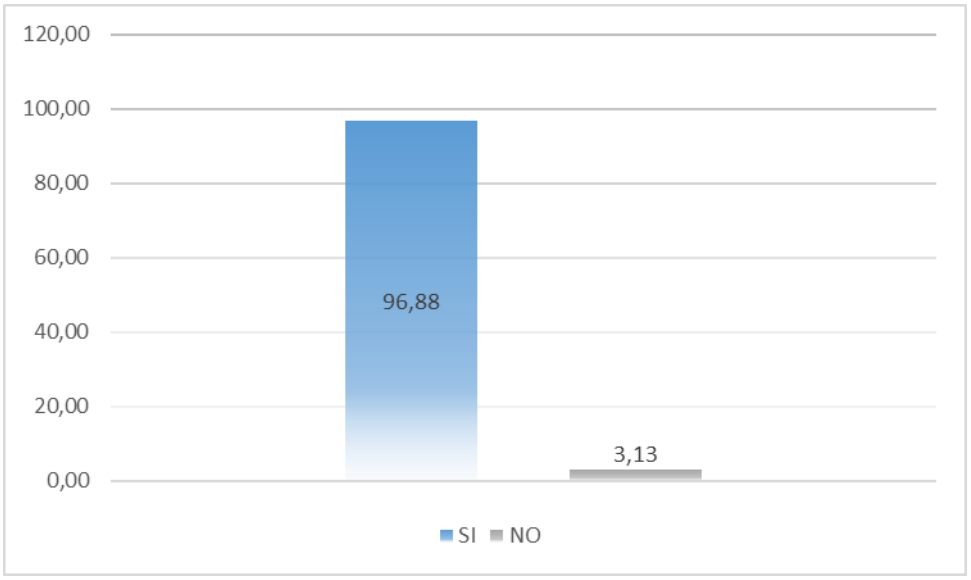
Conocimientos de las políticas de seguridad existentes

¿El personal de la municipalidad tiene conocimientos de las políticas de seguridad existentes?		
	Frecuencia	Porcentaje
SI	31	96,88
NO	1	3,13
Total	32	100,00

Nota: Resultado del programa SPSS

Figura 17

Conocimientos de las políticas de seguridad existentes



Nota: Resultado del programa SPSS

Análisis e Interpretación:

En la Tabla 20 y Figura 17 se observa que el 96.88% sostiene que el personal de la municipalidad si tiene conocimientos de las políticas de seguridad existentes y el 3.13% sostiene que el personal de la municipalidad no tiene conocimientos de las políticas de seguridad existentes.

Tabla 21

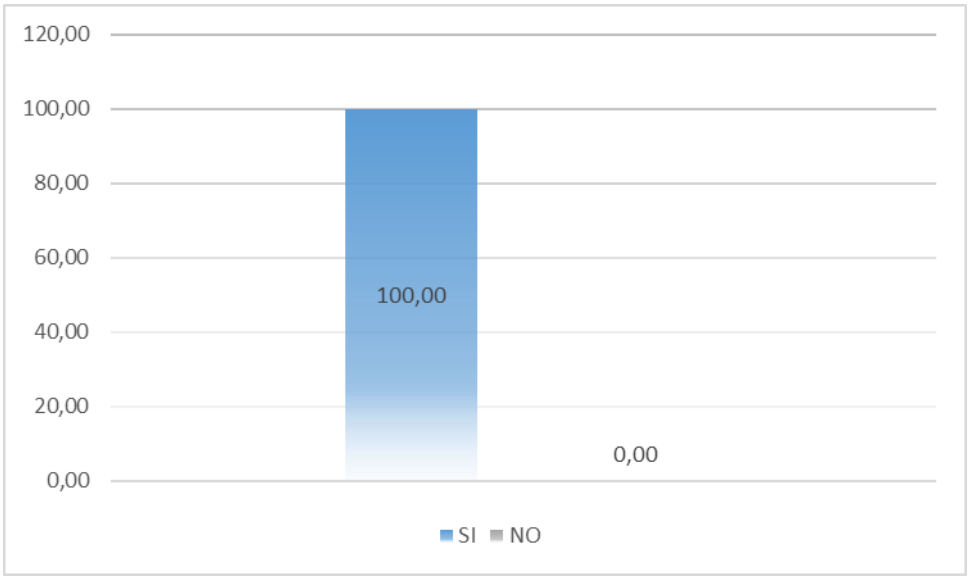
Responsabilidades para uso de los recursos de la municipalidad

¿Cada empleado tiene responsabilidades asignadas del uso de los recursos de la municipalidad?		
	Frecuencia	Porcentaje
SI	32	100,00
NO	0	0,00
Total	32	100,00

Nota: Resultado del programa SPSS

Figura 18

Responsabilidades para uso de los recursos de la municipalidad



Nota: Resultado del programa SPSS

Análisis e Interpretación:

En la Tabla 21 y Figura 18 se observa que el 100% sostiene que cada empleado SI tiene responsabilidades asignadas del uso de los recursos de la municipalidad.

Tabla 22

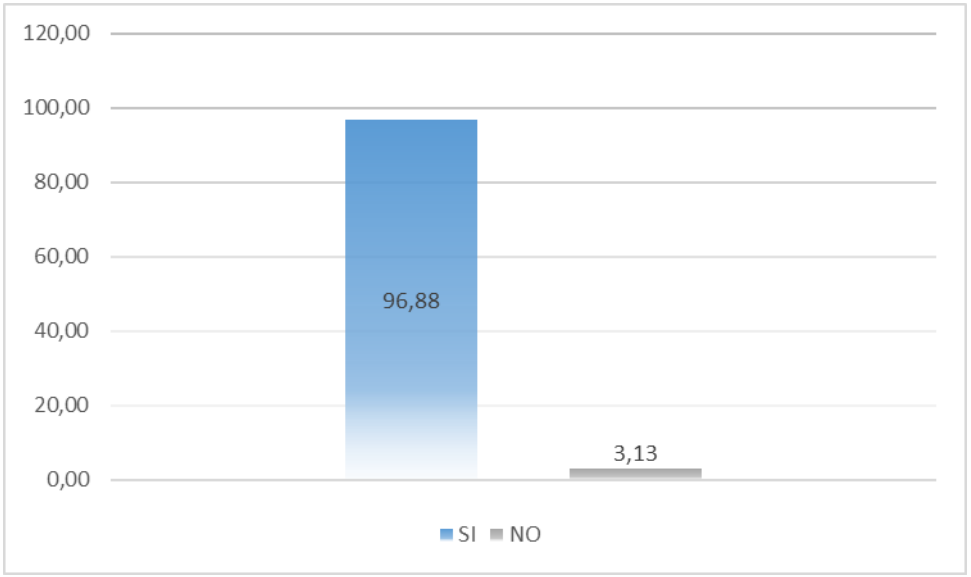
Control adecuado del acceso para que personas no autorizadas

¿Se lleva un control adecuado del acceso del personal para que personas no autorizadas no puedan acceder a los equipos y sistema de la municipalidad?		
	Frecuencia	Porcentaje
SI	31	96,88
NO	1	3,13
Total	32	100,00

Nota: Resultado del programa SPSS

Figura 19

Control adecuado del acceso para que personas no autorizadas



Nota: Resultado del programa SPSS

Análisis e Interpretación:

En la Tabla 22 y Figura 19 se observa que el 96.88% sostiene que si se lleva un control adecuado del acceso del personal para que personas no autorizadas no puedan acceder a los equipos y sistema de la municipalidad y el 3.13% sostiene que no se lleva un control adecuado del acceso del personal para que personas no autorizadas no puedan acceder a los equipos y sistema de la municipalidad.

Tabla 23

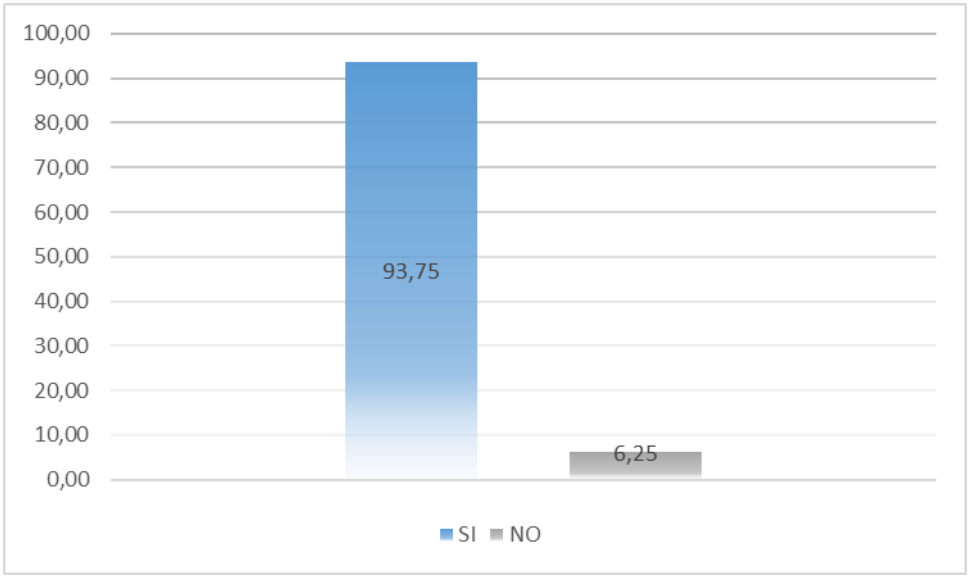
Existencia de controles de usuarios

¿ Se tiene establecido los debidos controles de usuarios con las debidas restricciones de acuerdo al perfil de cada uno?		
	Frecuencia	Porcentaje
SI	30	93,75
NO	2	6,25
Total	32	100,00

Nota: Resultado del programa SPSS

Figura 20

Existencia de controles de usuarios



Nota: Resultado del programa SPSS

Análisis e Interpretación:

En la Tabla 23 y Figura 20 se observa que el 93.75% sostiene que si se tiene establecido los debidos controles de usuarios con las debidas restricciones de acuerdo al perfil de cada uno y el 6.25% sostiene que no se tiene establecido los debidos controles de usuarios con las debidas restricciones de acuerdo al perfil de cada uno.

Tabla 24

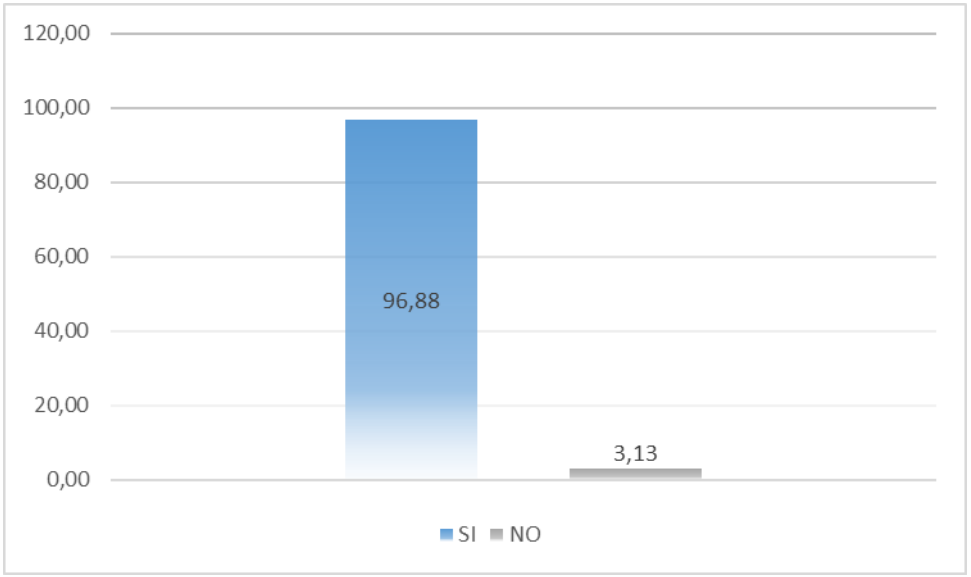
Características de contraseñas

¿Los sistemas al momento de ingresar una contraseña solicita que esta tenga letras números y caracteres especiales?		
	Frecuencia	Porcentaje
SI	31	96,88
NO	1	3,13
Total	32	100,00

Nota: Resultado del programa SPSS

Figura 21

Características de contraseñas



Nota: Resultado del programa SPSS

Análisis e Interpretación:

En la Tabla 24 y Figura 21 se observa que el 96.88% sostiene que los sistemas al momento de ingresar una contraseña si solicita que esta tenga letras números y caracteres especiales y el 3.13% sostiene que los sistemas al momento de ingresar una contraseña no solicita que esta tenga letras números y caracteres especiales.

Tabla 25

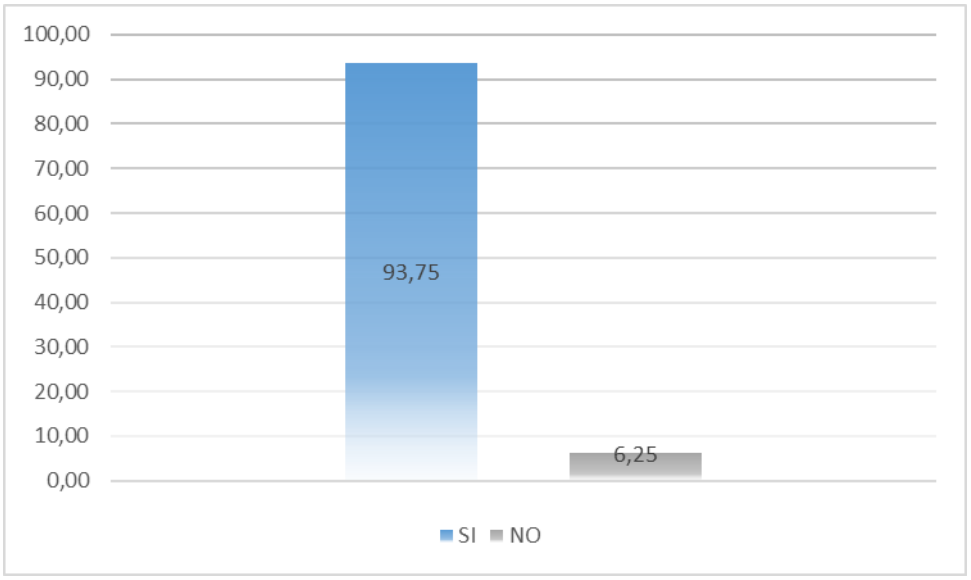
Mantenimiento correctivo y preventivo de los equipos

¿Se lleva a cabo periódicamente el mantenimiento correctivo y preventivo de los equipos de la municipalidad		
	Frecuencia	Porcentaje
SI	30	93,75
NO	2	6,25
Total	32	100,00

Nota: Resultado del programa SPSS

Figura 22

Mantenimiento correctivo y preventivo de los equipos



Nota: Resultado del programa SPSS

Análisis e Interpretación:

En la Tabla 25 y Figura 22 se observa que el 93.75% sostiene que si se lleva a cabo periódicamente el mantenimiento correctivo y preventivo de los equipos de la municipalidad y el 6.25% sostiene que no se lleva a cabo periódicamente el mantenimiento correctivo y preventivo de los equipos de la municipalidad.

Tabla 26

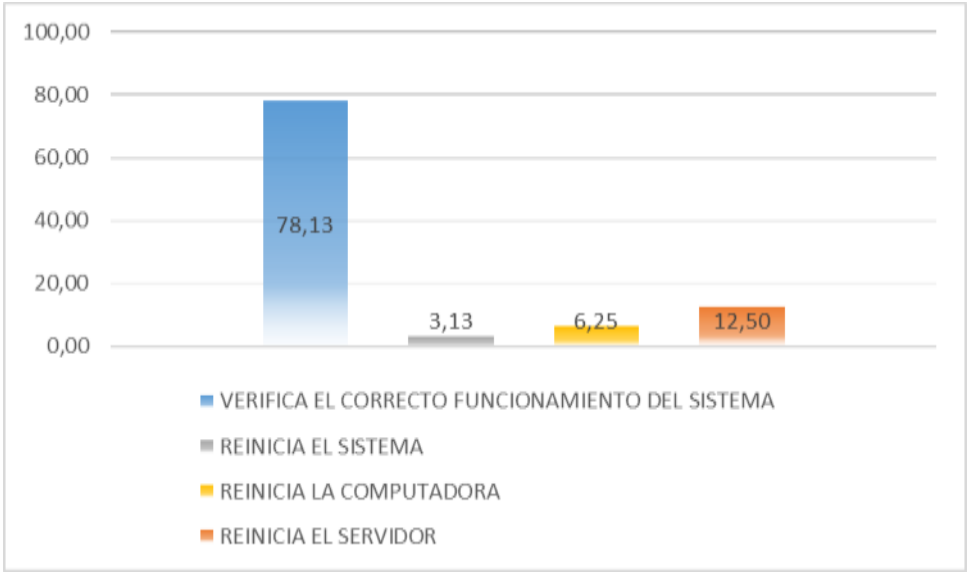
Actividades del departamento de Tecnología de la información

¿Qué hace el departamento de Tecnología de la información cuando el sistema tiene algún fallo?		
	Frecuencia	Porcentaje
VERIFICA EL CORRECTO FUNCIONAMIENTO DEL SISTEMA	25	78,13
REINICIA EL SISTEMA	1	3,13
REINICIA LA COMPUTADORA	2	6,25
REINICIA EL SERVIDOR	4	12,50
Total	32	100,00

Nota: Resultado del programa SPSS

Figura 23

Actividades del departamento de Tecnología de la información



Nota: Resultado del programa SPSS

Análisis e Interpretación:

En la Tabla 26 y Figura 23 se observa que ante la pregunta ¿qué hace el departamento de tecnología de la información cuando el sistema tiene algún fallo? el 78.13% sostiene que verifica el correcto funcionamiento del sistema; el 3.13% sostiene que reinicia el sistema; el 6.25% sostiene que reinicia la computadora; el 12.50% sostiene que reinicia el servidor.

Tabla 27

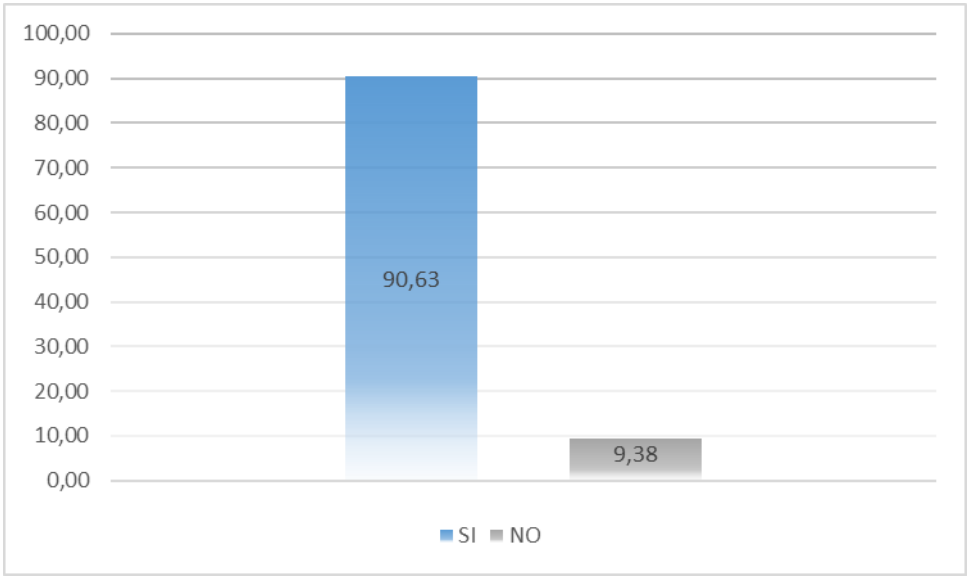
Existencia de monitoreo constantemente a los sistemas

¿Se realizan monitoreo constantemente a los sistemas para evitar cualquier eventualidad?		
	Frecuencia	Porcentaje
SI	29	90,63
NO	3	9,38
Total	32	100,00

Nota: Resultado del programa SPSS

Figura 24

Existencia de monitoreo constantemente a los sistemas



Nota: Resultado del programa SPSS

Análisis e Interpretación:

En la Tabla 27 y Figura 24 se observa que el 90.63% sostiene que si se realizan monitoreo constantemente a los sistemas para evitar cualquier eventualidad y el 9.38% sostiene que no se realizan monitoreo constantemente a los sistemas para evitar cualquier eventualidad.

Tabla 28

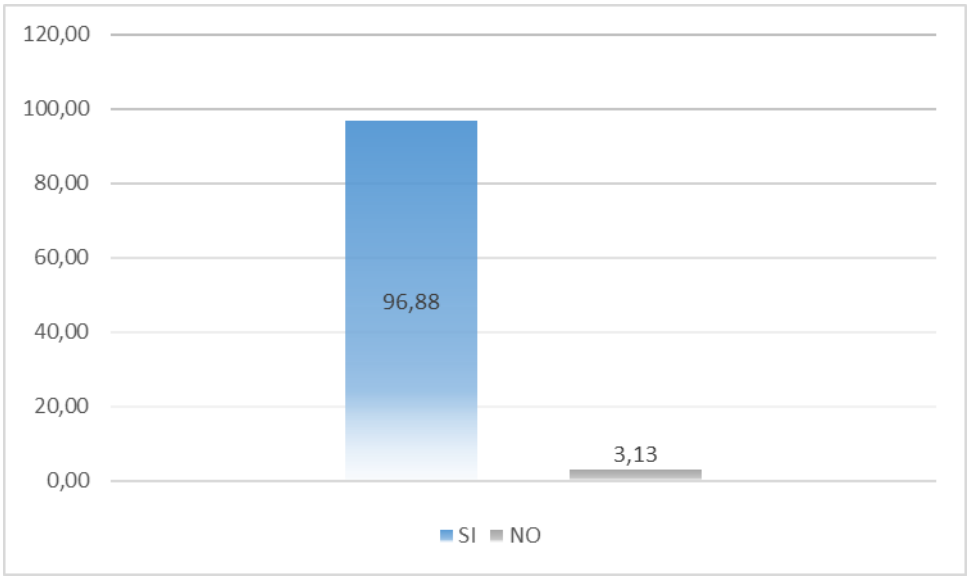
Sistema de inventario de recursos informáticos

¿Cuentan con un sistema de inventario de recursos informáticos de la institución?		
	Frecuencia	Porcentaje
SI	31	96,88
NO	1	3,13
Total	32	100,00

Nota: Resultado del programa SPSS

Figura 25

Sistema de inventario de recursos informáticos



Nota: Resultado del programa SPSS

Análisis e Interpretación:

En la Tabla 28 y Figura 25 se observa que el 96.88% sostiene que si se cuentan con un sistema de inventario de recursos informáticos de la institución y el 3.13% sostiene que no se cuentan con un sistema de inventario de recursos informáticos de la institución.

Tabla 29

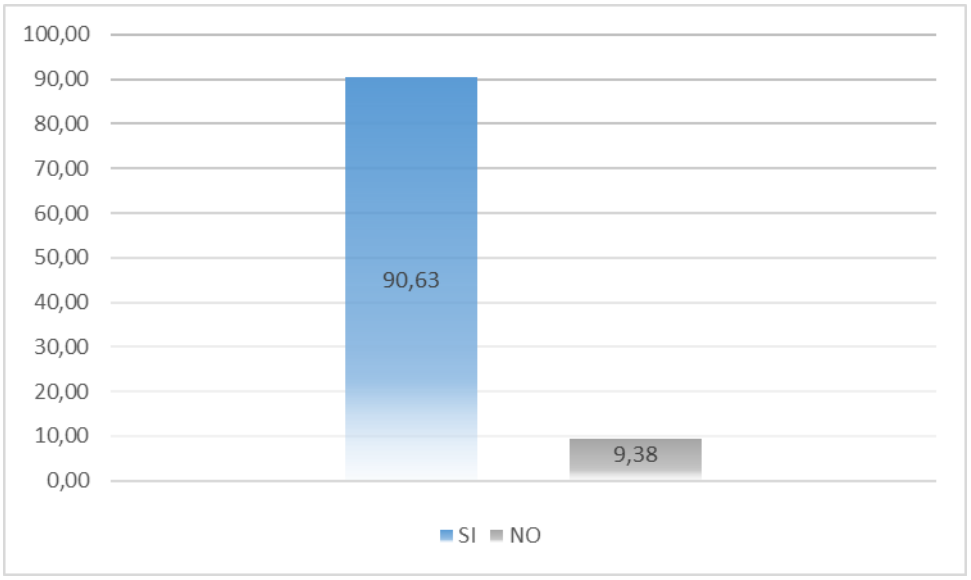
Conocimientos en seguridad de la información del personal

¿El departamento cuenta con personal que tengan amplios conocimientos en seguridad de la información?		
	Frecuencia	Porcentaje
SI	29	90,63
NO	3	9,38
Total	32	100,00

Nota: Resultado del programa SPSS

Figura 26

Conocimientos en seguridad de la información del personal



Nota: Resultado del programa SPSS

Análisis e Interpretación:

En la Tabla 29 y Figura 26 se observa que el 90.63% sostiene que el departamento si cuenta con personal que tengan amplios conocimientos en seguridad de la información y el 9.38% sostiene que el departamento no cuenta con personal que tengan amplios conocimientos en seguridad de la información.

Tabla 30

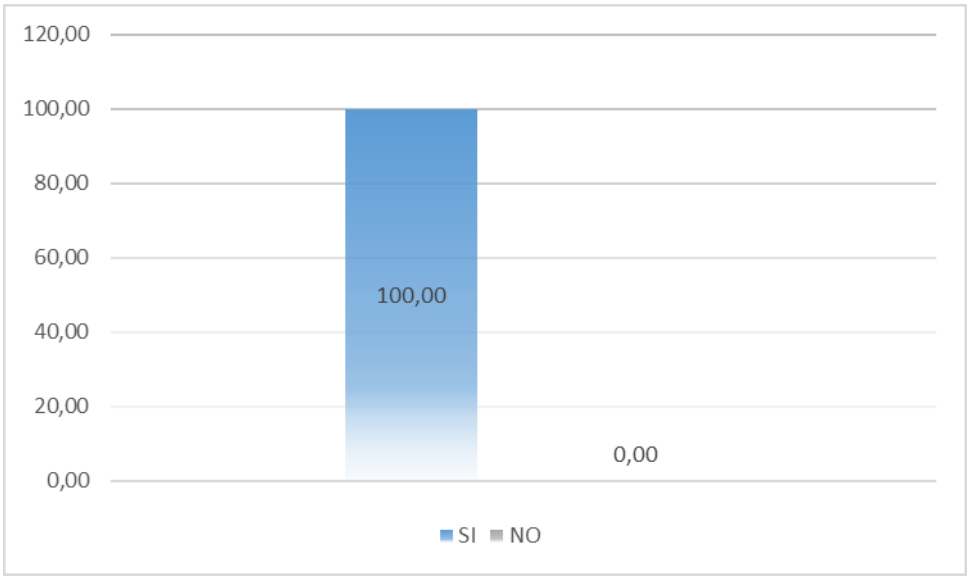
Políticas de seguridad por departamento

¿Cada departamento de la municipalidad tiene asignada políticas de seguridad?		
	Frecuencia	Porcentaje
SI	32	100,00
NO	0	0,00
Total	32	100,00

Nota: Resultado del programa SPSS

Figura 27

Políticas de seguridad por departamento



Nota: Resultado del programa SPSS

Análisis e Interpretación:

En la Tabla 30 y Figura 27 se observa que el 100% sostiene que cada departamento de la municipalidad si tiene asignada políticas de seguridad y el 0% sostiene que cada departamento de la municipalidad no tiene asignada políticas de seguridad.

Tabla 31

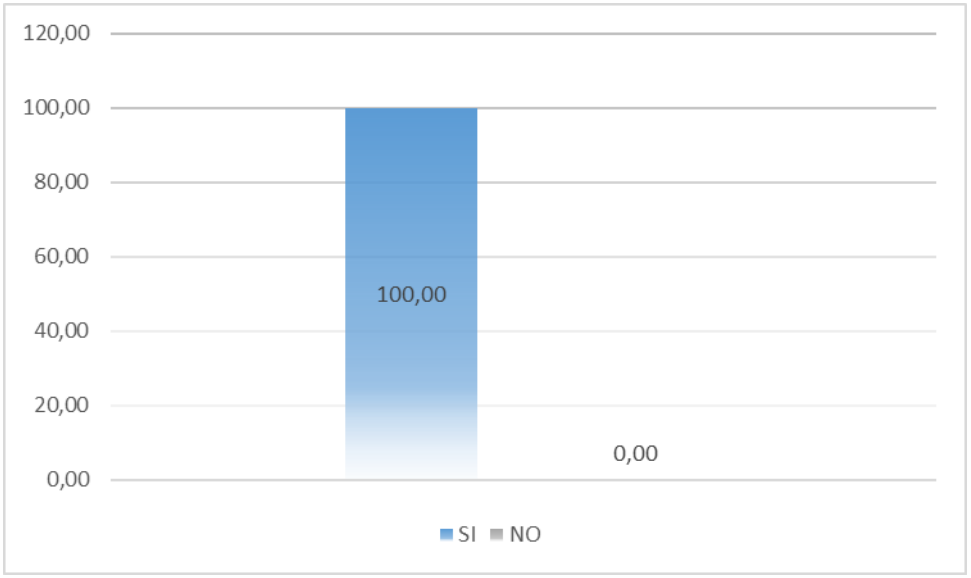
Existencia de política de confidencialidad de la información

¿Cuenta la municipalidad con algún tipo de política de confidencialidad de la información en el caso de que un empleado abandone el cargo se le supriman todos los accesos al sistema?		
	Frecuencia	Porcentaje
SI	32	100,00
NO	0	0,00
Total	32	100,00

Nota: Resultado del programa SPSS

Figura 28

Existencia de política de confidencialidad de la información



Nota: Resultado del programa SPSS

Análisis e Interpretación:

En la Tabla 31 y Figura 28 se observa que el 100% sostiene que la municipalidad si cuenta con algún tipo de política de confidencialidad de la información en el caso de que un empleado abandone el cargo se le supriman todos los accesos al sistema.

Tabla 32

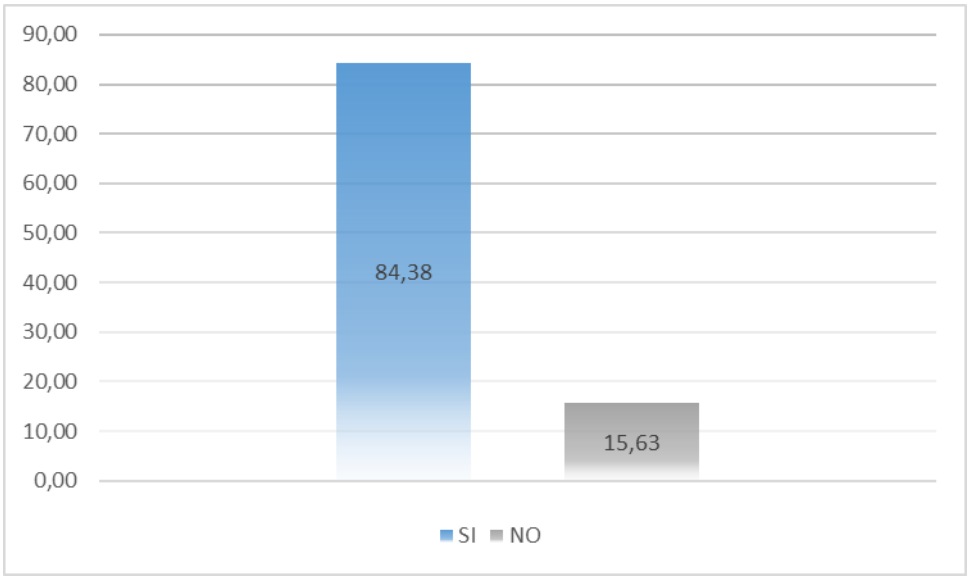
Revisión periódicamente el cableado en los departamentos de la municipalidad

¿Se revisa periódicamente el cableado en todos los departamentos de la municipalidad?		
	Frecuencia	Porcentaje
SI	27	84,38
NO	5	15,63
Total	32	100,00

Nota: Resultado del programa SPSS

Figura 29

Revisión periódicamente el cableado en los departamentos de la municipalidad



Nota: Resultado del programa SPSS

Análisis e Interpretación:

En la Tabla 32 y Figura 29 se observa que el 84.38% sostiene que si se revisa periódicamente el cableado en todos los departamentos de la municipalidad y el 15.63% sostiene que no se revisa periódicamente el cableado en todos los departamentos de la municipalidad.

Tabla 33

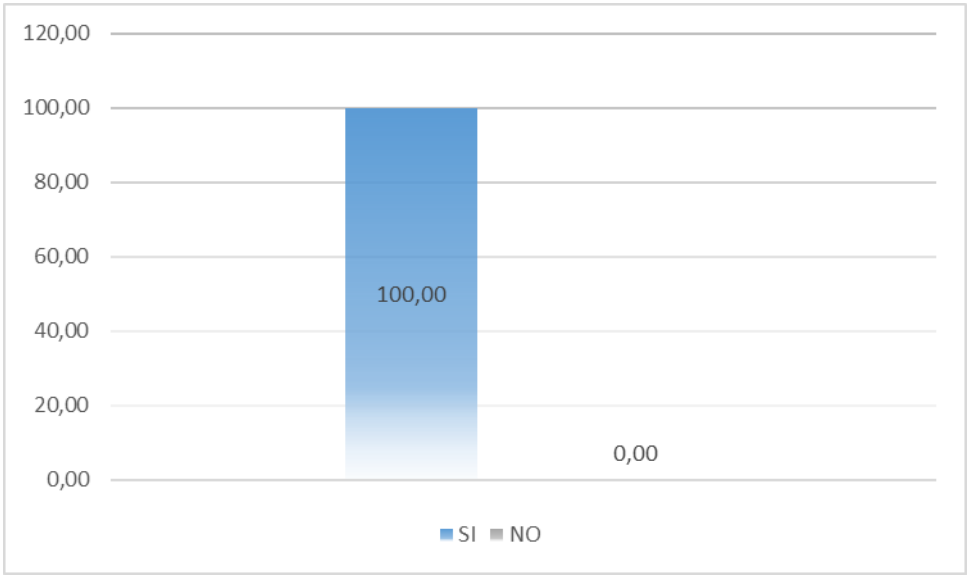
Copias de seguridad de la información

¿Se realizan copias de seguridad de la información?		
	Frecuencia	Porcentaje
SI	32	100,00
NO	0	0,00
Total	32	100,00

Nota: Resultado del programa SPSS

Figura 30

Copias de seguridad de la información



Nota: Resultado del programa SPSS

Análisis e Interpretación:

En la Tabla 33 y Figura 30 se observa que el 100% sostiene que si se realizan copias de seguridad de la información.

4.2. CONTRASTACIÓN DE HIPÓTESIS Y PRUEBA DE HIPÓTESIS

Se procedió a realizar la PRUEBA DE T DE STUDENT DE MUESTRAS RELACIONADAS para el presente trabajo de investigación haciendo uso del software estadístico SPSS (“STATISTICAL PACKAGE FOR THE SOCIAL SCIENCE”).

LA HIPÓTESIS

HIPÓTESIS GENERAL

H_g: realizar una auditoría de seguridad de la información, aplicando la Norma ISO/IEC 27001 mejorará la confiabilidad y seguridad de la información en la Municipalidad Distrital de Luyando.

H_0: realizar una auditoría de seguridad de la información, aplicando la Norma ISO/IEC 27001 no mejorará la confiabilidad y seguridad de la información en la Municipalidad Distrital de Luyando.

HIPÓTESIS ESPECIFICAS

H_1: Analizar la situación actual del manejo de la información mejorará la seguridad de la información en la Municipalidad Distrital de Luyando.

H_0: Analizar la situación actual del manejo de la información no mejorará la seguridad de la información en la Municipalidad Distrital de Luyando.

H_2: Realizar la auditoria con la norma ISO/IEC 27001 optimizará la confidencialidad y seguridad de la información en la Municipalidad Distrital de Luyando.

H_0: Realizar la auditoria con la norma ISO/IEC 27001 no optimizará la confidencialidad y seguridad de la información en la Municipalidad Distrital de Luyando

H_3: Generar un manual de políticas de seguridad para el manejo de la información optimizará el uso de los equipos en la Municipalidad Distrital de Luyando.

H_0: Generar un manual de políticas de seguridad para el manejo de la información no optimizará el uso de los equipos en la Municipalidad Distrital de Luyando.

NIVEL DE SIGNIFICANCIA

El nivel de significancia para el presente trabajo de investigación fue de 0.05

PRUEBA DE NORMALIDAD

Tabla 34

Resumen de procesamiento de casos

Resumen de procesamiento de casos

	Casos					
	Válido		Perdidos		Total	
	N	Porcentaje	N	Porcentaje	N	Porcentaje
pre_test	15	100,0%	0	0,0%	15	100,0%
post_test	15	100,0%	0	0,0%	15	100,0%

Descriptivos

			Estadístico	Error estándar
pre_test	Media		5,86	1,016
	95% de intervalo de confianza para la media	Límite inferior	3,66	
		Límite superior	8,05	
	Media recortada al 5%		5,73	
	Mediana		5,50	
	Varianza		14,440	
	Desviación estándar		3,800	
	Mínimo		1	
	Máximo		13	
	Rango		12	
	Rango intercuartil		6	
	Asimetría		,609	,597
	Curtosis		-,513	1,154
post_test	Media		10,79	,613
		Límite inferior	9,46	

95% de intervalo de confianza para la media	Límite superior	12,11	
Media recortada al 5%		10,98	
Mediana		11,50	
Varianza		5,258	
Desviación estándar		2,293	
Mínimo		5	
Máximo		13	
Rango		8	
Rango intercuartil		4	
Asimetría		-1,213	,597
Curtosis		1,712	1,154

Tabla 35

Pruebas de normalidad

Pruebas de normalidad

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
pre_test	,131	15	,200*	,934	15	,344
post_test	,202	15	,127	,856	15	,127

Muestras mayores > 30 Kolmogorov-Smirnov[a]

Muestras menores < 30 Shapiro-Wilk

Como la muestra es de 15 se tomara en cuenta la prueba de normalidad de Shapiro-Wilk

Criterios para determinar normalidad

P-valor => nivel de significancia: los datos provienen de una distribución normal

P-valor < nivel de significancia: los datos no provienen de una distribución normal

P-valor(pre_test) = 0.344

P-valor(post_test) = 0.127

Nivel de significancia = 0.05

Conclusión: los datos provienen de una distribución normal

PRUEBA DE T DE STUDENT DE MUESTRAS RELACIONADAS

Tabla 36

Estadísticas de muestras emparejadas

Estadísticas de muestras emparejadas

		Media	N	Desviación estándar	Media de error estándar
Par 1	pre_test	5,84	15	3,800	1,016
	post_test	10,77	15	2,293	,613

Correlaciones de muestras emparejadas

		N	Correlación	Sig.
Par 1	pre_test & post_test	15	,676	,008

Tabla 37

Prueba de muestras emparejadas

Prueba de muestras emparejadas

		Diferencias emparejadas					t	gl	Sig. (bilateral)
		Media	Desviación estándar	Media de error estándar	95% de intervalo de confianza de la diferencia Inferior	Superior			
Par 1	pre_test - post_test	-4,929	2,814	,752	-6,553	-3,304	-6,554	15	,000

CONCLUSION: ya que la sigma bilateral es 0.000, y es menor al Nivel de significancia 0.05. Entonces existe una diferencia significativa en las medias de pre_test y post_test

CONCLUSIONES ESTADÍSTICAS

Comprobando las muestras estadísticas se puede observar que la media del pre_test asume un valor de 5.84 y la media del post_test asume un valor de 10.77, entonces es evidente como después del proceso del presente trabajo de investigación la media entre ambos test adquiere una diferencia considerable.

Asimismo, en la prueba de muestras emparejadas la significancia es de 0.000 y es menor al nivel de significancia establecido.

Por lo tanto, se acepta las hipótesis de la investigación.

HIPÓTESIS GENERAL

H_g: realizar una auditoría de seguridad de la información, aplicando la Norma ISO/IEC 27001 mejorará la confiabilidad y seguridad de la información en la Municipalidad Distrital de Luyando.

HIPÓTESIS ESPECIFICAS

H_1: Analizar la situación actual del manejo de la información mejorará la seguridad de la información en la Municipalidad Distrital de Luyando.

H_2: Realizar la auditoria con la norma ISO/IEC 27001 optimizará la confidencialidad y seguridad de la información en la Municipalidad Distrital de Luyando.

H_3: Generar un manual de políticas de seguridad para el manejo de la información optimizará el uso de los equipos en la Municipalidad Distrital de Luyando.

PRESENTACIÓN DE RESULTADOS

RIESGOS OBTENIDOS

Según los resultados obtenidos en las encuestas, y en las visitas se observa que la Municipalidad Distrital de Luyando cuenta con políticas de seguridad básicas que no permiten el correcto aseguramiento de la información; razón por la cual es recomendable utilizar una normativa estricta y confiable que garantice la confidencialidad y seguridad de la información. Entre los riegos detectados se citan:

Los trabajadores de la institución desconocen a medias las políticas de seguridad, por lo que son propensos a la manipulación inadecuada de la información personal e institucional, debido a ello se debería realizar periódicamente la socialización de las políticas vigentes.

Durante el registro de nuevos usuarios y cambios de contraseña, los sistemas no requieren la utilización de caracteres especiales, letras y números; por este motivo el personal de la institución crea contraseñas simples, dando paso a que personal no autorizado y malintencionado pueda acceder a usuarios ajenos y realizar cambios no deseados en los sistemas.

Las instalaciones físicas no cuentan con las seguridades respectivas que brinden el aseguramiento de los recursos existentes en la Municipalidad Distrital de Luyando.

POLÍTICAS DE SEGURIDAD EXISTENTES DENTRO DE LA INSTITUCIÓN

- **Restricciones de usuarios**

Los trabajadores de los diferentes departamentos tienen restringido el acceso para instalación de programas innecesarios para el desempeño de sus actividades, y en caso de requerirlos el técnico de sistemas es quien ejecuta la instalación en el usuario de soporte mediante el ingreso de usuario y contraseña y una vez validado el acceso continúa con la instalación correspondiente.

- **Gestión de Contraseñas**

No se cuenta con un manual para el manejo adecuado de contraseñas en los sistema y equipos que permitan salvaguardar la información.

Las contraseñas no son modificadas periódicamente ya que no poseen una guía que indique el tiempo de vida útil de las mismas, y lo hacen en el momento que cada trabajador lo crea conveniente y con contraseñas de su elección sin tomar en cuenta las restricciones necesarias.

- **Copias de seguridad**

En cuanto a las copias de seguridad dentro de la municipalidad son llevadas a cabo de manera mensual, pero esto depende de cada sistema ya que al trabajar con software diseñados por diferentes personas y en diferentes plataformas no hay forma de unificar una sola copia de seguridad y en muchos de los casos se encuentran sistemas sin formas de realizar copias de seguridad.

- **Políticas, Normas y Estándares**

Para determinar las normas, estándares y políticas de seguridad existentes en la municipalidad, se realizaron entrevistas, encuestas, visitas al personal responsable de los departamentos de la institución, obteniendo la información siguiente:

- **Políticas de Seguridad**

La municipalidad carece de un manual con políticas de seguridad en caso de inconvenientes con los recursos informáticos, es por ello que el técnico a cargo decide la solución óptima sobre el activo, por ejemplo, cuando un equipo presenta un fallo el trabajador a cargo informa sobre el particular al técnico, quien acude al lugar donde fue solicitado y verifica que tipo de problema posee el equipo y lo repara, de no existir solución el equipo es reemplazado.

- **Problemas en el Sistema**

Cuando existe un problema en los sistemas y no pueden ser solucionado, el técnico encargado es notificados mediante una llamada telefónica para que éste dé solución en el momento que se detecta el fallo, procediendo con la suspensión del sistema para que no exista pérdida de información, en caso de que no se haya guardado o modificado algún dato, este se almacena en una tabla de respaldo y mediante la búsqueda conjuntamente con el trabajador que realizo esta actividad es restablecido al sistema.

- **Problemas en los equipos**

Los equipos con problemas correctivos el técnico encargado es notificados mediante una llamada telefónica para su reparación.

- **Gestión de Activos**

- **Activos Institucionales**

La municipalidad no cuenta con un inventario de activos confiable ya que cada departamento maneja un inventario empírico y nada detallado.

- **Seguridad del Personal**

  - **Confidencialidad en el manejo de información**

    La información manejada en los diferentes departamentos de la municipalidad es reservada y confidencial no puede ser divulgada. Para manejo de información entre departamentos se utiliza el correo institucional generado para cada funcionario a fin de evitar el uso de unidades de almacenamiento externas.

  - **Cumplimiento de reglamentos y actividades de funcionarios**

    Dentro de la municipalidad los funcionarios cumplen con los reglamentos establecidos, de acuerdo al perfil de cada trabajador tienen asignadas actividades a las cuales debe dar cumplimiento para justificar su jornada laboral.

  - **Utilización de correo institucional**

    Los funcionarios tienen un correo institucional el cual es utilizado para asignación de actividades, consultas entre los diferentes departamentos, videoconferencias, envío y recepción de documentación en el ámbito laboral.

  - **Recursos compartidos**

    Dentro de la municipalidad no se comparte recursos como computadoras, correos institucionales entre otros, a cada funcionario se le asigna su equipo y cuenta de correo desempeño de sus actividades.

  - **Uso de firmas electrónicas**

    El uso de firma electrónicas no está implementado en la municipalidad.

  - **Seguridad para soporte de la información**

    En la municipalidad existen cámaras de seguridad en algunas áreas, y el respectivo personal de seguridad.

- **Seguridad Física**

  - **Almacenamiento de información**

    En la municipalidad se manejar diferentes sistemas desarrollados como resultado de alguna necesidad de alguna área en específico, dichos sistemas no están interconectadas.

  - **Factores ambientales**

    En cada departamento de la municipalidad existe un extintor.

  - **Uso de UPS**

    La municipalidad no hace uso de ups como dispositivos de seguridad ante fallas eléctricas.

  - **Desastres naturales**

    La municipalidad está expuesta a catástrofes naturales como terremotos, inundaciones, incendios, entre otros; sin embargo, no se han realizado capacitaciones a nivel municipal en caso de ocurrir alguna de estas eventualidades.

  - **Utilización de antivirus en la Municipalidad**

    La institución utiliza el antivirus Nod32 como una de las medidas de seguridad de los equipos.

  - **Señalética**

    En la municipalidad existen señaléticas de peligro, prohibiciones, números de emergencias, señales para respetar el distanciamiento social y normas de bioseguridad.

  - **Instalaciones eléctricas**

    Las instalaciones eléctricas se revisan periódicamente para que no existan daños en el cableado.

- **Ingreso y salida del personal**

  El personal municipal debe registrar los ingresos y salidas (total 4) a la institución usando un lector de huella del iris del ojo instalado en la entrada de la institución.

ESTRATEGIA DE SOLUCIÓN TENIENDO EN CONSIDERACIÓN LA NORMATIVA ISO/IEC 27001

Después de haber realizado una auditoría de seguridad de la información, aplicando la Norma ISO/IEC 27001 de las vulnerabilidades y riesgos existentes dentro de la municipalidad se pudo determinar que no se cumplen con las respectivas medidas de seguridad, por ende, se adopta por implementar las siguientes medidas que ayuden mejorar la confiabilidad y seguridad de la información en la Municipalidad Distrital de Luyando, estas son:

1. Creación del área de servidores donde vayan los equipos que permitan llevar un correcto manejo de la información.

2. Creación de una unidad de gestión de la información conformada por un jefe de unidad y un asistente que realicen la implementación y administración del área de servidores además del soporte informático necesario para cumplir con las exigencias de toda la municipalidad.

3. Implementación de políticas de seguridad de la información.

En base a las recomendaciones anteriormente mencionadas se tomaron las siguientes acciones: se creó el área de servidores con el apoyo del área de informática de la municipalidad, se creó la unidad de gestión de la información con personal del área de informática que fue asignada para dichas funciones y se establecieron las nuevas políticas de seguridad de la información las cuales están detalladas a continuación:

POLÍTICAS DE SEGURIDAD DE SEGURIDAD DE LA INFORMACIÓN EN LA MUNICIPALIDAD DISTRITAL DE LUYANDO

1. Objetivos

- Mitigar riesgos existentes y resguardo de información en la Municipalidad Distrital de Luyando.
- Mejorar el ambiente laboral de los funcionarios de la municipalidad.
- Ampliar la confiabilidad de los recursos institucionales.

2. Control de Acceso a la Información

➢ **Responsabilidad del jefe de la unidad de gestión de la información**

- El jefe de la unidad es el responsable de informar, evaluar, establecer y promover mediante comunicados, socializaciones, capacitaciones, correos institucionales, redes sociales o por otros medios cada uno de los procedimientos de seguridad existentes. Además, es quien asigna responsabilidades al técnico de seguridad informática para que oportunamente realice las revisiones correspondientes, a fin de comprobar que se esté dando fiel cumplimiento de las políticas establecidas.

➢ **Privilegios asignados a usuarios**

- A los funcionarios municipales que tienen acceso a algún sistema, se les otorgarán los permisos únicamente para la ejecución de funciones conforme el cargo desempeñado.
- El personal de la municipalidad es responsable de las acciones que se hayan desarrollado dentro de cada usuario.
- Los funcionarios deben respetar el uso adecuado de su usuario, por ningún motivo debe utilizar la cuenta de otro empleado, así fuere el caso que éste lo hubiera autorizado.

- Los funcionarios están en la obligación de informar al jefe de su departamento, cualquier suceso que se haya detectado e interfiera con la confiabilidad de los datos con los que se encuentre trabajando, éste a su vez debe comunicar a la unidad de gestión de la información, para que realice las respectivas verificaciones y se dé solución al problema generado.

➢ **Asignación de cuentas**

- Cuando a los funcionarios se les asigna una cuenta de usuario deben firmar un documento en el que indique que conocen las políticas de seguridad.

- Para solicitar la asignación de una cuenta o modificación del cargo se debe hacer la petición por escrito a la unidad de gestión de la información misma que aprobará el requerimiento.

- No se debe crear usuarios para personal que no pertenezca a la municipalidad salvo el caso que cuenten con la autorización debidamente aprobada por la unidad de gestión de la información.

- Se debe llevar un estricto control de los privilegios de usuario de los funcionarios municipales para que no puedan acceder a modificaciones o eliminaciones personales si no están autorizados a realizar estas actividades.

- Se restringe la creación de usuarios que no especifiquen claramente quien es el responsable para evitar el mal uso de estos recursos.

- Las cuentas de usuarios que no se estén siendo utilizadas por un lapso 3 meses, deben ser suspendidas automáticamente en los sistemas.

- Cuando los funcionarios municipales cesen de sus funciones, se debe informar a la unidad de gestión de la información para que el técnico encargado suspenda la cuenta de inmediato.

- **Manejo de contraseñas**

  - Las contraseñas de los sistemas deben ser almacenadas en un gestor de contraseñas por contener información delicada.

  - Los funcionarios por ningún deben almacenar contraseñas en ningún tipo de archivo que sea guardado en USB u otros dispositivos, además no deben ser escritas en papeles que se hallen a la vista de terceros.

  - Se debe restringir el uso de contraseñas antiguas y evitar la utilización de contraseñas similares a las que ya hayan sido manejadas.

  - Cuando se crea el usuario respectivo, la contraseña para el primer ingreso será asignada por el técnico creador y luego de ello deberá ser modificada por la que el usuario crea conveniente respetando las sugerencias para la generación de la misma.

  - El número de intentos máximos consecutivos para el ingreso a los sistemas introduciendo una contraseña incorrecta es tres, y el usuario quedara bloqueado.

  - No se permitirá a los funcionarios la vulneración de los sistemas, y de ocurrir, esta se considerará como infracción leve o grave dependiendo de la contravención.

  - Es necesario que la longitud mínima de una contraseña sea de 8 caracteres, mismos que debe contener alternadamente la combinación entre números, letras mayúsculas, minúsculas y caracteres especiales.

  - En los servidores se recomienda la utilización de contraseñas largas y robustas, con una longitud mínima de 12 caracteres, siempre utilizando las combinaciones de caracteres numéricos y alfanuméricos.

  - Por ningún motivo se debe revelar el usuario y contraseña personal o permitir que se encuentre a la vista o alcance terceros.

  - Si por algún motivo los funcionarios sospechan que sus credenciales

de ingreso están siendo utilizadas por alguien, se debe realizar el cambio correspondiente y dar aviso al encargado de la unidad de gestión de la información.

- Las contraseñas no deben contener datos como nombre, fechas de nacimiento, números telefónicos, celulares o algún dato que pueda ser fácil de investigar.

- Cuando un funcionario pierda el acceso al equipo o sistema asignado deberá notificar a la unidad de gestión de la información para restablecimiento correspondiente.

- Los funcionarios por ningún motivo deben utilizar la misma contraseña de las cuentas personales para el manejo de equipos o sistemas dentro de la municipalidad.

➢ **Acceso a la información**

- Es necesario que la información sea protegida, para ello es recomendable que se utilicen algoritmos de cifrado para que personal no autorizado carezca de acceso a datos reservados.

- La información que es compartida mediante la red, debe estar protegida para contrarrestar el uso inadecuado de dicho recurso.

- El uso de dispositivos móviles no debe interferir en el desempeño laboral de cada uno de los funcionarios, tampoco se podrá acceder a la red sin la autorización de la unidad de gestión de la información, salvo que se realicen las justificaciones pertinentes.

- El manejo de información es delicado, es por ello que cuando se aplique la modalidad de teletrabajo, los entregables deberán ser remitidos a los jefes departamentales y ellos a su vez son los responsables de presentar los reportes de trabajo al departamento de personal.

- Se debe realizar monitorios contantes en la red de la municipalidad

para encontrar vulnerabilidades que puedan provocar la fuga de información.

- **Uso de correo institucional y sistemas municipales**

  - Los funcionarios están en la obligación de brindar la seguridad en el manejo de cuentas institucionales que estén a su cargo.

  - Los funcionarios deben ser cautelosos con la gestión de cuentas institucionales, y sistemas porque son los responsables de cualquier manejo inadecuado que se dé dentro de ellos.

  - Los funcionarios que no den el correcto uso a los sistemas existentes en la municipalidad deben ser sancionados siguiendo el procedimiento administrativo respectivo.

- **Gestión de privilegios en equipos**

  - La unidad de gestión de la información debe establecer usuarios en cada uno de los equipos asignados al personal, permitiendo única y exclusivamente el uso de los recursos que son necesarios para el desempeño de sus funciones.

  - Por ningún motivo los empleados que no pertenezcan al área de unidad de gestión de la información podrán tener acceso al usuario administrador.

  - Los empleados que requieran la instalación de aplicaciones extras deberán solicitar a la unidad de gestión de la información la ejecución de dicha acción.

- **Restricciones a personal externo**

  - Al personal que no trabaje en la municipalidad se restringe el uso de equipos informáticos y sistemas de carácter institucional.

- **Uso del internet**

  - Los empleados de la municipalidad no están autorizados a utilizar internet para actividades que no estén acorde con sus funciones.

  - Los empleados de la municipalidad que justifiquen el uso de internet podrán tener acceso al mismo, pero se les restringe el acceso a redes sociales o plataformas de entretenimiento que puedan interferir en el desempeño laboral. El requerimiento será mediante un informe detallado de las tareas para las cuales es indispensable su uso, el mismo que ira dirigido al jefe de la unidad de gestión de la información para su aprobación o negación luego de la evaluación correspondiente.

  - Realizar charlas para incentivar a los funcionarios a la concientización del uso inadecuado del recurso de internet y los peligros que conlleva la navegación por páginas de dudosa procedencia.

  - Incentivar a los funcionarios al no uso de la red para compartir información delicada con el propósito de mitigar las fugas de información.

  - Para la recepción o envío de información laboral los funcionaros deben hacer uso de las cuentas institucionales.

3. Responsabilidades del Personal

➢ Acceso del personal a la unidad de gestión de la información

- Se debe llevar un registro de ingreso del personal que no sea parte de la unidad.
- Restringir el acceso de personal no autorizado al área de servidores para evitar daños o pérdidas en los equipos.
- El personal de la unidad de gestión de la información es el único autorizado al ingreso en el cuarto de servidores para validar el buen funcionamiento de los mismos; no obstante, en caso de requerir personal externo este deberá ser acreditado por el jefe de la unidad.
- Es indispensable que el cuarto de servidores cuente con las seguridades de ingreso pertinentes.

➢ Informes de debilidades a nivel de seguridad

- Los funcionarios deben informar oportunamente los problemas relacionados con la seguridad de los equipos y la periodicidad de la ocurrencia para que la unidad de gestión de la información tome las medidas necesarias.
- Los técnicos de la unidad de gestión de la información deberán notificar al jefe inmediato la existencia de vulnerabilidades en el sistema.
- Los funcionarios deben saber que en caso de encontrar una vulnerabilidad y tratar de utilizarla para su beneficio están cometiendo una infracción por manejo inadecuado de los recursos institucionales.
- La unidad de gestión de la información es la responsable de instalar y desinstalar programas necesarios para las labores del personal.

➢ Normas de confidencialidad

- Los funcionarios por ningún motivo deberán divulgar información

reservada de la institución ni revelar sus credenciales de usuario.

- **Administración de sistemas dentro de la municipalidad**

  - La unidad de gestión de la información es la encargada de velar por el correcto funcionamiento de los sistemas y del mantenimiento oportuno del software.

  - Ejecutar controles periódicos que permitan evaluar el nivel del servicio brindado por parte del personal de la unidad de gestión de la información dentro de la municipalidad.

  - Actualizar oportunamente el inventario de los sistemas que forman parte de los activos institucionales.

4. Restricciones de Instalación

- **Instalación de protección antivirus**

  - Todas las computadoras y servidores de la municipalidad deberán contar con una protección antivirus con sus actualizaciones y configuraciones correspondientes.

  - Siempre que se instale software en los equipos la unidad de gestión de la información deberá verificar su procedencia para evitar riesgos a nivel de seguridad.

- **Copias de seguridad**

  - Los técnicos de la unidad de gestión de la información deben realizar copias de seguridad semanalmente, o cuando existan modificaciones en los ficheros para que en caso de ocurrir alguna eventualidad los datos puedan ser recuperados.

  - Cuando existe pérdida de información la unidad de gestión de la información se debe indagar hasta dar con la causa y documentar lo suscitado.

- El jefe de la unidad de gestión de la información es quien determina las medidas que se debe seguir con el almacenamiento de la información cuando un servidor no está funcionando correctamente.

Como resultado de las acciones adoptadas se cumplió con los objetivos de la presente investigación pues se mejoró la confidencialidad y seguridad de la información además de mejorar el uso de los equipos en la Municipalidad Distrital de Luyando.

CAPÍTULO V

DISCUSIÓN DE RESULTADOS

5.1. CONTRASTACIÓN DE LOS RESULTADOS DEL TRABAJO DE INVESTIGACIÓN

Santos (2020), afirma hoy en día, poder proteger adecuadamente los activos de información se ha convertido en un factor clave en el ámbito de la ciberseguridad. La aparición de conceptos como el Internet de las Cosas, los sistemas, las ciudades inteligentes o la llamada cuarta revolución industrial ha supuesto la transformación de sociedades analógicas tradicionales en sociedades digitales y plenamente conectadas. Este cambio tiene grandes beneficios para todos los participantes (gobiernos, empresas, ciudadanos), pero también trae consigo nuevos riesgos con enormes impactos.

Ante lo antes mencionado la Municipalidad Distrital de Luyando debe adecuarse a los tiempos actuales y venideros donde la información va a necesitar definir las normas de seguridad para un activo muy importante la cual es la información.

De igual forma Vásquez y Delgado (2019), Las Normas ISO no sólo son herramientas al alcance de las grandes empresas, sino que también las medianas o pequeñas empresas pueden conseguir los beneficios que se derivan de su implantación y su mantenimiento. La obtención de la información se consideró conveniente el uso de las técnicas de recolección de datos tales como las encuestas, para su posterior Análisis e Interpretación; y de esta manera medir la realidad problemática apoyado en el uso de la Norma ISO 27001, lográndose identificar las deficiencias para mejorar los niveles de seguridad y confiabilidad en los sistemas de información.

De igual manera la presente investigación realizó la recolección de datos en base a las reuniones y encuesta realizada a los trabajadores de la Municipalidad Distrital de Luyando, finalmente se diseñó una estrategia de solución teniendo en consideración la normativa ISO/IEC 27001.

Lucano (2019), encontró que en el banco el 33% del personal desconocía de la existencia de políticas en seguridad de la información, lo que contrasta con el 84.38% del personal que desconoce la existencia de políticas en seguridad de la información en la Municipalidad Distrital de Luyando al inicio de la investigación. Esto se pudo mejorar luego de la ejecución de la investigación ya que al finalizar el 96.88% del personal de la Municipalidad Distrital de Luyando conocía la existencia de las políticas de seguridad de la información.

Castro (2018), encontró que al finalizar su investigación el 98.9% del personal usa contraseñas seguras que contienen letras números y caracteres especiales, del mismo modo al finalizar la presente investigación el 96.8% del personal de la Municipalidad Distrital de Luyando usa contraseñas seguras que contienen letras números y caracteres especiales.

Ante lo mencionado anteriormente, es claro que la hipótesis de la investigación se confirma:

> H_g: realizar una auditoría de seguridad de la información, aplicando la Norma ISO/IEC 27001 mejorará la confiabilidad y seguridad de la información en la Municipalidad Distrital de Luyando.

CONCLUSIONES

1. En la Municipalidad Distrital de Luyando no existe un manual de acciones que se deban tomar en caso de ocurrir dificultades en el manejo de la información; motivo por el cual, el técnico encargado de los equipos es quien decide qué acciones y medidas tomar en estos casos.

2. Las instalaciones del cuarto de servidores son reducidas por cuanto no existen las adecuaciones necesarias para su correcto funcionamiento estando en riesgo los equipos de esta unidad.

3. Se evidenció gran parte de los funcionarios no cierran la sesión de usuario de los sistemas utilizados, quedando expuestos a que otro empleado realice modificaciones que afecten a la información de la institución.

4. Se corroboró que no se aplican los controles necesarios en cuanto al manejo y gestión de contraseñas por parte de los funcionarios municipales.

RECOMENDACIONES

1. La unidad de gestión de la información deberá establecer las políticas de seguridad en la municipalidad y sobre todo difundirlas con la finalidad de instaurar hábitos y lo que es más importante buenas prácticas en el manejo y gestión de la información.

2. Es indispensable que en la unidad de gestión de la información exista un técnico este netamente encargado del área de seguridad que realice el monitoreo constante y periódico de los procesos y normativas a seguir en caso de vulneración de la información.

3. Es indispensable que se apliquen controles que brinden seguridad a los sistemas para el uso adecuado de contraseñas puesto que los empleados utilizan contraseñas débiles ocasionando un riesgo inminente, además se debe notificar a los funcionarios que no almacenen su contraseña en lugares inseguros.

4. Se debe capacitar constantemente a los funcionarios respecto a las medidas de seguridad a tomar en cuanto al manejo de la información para garantizar su seguridad y confidencialidad.

REFERENCIAS BIBLIOGRÁFICAS

Ávila, R. (2001), *Metodología de la investigación. Como elaborar la tesis y/o investigación*. Edit. Estudios y Ediciones R.A. Lima - Perú.

Cano, J., (2004), *Inseguridad Informática: Un concepto dual ·en seguridad informática*, https:/ /ojsrevistaing.uniandes.edu.co/ojs/index.php/revista/article/download/437/640+ &cd=1&hl=es&ct=clnk&gl=ec.

Fernández, D., (2019), *Fases de un Ataque Informático*, https://recordandoeinnovando.wordpress.com/2014/07/29/las-5-fases-o-etapas-de-un-ataque-informatico/.

Fiallo, J., Cerezal, J. & Hedesa, Y., (2008), *La investigación Pedagógica una vía para elevar la calidad educativa*. Edit. Taller Gráficos San Remo. Lima- Perú.

Gallardo, E. E. (2017). *Metodología de la Investigación: manual auto formativo interactivo. Universidad Continental*. https://repositorio.continental.edu.pe/bitstream/20.500.12394/4278/1/DO_UC_EG_MAI_UC0584_2018.pdf

Hernández, R., Fernández, C. & Baptista, M., *Metodología de la investigación*, https://www.uca.ac.cr/wp-content/uploads/2017/10/Investigacion.pdf

Mazzinghi. (2011), *Gestión del riesgo en la seguridad informática: el nuevo escenario del control*, http://webcache.googleusercontent.com/search?q=cache:s_BoACRkLP8J:www. cidemconsult.cl/biblioteca/doc/40/raw+&cd=13&hl=es-419&ct=clnk&gl=ec

Mesquid, A., Mas, A. y Amengual, E., *Sistema de Gestión Integrado según las normas ISO 9001, ISO/IEC 20000 e ISO/IEC 27001. REICIS*. Revista Española de Innovación, Calidad e Ingeniería del Software, http://www.redalyc.org/articulo.oa?id=92218768002

Naranjo, j. y Reyes, J., (2017), *Auditoría informática dirigida al Centro de Cómputo de la Carrera de Ingeniería en Sistemas Computacionales de la Universidad de Guayaquil con base en las Normas ISO 27001 y 27002*, http://repositorio.ug.edu.ec/handle/redug/

Núñez, F., (2018), *SiRetrieved*, https://s3.amazonaws.com/academia.edu.documents/36974512/NOV_DOC_Tabla_AEN_22994_1.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1550719525&Signature=7ujHvX3FWis91JQg3%2F2wNr7IkFA%3D&response-content-disposition=inline%3B%20filename%3DNOV_DOC_Tabla_AEN_22994_1.pdf

Ponce, L., (2020), *Estudio de una auditoría en seguridad informática aplicando la Norma Internacional de calidad total ISO 27001 para la Empresa Maint de la ciudad de Guayaquil*, http://repositorio.ug.edu.ec/handle/redug/6978

Sánchez, R y Reyes, J., (2006). *Metodología y diseños en investigación científica*. Edit. Visión Universitaria. Lima – Perú.

Sánchez, R., (2015). *t-Student. Usos y abusos*. https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0188-21982015000100009

Software ISO, ISO 27001 - Software ISO 27001 de Sistemas de Gestión, https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001

COMO CITAR ESTE TRABAJO DE INVESTIGACIÓN

Evaristo Cipriano, A. (2024). *Auditoría de seguridad de la información aplicando la norma ISO/IEC 27001 en la Municipalidad Distrital de Luyando* [Tesis de pregrado, Universidad de Huánuco]. Repositorio Institucional UDH. http://...

ANEXOS

ANEXO 1

CUESTIONARIO DE ENCUESTA

1. ¿En la municipalidad se cuenta con políticas de seguridad para la gestión de información?

Si ( ) No ( )

Cuales

---

2. ¿El personal de la municipalidad tiene conocimientos de las políticas de seguridad existentes?

Si ( ) No ( )

3. ¿Cada empleado tiene responsabilidades asignadas del uso de los recursos de la municipalidad?

Si ( ) No ( )

4. ¿Se lleva un control adecuado del acceso del personal para que personas no autorizadas no puedan acceder a los equipos y sistema de la municipalidad?

Si ( ) No ( )

5. ¿Se tiene establecido los debidos controles de usuarios con las debidas restricciones de acuerdo al perfil de cada uno?

Si ( ) No ( )

6. ¿los sistemas al momento de ingresar una contraseña solicita que esta tenga letras números y caracteres especiales?

Si ( ) No ( )

7. ¿Se lleva a cabo periódicamente el mantenimiento correctivo y preventivo de los equipos de la municipalidad?

Si ( ) No ( )

Indique cada cuanto tiempo

a) 2 meses

b) 3 meses

c) 6 meses

d) cada ano

8. ¿Qué hace el departamento de Tecnología de la información cuando el sistema tiene algún fallo?

---

9. Se realizan monitoreo constantemente a los sistemas para evitar cualquier eventualidad.

Si ( ) No ( )

10. Cuentan con un sistema de inventario de recursos informáticos de la institución

Si ( ) No ( )

11. ¿El departamento cuenta con personal que tengan amplios conocimientos en seguridad de la información?

Si ( ) No ( )

12. ¿Cada departamento de la municipalidad tiene asignada políticas de seguridad?

Si ( ) No ( )

13. ¿Cuenta la municipalidad con algún tipo de política de confidencialidad de la información en el caso de que un empleado abandone el cargo se le supriman todos los accesos al sistema?

Si ( ) No ( )

14. ¿Se revisa periódicamente el cableado en todos los departamentos de la municipalidad?

Si ( ) No ( )
15. ¿Se realizan copias de seguridad de la información?

Si ( ) No ( )

Cada cuanto tiempo

ANEXO 2

MATRIZ DE CONSISTENCIA

AUDITORÍA DE SEGURIDAD DE LA INFORMACIÓN APLICANDO LA NORMA ISO/IEC 27001 EN LA MUNICIPALIDAD DISTRITAL DE LUYANDO.

PROBLEMA	OBJETIVO	HIPÓTESIS	VARIABLE	METODOLOGÍA
¿De qué manera realizar una auditoría de seguridad de la información, aplicando la Norma ISO/IEC 27001 mejorará la confiabilidad y seguridad de la información en la Municipalidad Distrital de Luyando?	**Objetivo General** Determinar la mejorar en la confiabilidad y seguridad de la información en la Municipalidad Distrital de Luyando al realizar una auditoría de seguridad de la información, aplicando la Norma ISO/IEC 27001. **Objetivos Específicos**. Mejorar la seguridad de la información en la Municipalidad Distrital de Luyando. Optimizar la confidencialidad y seguridad de la información en la Municipalidad Distrital de Luyando Optimizar el uso de los equipos en la Municipalidad Distrital de Luyando .	**HIPÓTESIS GENERAL** **Hg:** La implementación de la norma ISO/IEC 27001 mejorará la confiabilidad y seguridad de la información en la Municipalidad Distrital de Luyando. **H0:** La implementación de la norma ISO/IEC 27001 no mejorará la confiabilidad y seguridad de la información en la Municipalidad Distrital de Luyando. **HIPÓTESIS ESPECIFICAS** **H1:** Analizar la situación actual del manejo de la información mejorará la seguridad de la información en la Municipalidad Distrital de Luyando. **H0:** Analizar la situación actual del manejo de la información no mejorará la seguridad de la información en la Municipalidad Distrital de Luyando. **H2:** Realizar la auditoria con la norma ISO/IEC 27001 optimizará la confidencialidad y seguridad de la información en la Municipalidad Distrital de Luyando. **H0:** Realizar la auditoria con la norma ISO/IEC 27001 no optimizará la confidencialidad y seguridad de la información en la Municipalidad Distrital de Luyando **H3:** Generar un manual de políticas de seguridad para el manejo de la información optimizará el uso de los equipos en la Municipalidad Distrital de Luyando. **H0**: Generar un manual de políticas de seguridad para el manejo de la información no optimizará el uso de los equipos en la Municipalidad Distrital de Luyando.	**Variables Independientes** Auditoría de seguridad de la información aplicando la norma ISO/IEC 27001 **Variable Dependiente** Seguridad de la información en la Municipalidad Distrital de Luyando	**Enfoque** enfoque cuantitativo. **Alcance o Nivel** investigación explicativa. **Diseño** Pre experimental de “pre test” y “post test” **G O1 X O2** *Dónde:* **G** = Grupo de investigación (Los 32 funcionarios de la municipalidad) **X** = Aplicación (Aplicación de la norma ISO/IEC 27001) **O1** = Pre Observación **O2** = Post Observación

UNIVERSIDAD DE HUANUCO
Facultad de Ingeniería

P. A. DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

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

En la ciudad de Huánuco, siendo las 17:00 horas del día viernes 08 del mes de marzo de año 2024, se lleva a cabo la sustentación presencial en cumplimiento de lo señalado en el Reglamento de Grados y Títulos de la Universidad de Huánuco, quienes se reunieron los **Jurados Calificadores** integrado por los Docentes:

- Mg. Omar Iván Sulca Correa — PRESIDENTE.
- Mg. Carlos Enrique Suarez Paucar — SECRETARIO.
- Mg. German Lenin Espinoza Inocente — VOCAL.

Nombrados mediante la Resolución N° 0471-2024-D-FI-UDH para evaluar la Tesis intitulada: **"AUDITORÍA DE SEGURIDAD DE LA INFORMACIÓN APLICANDO LA NORMA ISO/IEC 27001 EN LA MUNICIPALIDAD DISTRITAL DE LUYANDO"** Presentado por el (la) **Bach: EVARISTO CIPRIANO, ALBERT ELVIS,** para optar el Título Profesional de Ingeniero(a) de Sistemas e Informática.

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

Habiendo absuelto las objeciones que le fueron formuladas por los miembros del Jurado y de conformidad con las respectivas disposiciones reglamentarias, procedieron a deliberar y calificar, declarándolo(a) APROBADO por UNANIMIDAD con el calificativo cuantitativo de 12 y cualitativo de SUFICIENTE según el (Art. 47).

Siendo las 19:44 horas del día 08 del mes de marzo del año 2024, los miembros del Jurado Calificador firman la presente Acta en señal de conformidad.

Mg. Omar Iván Sulca Correa
ORCID: 0000-0002-6442-588X
DNI: 42230320
Presidente

Mg. Carlos Enrique Suarez Paucar
ORCID: 0000-0001-5123-2088
DNI: 41836635
Secretario

Mg. German Lenin Espinoza Inocente
ORCID: 0009-0003-0405-3345
DNI: 22530218
Vocal

CONSTANCIA DE ORIGINALIDAD

Yo, BALDEON CANCHAYA, WALTER TEOFILO, asesor del PA Ingeniería de Sistemas e Informática y designado mediante documento: RESOLUCIÓN Nº 977-2022-D-FI-UDH, del bachiller EVARISTO CIPRIANO, ALBERT ELVIS, de la investigación titulada:"**AUDITORÍA DE SEGURIDAD DE LA INFORMACIÓN APLICANDO LA NORMA ISO/IEC 27001 EN LA MUNICIPALIDAD DISTRITAL DE LUYANDO**",

Puedo constar que la misma tiene un índice de similitud del 23% verificable en el reporte final del análisis de originalidad mediante el Software Turnitin. Por lo que concluyo que cada una de las coincidencias detectadas no constituyen plagio y cumple con todas las normas de la Universidad de Huánuco.

Se expide la presente, a solicitud del interesado para los fines que estime conveniente.

Huánuco, 11 de marzo de 2024

Walter Baldeon Canchaya

DNI: 22512084

Código Orcid:0000-0002-4270-073X