UNIVERSIDAD PRIVADA DE TACNA

FACULTAD DE INGENIERÍA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

TESIS

"SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SU RELACIÓN CON LA CALIDAD DE SERVICIO DE LAS REDES LAN EN LA MUNICIPALIDAD DISTRITAL DE ILABAYA"

PARA OPTAR:

TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS

PRESENTADO POR:

Bach. GALINDO YEFER MAQUERA MAMANI

TACNA – PERÚ

2022

UNIVERSIDAD PRIVADA DE TACNA

FACULTAD DE INGENIERÍA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

TESIS

"SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SU RELACIÓN CON LA CALIDAD DE SERVICIO DE LAS REDES LAN EN LA MUNICIPALIDAD DISTRITAL DE ILABAYA."

Tesis sustentada y aprobada el 25 de junio del 2022, estando el jurado calificador integrado por:

PRESIDENTE : Mtro. HUGO MANUEL BARRAZA VIZCARRA

SECRETARIO : Ing. HUGO MARTÍN ALCÁNTARA MARTÍNEZ

VOCAL : Mtro. RICARDO CARLOS INQUILLA QUISPE

ASESOR : Mag. RICARDO EDUARDO VALCÁRCEL ALVARADO

DECLARACIÓN JURADA DE ORIGINALIDAD

Yo, Galindo Yefer Maquera Mamani con documento de identidad 70259100, en calidad de: Bachiller en Ingeniería de Sistemas de la Escuela Profesional de Ingeniería de Sistemas.

Declaro bajo juramento que:

Soy autor de la tesis titulada: *"Sistema de Gestión de Seguridad de la Información y su relación con la calidad de servicio de las redes LAN en la Municipalidad Distrital de Ilabaya"*, la misma que presento para optar el Título Profesional De Ingeniero de Sistemas.

1. La tesis no ha sido plagiada ni total ni parcialmente, para la cual se han respetado las normas internacionales de citas y referencias para las fuentes consultadas.
2. La tesis presentada no atenta contra derechos de terceros.
3. La tesis no ha sido publicada ni presentada anteriormente para obtener algún grado académico previo o título profesional.
4. Los datos presentados en los resultados son reales, no han sido falsificados, ni duplicados, ni copiados.

Por lo expuesto, mediante la presente asumimos frente a la universidad cualquier responsabilidad que pudiera derivarse por la autoría, originalidad y veracidad presentada. En consecuencia, nos hacemos responsables frente a la universidad y a terceros, de cualquier daño que pudiera ocasionar, por el incumplimiento de lo declarado o que pudiera encontrar como causa del trabajo presentado, asumiendo todas las cargas pecuniarias que pudieran derivarse de ello a favor de terceros con motivo de acciones, reclamaciones o conflictos derivados del incumplimiento de los declarado o las que encontrasen causa en el contenido de tesis, libro y/o invento.

De identificarse fraude, piratería, plagio, falsificación o que el trabajo de investigación haya sido publicado anteriormente; asumo las consecuencias y sanciones que de mi acción se deriven, sometiéndome a la normatividad vigente de la Universidad Privada de Tacna.

Tacna, 01 de marzo del 2022.

Galindo Yefer Maquera Mamani

DNI: 70259100

DEDICATORIA

A Dios por la vida que nos ofrece, de corazón a mis padres Gregorio y mi santa madre Teófila que desde el cielo me acompaña, a mi hermana Dania por su gran cariño y apoyo incondicional.

AGRADECIMIENTO

A mi asesor Mag. Ricardo Eduardo Valcárcel Alvarado por su orientación, conocimiento y experiencia para el desarrollo de la presente investigación.

Al Ing. Antony Jesús Osco Joaquín responsable de la oficina de Tecnología de Información y comunicaciones de la Municipalidad Distrital de Ilabaya por la información brindada y conocimientos adquiridos.

ÍNDICE GENERAL

PÁGINA DE JURADO ii
DECLARACIÓN JURADA DE ORIGINALIDAD iii
DEDICATORIA iv
RESUMEN xii
ABSTRACT xiii
INTRODUCCIÓN 1
CAPÍTULO I: PLANTEAMIENTO DEL PROBLEMA 3
1.1. Descripción del Problema 3
1.2. Formulación del Problema 6
1.2.1. Problema General 6
1.2.2. Problema Específico 6
1.3. Justificación e Importancia 7
1.4. Objetivos 8
1.4.1. Objetivo General 8
1.4.2. Objetivos Específicos 8
1.5. Hipótesis 8
1.5.1. Hipótesis General 8
1.5.2. Hipótesis Específica 8
CAPÍTULO II: MARCO TEÓRICO 9
2.1. Antecedentes del Estudio 9
2.1.1. Antecedentes Internacionales 9
2.1.2. Antecedentes Nacionales 12
2.2. Bases Teóricas 13
2.2.1. Sistema de Gestión de Seguridad de la Información 13
2.2.2. Calidad de Servicio de las Redes LAN 16
2.3. Definición de Términos 17
CAPÍTULO III: MARCO METODOLÓGICO 20
3.1. Tipo y nivel de la Investigación 20
3.1.1 Tipo de Investigación 20
3.1.2 Diseño de Investigación 20
3.1.3 Nivel de Investigación 20
3.1. Población y Muestra de Estudio 21
3.1.1. Población 21
3.1.2. Muestra 22
3.2. Operacionalización de variables 22
3.3. Técnicas e instrumentos para la recolección de datos 24
3.3.1. Técnica 24
3.3.2. Instrumento 24

3.3.3. Validación de instrumento 25
3.4. Procesamiento y análisis de datos 26
CAPÍTULO IV: RESULTADOS 27
4.1. Análisis e interpretación de resultados 27
4.1.1. Confiabilidad de los instrumentos y escala de valoración 27
4.1.2. Resultado: Sistema de gestión de seguridad de la información 30
4.1.3. Análisis General: Sistema de gestión de seguridad de la información 37
4.1.4. Resultados: Calidad de servicio de las redes LAN 39
4.1.5. Análisis General: Calidad de servicio de las redes LAN 45
4.2. Contraste de hipótesis 47
4.2.1. Contraste de hipótesis especifica 47
4.2.2. Contraste de hipótesis general 53
4.3. Resultados descriptivos 57
4.3.1. Resultado descriptivo de la variable 1: Sistema de gestión de seguridad de la información 57
4.3.2. Resultado descriptivo de la variable 2: Calidad de Servicio de las redes LAN 58
4.3.3. Resultado descriptivo de la variable 1 y variable 2 59
4.3.4. Resultado descriptivo de frecuencia 60
CAPÍTULO V: DISCUSIÓN 69
CONCLUSIONES 70
RECOMENDACIONES 71
REFERENCIAS BIBLIOGRÁFICAS 72
ANEXOS 75

ÍNDICE DE TABLAS

Tabla 1. Oficinas de la Municipalidad Distrital de Ilabaya 21
Tabla 2. Población considerada en la Municipalidad Distrital de Ilabaya 22
Tabla 3. Estructura de operacionalización de SGSI 23
Tabla 4. Estructura de operacionalización con relación a la calidad de servicio de las redes LAN 23
Tabla 5. Instrumento SGSI 24
Tabla 6. Instrumento Calidad de servicio de redes LAN 25
Tabla 7. Indicador – Ítem “SGSI” 27
Tabla 8. Indicador - Ítem “Calidad de servicio de las redes LAN” 28
Tabla 9. Escala de valoración “SGSI” 28
Tabla 10. Escala de valoración “Calidad de servicio de las redes LAN” 29
Tabla 11. Alpha de Cronbach “SGSI” 29
Tabla 12. Alpha de Cronbach “Calidad de servicio de redes LAN” 29
Tabla 13. Confidencialidad 30
Tabla 14. Confidencialidad 30
Tabla 15. Confidencialidad 31
Tabla 16. Confidencialidad 31
Tabla 17. Confidencialidad 31
Tabla 18. Integridad 32
Tabla 19. Integridad 32
Tabla 20. Integridad 33
Tabla 21. Integridad 33
Tabla 22. Integridad 34
Tabla 23. Disponibilidad 35
Tabla 24. Disponibilidad 35
Tabla 25. Disponibilidad 35
Tabla 26. Disponibilidad 36
Tabla 27. Disponibilidad 36
Tabla 28. Sistema de Gestión de Seguridad 37
Tabla 29. Sistema de Gestión de Seguridad de la Información 37
Tabla 30. Sistema de Gestión de Seguridad de la Información 38
Tabla 31. Confiabilidad 39
Tabla 32. Confiabilidad 39
Tabla 33. Confiabilidad 39
Tabla 34. Confiabilidad 40

Tabla 35. Aseguramiento 41
Tabla 36. Aseguramiento 41
Tabla 37. Aseguramiento 41
Tabla 38. Aseguramiento 42
Tabla 39. Aseguramiento 42
Tabla 40. Capacidad de respuesta 43
Tabla 41. Capacidad de respuesta 43
Tabla 42. Capacidad de respuesta 44
Tabla 43. Capacidad de respuesta 44
Tabla 44. Capacidad de respuesta 44
Tabla 45. Calidad de las redes LAN 45
Tabla 46. Calidad de las redes LAN 46
Tabla 47. Calidad de las redes LAN 46
Tabla 48. Planteamiento de hipótesis 47
Tabla 49. Pruebas de normalidad Sistema de Gestión de la Seguridad de la Información 48
Tabla 50. Estadística para una muestra “Sistema de Gestión de Seguridad de la Información” 48
Tabla 51. Prueba para una muestra “Sistema de Gestión de Seguridad de la Información” 49
Tabla 52. Planteamiento de hipótesis 50
Tabla 53. Pruebas de normalidad “Calidad de Servicio de las redes LAN” 51
Tabla 54. Estadística para una muestra 51
Tabla 55. Prueba para una muestra 52
Tabla 56. Estadística descriptiva: V.I. SGSI 56
Tabla 57. Estadística descriptiva: V.D. Calidad de servicio de las redes LAN 56
Tabla 58. Resultados V.I. SGSI 57
Tabla 59. Resultado V.D. Calidad de servicio de las redes LAN 58
Tabla 60. Resultado V.I. y V.D. 60
Tabla 61. Encuestas válidas 61
Tabla 62. Resultado de Sexo / Género 62
Tabla 63. Resultado Edad 63
Tabla 64. Total Edad 63
Tabla 65. Resultado Gerencia / Unidad 64
Tabla 66. Resultado periodo laboral 65
Tabla 67. Total periodo laboral 66
Tabla 68. Resultados cargo 67

ÍNDICE DE FIGURAS

Figura 1. Topologías de red 3
Figura 2. Ubicación geográfica de la Municipalidad Distrital de Ilabaya 4
Figura 3. Contratación, verificación de QoS en infraestructura de una red LAN 10
Figura 4. Ciclo Deming o PDCA 14
Figura 5. Documentación SGSI ISO 27000 – 2014 15
Figura 6. Red de Área Local 17
Figura 7. Validación de Instrumento 26
Figura 8. Correlaciones 53
Figura 9. Estadístico CHI-CUADRADO 54
Figura 10. Prueba de Chi-cuadrado 54
Figura 11. Resultados del cuestionario en Excel 55
Figura 12. Resultado V.I. SGSI 58
Figura 13. Resultado V.D. Calidad de servicio de las redes LAN 59
Figura 14. Resultado V.I. y V.D. 60
Figura 15. Base de Datos en SPSS V.26 61
Figura 16. Resultado Sexo / Género 62
Figura 17. Resultado Edad 64
Figura 18. Resultado Gerencia / Unidad 65
Figura 19. Total periodo laboral 66
Figura 20. Resultado cargo 68

ÍNDICE DE ANEXOS

Anexo 1. Matriz de consistencia 76
Anexo 2. Desarrollo 77
Anexo 3. Resolución 109
Anexo 4. Instrumento Encuesta 112
Anexo 5. Encuestas Desarrolladas 116
Anexo 6. Manual de Instalación 126
Anexo 7. Manual de Usuario 130
Anexo 8. Políticas de Seguridad MDI 136
Anexo 9. Sistema SGSI_MDI 175

RESUMEN

Sistema de gestión de seguridad de la información y su relación con la calidad de servicio de las redes LAN en la Municipalidad Distrital de Ilabaya, la entidad presenta problemas de saturación de red, controles de seguridad obsoletos, ataques de virus constantes, poca efectividad de accesos a los servidores. La presente investigación determina la relación entre Sistema de Gestión de Seguridad de la Información y la calidad de servicio de las redes LAN en la Municipalidad Distrital de Ilabaya, ante estos escenarios se planteó un diseño de un SGSI tomando en cuenta la Norma Técnica Peruana NTP ISO/IEC 27001:2014. Se desarrolló mediante un enfoque cuantitativo donde se aplicó herramientas de recolección de datos, el tipo de investigación que se planteó para el desarrollo es aplicado de características descriptivas y correlacionales no experimental, de nivel Aprehensivo que corresponde a una investigación donde los objetivos implican analizar o comparar y posteriormente proponer. Para el contraste de correlación de Pearson se determinó que el valor hallado del coeficiente de correlación fue r = 0,540 (valor de p = 0,000); por lo tanto, existe una influencia directa y significativa entre el Sistema de Gestión de Seguridad de la Información y la Calidad de Servicio de la Red LAN de la Municipalidad Distrital de Ilabaya. En base a los resultados, se planteó al área encargada el diseño de Sistema de Gestión de Seguridad de la Información iniciando con un análisis situacional de la entidad posteriormente se desarrolló políticas y controles de seguridad para la Municipalidad distrital de Ilabaya, asimismo se desarrolló un sistema de control de riesgo como parte de un SGSI para la entidad.

Palabras claves: Seguridad, información, calidad, redes, confidencialidad, integridad y fiabilidad.

ABSTRACT

Information security management system and its relationship with the quality of service of LAN networks in the District Municipality of Ilabaya, the entity presents problems of network saturation, obsolete security controls, constant virus attacks, low access effectiveness to the servers. This research aims to determine the relationship between the Information Security Management System and the quality of service of LAN networks in the District Municipality of Ilabaya, given these scenarios, it seeks to propose a design of an ISMS taking into account the Peruvian Technical Standard ISO/IEC 27001:2014. It was developed through a quantitative approach where data collection tools were applied, the applied technique is a survey, the type of research that is proposed is applied with descriptive and non-experimental correlational characteristics, of an apprehensive level that corresponds to an investigation where the objectives imply analyze or compare and then propose. For the Pearson correlation contrast, it was determined that the value found for the correlation coefficient was r = 0.540 (p value = 0.000); therefore, there is a direct and significant influence between the Information Security Management System and the Quality of Service of the LAN Network of the District Municipality of Ilabaya. Based on the results, the design of the Information Security Management System was proposed to the area in charge, starting with a situational analysis of the entity, later security policies and controls were developed for the District Municipality of Ilabaya, as well as a system risk control as part of an ISMS for the entity.

Key words: Security, information, quality, networks, confidentiality, integrity and reliability.

INTRODUCCIÓN

En el mundo entero cual sea el país donde nos encontremos siempre tendremos la presencia de las redes, y la información digital que circula en este tipo de comunicación, la presencia de redes nos ayuda al intercambio de toda clase de información, multimedia, transmisión en vivo, videoconferencia, transacciones monetarias entre otros, basados en una tecnología de transferencia de información de calidad en el menor tiempo posible.

La tecnología se adapta a la geografía de cada país, el Perú es uno de los países que consta de tres (03) regiones geográficas, costa sierra y selva siendo las regiones sierra y selva los últimos en interactuar con las telecomunicaciones y la información digital por la difícil accesibilidad geográfica.

Las telecomunicaciones son indispensables en las organizaciones, instituciones públicas o privadas, empresas, colegios, universidades; entre otros, constan de una red LAN (Local Área Network) denominada en español como red de área local, quien tiene como función priorizar el intercambio de información entro dos (02) o más equipos electrónicos y sobre esta importancia la seguridad de la información cumple un rol prioritario para poder gestionarla en las diferentes organizaciones.

El problema común que la mayoría de las organizaciones presenta en la actualidad, es referenciado a la capacidad de respuesta en cuestión a la información digital, lo cual conlleva a vulnerabilidades, amenazas, riesgos, perdida de activos de información, robo de información, accesos mal intencionados o no autorizados, entre otros. Trayendo como consecuencia el retraso de cumplimiento de metas planteadas en las organizaciones.

Al referirnos a seguridad de información implica distintos componentes tales como: redes LAN, normas, estándares, políticas, controles, seguridad, almacenamiento, servidores, activos de información, internet, calidad de información, disponibilidad, confidencialidad, integridad de la información, entre otros. Siendo un tema de suma importancia razones por la cual se crean normas, estándares internacionales que tienen como finalidad regular, estandarizar la supervisión de los componentes mencionados. Para una mejor administración y control en las organizaciones, teniendo como finalidad adaptarse a las actualizaciones tecnológicas del mundo moderno.

Sistema de Gestión de Seguridad de la Información que a partir del despliegue del documento en algunos contextos lo referenciaremos con las siglas SGSI. Es el aseguramiento de la información lo cual permite la integridad, confidencialidad y la disponibilidad de la información que circula en las redes LAN de la Municipalidad Distrital de Ilabaya.

El problema común de las entidades públicas son la saturación de red, controles de seguridad obsoletos, ataques de virus constantes, poca efectividad de accesos a los servidores, entre otros, para lo cual la presente investigación busca determinar la relación entre SGSI y la calidad de servicio de las redes LAN en la Municipalidad Distrital de Ilabaya.

Para el desarrollo de esta investigación se tuvo que recorrer a distintas investigaciones tales como tesis, proyectos, informes, revistas, libros, ensayos, etc. Así como nacionales e internacionales todas relacionadas con SGSI y calidad de servicio de redes LAN.

Investigación desarrollada de tipo descriptivo correlacional, diseño no experimental mediante un enfoque cuantitativo donde se aplicó herramientas de recolección de datos, así como cuestionario como instrumento, posteriormente se analizó los resultados obtenidos con el software IBM SPSS 26 (Statiscal Package for Social Sciences) y Microsoft Office Excel.

Bajo este contexto, la presente investigación de tesis busca la relación que existe entre un SGSI y la calidad de servicio de la red LAN en la Municipalidad Distrital de Ilabaya, planteando una propuesta de mejora que se enfoca en un diseño de un SGSI con la finalidad de mejorar la calidad de servicio de la red LAN y la información digital de la entidad.

CAPÍTULO I: PLANTEAMIENTO DEL PROBLEMA

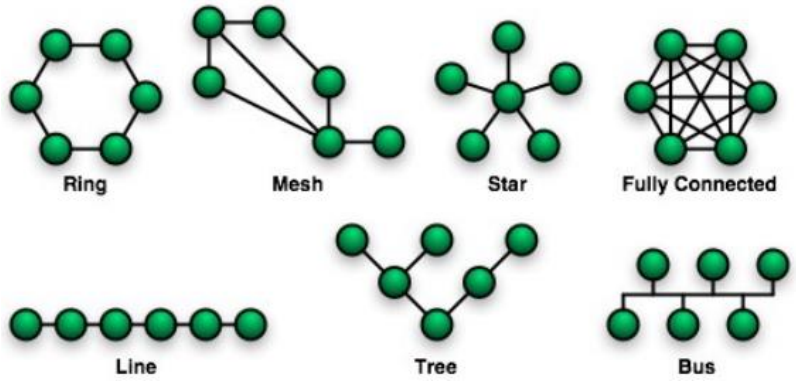
1.1. Descripción del Problema

La evolución de la tecnología en el mundo es constante lo cual tiene como prioridad garantizar la seguridad de la información y calidad de servicio, desplegándose en las últimas dos (02) décadas prácticamente en toda América Latina, siendo un medio de comunicación eficaz e indispensable para los seres humanos, interconectando con todos los continentes, a causa de este crecimiento global es que también surge la vulnerabilidad de la información, a lo cual ninguna entidad pública o privada es ajena, esto conlleva al aseguramiento de la información mediante un sistema de gestión de seguridad.

El uso constante de las telecomunicaciones y la calidad de servicio que brinda las redes en el Perú se maneja de una manera estándar, con topologías de red clásica tales como topología bus, anillo, estrella, árbol o mixto, con una administración básica lo cual no garantiza una administración eficaz de activos físico y/o digital en entidades públicas o privadas. En la figura 1, se muestra un ejemplo de funcionalidad de las redes según topología.

Figura 1

Topologías de red

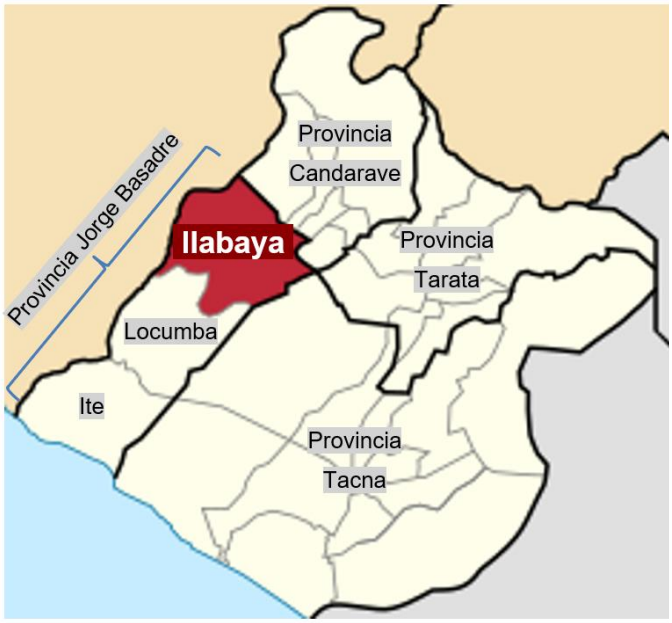


Nota. Los diseños de topologías de red son adaptados a las necesidades de las entidades. Fuente: Laborde, Ressi, & Rivoir (2006).

La Municipalidad Distrital de Ilabaya se sitúa entre los tres primeros distritos más importantes de la provincia Jorge Basadre departamento de Tacna. La entidad pública Municipalidad Distrital de Ilabaya según la ubicación geográfica de la región Tacna se encuentra situado en la parte Nor – Oeste de la provincia Jorge Basadre, Región de Tacna en la República del Perú (Ilabaya, s.f.). En la Figura 2, se puede apreciar la ubicación geográfica de la Municipalidad Distrital de Ilabaya en el departamento de Tacna.

Figura 2

Ubicación geográfica de la Municipalidad Distrital de Ilabaya



Nota. Distrito ubicado en la provincia Jorge Basadre
Fuente: Adaptado a la geografía de la región Tacna.

La Municipalidad Distrital de Ilabaya en los últimos periodos de gobierno ha ido creciendo notablemente en proceso de información por el incremento de gestión de proyectos, Inversiones de Optimización de Ampliación Marginal de Rehabilitación y de Reposición (IOARR), proyectos de mantenimientos en diferentes funciones. Esto conlleva al uso constante de las telecomunicaciones para ser específicos al uso de las infraestructuras de red interna denominada también red LAN (red de área local) de la Municipalidad Distrital de Ilabaya.

El mencionado distrito procesa una gran cantidad de información de suma importancia, dicha información se procesa mediante controles de seguridad muy

bajos, al no contar con un tipo de seguridad de información específica que pueda preservar la disponibilidad, integridad y la confidencialidad de la información.

La entidad cuenta con una infraestructura de red LAN tradicional sin considerar los riesgos naturales. Cabe mencionar que en el año 2019 ocurrió un desastre natural donde la Municipalidad Distrital de Ilabaya sufrió pérdidas de infraestructura e información trayendo como resultados desfavorables con una red inestable y dañada.

Considerando que la entidad no cuenta con un Sistema de Gestión de Seguridad de la Información (SGSI) para mejorar la calidad de servicio de la red LAN que brinda el área de Tecnología de Información y Comunicaciones de la entidad, la Municipalidad Distrital de Ilabaya presenta los siguientes problemas.

a) Saturación de la red, es considerado por la cantidad de información que procesa, falta de velocidad de internet, infraestructura con desgaste físico, equipos de interconexión reutilizados, entre otros.

b) Controles de seguridad obsoletos, la herramienta que más relevancia tenía la Municipalidad Distrital de Ilabaya para el control de usuarios se utilizaba Active Directory la cual permitía gestionar usuarios de forma ordenada, en la actualidad se encuentra obsoleto.

c) Ataque de virus constante, esto se debe a falta de licencia de antivirus ya que los antivirus gratuitos no te garantizan la seguridad de la información, ocasionando múltiples consecuencias tales como eliminación de archivos, robo de información, información dañada, computadora lenta, entre otros.

d) Poca efectividad de accesos a los servidores, la estructura desplegada para el uso de los sistemas integrados está constituido por lo siguiente: Sistema Integrado de Administración Financiera (SIAF), Sistema Integrado Municipal (SIMUN), Sistema Administrativo de Planillas (SAP), Spark Instant Messenger y Sistema Integrado de Gestión Administrativa (SIGA) mencionados sistemas no soportan el acceso remoto de múltiples usuarios.

A causa de tantas irregularidades en cuestión de redes e información en entidades públicas del estado peruano, es que la República del Perú publica una Resolución Ministerial N° 004-2016-PCM con fecha 8 de enero del 2016 (Anexo 03), la cual indica que determinadas entidades de la administración pública deben

implementar el Plan de Seguridad de Información bajo la Norma Técnica Peruana ISO/IEC27001:2014 y ISO/IEC 17799:2008 (República del Perú, 2016).

Ante estos escenarios, el presente proyecto planteó un diseño de un Sistema de Gestión de Seguridad de la Información para fortalecer la relación de SGSI con la calidad de servicio de la red LAN que brinda el área de Tecnologías de información y comunicación en la Municipalidad Distrital de Ilabaya, tomando en cuenta la Norma Técnica Peruana NTP ISO/IEC 27001:2014 y la Norma Técnica Peruana NTP – ISO/IEC 17799:2008, mejorando la gestión de posibles riesgos y estableciendo un umbral de riesgo aprobado por la alta dirección en aspectos de buenas prácticas para la seguridad de la información, lo cual se desarrolla en relación a la gestión de redes LAN.

En esta línea, la presente investigación de Tesis tiene como objetivo, implantar la Norma Técnica Peruana NTP ISO/IEC 27001:2014 en un futuro, para ello se planteó un diseño de un SGSI para la Municipalidad Distrital de Ilabaya como valor agregado, haciendo una evaluación de relación que se tiene entre SGSI y la calidad de servicio en la red LAN de la Municipalidad Distrital de Ilabaya.

1.2. Formulación del Problema

1.2.1. Problema General

¿Cuál es la relación entre SGSI y la calidad de servicio de la red LAN en la Municipalidad Distrital de Ilabaya?

1.2.2. Problema Específico

a. ¿Cuál es el nivel de SGSI que caracteriza a la Municipalidad Distrital de Ilabaya?
b. ¿Cuál es el nivel de calidad de servicio de la red LAN en la Municipalidad Distrital de Ilabaya?
c. ¿Cómo influye el SGSI en la calidad de servicio de la red LAN en la Municipalidad Distrital de Ilabaya?

1.3. Justificación e Importancia

La investigación planteada, ha contribuido a determinar el grado de correlación que tiene el SGSI con la calidad de servicio de red LAN de la Municipalidad Distrital de Ilabaya. Posteriormente se planteó un diseño de SGSI. De acuerdo con lo establecido, la Municipalidad Distrital de Ilabaya no cuenta con ningún tipo de antecedente que permita o facilite una investigación avanzada en relación con la seguridad de la información y calidad de servicio de la red LAN, bajo este contexto es que se consideró relevante realizar una investigación de relación entre SGSI con la calidad de servicio de la red LAN en la Municipalidad Distrital de Ilabaya.

En esta línea, la presente investigación dejó como valor agregado el análisis y diseño de un SGSI para la red LAN de la Municipalidad Distrital de Ilabaya bajo el enfoque de la Norma Técnica Peruana NTP ISO/IEC 27001:2014 y la Norma Técnica Peruana NTP – ISO/IEC 17799:2008.

En base al análisis que se realizó se hizo el planteamiento de un diseño de SGSI para contar con un servicio de calidad de redes LAN, lo cual permitirá optar por nuevas y mejoradas políticas de seguridad para un desempeño satisfactorio de la infraestructura de redes LAN en la Municipalidad Distrital de Ilabaya, esta investigación abarca los siguientes aspectos.

a) **Relevancia científico – social**; de acuerdo con las variables e indicadores se analizó exhaustivamente las incidencias en el SGSI relacionada con calidad de servicio de redes LAN dentro de la Municipalidad Distrital de Ilabaya, dando la prioridad debida a los activos de información de la entidad pública que analizamos.

   Levantamiento de información; la presente investigación permitió la recolección de datos de suma importancia dicha información se pretende considerar en los directivos de la entidad, de esta manera fomentar e intuir la seguridad de la información logrando guardar información de suma importancia en la Municipalidad Distrital de Ilabaya.

   Relevancia de información; toda información recolectada quedó como antecedente para la Municipalidad Distrital de Ilabaya, dicha investigación permitió valorar los activos de la información de la entidad, donde personal autorizado pueda tener acceso a estos y realizar una implantación futura de la Norma Técnica Peruana NTP ISO/IEC 27001:2014 hasta llegar a la certificación.

b) Relevancia práctico – institucional; porque los resultados de la investigación se desarrollaron bajo el uso de un SGSI, donde se evidenció la importancia de la aplicación del SGSI quien preserva la integridad, confidencialidad y la disponibilidad de toda información que circula en las infraestructuras de red LAN de la Municipalidad Distrital de Ilabaya, garantizando las buenas prácticas en gestión pública.

1.4. Objetivos

1.4.1. Objetivo General

Determinar la relación entre el SGSI y la calidad de servicio de las redes LAN en la Municipalidad Distrital de Ilabaya.

1.4.2. Objetivos Específicos

a. Determinar el nivel del SGSI que caracteriza a la Municipalidad Distrital de Ilabaya.
b. Determinar el nivel de calidad de servicio de redes LAN que caracteriza a la Municipalidad Distrital de Ilabaya.
c. Determinar la influencia del SGSI en la calidad de servicio de redes LAN en la Municipalidad Distrital de Ilabaya.

1.5. Hipótesis

1.5.1. Hipótesis General

Existe una relación directa y significativa entre SGSI y la calidad de servicio de las redes LAN en la Municipalidad Distrital de Ilabaya.

1.5.2. Hipótesis Específica

a. El nivel del SGSI que caracteriza a la Municipalidad Distrital de Ilabaya es regular.
b. El nivel de calidad de servicio de las redes LAN en la Municipalidad Distrital de Ilabaya es regular.
c. Existe una influencia del SGSI sobre la calidad de servicio de las redes LAN en la Municipalidad Distrital de Ilabaya.

CAPÍTULO II: MARCO TEÓRICO

2.1. Antecedentes del Estudio

2.1.1. Antecedentes Internacionales

Guerra Aleman (2020), en su proyecto de grado: “Sistema de gestión para la seguridad de la información basado en la metodología de identificación y análisis de riesgo en la biblioteca de la universidad de la costa”, realiza una investigación donde plantea desarrollar un Sistema de Gestión de la Información, centrado en la metodología de identificación y análisis de riesgo, para los procesos de biblioteca de la institución educativa superior donde desarrolla el proyecto de grado, el tipo de estudio que realiza es aplicada, retrospectiva, transversal, descriptivo y documental, dicha investigación busca la solución de un dilema o necesidad, la forma de obtener la información fue al inicio del estudio y en el proceso de la investigación, garantizando el buen desarrollo de la metodología adaptado a la normatividad de ISO/IEC 27001:2013. Esta normatividad tiene como finalidad analizar, disminuir el riesgo, mejorar y garantizar la información, pretendiendo establecer la estandarización de procesos en la biblioteca de la institución educativa superior Universidad de la Costa.

Coque V. & Kujundzic R. (2018), en su proyecto de grado: “Uso de la seguridad de la información en la dirección de proyectos”, define que la dirección de proyectos está establecida por un grupo de procesos de estandarización con la finalidad de garantizar las buenas prácticas, encontrándose con algunos obstáculos al momento de recolección de datos que ayuden con la disponibilidad, integridad y confidencialidad de la información relacionada con la metodología PMBOK®. Dicha investigación pretende mitigar los riesgos encontrados con relación a seguridad de la información a través de la normatividad ISO/IEC 27002:2013.

Rodríguez Criollo (2016), en su proyecto de investigación: “Evolución de las redes de telecomunicaciones y calidad de servicio en redes de nueva generación NGN en el Ecuador”, establece que las redes de telecomunicaciones o llamadas también redes de próxima generación (NGN) deben adaptarse a las nuevas tendencias que se va presentado mientras transcurre el pasar de los años, entonces debe adaptarse a los videoconferencias masivas, IPTV, VoIP y navegación de datos transaccionales muy concurrentes, esto conlleva a que las infraestructuras de telecomunicaciones teles como WAN (Red de Área Amplia), MAN (Red de Área

Metropolitano) y LAN (Red de Área Local), las topologías de red mencionadas bien planteadas permiten garantizar la seguridad de la información llevando información de calidad a su destino, menciona también que al analizar la estructura de capa servicio y transporte de la NGN es la que ofrece calidad de servicio relacionada con controles de seguridad de información. En la Figura 3, se muestra los niveles de evolución de las redes de telecomunicación.

Figura 3

Contratación, verificación de QoS en infraestructura de una red LAN

Nota. Niveles de evolución de las redes de telecomunicación y calidad de servicio en redes de nueva generación. Fuente: Rodríguez (2016).

Fernado Q. & Torrado G. (2015), en su proyecto: “Planeación del sistema de gestión de seguridad de la información para la empresa Katalinda Shoes”, mencionados autores realizan un estudio o planeación del SGSI según la norma internacional ISO/IEC 27001, enfocándose en los riesgos existentes y salvaguardar los activos de información estableciendo políticas y controles que permitan el ingreso no autorizado a los activos de información de la empresa Katalinda Shoes.

Tufiño Galán (2018), en su trabajo de disertación: “Diseño de un modelo de seguridad de información en redes LAN”, quien tiene como finalidad diseñar un modelo para determinar la seguridad de información en redes LAN enfocándose en vulnerabilidades y ataques que se presentan en el trascurso de intercambiar información dentro de una red, desarrollándose a través de metodologías puntuales con enfoques de redes LAN incluyendo sistemas operativos, aplicaciones, hacking y

análisis de escaneo de puertos. Para la corroboración de posibles ataques el autor realiza pruebas de ataques con herramientas tales como; máquinas virtuales y simulaciones de redes con Cisco Packet Tracer, obteniendo como resultados un análisis de mejora quien recurre a la estandarización mediante la norma internacional ISO 27000 tomando como guía para la evaluación, diseño, levantamiento de información y construcción de redes en cualquier tipo de entidades.

Felizzola et. al (2019), en su proyecto de grado: “Diseño del sistema de gestión de seguridad de la información SGSI basado en el estándar ISO 27001, en la Universidad Popular del Cesar seccional Aguachica”, los autores realizan una auditoría interna a lo cual obtiene como resultado de la auditoria que la Universidad no cuenta con sistemas basados a la norma estándar ISO 27001, en base a estos resultados los autores realizan un análisis situacional posteriormente estableciendo un sistema de gestión estableciendo roles y responsabilidades mediante políticas del sistema de seguridad de la información basado en la norma ISO 27001, con la implementación, los autores aseguran que la manejabilidad de los sistemas de información y comunicación permitirá mejorar la fluidez y confianza al intercambiar información de las diferentes dependencias.

Trujillo Niebles (2020), en su trabajo de grado: “Diseño de controles y políticas para la seguridad de la información en la red LAN en el Hotel Pipaton”, el autor pretende proteger la información de todas las áreas que cuenta el Hotel Pipaton, lo cual realiza un diseño de políticas y controles que minimizaran las vulnerabilidades existentes, dicha investigación lo desarrolla con la metodología Magerit, así también realiza la identificación de todos los activos de información para luego determinar el grado de riesgo existente para posteriormente subsanar. Las políticas y los controles de seguridad, el autor menciona que tendrán éxito si los usuarios concientizamos en salvaguardar los activos de información del Hotel Pipaton mediante la seguridad de la información, seguridad en redes LAN, seguridad informática, vulnerabilidades, políticas y controles relacionados con calidad de servicio.

Ley et. al (2021), Plantea como objetivo analizar la eficacia y la efectividad de la seguridad de las redes LAN utilizando métodos de revisión y técnica de encuesta, lo cual hace que la investigación sea descriptiva, llegando a la conclusión que se requiere el control de telecomunicaciones empleando firewall de mikrotik, para una mejor administración de las redes LAN y el control de la seguridad de información.

2.1.2. Antecedentes Nacionales

Blas Z. & Pretell R. (2020), en su proyecto de tesis: “Modelo de seguridad de la información para mejorar la gestión informática en la Municipalidad Distrital de Florencia de Mora”, pretende gestionar toda información y el total de los activos de la Municipalidad, disponibilidad de accesos informáticos, disponer la seguridad de las telecomunicaciones e implantar la seguridad física y ambiental con el objetivo de establecer un sistema de gestión de seguridad de la información, el tipo de investigación que realiza es descriptivo por lo que ayuda con la realización de la presente investigación, lo cual está desarrollada con el diseño de investigación no experimental, transversal ya que la obtención de datos se da en un único momento.

Cáceda Rodríguez (2021), plantea en su investigación: “Modelo dinámico para la gestión de seguridad de la infraestructura de las tecnologías de información y comunicación”, en relación con la infraestructura y redes LAN, menciona que la organización donde desarrollara su investigación no tiene establecido un modelo de gestión de seguridad de la infraestructura de las (TIC) Tecnología de Información y comunicaciones, plantea que los ataques cibernéticos al pasar de los años evolucionan a la par con la tecnología lo cual ocasiona que la ciberseguridad sea uno de los riesgos más críticos en las redes de telecomunicaciones trayendo como consecuencia un nivel alto de riesgo en los procesos.

Vergara Quiroz (2016), en su proyecto de tesis de grado: “Seguridad de información y calidad de servicio en la Universidad Nacional Federico Villarreal”, desarrolla un estudio para determinar la relación existente de seguridad de información y calidad de servicio en la institución educativa superior Universidad Nacional Federico Villa Real, la investigación que realiza en su proyecto es de tipo descriptivo correlacional, porque todo el proyecto lo enfoca en conocer la relación o grado de asociación existente entre dos o más variables en un ámbito especifico con un enfoque cuantitativo y método hipotético, la técnica que aplica para la obtención de datos es encuesta y como instrumento cuestionario, el diseño de investigación es no experimental investigación que se realiza son la modificación de variables naturalmente para un posterior análisis.

2.2. Bases Teóricas

2.2.1. Sistema de Gestión de Seguridad de la Información

Conceptos:

a) Según Trujillo Niebles (2020), SGSI es un sistema de gestión de seguridad de la información quien tiene como responsabilidad proporcionar varios procesos y herramientas basados en el estándar ISO27001, esta norma permite a diferentes organizaciones o entidades identificar las debilidades con respecto a la seguridad de la información, guiando al usuario para una eficaz administración de los riesgos identificados.

b) Para ISO 27001 (como se citó en Castro Siguas, 2018), la implementación de un SGSI se basa en la norma ISO27001, quien presenta en su investigación un sistema de gestión basado en el ciclo Deming, dicho sistema es el más considerado para implantar a un plan de mejora continua. Como se puede apreciar de manera gráfica en la Figura 4.

Planificar: para ISO 27001 (como se citó en Castro Siguas, 2018), se define el alcance y la política de seguridad, se empieza con un análisis de riesgo que refleja el estado actual de la entidad y, una vez implementado, define un plan de tratamiento de información y de riesgos, esto conlleva a la implementación de controles para los diversos riesgos que la administración no está tomando en cuenta.

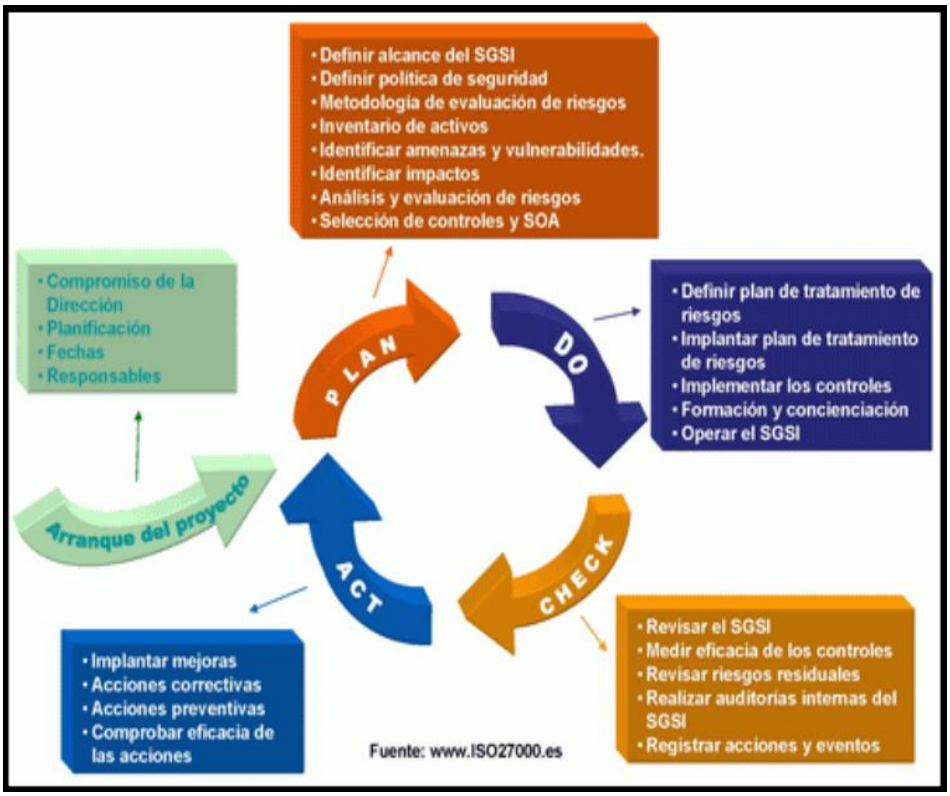
Hacer: para ISO 27001 (como se citó en Castro Siguas, 2018), esta fase del ciclo Deming o ciclo PDCA se centra en la planificación de los tratamientos de riesgos, esto influye a la concientización de los usuarios, y la definición de métricas para los distintos controles a aplicar.

Verificar: para ISO 27001 (como se citó en Castro Siguas, 2018), esta fase incluye la realización de auditorías para verificar la correcta implementación del SGSI, la realización de auditorías internas y la gestión general de la empresa.

Actuar: para ISO 27001 (como se citó en Castro Siguas, 2018), este es el resultado de la auditoria y se debe tomar diversas acciones correctivas, preventivas o de mejora.

Figura 4

Ciclo Deming o PDCA



Nota. ciclo Deming para implantar a un plan de mejora continua en entidades públicas o privadas. Fuente: ISO 27001 (como se citó en Castro Siguas, 2018).

c) Para ISO 27000 (como se citó en Castro Siguas, 2018), define SGSI como un conjunto de elementos interrelacionados o que interactúan en: estructura organizacional, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos utilizados por una organización para establecer políticas y objetivos de la seguridad de la información, como se muestra en la Figura 5.

Figura 5

Documentación SGSI ISO 27000 – 2014

Nota. Procedimientos y recursos utilizados por una organización para establecer políticas y objetivos de la seguridad de la información. Fuente: ISO 27000 (como se citó en Castro Siguas, 2018)

d) Según Gómez & Fernández (como se citó en Ccesa Quincho, 2017), Un sistema de gestión de seguridad de la información se define como un conjunto de procesos que permite a una organización o entidades establecer, implementar, mantener y mejorar continuamente la seguridad de la información de acuerdo con los riesgos que se enfrenta, también mencionan la configuración preestablecida de la configuración asumida del SGSI. Procesos formales y definiciones claras de responsabilidades basadas en un conjunto de políticas, planes y procedimientos que deben incorporarse.

e) Según Najar & Suarez (como se citó en Diaz Lara, 2021), La información es altamente reveladora porque depende de factores internos y externos; los autores concluyeron que la información es considerada como uno de los activos más relevantes e importante, y se le debe dar especial cuidado y protección, pues sin ella sería explotada por los ciberdelincuentes a nivel mundial afectando a todo tipo de sectores públicos y privados.

2.2.2. Calidad de Servicio de las Redes LAN

Conceptos:

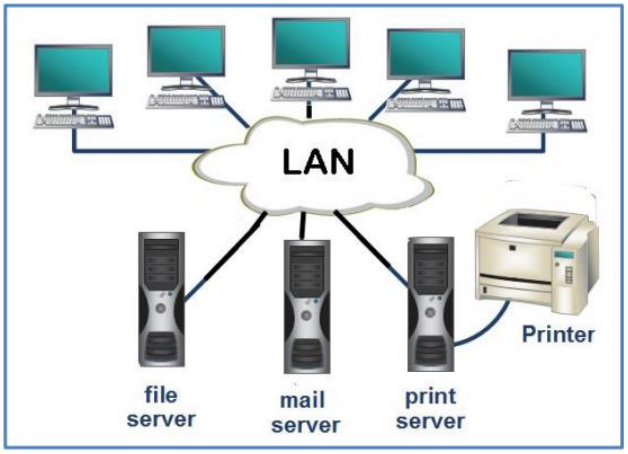
a) Según Jamieson & Low (como se citó en Ley et. al, 2021), una LAN se considera un recurso técnico eficiente que permite el intercambio de información entre dispositivos informáticos interconectados: es un grupo de dispositivos interconectados físicamente, como una oficina corporativa o una habitación en una casa; pueden ser grandes o pequeños, que puede ser un solo usuario conectado a una red doméstica, o miles de personas conectadas a una empresa, organización, institución o red corporativa.

b) Según Cacuango Lagla (2019), la calidad de servicio en una red administra y controla los parámetros de varios flujos de tráfico, como audio, video y datos digitales (software, documentos, base de datos y archivos), así como también controla la provisión de servicios a medida que viajan a través de la red, para que se pueda proporcionar información precisa a los usuarios sin perder información o datos.

c) Según Zheng Huang (2017), define la red LAN como una red de datos que cubre un área geográfica pequeña y limitada, conectando estaciones de trabajo, terminales o equipos en edificios, oficina o campus, una red LAN incluye computadoras, periféricos, dispositivos de red y tarjetas de interfaz de red (NIC). Proporciona conectividad las 24 horas del día, los 7 días de la semana y utilizan los estándares de la capa física y la capa de enlace de datos del modelo OSI, Ethernet, FDDI y Token Ring son las tecnologías LAN más populares, aunque el estándar más utilizado es Ethernet. El estándar Ethernet es la conectividad más segura y estable para las entidades públicas o privadas, garantizando una fluidez de datos estable y el intercambio de datos suele ser de manera inmediata. En la Figura 6 podemos observar cómo se interconectan computadoras, servidores, teléfono, impresora, fax, entre otros.

Figura 6

Red de Área Local



Nota. Diseño e Implementación de una red LAN para la empresa Palinda. Fuente: Zheng Huang (2017)

d) Universidad Rafael Belloso Chacín URBC (2011) en referencia a calidad de servicio de las redes LAN detalla que calidad general de la gestión de red son evaluadas mediante rigurosos criterios tales como importancia e significación de gestión de redes, eficacia y eficiencia, manejabilidad, interactividad, seguridad, calidad técnica general, acceso a la red, diseño y rendimiento.

e) Berry, Bennett, & Brown (1989) en términos generales definen que calidad de servicio es la conformidad de los usuarios receptores y realidad en la percepción, lo que los usuarios deseen es la preservación de la información mediante las dimensiones tangibilidad, confiabilidad, tiempo de respuesta, seguridad y empatía.

2.3. Definición de Términos

2.3.1 Gestión:

La gestión es el arte de crear lecciones y lograr objetivos en medio de eventos difíciles e impredecibles, no se trata de evitar dificultades o prevenir conflictos, sino de crear alternativas reales al proceso que atraviesa un grupo, organización o institución. Para ello necesitamos pensar negociar y crear continuamente nuevos

consensos, porque cuando hablamos de gestión, en última instancia, estamos hablando de acción política, por lo tanto, en el camino se debe presentar atención a diversas señales que indican dificultades o confirman el camino recorrido, en este sentido el comportamiento de la gerencia es similar al comportamiento de “el perseguidor” (Huergo, 2004).

2.3.2 Seguridad de Información

La seguridad de la información es una disciplina tradicionalmente asociada a la gestión de las TIC con el objetivo de mantener niveles aceptables de riesgo de la información lo cual permite su recolección, procesamiento, acceso, intercambio, almacenamiento, transformación y adecuada presentación. La norma ISO/IEC 27000 la define como la protección de la confidencialidad, integridad y disponibilidad de la información, términos que se consideró como dimensiones para la variable 1 Sistema de Gestión de Seguridad de la Información (Valencia D. & Orozco A., 2017).

2.3.3 Calidad de Servicio

Calidad de servicio en relación con las telecomunicaciones se define como el desempeño de servicio que determina la satisfacción del usuario final, también se define como un conjunto de periféricos o dispositivos de red donde los administradores realizan la distribución de la red de una manera óptima (Cacuango Lagla 2019).

2.3.4 Redes de Área Local LAN

Define la red LAN como una red de datos que cubre un área geográfica pequeña y limitada, conectando estaciones de trabajo, terminales o equipos en edificios, oficinas o campus, una red LAN incluye computadores, periféricos, dispositivos de red y tarjetas de interfaz de red (NIC). Proporciona conectividad las 24 horas del día, los 7 días de la semana y utilizan los estándares de la capa física y la capa de enlace de datos del modelo OSI, Ethernet, FDDI y Token Ring son las tecnologías LAN más populares, aunque el estándar más utilizado es Ethernet (Huang 2017).

2.3.5 Servqual

Se refiere a un cuestionario de preguntas que ya están establecidas con la finalidad de medir la Calidad de servicio, lo cual tiene dimensiones ya establecidas, para investigación adaptamos nuestras dimensiones; Confiabilidad, Aseguramiento y Capacidad de respuesta, para un mejor desarrollo de la investigación.

CAPÍTULO III: MARCO METODOLÓGICO

3.1. Tipo y nivel de la Investigación

3.1.1 Tipo de Investigación

El tipo de investigación que se planteó para el desarrollo es aplicado de características descriptivo y correlacional, descriptivo porque implica visualizar y transcribir los eventos así mismo situaciones, las cuales no influye sobre él en ninguna situación. Correlacional porque su función es medir dos variables lo cual requiere hipótesis y pruebas estadísticas.

3.1.2 Diseño de Investigación

El problema de la Municipalidad Distrital de Ilabaya se estudió mediante el diseño documental no experimental considerando la propuesta de mejora. La información se recabó de tipo corte transversal (en un momento del tiempo). Se desarrolló mediante un enfoque cuantitativo donde se aplicó herramientas de recolección de datos, esta información se analizó y comparo mediante patrones estadísticos.

3.1.3 Nivel de Investigación

El nivel de investigación es de nivel Aprehensivo que corresponde a una investigación donde los objetivos implican analizar o comparar y posteriormente proponer, asimismo el marco metodológico se presenta en el anexo 01.

Según Sampieri (2018) una investigación de correlación debe contener las siguientes pautas primordiales para su desarrollo: realizar un análisis de datos, funcionalidades de la información, resultados de la investigación y establecer hipótesis o predicción, finalmente realizar el contraste de hipótesis.

Se identificó si hay o no relación entre SGSI y la calidad de servicio de redes LAN. Para el desarrollo del presente estudio se consideró dos (02) variables:

a) Variable 1

Sistema de Gestión de Seguridad de la Información.

b) Variable 2

Calidad de Servicio de Redes LAN.

En la presente investigación las variables se midieron mediante la técnica encuesta, las encuestas se aplicaron en la Municipalidad Distrital de Ilabaya, se está considerando las siguiente gerencias, unidades, oficinas y áreas más relevantes con relación a SGSI y calidad de servicio en redes LAN. Como se muestra en la Tabla 1.

Tabla 1

Oficinas de la Municipalidad Distrital de Ilabaya

Municipalidad Distrital de Ilabaya	
Gerencia de administración y finanzas	Unidad de contabilidad
	Unidad de tesorería
	Unidad de abastecimiento
	Unidad de recursos humanos
	Oficina de control patrimonial
	Área de tecnología de información y comunicaciones
Gerencia de Planificación Presupuesto	Oficina de programación multianual de inversiones

Nota. Gerencias seleccionadas donde se aplicaron las encuestas. Fuente: Organigrama de la Municipalidad Distrital de Ilabaya.

3.1. Población y Muestra de Estudio

3.1.1. Población

La población considerada para este estudio está constituida por 93 funcionarios y servidores públicos, cabe mencionar que en el mes de enero y primeras semanas de febrero la Municipalidad Distrital de Ilabaya contaba con 93 personas con vínculo laboral quienes están comprendidos por la Gerencia de administración y finanzas y Gerencia de planificación presupuesto, quienes están conformados de la siguiente manera, Tabla 2.

Tabla 2

Población considerada en la Municipalidad Distrital de Ilabaya

Municipalidad Distrital de Ilabaya		
GERENCIA/UNIDADES/OFICINAS/AREAS		**Cantidad personal**
Gerencia de administración y finanzas	Unidad de contabilidad	11
	Unidad de tesorería	13
	Unidad de abastecimiento	26
	Unidad de recursos humanos	16
	Área de tecnología de información y comunicaciones	12
Gerencia de Planificación Presupuesto	Oficina de programación multianual de inversiones	15
	Total	93

Nota. La población es considerada solo en las dos gerencias seleccionadas de la Municipalidad Distrital de Ilabaya. Fuente: Organigrama de la Municipalidad Distrital de Ilabaya

3.1.2. Muestra

Como muestra se tomó a 63 personas comprendidos por funcionarios y empleados públicos que más relevancia tienen en cuestión de uso de los sistemas integrados de la Municipalidad distrital de Ilabaya, quienes tienen a su cargo las diferentes funciones con relación a sus áreas. En la actualidad el área de Tecnología de Información y comunicaciones es el encargado de manipular los controles de seguridad existente en la entidad. Esta muestra nos ayudó a analizar el estado de SGSI en la entidad e interpretar sus resultados con métricas de Integridad, Disponibilidad y Confidencialidad.

3.2. Operacionalización de variables

a) **Variable 1:** Sistema de Gestión de Seguridad de la Información.

En la Tabla 3 mostramos la distribución de la variable 1 lo cual consiste en dimensiones, indicadores, ítems y escala de medición.

Tabla 3

Estructura de operacionalización de SGSI

Dimensiones	Indicadores	Ítems	Escala de medición
Confidencialidad	- Seguridad de Personal - Privacidad de la información	1-4	1) Nunca 2) Casi Nunca 3) A veces 4) Casi Siempre 5) Siempre
Integridad	- Seguridad lógica - Seguridad Física y Ambiental - Gestión de Incidentes de seguridad de Información - Administración de las Operaciones y comunicaciones	5-13	
Disponibilidad	- Inventario de Activos y clasificación de la información - Procedimientos de Respaldo	14-18	

Nota. Fuente: Adaptado a seguridad de la información.

b) Variable 2: Calidad de Servicio de las redes LAN.

En la Tabla 4 mostramos la distribución de la variable 2 lo cual consiste en dimensiones, indicadores, ítems y escala de medición.

Tabla 4

Estructura de operacionalización con relación a la calidad de servicio de las redes LAN

Dimensiones	Indicadores	Ítems	Escala de medición
Confiabilidad	- Eficiencia - Efectividad	1-4	1) Nunca 2) Casi Nunca 3) A veces 4) Casi Siempre 5) Siempre
Aseguramiento	- Confianza - Credibilidad	5-8	
Capacidad de respuesta	- Tiempo de respuesta - Mejora continua	9-12	

Nota. Fuente: Adaptado al modelo Servqual.

3.3. Técnicas e instrumentos para la recolección de datos

3.3.1. Técnica

La técnica que aplicamos para la obtención de datos es la encuesta ya que la mayoría de los usuarios se familiariza mejor con esta técnica.

3.3.2. Instrumento

En coordinación con el asesor a cargo y el responsable del área de tecnología de información y comunicación de la Municipalidad Distrital de Ilabaya se acordó tomar el cuestionario como instrumento.

Siguiendo un proceso definido para la ejecución del desarrollo de un cuestionario tipo Likert de cinco (05) ítems, que dará respuestas basadas en las percepciones de las personas de una muestra seleccionada.

De acuerdo a lo mencionado la herramienta de medición se presenta en el Anexo 04, la cual consta de 30 las preguntas fueron elaboradas de acuerdo a las dimensiones de cada variable 1 Tabla 5 y variable 2 Tabla 6 de acuerdo al proceso de operacionalización de variables.

Tabla 5

Instrumento Sistema de Gestión de Seguridad de la Información

Ficha Técnica	
Instrumento	SGSI
Autor y año	Galindo Yefer Maquera Mamani, 2022
Población	93 usuarios
Nivel de confianza	95.0%
Margen de error	5.0%
Tipo de técnica / instrumento	Encuesta / cuestionario
Método de medición	Escala de Likert: 1: Nunca 2: Casi nunca 3: A veces 4: Casi siempre 5: Siempre

Nota. Adaptado de Ficha Técnica. Fuente: Vergara Quiroz (2016).

Tabla 6

Instrumento Calidad de servicio de redes LAN

Ficha Técnica	
Instrumento	Calidad de servicio de redes LAN
Autor y año	Galindo Yefer Maquera Mamani, 2022
Población	93
Nivel de confianza	95.0%
Margen de error	5.0%
Tipo de técnica / instrumento	Encuesta / cuestionario
Método de medición	Escala de Likert; 1: Nunca 2: Casi nunca 3: A veces 4: Casi siempre 5: Siempre

Nota. Adaptado de Ficha Técnica. Fuente: Vergara Quiroz (2016).

3.3.3. Validación de instrumento

a) Municipalidad Distrital de Ilabaya
   Ing. Antony Jesús Osco Joaquín

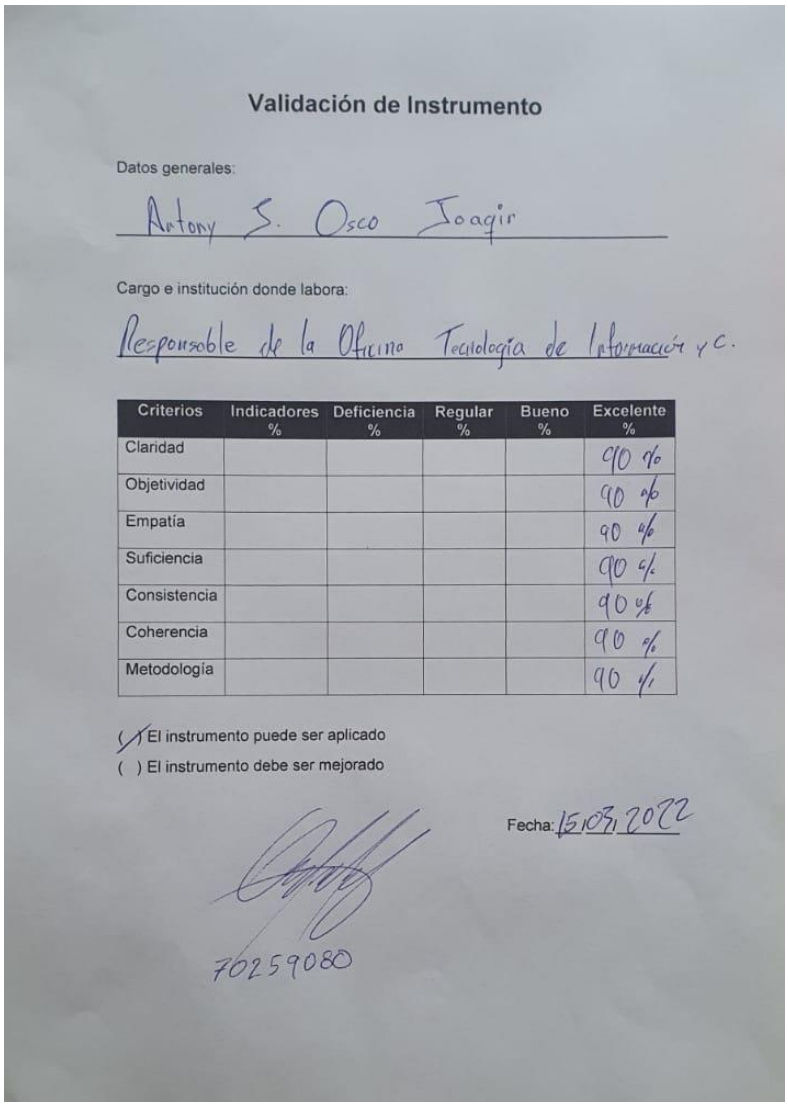
Para un mejor resultado de recolección de datos es que se validó el instrumento con el responsable de la Oficina de Tecnología de Información y Comunicaciones, Figura 7.

b) Universidad Privada de Tacna
   Ing Ricardo Valcarcel Alvarado

Por parte de la Universidad Privada de Tacna la validación lo realiza el asesor asignado, a quien se considera como profesional experto en la Escuela profesional de Ingeniería de Sistemas.

Figura 7

Validación de Instrumento



Validación de Instrumento

Datos generales:

Antony S. Osco Joaqir

Cargo e institución donde labora:

Responsable de la Oficina Tecnología de Información y C.

Criterios	Indicadores %	Deficiencia %	Regular %	Bueno %	Excelente %
Claridad					90 %
Objetividad					90 %
Empatía					90 %
Suficiencia					90 %
Consistencia					90 %
Coherencia					90 %
Metodología					90 %

(✓) El instrumento puede ser aplicado

( ) El instrumento debe ser mejorado

Fecha: 15/03/2022

70259080

Nota. Fuente: Municipalidad Distrital de Ilabaya.

3.4. Procesamiento y análisis de datos

Asimismo, se utilizó el software IBM SPSS 26 (Statiscal Package for Social Sciences) en su versión trial como también fue necesario utilizar Microsoft Office Excel, y posteriormente aplicar la estadística descriptiva para elaborar y obtener resultados en tablas de frecuencia y la estadística inferencial para posteriormente contrastar la hipótesis planteada en la presente investigación.

También utilizamos Alpha de Cronbach para la confiabilidad de los cuestionarios a expertos.

CAPÍTULO IV: RESULTADOS

4.1. Análisis e interpretación de resultados

4.1.1. Confiabilidad de los instrumentos y escala de valoración

Sobre la determinación de la confiabilidad del instrumento aplicado, se planteó y utilizó el estadístico Alpha de Cronbach, donde la interpretación es: Mientras más cercano su valor a 1 implica que el instrumento utilizado es más confiable para la interpretación de resultados.

Para el análisis y determinación de los resultados, se aplicó la Escala de Likert (valores cercanos a 1 implica que se está muy en desacuerdo con lo afirmado en el ítem, y valores cercanos a 5 implica estar muy de acuerdo con lo afirmado en el ítem); se estableció una escala de valoración para un mejor y avanzada análisis de estadística de la variable 1 y variable 2 planteada en esta investigación.

Para el inicio de la obtención de resultados se establece la relación de cada pregunta planteada con su respectivo indicador como se muestra en la Tabla 7, variable 1.

Tabla 7

Indicador – Ítem Sistema de Gestión de Seguridad de la Información

Variable	Dimensiones	Indicadores	Ítem
Sistema de Gestión de Seguridad de la Información	Confidencialidad	Seguridad de Personal	1,2
		Privacidad de la Información	3,4
	Integridad	Seguridad Lógica	5,6
		Seguridad Física y Ambiental	7,8
		Gestión de incidentes de seguridad de información	9,10
		Administración de la operaciones y comunicaciones	11,12,13
	Disponibilidad	Inventario de activos y clasificación de la información	14,15,16
		Procedimiento de respaldo	17,18

Nota. Resultado obtenido en SPSS V.26. Fuente: Cuestionario de SGSI.

Para el inicio de la obtención de resultados se establece la relación de cada pregunta planteada con su respectivo indicador como se muestra en la Tabla 8, variable 2.

Tabla 8

Indicador - Ítem Calidad de servicio de las redes LAN

Variable	Dimensiones	Indicadores	Ítem
Calidad de Servicio de las redes LAN	Confiabilidad	Eficiencia	1,2
		Efectividad	3,4
	Aseguramiento	Confianza	5,6
		Credibilidad	7,8
	Capacidad de respuesta	Tiempo de respuesta	9,10
		Mejora Continua	11,12

Nota. Resultado obtenido en SPSS V.26. *Fuente: Cuestionario de "Calidad de servicio de las redes LAN".*

En primera instancia se realizó el análisis global de la variable "SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN", donde se determinó una Escala de Valoración, en base a las 18 preguntas que considera el instrumento planteado; por lo tanto, sus valores extremos oscilan entre 18 y 90 puntos, Tabla 9. Para el análisis global de la variable "Calidad de servicio de las Redes LAN", se tomaron en cuenta las 12 preguntas planteadas y desplegadas en la entidad; por tanto, sus valores establecidos extremos oscilan entre 12 y 60 puntos, Tabla 10 se tiene:

Tabla 9

Escala de valoración Sistema de Gestión de Seguridad de la Información

Nivel	Intervalo
Sistema de Gestión de Seguridad de la información muy inadecuado	18 – 32
Sistema de Gestión de Seguridad de la información inadecuado	33 – 47
Inteligencia de Negocios regular	48 – 62
Sistema de Gestión de Seguridad de la información adecuado	63 – 77
Sistema de Gestión de Seguridad de la información muy adecuado	78 - 90

Nota. Resultado obtenido en SPSS V.26. Fuente: Cuestionario "SGSI".

Tabla 10

Escala de valoración "Calidad de servicio de las redes LAN"

Nivel	Intervalo
Calidad de Servicio de Redes LAN muy inadecuado	12 – 21
Calidad de Servicio de Redes LAN inadecuado	22 – 31
Calidad de Servicio de Redes LAN regular	32 – 41
Calidad de Servicio de Redes LAN adecuado	42 – 51
Calidad de Servicio de Redes LAN muy adecuado	52 - 60

Nota. Resultado obtenido en SPSS V.26. Fuente: Cuestionario de "Calidad de servicio de las redes LAN".

A través del SPSS 26.0 se obtuvo el resultado estadístico Alpha de Cronbach, siendo el reporte para las dimensiones de las variables, obtenido para ambos instrumentos, como se muestra en la Tabla 11.

Tabla 11

Alpha de Cronbach Sistema de Gestión de Seguridad de la Información

Estadísticas de fiabilidad	
Alfa de Cronbach	**N de elementos**
,914	18

Nota. Resultado obtenido en SPSS V.26. Fuente: Reporte del SPSS 26.

El valor que se obtiene es de 0,914 este resultado implica que la fiabilidad del instrumento aplicado en la investigación es muy adecuada para el desarrollo de la investigación, donde se obtuvo el siguiente resultado Tabla 12.

Tabla 12

Alpha de Cronbach "Calidad de servicio de redes LAN"

Estadísticas de fiabilidad	
Alfa de Cronbach	**N de elementos**
,902	12

Nota. Resultado obtenido en SPSS V.26. Fuente: Reporte del SPSS 26.

El valor que se obtiene es de 0,902 este resultado implica que la fiabilidad del instrumento aplicado es adecuada para el desarrollo de la investigación.

4.1.2. Resultado: Sistema de gestión de seguridad de la información

a) Análisis por dimensión

Análisis realizado para cada dimensión respectivamente estadística descriptiva Tabla 13, preguntas Tabla 14, sexo Tabla 15, rango por antigüedad Tabla16 y cargo Tabla17.

Tabla 13

Confidencialidad

Estadísticos descriptivos			
	N	**Media**	**Desv. típ.**
Confidencialidad	63	2.8571	,51727

Nota. Resultado obtenido del cuestionario donde N es la muestra para posteriormente obtener la media y el desvío respectivamente. Fuente: Cuestionario de “SGSI”.

Tabla 14

Confidencialidad

	Media	**Desv. típ.**
1.1 ¿Se han definido funciones y roles para la seguridad de la información?	2,84	0,745
1.2 ¿Se han definido procedimientos en caso de cese de personal, que incluyan la confidencialidad de la información en la entidad	2,81	0,692
1.3 ¿Existen políticas de seguridad de la información?	2,87	0,635
1.4 ¿Se han adoptado controles que ayuden a resguardar la privacidad de la información?	2,90	0,615

Nota. Resultado obtenido en SPSS V.26. Fuente: Cuestionario de “SGSI”.

Tabla 15

Confidencialidad

	Sexo	
	Masculino	**Femenino**
	Media	**Media**
Confidencialidad	2,8393	2,8714

Nota. Resultado obtenido en SPSS V.26. Fuente: Cuestionario de “SGSI”.

Tabla 16

Confidencialidad

	Rango por Antigüedad		**Estadístico**
Confidencialidad	**Menor a 1 año**	Media	2,7500
		Desv. típ.	,53831
	Entre 1 a 2 años	Media	2,9907
		Desv. típ.	,51179
	Mayor a 2 año	Media	2,7692
		Desv. típ.	,46167

Nota. Resultado obtenido en SPSS V.26. Fuente: Cuestionario de “SGSI”.

Tabla 17

Confidencialidad

	Cargo		**Estadístico**
Confidencialidad	**Administrativo**	Media	3,0000
		Desv. típ.	,43301
	Asistente	Media	2,6250
		Desv. típ.	,58977
	Especialista	Media	2,9375
		Desv. típ.	,47716
	Técnico	Media	3,0833
		Desv. típ.	,25820

Nota. Fuente: Resultado obtenido en SPSS V.26. Cuestionario de “SGSI”.

Análisis

Los resultados que se llegaron a obtener en los cuadros anteriores se relacionan con el dominio denominado “Confidencialidad”; donde el valor medio fue de 2,8571 y una desviación estándar del, 51727, resultado que nos lleva a deducir que el personal de la Municipalidad Distrital de Ilabaya considera que la Confidencialidad en cuanto a seguridad de la información se da a veces. De acuerdo a las preguntas y posteriormente al revisar cada pregunta, el aspecto más relevante de este fue que el personal de la entidad considera que la privacidad de la información para la seguridad de la información se ejerce a veces; siendo el aspecto a reforzar la definición de procedimientos que incluyan la confidencialidad de la información en la entidad.

Siendo el personal masculino los que menos resaltan este dominio, al igual que los trabajadores con menos de 01 año de antigüedad. Al comparar por cargo, son los Técnicos los que más destacan este Dominio.

Continuando con el análisis realizado para cada dimensión respectivamente, en este caso se realizó estadística descriptiva para la dimensión Integridad Tabla 18, preguntas Tabla 19, sexo Tabla 20, rango por antigüedad Tabla 21 y cargo Tabla 22.

Tabla 18

Integridad

Estadísticos descriptivos			
	N	**Media**	**Desv. típ.**
Integridad	63	2.9012	,52728

Nota. Resultado obtenido en SPSS V.26. Fuente: Cuestionario de “SGSI”.

Tabla 19

Integridad

	Media	**Desv. típ.**
1.5 ¿Se realizan evaluaciones periódicas a los accesos concedidos de los usuarios?	2,83	0,773
1.6 ¿Los usuarios cuentan con identificación única en caso de posibles responsabilidades que puedan ser identificadas?	3,06	0,759
1.7 ¿Cree Ud. que las medidas de seguridad física y ambiental utilizadas son suficientes para proteger la	2,78	0,634

información?		
1.8 ¿Se realiza prevención ante pérdidas daños o robos de información?	2,86	0,644
1.9 ¿Existen reportes para incidentes de seguridad de la información?	2,84	0,766
1.10 ¿Se da respuesta a los incidentes según su importancia?	2,94	0,759
1.11 ¿Existen controles que ayuden a estandarizar el intercambio de información?	3,06	0,644
1.12 ¿Existen controles preventivos para identificar el uso de software malicioso virus u otros similares?	3,03	0,803
1.13 ¿Existen procedimientos para la operación de los sistemas?	2,71	0,958

Nota. Resultado obtenido en SPSS V.26. Fuente: Cuestionario *Sistema de Gestión de Seguridad de la Información*.

Tabla 20

Integridad

	Sexo	
	Masculino	**Femenino**
	Media	**Media**
Integridad	2,8294	2,9587

Nota. Resultado obtenido en SPSS V.26. Fuente: Cuestionario *Sistema de Gestión de Seguridad de la Información*.

Tabla 21

Integridad

	Rango por Antigüedad		**Estadístico**
Integridad	**Menor a 1 año**	Media	2,7391
		Desv. típ.	,58374
	Entre 1 a 2 años	Media	3,0370
		Desv. típ.	,46019
	Mayor a 2 año	Media	2,9060
		Desv. típ.	,51088

Nota. Resultado obtenido en SPSS V.26. Fuente: Cuestionario *Sistema de Gestión de Seguridad de la Información.*

Tabla 22

Integridad

	Cargo		Estadístico
Integridad	**Administrativo**	Media	3,0178
		Desv. típ.	,44407
	Asistente	Media	2,7546
		Desv. típ.	,60768
	Especialista	Media	3,0000
		Desv. típ.	,59391
	Técnico	Media	2,8704
		Desv. típ.	,34724

Nota. Resultado obtenido en SPSS V.26. Fuente: Cuestionario *Sistema de Gestión de Seguridad de la Información.*

Análisis

Los resultados encontrados en las tablas anteriores se relacionan con el dominio denominado “Confidencialidad”; cuyo valor medio fue de 2,9012 y una desviación estándar del ,52728, donde los resultados oscilan que el personal de la Municipalidad Distrital de Ilabaya considera que la Integridad en cuanto a seguridad de la información se da a veces. Para ello se analiza por pregunta, el aspecto más destacado para este proceso fue que el personal de la municipalidad considera que la Seguridad Lógica y la Administración de las operaciones y comunicaciones para la seguridad de la información se ejerce a veces; siendo el aspecto a reforzar la seguridad física y ambiental que incluyan la integridad de la información en la entidad.

Siendo el personal masculino los que menos resaltan este dominio, al igual que los trabajadores con menos de 01 año de antigüedad.

Después de realizar los análisis correspondientes de los datos obtenidos del software SPSS V.26. se compara por cargo, donde los Administrativos son los que más destacan este Dominio.

Los análisis para cada dimensión son importantes para el contraste de hipótesis es por ello que se realiza por dimensiones, en este caso se realizó estadística

descriptiva para la dimensión Disponibilidad Tabla 23, preguntas Tabla 24, sexo Tabla 25, rango por antigüedad Tabla 26 y cargo Tabla 27.

Tabla 23

Disponibilidad

Estadísticos descriptivos			
	N	**Media**	**Desv. típ.**
Disponibilidad	63	2.8444	,55001

Nota. Resultado obtenido en SPSS V.26. Fuente: Cuestionario *Sistema de Gestión de Seguridad de la Información.*

Tabla 24

Disponibilidad

	Media	**Desv. típ.**
1.14 ¿Se realiza inventario de activos de información?	2,89	0,698
1.15 ¿Se realiza clasificación de información que ayude a controlar el nivel de riesgo existente en la Municipalidad?	2,87	0,793
1.16 ¿Se toman medidas apropiadas de control asociadas a los riesgos existentes?	2,78	0,750
1.17 ¿Se realizan procedimientos de respaldo periódicamente?	2,83	0,708
1.18 ¿Se realizan pruebas de restauración que garanticen que la información es exacta?	2,86	0,715

Nota. Resultado obtenido en SPSS V.26. Fuente: Cuestionario *Sistema de Gestión de Seguridad de la Información.*

Tabla 25

Disponibilidad

	Sexo	
	Masculino	**Femenino**
	Media	**Media**
Disponibilidad	2,8357	**2,8514**

Nota. Resultado obtenido en SPSS V.26. Fuente: Cuestionario *Sistema de Gestión de Seguridad de la Información.*

Tabla 26

Disponibilidad

	Rango por Antigüedad		Estadístico
Disponibilidad	**Menor a 1 año**	Media	2,8435
		Desv. típ.	,55582
	Entre 1 a 2 años	Media	**2,9481**
		Desv. típ.	,42460
	Mayor a 2 año	Media	2,6308
		Desv. típ.	,72959

Nota. Resultado obtenido en SPSS V.26. Fuente: Cuestionario “SGSI”

Tabla 27

Disponibilidad

	Cargo		Estadístico
Disponibilidad	**Administrativo**	Media	**2,9680**
		Desv. típ.	,47847
	Asistente	Media	2,8500
		Desv. típ.	,55089
	Especialista	Media	2,5750
		Desv. típ.	,75166
	Técnico	Media	2,6667
		Desv. típ.	,48442

Nota. Resultado obtenido en SPSS V.26. Fuente: Cuestionario “SGSI”

Análisis

Los resultados encontrados en las tablas anteriores se relacionan con el dominio denominado “Disponibilidad”; cuyo valor medio fue de 2,8444 y una desviación estándar del ,55001, donde los resultados oscilan que el personal de la Municipalidad Distrital de Ilabaya considera que la Disponibilidad en cuanto a seguridad de la información se da a veces. De acuerdo a las preguntas y al analizar

por pregunta, el aspecto con más relevancia fue que el personal de la municipalidad considera que la Inventario de activos y clasificación de la información para la seguridad de la información se ejerce a veces; siendo el aspecto a reforzar los procedimientos de respaldo que incluyan la disponibilidad de la información en la entidad.

Siendo el personal masculino los que menos resaltan este dominio, al igual que los trabajadores con más de 02 años de antigüedad.

Al comparar por cargo, son los Administrativos los que más destacan este Dominio.

4.1.3. Análisis General: Sistema de gestión de seguridad de la información

Para un entendimiento más completo fue necesario obtener las estadísticas descriptivas para la variable 1 Sistema de Gestión de Seguridad de la Información, asimismo los resultados generales de la variable 1 estadísticos descriptivos Tabla 28, cargo Tabla 29 y rango por antigüedad Tabla 30.

Tabla 28

Sistema de Gestión de Seguridad

Estadísticos descriptivos			
	N	**Media**	**Desv. típ.**
Sistema de Gestión de Seguridad de la Información	63	**51,7619**	8,39876

Nota. Resultado obtenido en SPSS V.26. Fuente: Cuestionario *Sistema de Gestión de Seguridad de la Información.*

Tabla 29

Sistema de Gestión de Seguridad de la Información

Estadísticos descriptivos			
	Cargo		**Estadístico**
Sistema de Gestión de Seguridad de la Información	**Administrativo**	Media	54,00000
		Desv. típ.	7,00000
	Asistente	Media	49,5417

		Desv. típ.	9,53246
	Especialista	Media	51,6250
		Desv. típ.	9,9991
	Tecnico	Media	51,5000
		Desv. típ.	5,71839

Nota. Resultado obtenido en SPSS V.26. Fuente: Cuestionario *Sistema de Gestión de Seguridad de la Información*.

Tabla 30

Sistema de Gestión de Seguridad de Información

		Rango por Antigüedad	**Estadístico**
Sistema de Gestión de Seguridad de la Información	**Menor a 1 año**	Media	49,8696
		Desv. típ.	9,34833
	Entre 1 a 2 años	Media	**54,0370**
		Desv. típ.	7,23497
	Mayor a 2 año	Media	50,3846
		Desv. típ.	8,38191

Nota. Resultado obtenido en SPSS V.26. Fuente: Cuestionario *Sistema de Gestión de Seguridad de la Información.*

Análisis

Después de analizar cada uno de los resultados obtenidos en los indicadores de la variable, se procede a desarrollar un análisis global, lográndose un valor medio de 51,7619 y una desviación estándar de 8,39876; el cual, al identificar en la escala de valoración indica que el nivel denominado “SGSI regular”; es decir, el personal de la Municipalidad de Ilabaya considera que el nivel de SGSI que los caracteriza es regular.

Al comparar por cargo, son los Administrativos los que más destacan esta variable; y al comparar por años de antigüedad, son los trabajadores que se encuentran entre 1 a 2 años de antigüedad los que más destacan al SGSI que los caracteriza.

4.1.4. Resultados: Calidad de servicio de las redes LAN

Los resultados generales por variables son indispensables, es por ello que se desarrolló la estadística descriptiva para la variable 2 Calidad de servicio de las redes LAN, tomando en cuenta sus dimensiones correspondientes, iniciando con la dimensión Confiabilidad donde se obtuvieron los Estadísticos descriptivo Tabla 31, preguntas correspondientes Tabla 32, sexo Tabla 33 y rango por antigüedad Tabla 34 y para finalizar se realizó un análisis de la variable 2.

Tabla 31

Confiabilidad

Estadísticos descriptivos			
	N	**Media**	**Desv. típ.**
Confiabilidad	63	**3,1984**	0,60435

Nota. Resultado obtenido en SPSS V.26. Fuente: Cuestionario "Calidad de servicio de las redes LAN".

Tabla 32

Confiabilidad

	Media	**Desv. típ.**
2.1 ¿La calidad de servicio de redes LAN es eficiente en la Municipalidad Distrital de Ilabaya?	3,02	0,729
2.2 ¿Considera que la eficiencia de las redes LAN es primordial en la Municipalidad Distrital de Ilabaya?	**3,70**	0,927
2.3 ¿Los accesos a la información por medio de la Red LAN hacia los servidores son efectivas?	3,03	0,803
2.4 ¿Qué tan efectiva es la configuración de la Red LAN para tener acceso a los sistemas integrados de la Municipalidad Distrital de Ilabaya?	3,05	0,792

Nota. Resultado obtenido en SPSS V.26. Fuente: Cuestionario de "Calidad de servicio de las redes LAN".

Tabla 33

Confiabilidad

	Sexo	
	Masculino	**Femenino**
	Media	**Media**
Confiabilidad	3,1696	**3,2214**

Nota. Resultado obtenido en SPSS V.26. Fuente: Cuestionario de "Calidad de servicio en las redes LAN"

Tabla 34

Confiabilidad

	Rango por Antigüedad		Estadístico
Confiabilidad	**Menor a 1 año**	Media	3,1522
		Desv. típ.	,47517
	Entre 1 a 2 años	Media	**3,1852**
		Desv. típ.	,73246
	Mayor a 2 año	Media	2,9804
		Desv. típ.	,54154

Nota. Resultado obtenido en SPSS V.26. Fuente: Cuestionario de "Calidad de servicio de las redes LAN".

Análisis

Los resultados encontrados se relacionan con el dominio denominado "Confiabilidad"; cuyo valor medio fue de 3,1984 y una desviación estándar del ,60435, según los resultados obtenidos implica que el personal de la Municipalidad Distrital de Ilabaya considera que la Confiabilidad en cuanto a la calidad de servicio de la red LAN se da a veces. Al detallar por pregunta, el aspecto más relevante de este fue que el personal de la municipalidad considera que la Eficiencia para la calidad de servicio de la red LAN se da a veces; siendo el aspecto a reforzar la Efectividad en el Servicio de la Red LAN en la entidad.

Siendo el personal masculino los que menos resaltan este dominio, al igual que los trabajadores con más de 02 años de antigüedad.

Al comparar por cargo, son los Técnicos los que más destacan este Dominio.

Continuando con el análisis realizado para cada dimensión respectivamente en la variable 2 Calidad de servicio de las redes LAN, en este caso se realizó estadística descriptiva para la dimensión Aseguramiento Tabla 35, preguntas Tabla 36, sexo Tabla 37, rango por antigüedad Tabla 38 y cargo Tabla 39.

Tabla 35

Aseguramiento

Estadísticos descriptivos			
	N	**Media**	**Desv. típ.**
Aseguramiento	63	**2,9841**	0,70120

Nota. Resultado obtenido en SPSS V.26. Fuente: Cuestionario de "Calidad de servicio de las redes LAN".

Tabla 36

Aseguramiento

	Media	**Desv. típ.**
2.5 ¿Cómo le parece el trato que se le da vía telefónica y en el centro de atención en cuanto a fallas de red LAN de comunicación?	2,90	0,837
2.6 ¿Cómo califica la capacidad de respuesta cuando usted utiliza cualquier servicio tecnológico por intermedio de la Red LAN?	2,92	0,829
2.7 ¿Los datos consultados por medio de la Red LAN tienen un alto grado de fiabilidad?	3,02	0,833
2.8 ¿La disponibilidad de la Red LAN en la Municipalidad Distrital de Ilabaya es garantizada por equipo de respaldo?	**3,10**	0,777

Nota. Resultado obtenido en SPSS V.26. Fuente: Cuestionario de "Calidad de servicio de las redes LAN"

Tabla 37

Aseguramiento

	Sexo	
	Masculino	**Femenino**
	Media	**Media**
Aseguramiento	2,9821	**2,9857**

Nota. Resultado obtenido en SPSS V.26. Fuente: Cuestionario de "Calidad de servicio de las redes LAN".

Tabla 38

Aseguramiento

	Rango por Antigüedad		Estadístico
Aseguramiento	**Menor a 1 año**	Media	**3,000**
		Desv. típ.	,54876
	Entre 1 a 2 años	Media	2,9722
		Desv. típ.	,85859
	Mayor a 2 año	Media	2,9808
		Desv. típ.	,62468

Nota. Resultado obtenido en SPSS V.26. Fuente: Cuestionario de "Calidad de servicio de las redes LAN".

Tabla 39

Aseguramiento

	Cargo		Estadístico
Aseguramiento	**Administrativo**	Media	3,0000
		Desv. típ.	,82916
	Asistente	Media	2,7917
		Desv. típ.	,62843
	Especialista	Media	3,0938
		Desv. típ.	,46170
	Técnico	Media	**3,5417**
		Desv. típ.	,33229

Nota. Resultado obtenido en SPSS V.26. Fuente: Cuestionario de "Calidad de servicio de las redes LAN".

Análisis

Los resultados obtenidos en las tablas anteriores se relacionan con el dominio denominado "Aseguramiento"; cuyo valor medio fue de 2,9841 y una desviación estándar del ,70120, según los resultados podemos deducir que el personal de la Municipalidad Distrital de Ilabaya considera que el Aseguramiento en cuanto a la calidad de servicio de la red LAN se da a veces. Al detallar por pregunta, el aspecto

con más relevancia fue que el personal de la municipalidad considera que la Credibilidad en la disponibilidad para la calidad de servicio de la red LAN se da con una regularidad (a veces); siendo el aspecto a reforzar la confianza en el Servicio de la Red LAN en la entidad.

Siendo el personal masculino los que menos resaltan este dominio, al igual que los trabajadores que se encuentran entre 01 y 02 años de antigüedad.

Al comparar por cargo, son los Técnicos los que más destacan este Dominio.

Continuando con el análisis realizado para cada dimensión respectivamente en la variable 2 Calidad de servicio de las redes LAN, en este caso se realizó estadística descriptiva para la dimensión Capacidad de Respuesta Tabla 40, preguntas Tabla 41, sexo Tabla 42, rango por antigüedad Tabla 43 y cargo Tabla 44.

Tabla 40

Capacidad de respuesta

Estadísticos descriptivos			
	N	**Media**	**Desv. típ.**
Capacidad de respuesta	63	**2,4683**	0,66371

Nota. Resultado obtenido en SPSS V.26. Fuente: Cuestionario de “Calidad de servicio de las redes LAN”.

Tabla 41

Capacidad de respuesta

	Media	**Desv. típ.**
2.9 ¿El tiempo de respuesta en atención a requerimientos de redes LAN influye en la seguridad de la información?	**3,00**	0,696
2.10 ¿El tiempo de respuesta de información de calidad es considerable?	**3,00**	0,783
2.11 ¿Existen medios por donde el cliente interno podría realizar algunos comentarios sobre la calidad de servicio de la Red LAN de la entidad?	2,16	0,954
2.12 ¿Se lanzan encuestas y/o cuestionarios para saber la perspectiva desde el usuario interno sobre la calidad de servicio de la red LAN en la Municipalidad Distrital de Ilabaya?	1,71	0,923

Nota. Resultado obtenido en SPSS V.26. Fuente: Cuestionario de “Calidad de servicio de las redes LAN”.

Tabla 42

Capacidad de Respuesta

	Sexo	
	Masculino	**Femenino**
	Media	**Media**
Capacidad de respuesta	2,3839	**2,5357**

Nota. Resultado obtenido en SPSS V.26. Fuente: Cuestionario de "Calidad de servicio de las redes LAN"

Tabla 43

Capacidad de respuesta

	Rango por Antigüedad		Estadístico
Capacidad de respuesta	**Menor a 1 año**	Media	**2,5326**
		Desv. típ.	,66702
	Entre 1 a 2 años	Media	2,5000
		Desv. típ.	,68990
	Mayor a 2 año	Media	2,2885
		Desv. típ.	,61953

Nota. Resultado obtenido en SPSS V.26. Fuente: Cuestionario de "Calidad de servicio de las redes LAN".

Tabla 44

Capacidad de respuesta

	Cargo		Estadístico
Capacidad de respuesta	**Administrativo**	Media	**2,6200**
		Desv. típ.	,63377
	Asistente	Media	2,3021
		Desv. típ.	,73344
	Especialista	Media	2,4688
		Desv. típ.	,63298
	Tecnico	Media	2,5000
		Desv. típ.	,5000

Nota. Resultado obtenido en SPSS V.26. Fuente: Cuestionario de “Calidad de servicio de las redes LAN”

Análisis

Los resultados encontrados en las tablas anteriores se relacionan con el dominio denominado “Capacidad de respuesta”; cuyo valor medio fue de 2,4683 y una desviación estándar del ,66371, según resultados implica que el personal de la Municipalidad Distrital de Ilabaya considera que Capacidad de respuesta del Servicio de red LAN se da a veces o de forma regular. De acuerdo a las preguntas y al detallar por pregunta, el aspecto más relevante fue que el personal de la municipalidad considera que el tiempo de respuesta para la calidad de servicio de la red LAN se da con una regularidad (a veces); siendo el aspecto a reforzar la mejora continua en el Servicio de la Red LAN en la entidad.

Siendo el personal masculino los que menos resaltan este dominio, al igual que los trabajadores con una antigüedad menor de 01 año.

Al comparar por cargo, son los Administrativo los que más destacan este Dominio.

4.1.5. Análisis General: Calidad de servicio de las redes LAN

Para un entendimiento más completo fue necesario obtener las estadísticas descriptivas para la variable 2 Calidad de servicio de las redes LAN, asimismo los resultados generales de la variable 2 estadísticos descriptivos Tabla 45, cargo Tabla 46 y rango por antigüedad Tabla 47.

Tabla 45

Calidad de las redes LAN

Estadísticos descriptivos			
	N	**Media**	**Desv. típ.**
CALIDAD DE LA RED LAN	63	**34,60**	6,89212

Nota. Resultado obtenido en SPSS V.26. Fuente: Cuestionario de “Toma de decisiones”.

Tabla 46

Calidad de las redes LAN

Estadísticos descriptivos			
	Cargo		**Estadístico**
CALIDAD DE LA RED LAN	**Administrativo**	Media	35,0400
		Desv. típ.	7,44133
	Asistente	Media	32,7917
		Desv. típ.	6,61999
	Especialista	Media	35,6250
		Desv. típ.	6,50137
	Técnico	Media	**38,6667**
		Desv. típ.	4,92612

Nota. Resultado obtenido en SPSS V.26. Fuente: Cuestionario de “Calidad de servicio de las redes LAN”.

Tabla 47

Calidad de las redes LAN

	Rango por Antigüedad		**Estadístico**
Mejora Continua	**Menor a 1 año**	Media	**34,7391**
		Desv. típ.	5,42902
	Entre 1 a 2 años	Media	34,6296
		Desv. típ.	8,26088
	Mayor a 2 año	Media	34,3077
		Desv. típ.	6,58767

Nota. Resultado obtenido en SPSS V.26. Fuente: Cuestionario de “Calidad de servicio de las redes LAN”.

Análisis

Después de analizar cada uno de los resultados obtenidos en los indicadores de la variable, se procede a desarrollar un análisis global, lográndose un valor medio de 34,60 y una desviación estándar de 6,89212; el cual, al indicar en la escala de

valoración establece en el nivel denominado “Calidad de Servicio de la Red LAN regular”; es decir, el personal de la Municipalidad Distrital de Ilabaya considera que su nivel de Calidad de Servicio de la Red LAN es regular.

Al comparar por cargo, son los Técnicos los que más destacan esta variable; y al comparar por antigüedad, son los trabajadores con una antigüedad menor a 01 año los que más destacan la Calidad de Servicio de la Red LAN que los caracteriza.

4.2. Contraste de hipótesis

4.2.1. Contraste de hipótesis especifica

a) **La primera hipótesis específica planteada establece que** “El nivel de SGSI que caracteriza a la Municipalidad de Ilabaya es regular”.

En el análisis general de la variable 1, se encontró que un valor medio general fue de 51,76 con una desviación típica de 8,39; que al ubicarlo en la escala de valoración cae en el nivel denominado “Sistema de Gestión de Seguridad de la Información regular”; es decir, el personal de la Municipalidad de Ilabaya considera que el nivel del SGSI que los caracteriza es regular.

Para complementar dichos resultados, se plantea la siguiente prueba de hipótesis para la media de las respuestas afines a la variable 1, de donde se plantea con los siguientes datos y se muestra los resultados en la Tabla 48:

H_0: μ ≥ 63 (SGSI adecuado ó muy adecuado)

H_1: μ < 63 (SGSI regular, inadecuado ó muy inadecuado)

Tabla 48

Planteamiento de hipótesis

1	**Plantear Hipótesis** Ho: El nivel de SGSI que caracteriza a la Municipalidad de Ilabaya **no** es regular H1: El nivel de SGSI que caracteriza a la Municipalidad de Ilabaya es regular
2	**Establecer un nivel de significancia** Nivel de Significancia (alfa) α = 5%
3	**Seleccionar estadístico de prueba:** **a)** T student para una muestra b) T para grupos independientes

c) T para medidas repetidas
d) Análisis de la varianza

4 Verificar el cumplimiento del supuesto de Distribución Normal con la prueba:

Planteamiento de la hipótesis para la normalidad

Ho: Los datos provienen de una distribución normal

H1: Los datos no pro vienen de una distribución normal

Pruebas de normalidad como se muestra en la Tabla 49:

Tabla 49

Pruebas de normalidad Sistema de Gestión de la Seguridad de la Información

Pruebas de normalidad						
	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
Sistema de Gestión de la Seguridad de la información	,081	63	,200*	,982	63	,507
*. Esto es un límite inferior de la significación verdadera.						
a. Corrección de significación de Lilliefors						

Nota. Resultado obtenido en SPSS V.26. Fuente: Cuestionario de Sistema de Gestión de la Seguridad de la Información.

p-valor > 0.05 ==➔ Aceptamos Ho= los datos provienen de una distribución normal

Conclusión= Los datos proviene de una distribución normal

Toma de decisiones

Para la toma de decisiones se realizó la estadística para muestra como se muestra en la Tabla 50.

Tabla 50

Estadística para una muestra "Sistema de Gestión de Seguridad de la Información"

Estadísticas para una muestra				
	N	Media	Desv.	Desv. Error

			Desviación	promedio
Sistema de Gestión de la Seguridad de la información	63	51,7619	8,39876	1,05814

Nota. Resultado obtenido en SPSS V.26. Fuente: Cuestionario de Sistema de Gestión de la Seguridad de la Información.

Para complementar la toma de decisiones se realizó la prueba para una muestra respectivamente, donde se muestra los resultados correspondiente tabla 51.

Tabla 51

Prueba para una muestra "Sistema de Gestión de Seguridad de la Información"

Prueba para una muestra						
	Valor de prueba = 63					
	t	gl	Sig. (bilateral)	Diferencia de medias	95% de intervalo de confianza de la diferencia	
					Inferior	Superior
Sistema de Gestión de la Seguridad de la información	-10,621	62	,000	-11,23810	-13,3533	-9,1229

Nota. Resultado obtenido en SPSS V.26. Fuente: Cuestionario de Sistema de Gestión de la Seguridad de la Información.

P -valor = ,000 * 100 = 0%

Con una probabilidad del error del 0% menor al nivel de significancia del 5% se concluye que: se acepta H1: **El nivel de SGSI que caracteriza a la Municipalidad de Ilabaya es regular**

Nota. Resultado obtenido en SPSS V.26. Fuente: Cuestionario de Sistema de Gestión de la Seguridad de la Información.

b) La segunda hipótesis específica planteada establece que "El nivel de calidad de servicio de la Red LAN en la Municipalidad de Ilabaya es regular".

En el análisis general de la variable 2, se encontró que un valor medio general fue de 34,60 con una desviación típica de 6,89212; que al ubicarlo en la escala de valoración cae en el nivel denominado “Calidad de Servicio de la Red LAN es regular”; es decir, el personal de la Municipalidad Distrital de Ilabaya considera que el nivel de la Calidad de Servicio de la Red LAN es regular.

Para complementar los resultados obtenidos, se establece la siguiente prueba de hipótesis para la media de las respuestas afines a la variable 2, en donde con los siguientes datos se obtiene los resultados en la Tabla 52:

H_0: μ ≥ 32 (Calidad de Servicio de Redes LAN adecuado ó muy adecuado)

H_1: μ < 32 (Calidad de Servicio de Redes LAN regular, inadecuado ó muy inadecuado)

Tabla 52

Planteamiento de hipótesis

1	**Plantear Hipótesis** Ho: El nivel de calidad de servicio de la Red LAN en la Municipalidad de Ilabaya **no** es regular H1: El nivel de calidad de servicio de la Red LAN en la Municipalidad de Ilabaya es regular.
2	**Establecer un nivel de significancia** Nivel de Significancia (alfa) α = 5%
3	**Seleccionar estadístico de prueba:** **e)** T student para una muestra f) T para grupos independientes g) T para medidas repetidas h) Análisis de la varianza
4	**Verificar el cumplimiento del supuesto de Distribución Normal con la prueba:** Planteamiento de la hipótesis para la normalidad Ho: Los datos provienen de una distribución normal

H1: Los datos no pro vienen de una distribución normal

Pruebas de normalidad se muestra en la Tabla 53 donde se muestra los resultados obtenidos de las encuestas:

Tabla 53

pruebas de normalidad "Calidad de Servicio de las redes LAN"

Pruebas de normalidad

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	**gl**	**Sig.**	**Estadístico**	**gl**	**Sig.**
Calidad de Servicio Redes LAN	,091	63	,200*	,977	63	,296

*. Esto es un límite inferior de la significación verdadera.

a. Corrección de significación de Lilliefors

Nota. Resultado obtenido en SPSS V.26. Fuente: Cuestionario de Sistema de Gestión de la Seguridad de la Información.

p-valor > 0.05 ==➔ Aceptamos Ho= los datos provienen de una distribución normal

Conclusión= Los datos proviene de una distribución normal

Toma de decisiones

Para la toma de decisiones se realizó el siguiente cuadro: Estadística para una muestra Tabla 54.

Tabla 54

Estadística para una muestra

Estadísticas para una muestra

	N	**Media**	**Desv. Desviación**	**Desv. Error promedio**
Calidad de Servicio Redes LAN	63	34,6032	6,89212	,86833

Nota. Resultado obtenido en SPSS V.26. Fuente: Cuestionario de Sistema de

Gestión de la Seguridad de la Información.

Para la toma de decisiones se realizó el siguiente cuadro: Prueba para una muestra Tabla 55.

Tabla 55

Prueba para una muestra

Prueba para una muestra						
	Valor de prueba = 32					
	t	gl	Sig. (bilateral)	Diferencia de medias	95% de intervalo de confianza de la diferencia	
					Inferior	Superior
Sum Red LAN	2,998	62	,004	2,60317	,8674	4,3389

Nota. Resultado obtenido en SPSS V.26. Fuente: Cuestionario de Sistema de Gestión de la Seguridad de la Información.

P -valor = ,004 * 100 = 0,4%

Con una probabilidad del error del 0,4% menor al nivel de significancia del 5% se concluye que: se acepta H1: ***El nivel de Calidad de servicio de la Red LAN que caracteriza a la Municipalidad de Ilabaya es regular***

Nota. Resultado obtenido en SPSS V.26. Fuente: Cuestionario de Sistema de Gestión de la Seguridad de la Información.

c) **La tercera hipótesis específica planteada establece que** "Existe una influencia del SGSI sobre la calidad de servicio de las redes LAN en la Municipalidad Distrital de Ilabaya".
   Para el contraste de la hipótesis general se aplicó el eficiente de Correlación de Pearson, siendo el reporte del SPSS 26,0.

   Según los reportes realizados en el software es que se obtuvo los siguientes resultados mostrado enla Figura 8.

Figura 8

Correlaciones

Correlaciones

		Sistema de Gestión de Seguridad de la Informacion	Calidad de Servicio de la Red LAN
Sistema de Gestión de Seguridad de la Informacion	Correlación de Pearson	1	,540**
	Sig. (bilateral)		0,000
	N	63	63
Calidad de Servicio de la Red LAN	Correlación de Pearson	,540**	1
	Sig. (bilateral)	0,000	
	N	63	63

**. La correlación es significativa en el nivel 0,01 (bilateral).

Nota. Se visualiza en la figura que, según los resultados obtenidos de la variable 1 y la variable 2 es que se realiza la correlación de las dos variables Fuente: Ambos instrumentos.

El valor hallado del coeficiente de correlación fue r = 0,540 (valor de p = 0,000); por lo tanto, existe una influencia directa y significativa entre el Sistema de Gestión de la Seguridad de la Información y la Calidad de Servicio de la Red LAN de la Municipalidad Distrital de Ilabaya.

4.2.2. Contraste de hipótesis general

La hipótesis general planteada establece que "**Existe una relación directa y significativa entre el SGSI y la Calidad de Servicio de las redes LAN en la Municipalidad Distrital de Ilabaya.".**

Para contrastar dicha hipótesis específica, se utilizó el estadístico chi-cuadrado; cuyo reporte del SPSS 26,0 es el siguiente: Figura 9.

Figura 9

Estadístico CHI-CUADRADO

		Calidad del Servicio de Red LAN				Total
		Muy Inadecuado	Inadecuado	Regular	Adecuado	
Sistema de Gestión de Seguridad de la Información	Muy Inadecuado	0	2	0	0	2
	Inadecuado	1	5	7	1	14
	Regular	1	9	27	4	41
	Adecuado	0	0	3	3	6
Total		2	16	37	8	63

Nota. Fuente: Ambos instrumentos.

Se realizó también la prueba de Chi-cuadrado como se muestra en la Figura 10.

Figura 10

Prueba de Chi-cuadrado

Pruebas de chi-cuadrado

	Valor	df	Significación asintótica (bilateral)
Chi-cuadrado de Pearson	16,940[a]	9	0,050
Razón de verosimilitud	15,289	9	0,083
Asociación lineal por lineal	9,315	1	0,002
N de casos válidos	63		

a. 12 casillas (75,0%) han esperado un recuento menor que 5. El recuento mínimo esperado es ,06.

Nota. Fuente: Ambos instrumentos.

El valor del chi-cuadrado calculado fue de 16,940 (valor de p = 0,050), se denota que el valor de p es igual al nivel de significancia del 5%; con lo cual, **existe una relación estadísticamente significativa entre el Sistema de Gestión de Seguridad de la Información sobre la Calidad de servicio de la Red LAN en la Municipalidad Distrital de Ilabaya.**

Con el apoyo de los gerentes, jefe de unidad y responsables de oficinas de la Municipalidad Distrital de Ilabaya, es que se logró distribuir satisfactoriamente las 63 encuestas Anexo 04, así mismos se desarrolló al 100% las 30 preguntas planteadas por encuesta Anexo 05, obteniendo como resultado en la Figura 11:

Figura 11

Resultados del cuestionario en Excel

CARGO	SEXO	EDAD	SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION																	CALIDAD DE SERVICIO DE LAS REDES LAN											
			01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	01	02	03	04	05	06	07	08	09	10	11	12
ASISTENTE CONTABLE	M	26	2	3	2	3	3	3	3	3	3	3	2	3	3	3	3	2	3	3	3	3	2	2	2	2	2	2	2	2	1	1
ADMINISTRATIVO CONTABLE	F	29	2	3	3	3	3	3	2	2	3	3	3	3	3	2	2	2	3	3	3	4	3	3	3	3	3	3	3	3	2	2
ADMINISTRATIVO	F	26	2	3	3	3	2	2	2	2	3	3	3	2	2	3	2	2	3	3	3	3	3	2	3	3	2	3	3	3	3	3
ESPECIALISTA	F	34	3	3	4	3	2	3	3	3	2	3	3	2	3	3	3	2	1	1	3	5	3	3	3	2	2	3	3	3	1	1
ASISTENTE CONTABLE	F	37	2	2	2	2	2	3	2	2	2	2	3	3	2	3	2	3	2	2	3	5	3	3	2	3	3	3	3	3	3	1
ADMINISTRATIVO	M	30	4	3	3	3	3	4	4	3	2	3	3	3	3	4	3	3	3	3	2	5	2	3	3	3	3	3	4	3	3	1
GIRADOR	F	28	2	1	3	3	1	2	2	1	1	3	3	4	2	2	2	2	2	2	3	5	2	3	3	3	2	2	2	2	2	1
ASISTENTE MULTIDICIPLINARIO	F	28	3	3	3	3	4	4	3	3	4	4	4	4	4	4	4	4	3	3	4	4	3	3	3	3	4	4	3	4	1	1
ASISTENTE ADMINISTRATIVO	M	25	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	4	4	4	4	4	4	4	4	4	4	3	3
ADMINISTRATIVO	F	29	3	2	3	3	3	3	2	2	2	3	3	2	3	2	2	2	2	2	1	1	1	1	1	1	1	1	1	1	1	1
ADMINISTRATIVO	F	28	3	3	2	2	2	2	2	2	3	3	3	3	3	3	3	3	3	2	4	5	5	5	5	5	4	4	4	4	4	1
ADMINISTRATIVO	F	26	3	3	3	3	2	4	3	3	3	3	2	2	2	4	4	4	4	3	3	3	4	3	2	2	3	3	3	3	3	1
ESPECIALISTA ADMINISTRATIVO	F	35	3	4	3	3	4	4	4	4	4	3	4	4	3	4	4	4	3	3	4	4	3	4	3	3	4	4	3	3	3	1
ADMINISTRATIVO	F	27	4	4	4	4	4	4	3	4	3	3	3	4	3	3	2	3	3	3	4	4	4	3	3	3	4	4	4	4	2	1
ASISTENTE MULTIDICIPLINARIO	F	36	3	3	3	3	4	4	3	3	3	4	3	3	2	2	1	2	2	1	3	3	3	3	3	3	2	2	3	3	1	1
ASISTENTE MULTIDICIPLINARIO	F	34	2	2	3	3	3	3	3	3	4	3	3	3	3	3	4	4	3	3	3	3	3	4	3	4	4	3	3	3	3	3
ADMINISTRATIVO	F	30	4	3	4	4	4	3	4	3	4	5	4	5	5	3	4	3	4	3	3	5	3	4	4	3	4	4	3	4	3	3
ASISTENTE MULTIDICIPLINARIO	F	29	2	3	2	3	3	3	3	3	3	3	2	2	2	3	2	3	3	3	3	3	2	2	1	1	3	3	2	2	1	1
ADMINISTRATIVO	M	26	2	2	3	3	3	2	3	3	3	3	3	3	2	3	2	2	3	3	3	3	2	2	2	2	2	3	3	3	1	1
MULTIDICIPLINARIO	F	26	3	3	4	3	3	3	3	3	2	3	3	2	2	3	3	4	4	4	4	4	3	3	4	3	4	3	3	3	2	2
ASISTENTE MULTIDICIPLINARIO	M	32	3	3	2	2	2	3	2	3	3	3	3	3	3	4	4	4	2	2	3	3	2	2	2	2	1	1	1	1	1	1
ASISTENTE ADMINISTRATIVO	F	26	2	3	2	2	2	2	2	3	3	3	3	4	3	3	3	2	3	3	3	3	3	3	3	3	2	2	3	3	2	2
ADMINISTRATIVO	F	31	4	3	2	3	3	4	3	4	4	3	3	4	4	3	3	3	3	2	3	4	3	3	3	4	3	4	3	3	3	3
ADMINISTRATIVO	M	27	3	3	3	2	3	3	3	2	3	3	3	3	3	3	4	3	2	3	3	3	3	3	2	3	4	3	3	3	3	3
ASISTENTE ADMINISTRATIVO	M	30	2	2	3	2	2	3	2	3	2	2	2	2	3	3	3	2	3	3	3	3	2	2	2	2	3	3	3	3	2	2
ADMINISTRATIVO	M	29	4	4	3	3	3	4	3	3	3	3	3	3	2	2	3	3	3	3	3	3	3	2	2	2	2	3	3	3	1	1
ASISTENTE	M	25	2	3	3	3	2	2	2	3	3	3	3	2	2	3	3	3	3	3	3	4	3	3	3	3	3	3	3	3	1	1
ESPECIALISTA PROCESOS	F	34	4	3	3	4	4	4	4	3	4	3	4	4	4	3	3	3	3	3	4	5	4	4	4	4	4	4	4	4	3	3
ASISTENTE ADMINISTRATIVO	M	28	3	3	3	3	3	2	2	3	2	3	3	3	2	2	2	3	3	3	3	3	3	3	3	2	2	2	2	1	1	1
ADMINISTRATIVO	M	26	3	2	2	2	3	3	3	3	4	4	3	3	2	3	3	3	2	2	3	3	3	3	4	4	4	3	3	4	3	3
SERVIDOR PROFESIONAL	M	27	3	3	3	3	2	2	2	2	3	3	2	3	2	3	2	2	2	2	4	3	3	3	3	3	3	3	3	3	1	1
ASISTENTE ADMINISTRATIVO	M	27	3	2	3	3	4	4	3	3	3	3	3	3	2	3	3	3	4	4	2	5	3	3	3	4	3	3	3	3	3	2
ASISTENTE PROCESOS	F	32	2	2	2	3	3	3	3	3	3	3	2	2	2	3	3	3	2	2	3	3	3	3	2	2	3	3	3	3	3	3
ASISTENTE TECNICO	F	27	3	1	1	1	1	1	1	1	2	1	4	1	1	1	4	1	1	4	1	5	1	4	4	4	2	4	2	2	1	1
ADMINISTRATIVO	M	24	3	3	3	3	4	4	3	3	3	3	3	2	2	2	3	3	3	3	3	3	3	3	2	2	2	3	3	3	1	1
ADMINISTRATIVO	F	27	3	3	4	3	3	4	3	3	3	2	3	3	4	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
ADMINISTRATIVO	M	38	3	4	3	3	3	3	3	4	3	3	3	3	4	3	4	3	4	4	2	5	3	3	3	3	4	4	4	4	4	1
ADMINISTRATIVO	F	31	3	3	3	3	3	2	3	4	3	4	3	4	3	4	3	3	4	4	3	3	3	4	4	3	4	3	4	3	2	1
ADMINISTRATIVO	F	30	3	3	3	4	4	3	3	3	3	4	4	4	3	3	3	3	3	3	3	3	3	4	4	4	4	4	4	4	2	1
ASISTENTE ADMINISTRATIVO	F	34	3	3	3	3	4	4	3	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
ASISTENTE MULTIDICIPLINARIO	F	32	4	4	4	4	3	4	3	3	4	4	4	3	3	4	4	3	3	3	4	4	4	3	2	2	3	3	3	3	2	2
ADMINISTRATIVO	F	29	2	3	3	4	4	4	4	3	4	2	3	4	4	3	3	4	3	4	3	4	4	4	4	3	4	4	4	4	3	4
ASISTENTE ADMINISTRATIVO	F	32	4	4	3	3	3	3	3	3	2	3	4	4	4	4	4	3	3	3	3	5	4	3	3	3	3	3	3	3	1	1
ADMINISTRATIVO	M	37	3	3	3	3	3	3	4	3	4	4	4	3	3	4	3	3	4	4	2	5	3	4	3	3	4	3	3	3	1	1
ADMINISTRATIVO MULTICIPLINARIO	F	27	3	3	2	2	3	2	3	3	3	3	3	3	3	3	3	3	3	3	3	5	1	1	1	1	1	1	2	3	3	3
ADMINISTRATIVO	F	23	4	3	3	4	3	3	3	3	3	3	4	3	4	4	4	3	3	4	3	4	3	2	3	3	3	3	4	3	3	3
TECNICO	M	25	3	3	3	3	3	3	3	3	2	3	3	3	3	2	2	2	2	2	3	4	3	3	4	4	3	3	3	3	2	1
ESPECIALISTA SISTEMAS	M	38	3	3	4	3	3	4	3	3	3	3	4	4	3	2	2	3	3	3	4	5	4	4	3	3	3	3	4	4	3	1
TECNICO SOPORTE	M	23	2	3	3	3	3	2	2	2	3	3	3	3	3	2	2	2	3	3	3	3	3	3	3	4	4	3	3	2	1	1
RESPONSABLE SISTEMAS	M	42	4	3	3	3	3	4	3	3	2	3	3	4	3	3	3	3	3	3	4	4	4	4	3	3	4	4	3	3	2	1
TECNICO	M	24	3	3	4	4	3	4	3	3	2	4	4	4	3	3	3	3	3	3	4	4	4	4	4	4	3	4	3	4	4	2
ECARGADO SOPORTE	M	31	4	3	2	3	2	4	3	3	2	3	4	4	2	3	3	3	3	4	4	4	5	4	4	4	4	4	4	3	3	2
ASISTENTE SOPORTE TECNICO	M	27	4	4	3	3	3	2	4	4	3	4	3	3	3	3	3	4	4	3	2	5	3	4	4	2	4	3	4	3	2	3
ADMINISTRATIVO	M	40	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	2	2
ESPECIALISTA ADMINISTRATIVO	F	31	2	2	3	2	2	2	2	2	3	3	3	3	1	1	1	2	1	1	4	3	3	3	3	3	3	3	3	3	1	1
ESPECIALISTA TECNICO	F	30	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
ESPECIALISTA ADMINISTRATIVO	F	27	2	3	3	3	3	3	3	2	3	3	3	2	3	3	3	3	3	3	2	3	3	2	3	3	3	3	3	3	1	1
ASISTENTE ADMINISTRATIVO	F	29	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
ASISTENTE MULTIDICIPLINARIO	F	29	3	2	2	3	3	3	3	3	2	3	3	2	3	4	2	3	2	3	3	3	3	3	3	2	3	2	3	3	2	1
ESPECIALISTA ADM PRESUPUESTO	M	30	2	2	3	2	1	2	3	3	2	2	3	2	2	3	2	2	2	2	2	2	3	2	2	3	3	3	2	2	2	1
ASISTENTE MULTIDICIPLINARIO	M	29	2	3	3	3	2	3	2	3	3	3	3	3	3	3	2	3	3	3	3	3	3	3	2	3	3	3	3	3	3	1
ASISTENTE ADMINISTRATIVO	M	27	2	2	3	3	2	3	3	3	2	3	3	3	2	3	2	2	2	3	2	4	3	3	2	3	3	3	4	3	2	2
ASISTENTE ADMINISTRATIVO	M	27	1	1	2	2	2	2	2	2	1	1	1	1	1	2	2	3	2	3	2	4	3	3	2	3	3	3	2	3	1	1

Leyenda	
1	Nunca
2	Casi Nunca
3	A veces
4	Casi Siempre
5	Siempre

SEXO	
M	Masculino
F	Femenino

Nota. Resultado obtenido en Microsoft Excel. Fuente: Elaboración propia.

Interpretación: Una vez obtenido los resultados en Microsoft Office Excel Figura 11, se procedió importar los resultados al software IBM SPSS 26 para obtener los resultados estadísticos descriptivo y posteriormente contrarrestar los resultados con la hipótesis planteada:

Para iniciar el desarrollo de los cuadros estadísticos es necesario tener Perdidos 0 como muestra la Tabla 59, la tabla mencionada corresponde a la variable 1 Sistema de Gestión de Seguridad de la Información, mencionada tabla muestra las dimensiones y las encuestas válidas para ser desarrolladas, un total de 63, Perdidos corresponde en caso de ver alguna pregunta no marcada de manera que tenemos 0 Perdidos. Con estos resultados podemos continuar con el desarrollo de los cuadros estadísticos.

Tabla 56

Estadística descriptiva: V.1. SGSI

Estadística Descriptiva: SGSI				
		CONFIDENCIALIDAD (Agrupada)	**INTEGRIDAD (Agrupada)**	**DISPONIBILIDAD (Agrupada)**
N	**Válido**	63	63	63
	Perdidos	0	0	0

Nota. Resultado obtenido en Microsoft Excel. Fuente: Cuestionario de Sistema de Gestión de la Seguridad de la Información.

En la Tabla 60 muestran las dimensiones de la variable 2 calidad de servicio de las redes LAN, obteniendo como resultado 63 casos válidos y 0 casos perdidos, lo cual indica que nuestra base de datos en el software SPSS son correctos, bajo este contexto podemos realizar los procesos estadísticos tales como para la variable 1 y variable 2.

Tabla 57

Estadística descriptiva: V.2. Calidad de servicio de las redes LAN

Estadística descriptiva: Calidad de servicio de las redes LAN			
	CONFIABILIDAD (Agrupada)	**ASEGURAMIENTO (Agrupada)**	**CAPACIDAD DE RESPUESTA (Agrupada)**

N	**Válido**	63	63	63
	Perdidos	0	0	0

Nota. Resultado obtenido en Microsoft Excel. Fuente: Cuestionario de Calidad de Servicio de las Redes LAN.

4.3. Resultados descriptivos

4.3.1. Resultado descriptivo de la variable 1: Sistema de gestión de seguridad de la información

Según se observa en la Tabla 61, muestra los datos válidos en relación a la variable 1, encuestado a 63 usuarios de la Municipalidad Distrital de Ilabaya. La encuesta fue desarrollada bajo la metodología de escala de Likert lo cual consta de 5 respuestas Nunca, Casi nunca, A veces, Casi siempre y Siempre. De igual manera se interpreta de forma gráfica los resultados en la Figura 12, con la finalidad de una visualización amigable, donde muestra con un porcentaje considerable la respuesta "A veces" 57,3%.

Tabla 58

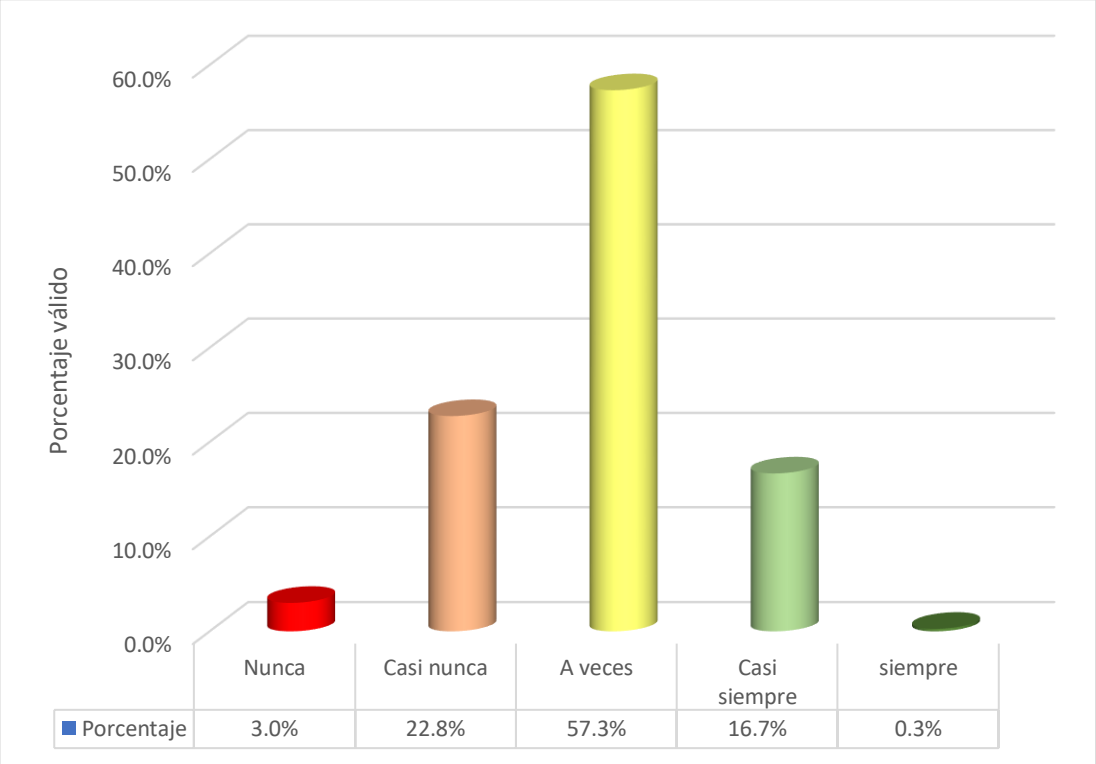
Resultados V.1. Sistema de Gestión de Seguridad de la Información

Sistema de Gestión de Seguridad de la Información				
		Total, SGSI	**Porcentaje**	**Porcentaje válido**
Válido	**Nunca**	34	3,0%	3,0%
	Casi nunca	258	22,8%	22,8%
	A veces	650	57,3%	57,3%
	Casi siempre	189	16,7%	16,7%
	Siempre	3	0,3%	0,3%
	Total	63	100,0%	100,0%

Nota. Resultado obtenido en Microsoft Excel. Fuente: Cuestionario de Sistema de Gestión de la Seguridad de la Información.

Figura 12

Resultado V.1. Sistema de Gestión de Seguridad de la Información



Nota. Resultado obtenido en Microsoft Excel. Fuente: Cuestionario de Sistema de Gestión de la Seguridad de la Información.

4.3.2. Resultado descriptivo de la variable 2: Calidad de Servicio de las redes LAN

Según se observa en la Tabla 62 se muestra los datos como resultado de la variable 2 calidad de servicio de las redes LAN en la Municipalidad Distrital de Ilabaya siendo encuestado a 63 usuarios de la entidad, asimismo se detalla de manera gráfica en la Figura 13, los resultados obtenidos son similares a la variable 1 con un resultado de 49,5% en la respuesta “A veces”.

Tabla 59

Resultado V.2. Calidad de servicio de las redes LAN

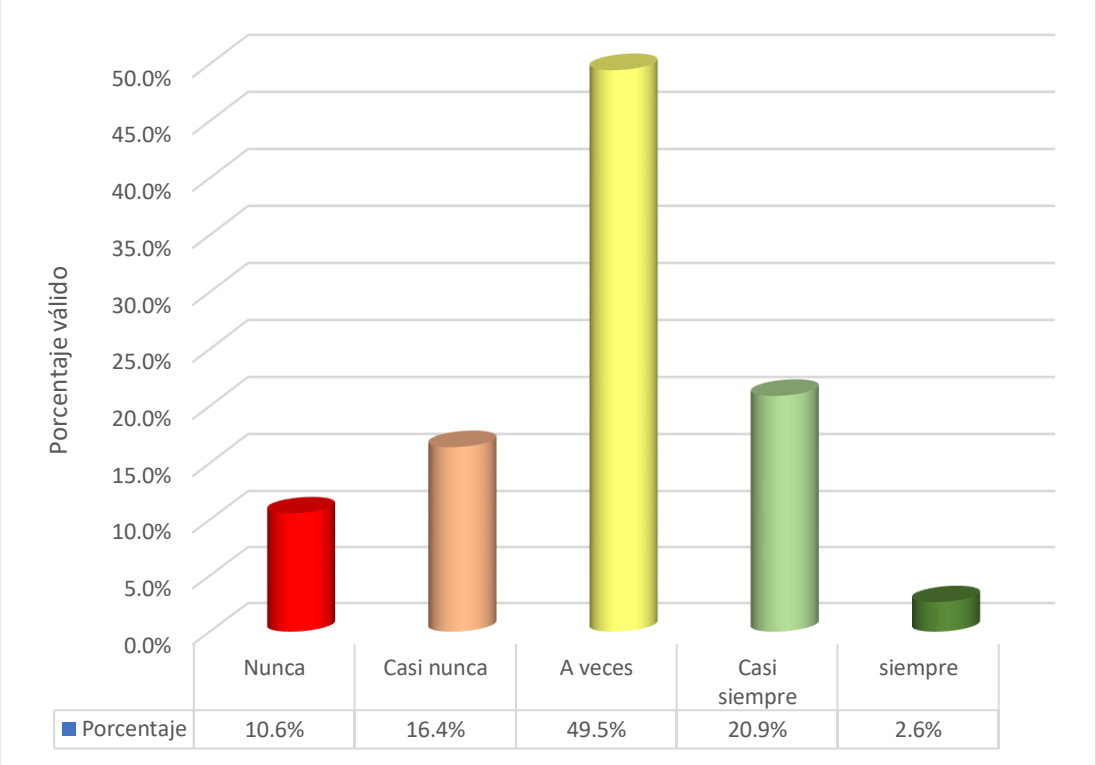
Calidad de Servicio de las Redes LAN				
		Total, SGSI	**Porcentaje**	**Porcentaje válido**
Válido	**Nunca**	80	10.6%	10.6%

	Casi nunca	124	16.4%	16.4%
	A veces	374	49.5%	49.5%
	Casi siempre	158	20.9%	20.9%
	Siempre	20	2.6%	2.6%
	Total	63	100,0%	100,0%

Nota. Resultado obtenido en Microsoft Excel. Fuente: Cuestionario de Calidad de Servicio de las Redes LAN.

Figura 13

Resultado V.2. Calidad de servicio de las redes LAN



Nota. Resultado obtenido en Microsoft Excel. Fuente: Cuestionario de Calidad de Servicio de las Redes LAN.

4.3.3. Resultado descriptivo de la variable 1 y variable 2

En la Tabla 63 y la Figura 14 se muestra los resultados de las dos variables variable 1 y variable 2 respectivamente, obteniendo como resultado al 100% de las encuestas, desarrolladas por 63 usuarios de la entidad Municipalidad Distrital de Ilabaya.

Tabla 60

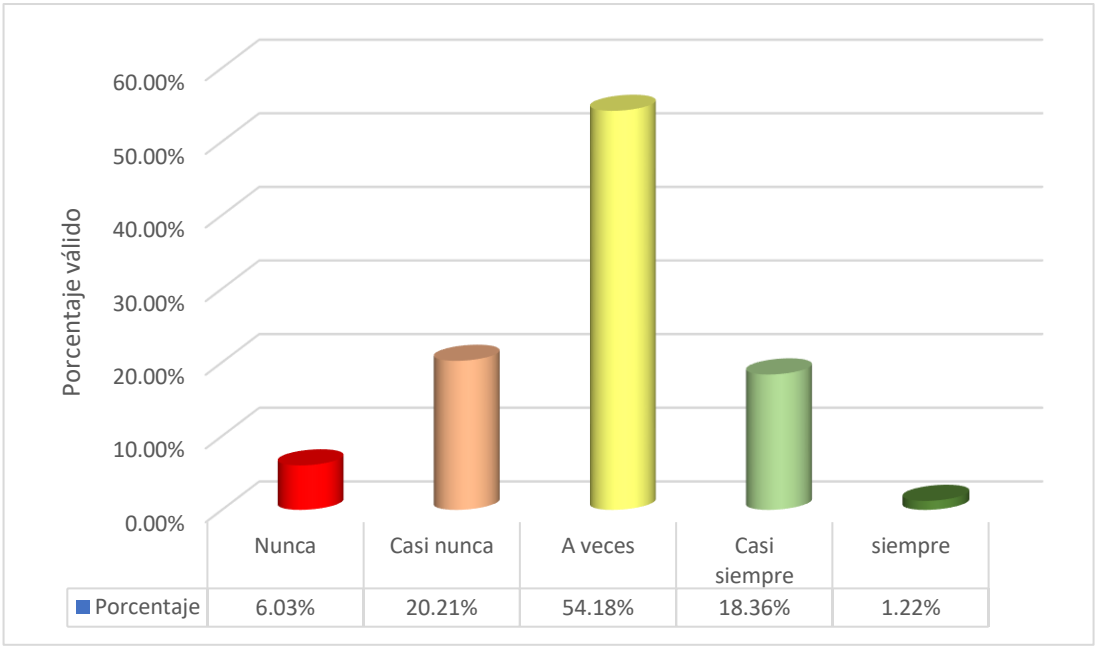
Resultado V.1 Sistema de Gestión de Seguridad de la Información y V.2 Calidad de Servicio de las Redes LAN

SGSI y Calidad de Servicio de las Redes LAN				
		Total	**Porcentaje**	**Porcentaje válido**
Válido	**Nunca**	114	6.03%	6.03%
	Casi nunca	382	20.21%	20.21%
	A veces	1024	54.18%	54.18%
	Casi siempre	347	18.36%	18.36%
	Siempre	23	1.22%	1.22%
	Total	63	100,0%	100,0%

Nota. Resultado obtenido en Microsoft Excel. Fuente: Cuestionario de las variables.

Figura 14

Resultado V.1 Sistema de Gestión de Seguridad de la Información y V.2 Calidad de Servicio de las Redes LAN



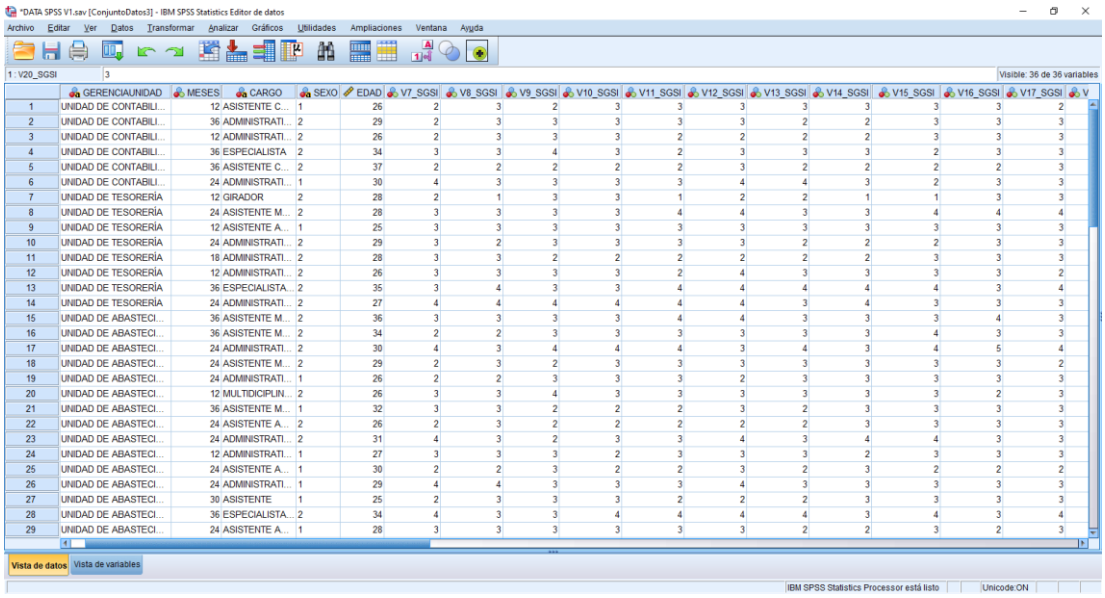
Nota. Resultado obtenido en Microsoft Excel. Fuente: Cuestionario de las variables.

4.3.4. Resultado descriptivo de frecuencia

Para un correcto análisis de datos se importó los resultados de la encuesta en SPSS creando una Base de Datos como se muestra en la Figura 15, y posteriormente realizar los análisis descriptivos de frecuencia, sin antes olvidar que los datos deben ser ingresados correctamente como muestra en la Tabla 64.

Figura 15

Base de Datos en SPSS V.26



Nota. Resultado obtenido en SPSS V.26. Fuente: Elaboración propia.

Tabla 61

Encuestas válidas

Estadísticos		
	Sexo	
N	**Válido**	63
	Perdidos	0

Nota. Resultado obtenido en SPSS V.26. Fuente: Elaboración propia.

Como podemos observar en la Tabla 65 y la Figura 16 los usuarios que más participaron en la encuesta son de género Femenino con 55,56% a diferencia del género Masculino con 44,44%.

Tabla 62

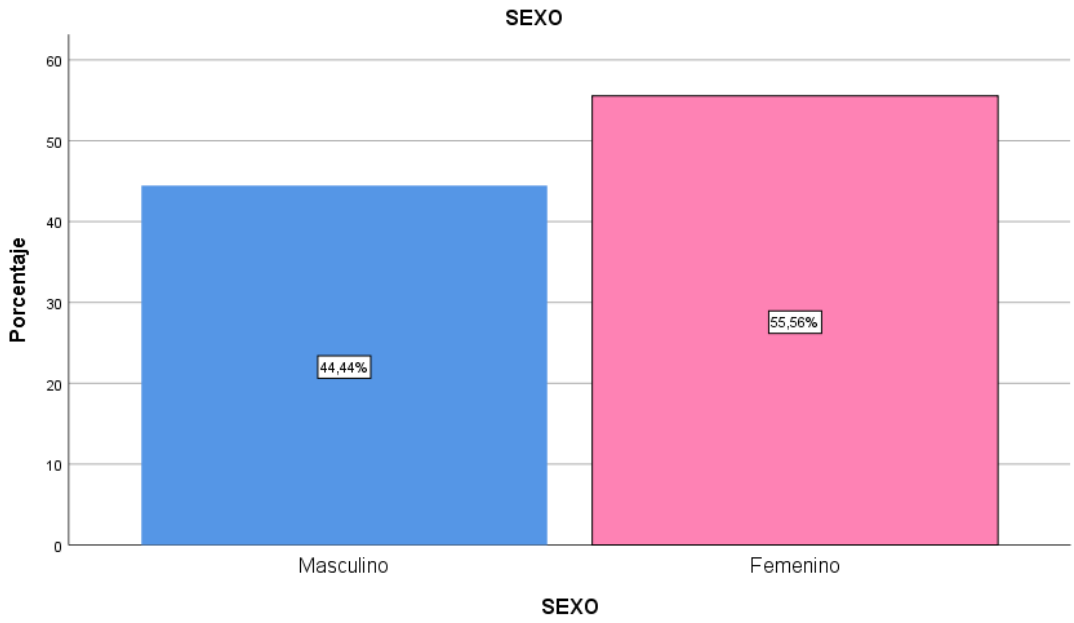
Resultado de Sexo / Género

Sexo					
		Frecuencia	**Porcentaje**	**Porcentaje válido**	**Porcentaje acumulado**
Válido	Masculino	28	44,4	44,4	44,4
	Femenino	35	55,6	55,6	100,0
	Total	63	100,0	100,0	

Nota. Resultado obtenido en SPSS V.26. Fuente: Elaboración propia.

Figura 16

Resultado Sexo / Género



Nota. Resultado obtenido en SPSS V.26. Fuente: Elaboración propia.

Cómo se puede observar en la Tabla 66, 67 y la Figura 17, son los resultados promedio de edad de los usuarios de la entidad pública Municipalidad Distrital de Ilabaya encuestada a 63 usuarios, se puede considerar que cuenta con trabajadores jóvenes.

Tabla 63

Resultado Edad

Estadísticos		
EDAD		
N	**Válido**	63
	Perdidos	0
Moda		27

Nota. Resultado obtenido en SPSS V.26. Fuente: Elaboración propia.

Tabla 64

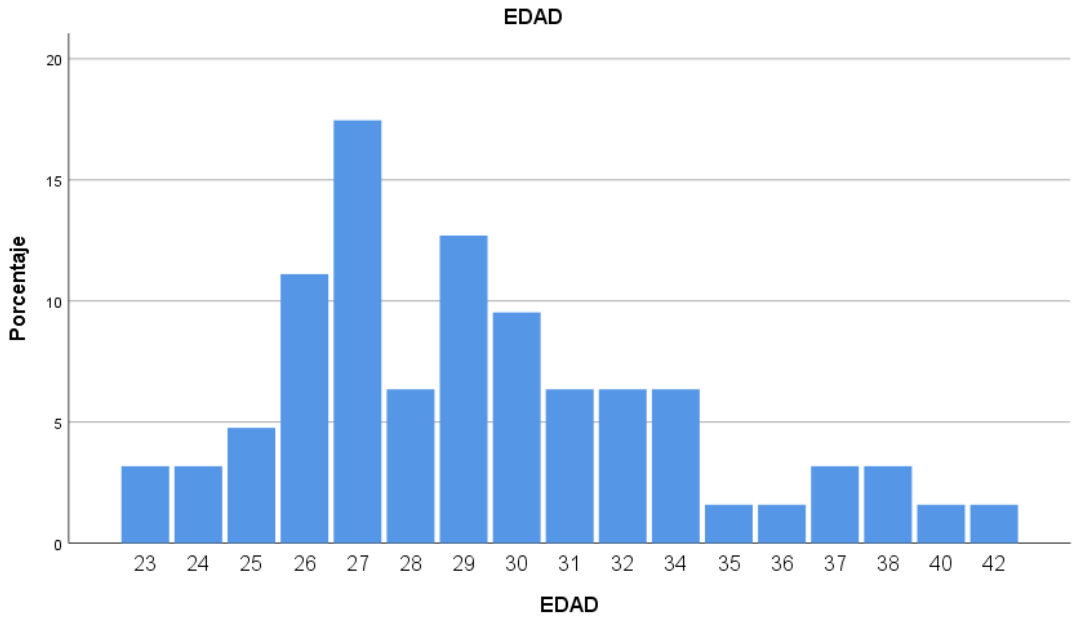
Total Edad

Edad					
		Frecuencia	**Porcentaje**	**Porcentaje válido**	**Porcentaje acumulado**
Válido	23	2	3,2	3,2	3,2
	24	2	3,2	3,2	6,3
	25	3	4,8	4,8	11,1
	26	7	11,1	11,1	22,2
	27	11	17,5	17,5	39,7
	28	4	6,3	6,3	46,0
	29	8	12,7	12,7	58,7
	30	6	9,5	9,5	68,3
	31	4	6,3	6,3	74,6
	32	4	6,3	6,3	81,0
	34	4	6,3	6,3	87,3
	35	1	1,6	1,6	88,9
	36	1	1,6	1,6	90,5
	37	2	3,2	3,2	93,7
	38	2	3,2	3,2	96,8
	40	1	1,6	1,6	98,4
	42	1	1,6	1,6	100,0
	Total	63	100,0	100,0	

Nota. Resultado obtenido en SPSS V.26. Fuente: Elaboración propia.

Figura 17

Resultado Edad



Nota. Resultado obtenido en SPSS V.26. Fuente: Elaboración propia.

En la Tabla 68 y la Figura 18 la Unidad de Abastecimiento perteneciente a la Gerencia de Administración y Finanzas es oficina con más personal con relación a SGSI y Calidad de servicio de las redes LAN.

Tabla 65

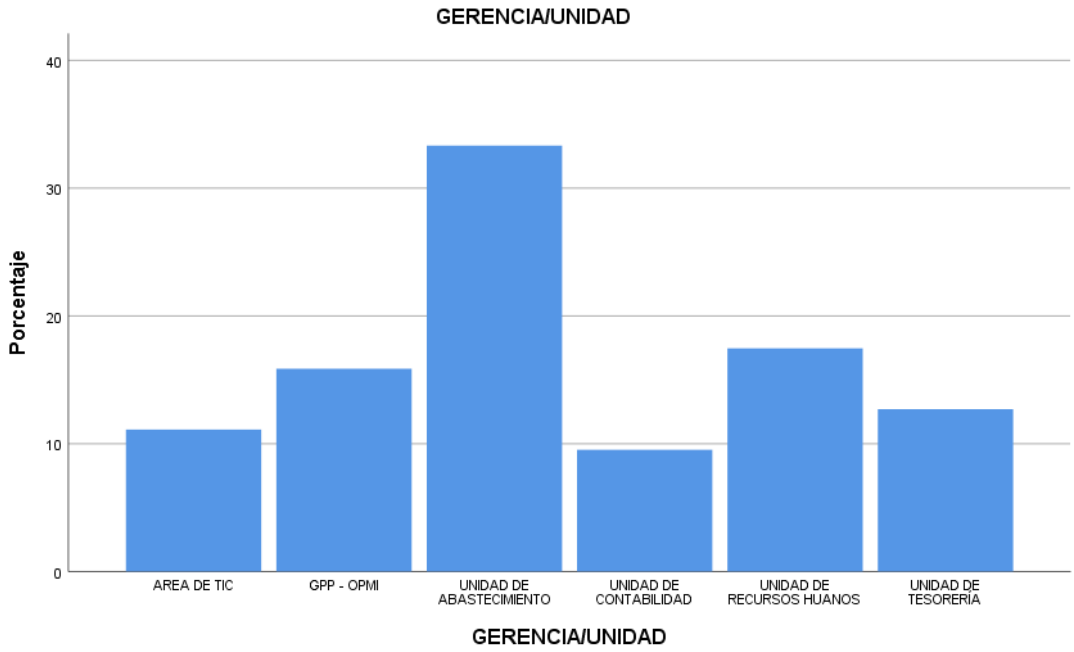
Resultado Gerencia / Unidad

GERENCIA/UNIDAD					
		Frecuencia	**Porcentaje**	**Porcentaje válido**	**Porcentaje acumulado**
Válido	AREA DE TIC	7	11,1	11,1	11,1
	GPP - OPMI	10	15,9	15,9	27,0
	UNIDAD DE ABASTECIMIENTO	21	33,3	33,3	60,3
	UNIDAD DE CONTABILIDAD	6	9,5	9,5	69,8
	UNIDAD DE RECURSOS HUANOS	11	17,5	17,5	87,3
	UNIDAD DE TESORERÍA	8	12,7	12,7	100,0
	Total	63	100,0	100,0	

Nota. Resultado obtenido en SPSS V.26. Fuente: Elaboración propia.

Figura 18

Resultado Gerencia / Unidad



Nota. Resultado obtenido en SPSS V.26. Fuente: Elaboración propia.

En la Tabla 69, 70 y la Figura 19 se puede observar los resultados válidos, frecuencia y porcentaje, los resultados de periodo laboral se interpretó por meses para un mejor análisis en el software SPSS, obteniendo como resultado 24 meses correspondiente a 2 años, ante estos resultados podemos deducir que la mayoría del personal encuestado cuenta con experiencia en la entidad pública Municipalidad Distrital de Ilabaya.

Tabla 66

Resultado Estadístico Periodo Laboral

Estadísticos		
Periodo Laboral		
N	Válido	63
	Perdidos	0
Moda		24

Nota. Resultado obtenido en SPSS V.26. Fuente: Elaboración propia.

Tabla 67

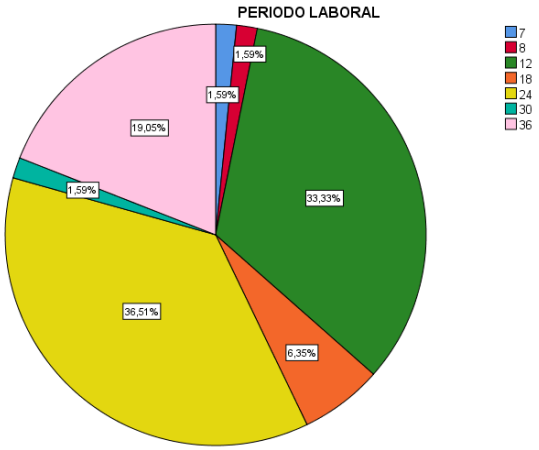
Total periodo laboral

Periodo Laboral					
		Frecuencia	**Porcentaje**	**Porcentaje válido**	**Porcentaje acumulado**
Válido	7	1	1,6	1,6	1,6
	8	1	1,6	1,6	3,2
	12	21	33,3	33,3	36,5
	18	4	6,3	6,3	42,9
	24	23	36,5	36,5	79,4
	30	1	1,6	1,6	81,0
	36	12	19,0	19,0	100,0
	Total	63	100,0	100,0	

Nota. Resultado obtenido en SPSS V.26. Fuente: Elaboración propia.

Figura 19

Total periodo laboral



Nota. Resultado obtenido en SPSS V.26. Fuente: Elaboración propia.

Los resultados por cargo se pueden apreciar en la Tabla 71 y la Figura 20, donde se visualiza los resultados de los cargos del personal de la entidad, siendo los Administrativos que más relación tienen con los sistemas integrados de la entidad.

Tabla 68

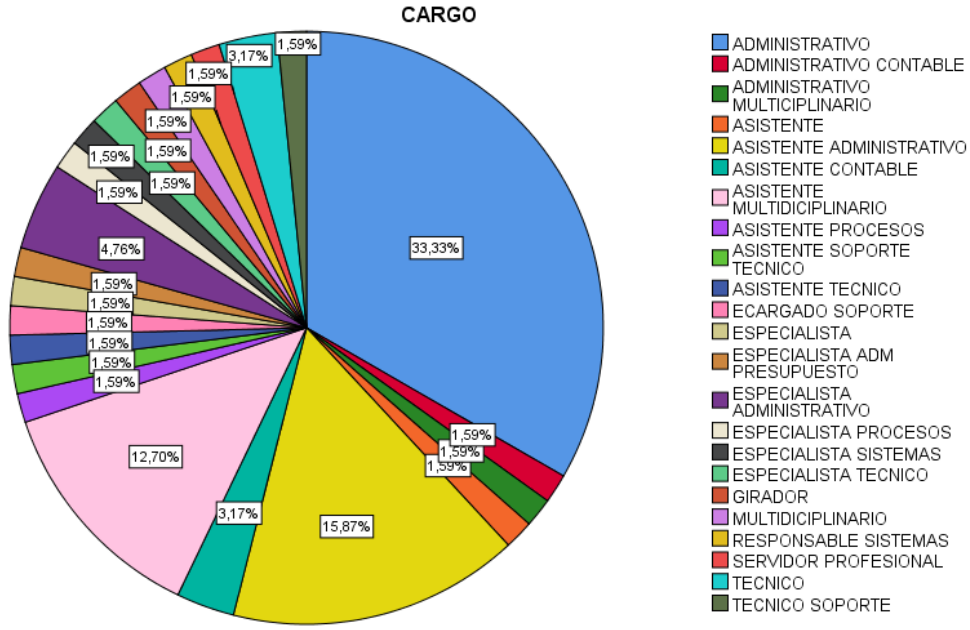
Resultados cargo.

Cargo					
		Frecuencia	**Porcentaje**	**Porcentaje válido**	**Porcentaje acumulado**
Válido	ADMINISTRATIVO	21	33,3	33,3	33,3
	ADMINISTRATIVO CONTABLE	1	1,6	1,6	34,9
	ADMINISTRATIVO MULTICIPLINARIO	1	1,6	1,6	36,5
	ASISTENTE	1	1,6	1,6	38,1
	ASISTENTE ADMINISTRATIVO	10	15,9	15,9	54,0
	ASISTENTE CONTABLE	2	3,2	3,2	57,1
	ASISTENTE MULTIDICIPLINARIO	8	12,7	12,7	69,8
	ASISTENTE PROCESOS	1	1,6	1,6	71,4
	ASISTENTE SOPORTE TECNICO	1	1,6	1,6	73,0
	ASISTENTE TECNICO	1	1,6	1,6	74,6
	ECARGADO SOPORTE	1	1,6	1,6	76,2
	ESPECIALISTA	1	1,6	1,6	77,8
	ESPECIALISTA ADM PRESUPUESTO	1	1,6	1,6	79,4
	ESPECIALISTA ADMINISTRATIVO	3	4,8	4,8	84,1
	ESPECIALISTA PROCESOS	1	1,6	1,6	85,7
	ESPECIALISTA SISTEMAS	1	1,6	1,6	87,3
	ESPECIALISTA TECNICO	1	1,6	1,6	88,9
	GIRADOR	1	1,6	1,6	90,5
	MULTIDICIPLINARIO	1	1,6	1,6	92,1
	RESPONSABLE SISTEMAS	1	1,6	1,6	93,7
	SERVIDOR PROFESIONAL	1	1,6	1,6	95,2
	TECNICO	2	3,2	3,2	98,4
	TECNICO SOPORTE	1	1,6	1,6	100,0
	Total	63	100,0	100,0	

Nota. Resultado obtenido en SPSS V.26. Fuente: Elaboración propia.

Figura 20

Resultado cargo.



Nota. Resultado obtenido en SPSS V.26. Fuente: Elaboración propia.

CAPÍTULO V: DISCUSIÓN

Para el inicio de una implementación de SGSI es necesario realizar un análisis de estado a la entidad pública Municipalidad Distrital de Ilabaya, en este caso se realizó una correlación de SGSI y la Calidad de servicio de las redes LAN.

Los resultados obtenidos en la presente investigación se realizaron mediante la técnica encuesta y como instrumento cuestionario de escala Likert de cinco ítems en ese sentido se procede a desarrollar un análisis global, lográndose un valor medio de 51,7619 y una desviación estándar de 8,39876; el cual, al ubicarlo en la escala de valoración cae en el nivel denominado “SGSI regular”; es decir, el personal de la Municipalidad de Ilabaya considera que el nivel de SGSI que los caracteriza es regular.

Después de analizar cada uno de los resultados obtenidos en los indicadores de la variable, se procede a desarrollar un análisis global, lográndose un valor medio de 34,60 y una desviación estándar de 6,89212; el cual, al indicar en la escala de valoración establece que el nivel denominado “Calidad de Servicio de la Red LAN regular”; es decir, el personal de la Municipalidad Distrital de Ilabaya considera que su nivel de Calidad de Servicio de la Red LAN es regular.

La relación de variables en esta investigación indica que existe una influencia directa y significativa entre el SGSI y la calidad de servicio de las redes LAN en la Municipalidad Distrital de Ilabaya.

La iniciación de un SGSI en una entidad pública es de suma importancia por el constante cambio de gestión, esto conlleva a una mala administración de activos de información siendo la investigación “SGSI y su relación con la calidad de servicio de las redes LAN en la Municipalidad Distrital de Ilabaya” un gran aporte para la entidad.

CONCLUSIONES

En base a los resultados estadísticos planteado a la variable 1 se llega a la conclusión que con una probabilidad del error del 0% menor al nivel de significancia del 5% se caracteriza el nivel de SGSI es regular en la Municipalidad Distrital de Ilabaya.

En base a los resultados estadísticos planteado a la variable 2 se llega a la conclusión que con una probabilidad del error del 0% menor al nivel de significancia del 5% se caracteriza el nivel de Calidad de servicio de las redes LAN es regular en la Municipalidad Distrital de Ilabaya.

Para el contraste de correlación de Pearson se determinó que el valor hallado del coeficiente de correlación fue r = 0,540 (valor de p = 0,000); por lo tanto, existe una influencia directa y significativa entre el SGSI y la Calidad de Servicio de la Red LAN de la Municipalidad Distrital de Ilabaya.

De acuerdo al análisis estadístico realizado se llega a la conclusión que “Existe una relación directa y significativa entre el SGSI y la Calidad de Servicio de las redes LAN en la Municipalidad Distrital de Ilabaya.”, llegando a la conclusión que es evidencia necesaria para el inicio de la implementación de un SGSI, lo cual se planteó al área encargada el diseño de SGSI iniciando con un análisis situacional de la entidad posteriormente se desarrolló políticas y controles de seguridad para la Municipalidad distrital de Ilabaya.

Asimismo, es necesario resaltar los riesgos por la cual pasa la seguridad de información en las redes LAN de la entidad, es por ello que se desarrolló un sistema de control de riesgos como parte de un SGSI para la entidad con la finalidad de poder monitorear los riesgos definidos para los activos de la información que están involucrados en el servicio de la Red LAN de la municipalidad distrital de Ilabaya.

RECOMENDACIONES

Al determinar el nivel regular de SGSI se recomienda asignar un personal especializado y permanente para dar inicio de implementación de sistemas de seguridad para el respaldo de la información y el aseguramiento de activos informáticos cumpliendo políticas y controles de seguridad bajo la Norma Técnica Peruana ISO27001.

Se recomienda una capacitación de seguridad de información y la calidad de servicio de redes LAN en la entidad resaltando la cultura de buenas prácticas en cuanto a seguridad de la información y las funciones que debe cumplir como usuario de la entidad pública Municipalidad Distrital de Ilabaya.

Al determinar la existencia de una influencia directa y significativa entre el SGSI y la Calidad de Servicio de la Red LAN se recomienda el inicio de implementación de seguridad de información mediante un diseño de Sistema de Gestión de Seguridad de la Información en la Municipalidad distrital de Ilabaya.

Al obtener resultados estadísticos como regular tanto para la variable 1 y la variable 2 se recomienda implementar un área denominada Oficina de Seguridad de Información en un acuerdo de concejo municipal con el señor alcalde, regidores y gerente municipal, con los documentos correspondientes e iniciar con los tramites de SGSI para el resguardo de la información y una mejor organización de activos asegurando el desempeño de la entidad.

Se recomienda la capacitación del sistema desarrollado a quien se denomina sistema de control de riesgos, como parte del diseño del SGSI para un control adecuado de los activos de información y la administración de estos, con la finalidad de mantener una sincronía en diferentes gestiones de gobierno.

REFERENCIAS BIBLIOGRÁFICAS

Berry, L. L., Bennett, D. R., & Brown, C. W. (1989). Calidad de Servicio. Ediciones Diaz de Santos.

Blas Z., W. D., & Pretell R., G. F. (2020). Modelo de seguridad de la información para mejorar la gestión informática en la Municipalidad Distrital de Florencia de Mora. Trujillo - Perú.

Cáceda Rodríguez, C. R. (2021). Modelo dinámico para la gestión de seguridad de la infraestructura de las tecnologías de información y comunicación. Lima.

Cacuango Lagla, S. E. (2019). Evaluación de una Red LAN para el establecimiento de las Políticas de la Calidad de Servicio. Quito.

Castro Siguas, J. J. (2018). 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, Callao - 2017. Lima - Callao.

Ccesa Quincho, M. (2017). Diseño de un sistema de seguridad de la información bajo la NTP ISO/IEC 27001:2014 para la Municipalidad Provincial de Huamanga, 2016. Ayacucho.

Composer. (s.f.). Composer. Obtenido de Composer: https://getcomposer.org/

Coque V., J., & Kujundzic R., M. D. (2018). Uso de la seguridad de la información en la dirección de proyectos. Santiago de Cali.

Diaz Lara, V. L. (2021). Percepción de la implementación de la NTP-ISO/IEC 27001:2014 en base a la información documentada del gobierno central del Perú, año 2021. Lima.

Felizzola C., L. M., Navarro C., A. J., Lizcano R., R. O., & Guerrero S., D. F. (2019). Diseño del sistema de gestión de seguridad de la información SGSI basado en el estándar ISO 27001, en la Universidad popular del Cesar, seccional Aguachica. Ocaña.

Fernado Q., Y., & Torrado G., W. S. (2015). Planeación del sistema de gestión de seguridad de la información para la empresa Katalinda shoes. Ocaña.

Guerra Aleman, E. (2020). Sistema de gestión para la seguridad de la información basado en metodología de identificación y análisis de riesgo en la biblioteca de la universidad de la costa. Barranquilla.

Huergo, J. (2004). Los procesos de gestión. Comunicación en las organizaciones públicas. Provincia de Bs.

Ilabaya, M. D. (s.f.). Municipalidad Distrital de Ilabaya. Obtenido de Municipalidad Distrital de Ilabaya: https://www.gob.pe/muniilabaya

Laborde, S., Ressi, S., & Rivoir, A. (2006). Diseño de topologías de red confiables.

Laravel. (s.f.). Laravel. Obtenido de Laravel: https://laravel.com/

Ley l., N. V., Granda A., D. M., Benítez F., C. R., & Guamán G., V. J. (2021). Eficacia y eficiencia de la seguridad de las redes LAN. Cantón Pasaje. Sociedad & Tecnología.

PHP. (s.f.). PHP. Obtenido de PHP: https://www.php.net/

República del Perú. (08 de Enero de 2016). Resolución Ministerial. N° 004-2016-PCM . Lima, Perú.

Rodríguez Criollo, A. J. (2016). Evolución de las redes de telecomunicaciones y calidad de servicio en redes de nueva generación NGN en el Ecuador. Quito.

Sampieri, R. H. (2018). Metodología de la investigación: las rutas cuantitativas, cualitativas y mixta.

Trujillo Niebles, W. A. (2020). Diseño de controles y políticas para la seguridad de la información en la red LAN en el Hotel Pipaton. Barrancabermaja - Santander.

Tufiño Galán, A. C. (2018). Diseño de un modelo de seguridad de información en redes LAN. Quito.

Universidad Rafael Belloso Chacín URBC. (2011). Criterios de calidad de servicio para la evaluacion de la gestion de redes LAN. Revista Electrónica de Estudios Telemáticos.

Valencia D., F. J., & Orozco A., M. (2017). Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC. Revista Ibérica de Sistemas e Tecnologias de Informação.

Vergara Quiroz, G. (2016 - 2017). Seguridad de información y calidad de servicio en la Universidad Nacional Federico Villarreal. Perú.

XAMPP. (s.f.). XAMPP. Obtenido de XAMPP: https://www.apachefriends.org/es/index.html

Zheng Huang, L. P. (2017). DISEÑO E IMPLEMENTACIÓN DE UNA RED LAN PARA LA EMPRESA PALINDA. Quito.

ANEXOS

Para acceder a los anexos digital ingresar al siguiente link:

https://drive.google.com/drive/folders/1-wuNtrwFLIuHJsDO29T23eBDfzU4jhoX?usp=sharing

Anexo 1. Matriz de consistencia

PROBLEMA	OBJETIVOS	HIPÓTESIS	VARIABLES E INDICADORES	METODOLOGÍA
Problema principal ¿Cuál es la relación entre el SGSI y la calidad de Servicio de la Red LAN en la Municipalidad Distrital de Ilabaya?	**Objetivo principal** Determinar la relación entre el SGSI y la calidad de servicio de la Red LAN en la Municipalidad Distrital de Ilabaya.	**Hipótesis Principal** Existe una relación directa y significativa entre el SGSI y la Calidad de Servicio de las redes LAN en la Municipalidad Distrital de Ilabaya.	**V.I.** Sistema de Gestión de Seguridad de la Información **INDICADORES** Confidencialidad Integridad Disponibilidad	**1. Tipo de investigación** Descriptivo Correlacional **2. Diseño de investigación** No experimental **3. Nivel de investigación** Aprehensivo **4. Población** 93 **5.Muestra :** **63** **6.Técnicas** Encuesta **7. Instrumentos** Cuestionario
Problemas específicos ¿Cuál es nivel del SGSI que caracteriza a la Municipalidad Distrital de Ilabaya? ¿Cuál es el nivel de Calidad de Servicio de la Red LAN que caracteriza a la Municipalidad Distrital de Ilabaya ? ¿Cómo influye el SGSI en la calidad de Servicio de la Red LAN en la Municipalidad Distrital de Ilabaya?	**Objetivos específicos** Determinar el nivel del SGSI que caracteriza a la Municipalidad Distrital de Ilabaya. Determinar el nivel de calidad de servicio de redes LAN que caracteriza a la Municipalidad Distrital de Ilabaya. Determinar la influencia del SGSI en la calidad de servicio de Redes LAN en la Municipalidad Distrital de Ilabaya.	**Hipótesis especificas** El nivel del SGSI que caracteriza a la Municipalidad de Ilabaya es regular. El nivel de calidad de servicio de la Red LAN en la Municipalidad de Ilabaya es regular. Existe una influencia del SGSI sobre la calidad de servicio de las redes LAN en la municipalidad de Ilabaya.	**V.D.** Calidad de servicio de redes LAN **INDICADORES** Confiabilidad Aseguramiento Resultado del proceso	

Anexo 2. Desarrollo

Sistema de Gestión de Seguridad de la Información en la Municipalidad Distrital de Ilabaya

La presente investigación de tesis se desarrolló con la finalidad de dar inicio a la regularización de las normas internacionales ISO 27001, cabe resaltar que la republica de Perú cuenta con una Norma Técnica Peruana ISO/IEC27001:2014, asimismo el estado hace público la implementación de la noma mencionada en entidades públicas Anexo 02, lo cual trabaja en base al estándar ISO 27001.

Para su implementación se realizó una investigación de correlación de sistema de gestión de seguridad de la información y su relación con la calidad de servicio de las redes LAN en la Municipalidad Distrital de Ilabaya, con la finalidad de averiguar el estado situacional de la entidad en relación a seguridad de la información en redes LAN.

De acuerdo con los resultados de la investigación es que plantearemos la estructura de un sistema de gestión de seguridad y el diseño de un sistema para optimizar los riesgos y la mejor fluidez de la información en la estructura de red de la Municipalidad Distrital de Ilabaya, siguiendo los procedimientos ya establecidos por la normal internacional ISO 27001. Según las actividades planteadas en la Figura 17: Procedimiento SGSI, es que en esta investigación nos enfocaremos a la actividad 12 Seguridad en la Operativa y la actividad 13 Seguridad en las Telecomunicaciones.

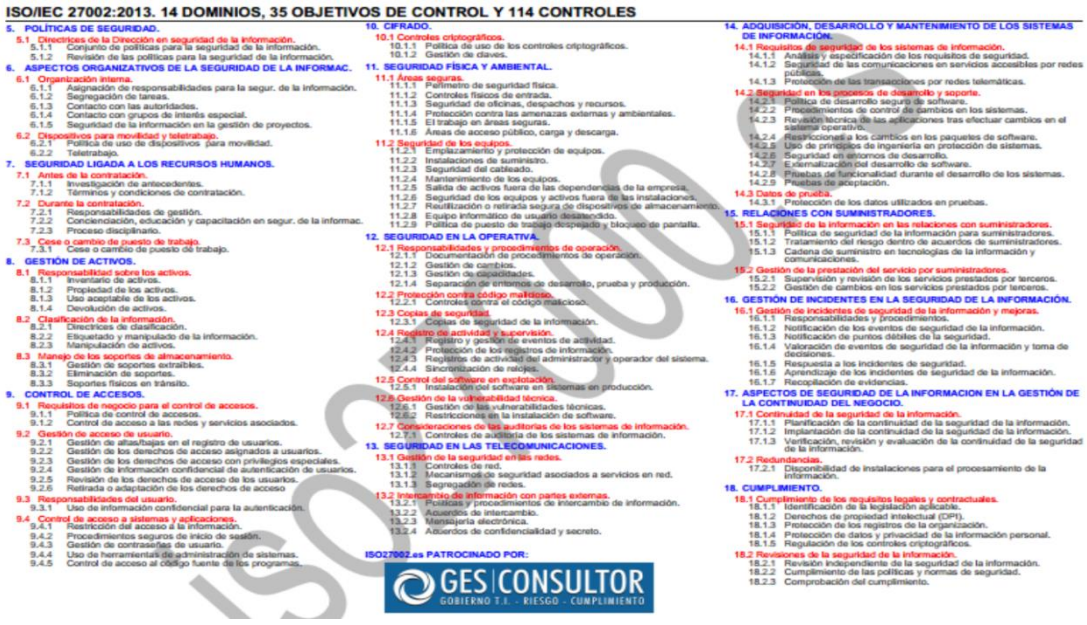


Figura 01: Procedimiento SGSI

Fuente: Página oficial ISO 27001

El desarrollo del sistema de gestión de seguridad de la información en la Municipalidad Distrital de Ilabaya se va plantear por fases:

1.1 Fase I: Diagnostico del SGSI

Para el análisis del diagnóstico situacional de la Municipalidad Distrital de Ilabaya se realizará algunas actividades frente a la seguridad de la información y redes LAN.

En coordinación con el responsable de la oficina Tecnología de Información y comunicaciones se evaluó distintos puntos en relación a SGSI por lo que se inició con la evaluación inicial de la Municipalidad Distrital de Ilabaya en la siguiente tabla.

Tabla 01: Diagnóstico inicial

REQUERIMIENTO DE LA NTP ISO/IEC 27001:2014	ESTADO	EVIDENCIA / SUGERENCIA
Contexto de la entidad	No diseñado	La entidad no cuenta con una organización con respecto a la seguridad de información se sugiere comprender los aspectos internos y externos y requisitos principales al SGSI
Funcionalidad de la entidad	Regularmente diseñado	La entidad posee documentos tales como POI, PEI, organigrama, etc.
Comprender la necesidad de la entidad	No diseñado	Comprender las necesidades y la expectativa de la entidad
Determinar alcance	No diseñado	Determinar alcance de SGSI en relación con la calidad de servicio de las redes LAN en
Sistema de gestión de seguridad de la información	No diseñado	Establecer diferentes herramientas que agilicen el proceso gestión de seguridad de información.
Políticas	No diseñado	La entidad debe establecer políticas de seguridad acorde al propósito

Fuente: Municipalidad Distrital de Ilabaya

De acuerdo a la Tabla 01: Diagnóstico inicial es que desarrollamos políticas de seguridad para la entidad Municipalidad Distrital de Ilabaya

1.2 Fase II: Preparación del SGSI

En la fase II de preparación daremos a detallar como se realiza el proceso de subsanación de riesgos, amenazas y vulnerabilidades, para ello es necesario conocer a fondo la entidad pública Municipalidad Distrital de Ilabaya.

1.2.1 Contexto de la entidad

El sistema de gestión de seguridad de la información debe alinearse con la cultura y la estrategia de la entidad. Para ello daremos a conocer algunos aspectos importantes de la entidad pública Municipalidad Distrital de Ilabaya.

A) Misión

Misión institucional

"Somos una Institución de servicio, cuyo fin es mejorar la calidad de vida de la población de Ilabaya, prestando servicios de calidad, promoviendo la igualdad de oportunidades para el desarrollo económico social y ambiental, administrando responsable y transparentemente los recursos municipales" (Ilabaya, s.f.).

B) Visión

Visión gestión 2019-2022

"Ser un distrito sostenible, que trabaja en perfecta armonía con todos sus factores de producción, respetando en todo momento la dignidad de las personas y el medio ambiente" (Ilabaya, s.f.).

Visión concertada

"Ilabaya es un distrito con liderazgo, democrático, concertador e inclusivo que promueve el desarrollo planificado de su población, priorizando la integración de los jóvenes del distrito. Siendo líderes en educación, promoción del turismo y la capacidad artesanal y agroexportadora, producto de la innovación e investigación tecnológica que el gobierno local ha incentivado en cada uno de ellos" (Ilabaya, s.f.).

C) Organigrama

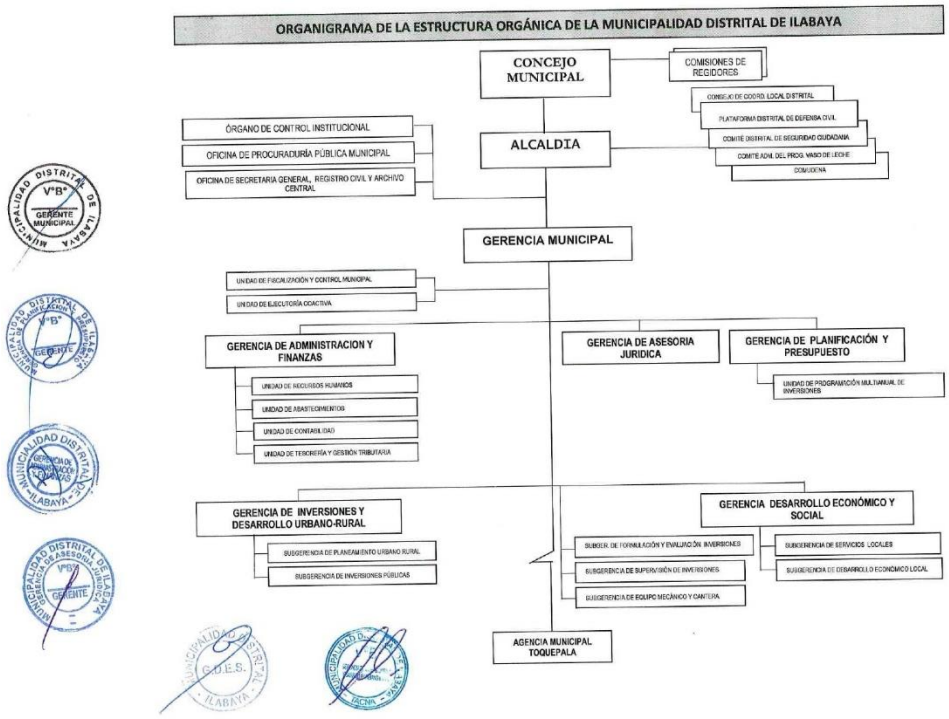


Figura 02: Organigrama Municipalidad Distrital de Ilabaya

Fuente: Portal de Transparencia - Municipalidad Distrital de Ilabaya

1.2.2 Proceso actual de SGSI y funcionalidad de la entidad

En la actualidad la Municipalidad Distrital de Ilabaya no cuenta con un Sistema de Gestión de Seguridad de la Información, esto conlleva a una mala organización y administración de activos de información ya que el proceso se realiza manualmente, en el caso de mitigar riesgo las oficinas reportan de manera verbal y la oficina de Tecnologías de Información y comunicaciones subsana los problemas sin tener un reporte o evidencia de la solución realizada.

Los activos de información son guardados de manera personal por oficinas y no en los servidores, trayendo como consecuencias perdidas de información o ataques de virus constante. Los procesos manuales no siempre son la forma más segura del aseguramiento de información, para ello es que se realiza el sistema de control de Amenazas y Vulnerabilidades como parte de Diseño de un Sistema de Gestión de Seguridad de la Información. El sistema a implementar permite tener un historial de todos los riesgos, amenazas y vulnerabilidades de la Municipalidad Distrital de Ilabaya albergando toda la

información en una base de datos, teniendo la posibilidad de realizar todos los reportes necesarios para los tramites que se amerite según corresponda.

En este contexto se ha procedido a analizar los riesgos (bajo la metodología MAGERIT) que podrían presentarse ante la puesta en marcha de la migración de los servicios críticos a la nueva infraestructura, que se detalla a continuación:

1.2.3 Comprender la necesidad de la entidad

a) Identificación de componentes, se han definido los siguientes componentes:
   - ✓ Hardware, componentes físicos del sistema: Servidores.
   - ✓ Software, software, base de datos, herramientas de desarrollo y licenciamiento.
   - ✓ Seguridad, Elementos de protección y seguridad de la información accesos y sistema.
   - ✓ Personal, capital humano involucrado en el despliegue del proceso de migración.
   - ✓ Continuidad del Negocio, aspectos que garantizan la continuidad del negocio.

b) Identificación de amenazas y probabilidades, la identificación de las amenazas se debe clasificar en un nivel de probabilidad (NP) y con este objetivo se crea una escala para clasificar la probabilidad de ocurrencia que se describe a continuación:

Nivel	Descripción de probabilidad
1	Improbable y no se tiene evidencia de que ha ocurrido
2	Probable que se produzca una vez cada dos años
3	Probable que se produzca una vez cada trimestre

Tabla 02: Escala de probabilidad de ocurrencia

Fuente: Elaboración propia

Con la tabla 03 se procede a clasificar cada amenaza identificada:

COMPONENTES	Amenazas	Descripción	Vulnerabilidad	Descripción	NP
A. HARDWARE	A1	Daños en el Servidor	V1	Fallas de energía, deterioro fisico y daños en General	1
	A2	Ausencia de soporte técnico para el Servidor	V2	No contar con contratos de soporte para las funciones	2
B. SOFTWARE	A3	Configuración del Software	V3	Degradación en la disponibilidad de los servicios del Servidor	1
	A4	Aspectos legales	V4	Licenciamiento del Software para los servidores	1
C. SEGURIDAD	A5	Derechos de acceso del usuario	V5	Acceso indebidos por parte de los usuarios ante la presencia de perfiles inadecuados	1
	A6	No disponibilidad de la información	V6	Ausencia de plan de pruebas post migración del Servidor	1
D. PERSONA	A7	Impericia del Personal	V7	Personal no cuenta con las competencias ni las capacidades para realizar la actividad	1
E. CONTINUIDAD DEL NEGOCIO	A8	Garantizar la continuidad del servicio	V8	No se consideraron mecanismos de protección que permitieran al sistema mantener su operación durante la migracion	1

Tabla 03: Amenazas y Vulnerabilidades de la Infraestructura Actual de Servidores

Fuente: Elaboración propia

Asimismo, se configura una tabla de Impacto para poder clasificar las amenazas en caso se materialice y que a continuación se describe:

Valor	Descriptor	Descripción del impacto
1	Insignificante	Si el hecho llegara a presentarse, tendría consecuencias o efectos mínimos sobre la entidad.
2	Menor	Si el hecho llegara a presentarse, tendría bajo impacto o efecto sobre la entidad.
3	Moderado	Si el hecho llegara a presentarse, tendría medianas consecuencias o efectos sobre la entidad
4	Mayor	Si el hecho llegara a presentarse, tendría altas consecuencias o efectos sobre la entidad
5	Catastrófico	Si el hecho llegara a presentarse, tendría desastrosas consecuencias o efectos sobre la entidad.

Tabla 04: Escala de Impacto

Fuente: Elaboración propia

También definimos el mapa de calor para ubicar en las zonas de riesgo que se derivaran del producto de los valores de impacto y probabilidad (NP) y que a continuación se describe:

Probabilidad	Impacto				
	Insignificante (1)	Menor (2)	Moderado (3)	Mayor (4)	Catastrófico (5)
1	B (1)	B (2)	B (3)	B (4)	M (5)
2	B (2)	B (4)	M (6)	A (8)	E (10)
3	B (3)	M (6)	A (9)	E (12)	E (15)
	B: Zona de riesgo baja: Asumir el riesgo. (1-4)				
	M: Zona de riesgo moderada: Asumir el riesgo, reducir el riesgo. (5-7)				
	A: Zona de riesgo Alta: Reducir el riesgo, evitar, compartir o transferir. (8-9)				
	E: Zona de riesgo extrema: Reducir el riesgo, evitar, compartir o transferir. (10-15)				

Tabla 05: Mapa de calor – Zona de Riesgo

Fuente: Elaboración propia

Con estas tablas se procede a clasificar las amenazas para poder calcular el Riesgo potencial, que a continuación se describe:

COMPONENTES	Amenazas	Descripción	Vulnerabilidad	Descripción	NP	Impacto	Riesgo Potencial
A. HARDWARE	A1	Daños en el Servidor	V1	Fallas de energía, deterioro físico y daños en General	1	3	3
	A2	Ausencia de soporte técnico para el Servidor	V2	No contar con contratos de soporte para las funciones	2	3	6
B. SOFTWARE	A3	Configuración del Software	V3	Degradación en la disponibilidad de los servicios del Servidor	1	3	3
	A4	Aspectos legales	V4	Licenciamiento del Software para los servidores	1	3	3
C. SEGURIDAD	A5	Derechos de acceso del usuario	V5	Acceso indebidos por parte de los usuarios ante la presencia de perfiles inadecuados	1	2	2
	A6	No disponibilidad de la información	V6	Ausencia de plan de pruebas post migración del Servidor	1	3	3
D. PERSONA	A7	Impericia del Personal	V7	Personal no cuenta con las competencias ni las capacidades para realizar la actividad	1	2	2
E. CONTINUIDAD DEL NEGOCIO	A8	Garantizar la continuidad del servicio	V8	No se consideraron mecanismos de protección que permitieran al sistema mantener su operación durante la migracion	1	3	3

Tabla 06: Clasificación de las amenazas según Nivel de probabilidad –

Impacto y Riesgo Potencial de la Infraestructura actual de Servidores

Fuente: Elaboración propia

Se ha logrado identificar ocho (08) amenazas con sus respectivas vulnerabilidades y su clasificación de nivel de probabilidad de ocurrencia, de las cuales según el resultado del Riesgo potencial se clasifican en:

- ✓ 01 amenazas en zona de riesgo potencial moderada lo cual involucra plantear estrategias de asumir el riesgo o de reducirlos.
- ✓ 07 amenazas en zona de riesgo potencial bajo, lo cual se podría asumir el riesgo.

Asimismo, estas amenazas traen los riesgos que se definen a continuación con sus respectivas causas y efectos:

COMPONENTES	Amenazas	Vulnerabilidad	Riesgo	Descripción
A. HARDWARE	A1	V1	R01	Degradacion de la Alta disponibilidad de Servidores
	A2	V2	R02	Ausencia de personal técnico y contratos para el soporte de la infraestructura de servidores
B. SOFTWARE	A3	V3	R03	Falla en la configuración de software del servidor
	A4	V4	R04	Falta de licencias de software para la configuración de servidores
C. SEGURIDAD	A5	V5	R05	Posible acceso indebido de diferentes usuarios en los diferentes perfiles definidos
	A6	V6	R06	Falta de evidencia de pruebas en los servicios criticos post migracion del servidor
D. PERSONA	A7	V7	R07	Falta de personal con las capacidades necesarias
E. CONTINUIDAD DEL NEGOCIO	A8	V8	R09	Caida del Servicio

Tabla 07-1: Riesgos Potenciales en la Infraestructura actual de Servidores

Fuente: Elaboración propia

Causa	Efecto
Deterioro de elementos informáticos incremental	Perdida de elementos de información necesarios para la consistencia del sistema que hacen que se pierda la integridad de la información
No contar con contratos de personal experto "in house" ni con contratos para las funciones requeridas	El soporte de la infraestructura de servidores se vea comprometido por la ausencia de personal calificado
No realizar el mantenimiento preventivo al software	Mal funcionamiento del software en el Servidor en fase crítica, Perdida de continuidad del servicio, caidas y degradación del servicio
Falta de presupuesto de la actividad	Incumplimeinto de aspectos de propiedad intelectual
No verificación de los perfiles y permisos que correspondan a los asignados	Acceso indebido por parte de los usuarios ante la presencia de perfiles inadecuados, perdiendose la confidencialidad de la información
Saturación de actividades o falta de programación que impiden elaborar dicho plan de pruebas y/o certificación	Degradación en la disponibilidad de la información por parte de los usuarios
Personal no cuenta con las competencias ni las capacidades para conformar el equipo de migración	Falta de capacitación y curva de aprendizaje muy lenta
No se consideraron mecanismos de protección que permitieran al sistema mantener su operación durante la migracion	La continuidad del negocio se ve afectada ante una interrupción de sus operaciones

Tabla 07-2: Riesgos Potenciales en la Infraestructura actual de Servidores

Fuente: Elaboración propia

c) Salvaguarda o controles existentes, con esta visión preliminar del impacto potencial y los riesgos potenciales, se procedió a verificar los controles por cada riesgo identificado, para lo cual se creó una matriz para poder definir el control (la acción a ejecutar para mitigar el riesgo).

Asimismo, para determinar el nivel de efectividad del control se presenta el siguiente cuadro:

Nivel	Descripción de la efectividad del control
3	Control está garantizado para funcionar eficazmente en cada caso de ocurrencia de la amenaza.
2	El control es parcialmente eficaz y podría funcionar la mayor parte del tiempo en el caso de que se produzca una amenaza.
1	El control es probable que falle en todos los casos de ocurrencia de la amenaza o No existe un control para mitigar esta amenaza.

Tabla 08: Escala de efectividad del Control

Fuente: Elaboración propia

d) Impacto Residual, luego de definir los controles existentes por el Área de TIC, se obtiene el impacto residual, que sale del cálculo de los valores de impacto potencial sobre la eficacia del control.

e) Riesgo Residual, este paso final del análisis es la identificación del riesgo residual, para calcularlo se toma el valor del impacto residual por el nivel de probabilidad de ocurrencia.

A continuación, se detalla la Matriz de impacto residual y riesgo residual:

COMPONENTES	Amenazas	Vulnerabilidad	Riesgo	Descripción
A. HARDWARE	A1	V1	R01	Degradacion de la Alta disponibilidad de Servidores
	A2	V2	R02	Ausencia de contratos para el soporte de la infraestructura de servidores
B. SOFTWARE	A3	V3	R03	Falla en la configuración de software del servidor
	A4	V4	R04	Falta de licencias de software para la configuración de servidores
C. SEGURIDAD	A5	V5	R05	Posible acceso indebido de diferentes usuarios en los diferentes perfiles definidos
	A6	V6	R06	Falta de evidencia de pruebas en los servicios criticos post migracion de la infraestructura de servidores
D. PERSONA	A7	V7	R07	Falta de personal con las capacidades necesarias
E. CONTINUIDAD DEL NEGOCIO	A8	V8	R09	Caida del Servicio

Tabla 09-1: Matriz de Impacto Residual y Riesgo Residual de la Infraestructura Actual de Servidores

Fuente: Elaboración propia

Control	Tipo de Control	Eficacia del Control	Impacto Potencial	Impacto residual	Probabilidad	Riesgo Residual
Migración a una nueva Infraestructura de Servidores	Minimizador	3	3	1.00	1	1.00
Migración a una nueva Infraestructura de Servidores	Minimizador	3	3	1.00	2	2.00
Elaboración de actas y/o formatos que evidencien las revisiones de los servicios críticos en la nueva infraestructura de servidores	Minimizador	3	3	1.00	1	1.00
Provisionamiento de Licencias de Software para Servidores en la nueva infraestructura	Minimizador	3	3	1.00	1	1.00
Realización de Configuraciones previas a la migración de los servicios críticos a la nueva infraestructura de servidores	Minimizador	3	2	0.67	1	0.67
Elaboración de actas y/o formatos que evidencien las revisiones de los servicios críticos en la nueva infraestructura de servidores	Minimizador	3	3	1.00	1	1.00
Personal in house certificado mas el soporte del proveedor para realizar actividad de migración de los servicios críticos	Minimizador	3	2	0.67	1	0.67
Poseer respaldo con el Servidor de Producción actual	Minimizador	3	3	1.00	1	1.00

Tabla 09-2: Matriz de Impacto Residual y Riesgo Residual de la Infraestructura Actual de Servidores

Fuente: Elaboración propia

De acuerdo a lo anterior es que se desarrolla el sistema web control de amenazas y vulnerabilidades como parte de un diseño de SGSI en la Municipalidad Distrital de Ilabaya, con la finalidad de automatizar el proceso actual para un mejor control de riesgos en la entidad pública Municipalidad Distrital de Ilabaya.

1.2.4 Determinar alcance

Proceso que se determina en políticas de seguridad de la Municipalidad Distrital de Ilabaya **Anexo 08.**

1.2.5 Sistema de gestión de seguridad de la información

Como aporte a la investigación y diseño de un SGSI es que se desarrolló un sistema de control de amenazas y vulnerabilidades enfocado a la tecnología y telecomunicaciones de la Municipalidad Distrital de Ilabaya **Anexo 07.**

1.2.6 Políticas

Es uno de los requisitos más importantes para la implementación de un SGSI en la Municipalidad Distrital de Ilabaya para ello se elaboró políticas de seguridad para la entidad **Anexo 08**.

1.3 Fase III: Planificación del SGSI

En esta última fase nos enfocaremos en las amenazas y vulnerabilidades en la entidad pública Municipalidad Distrital de Ilabaya. Para ello se desarrolló el siguiente sistema; quien permitirá la mitigación de los riesgos de la entidad.

1.3.1 Herramientas a utilizar

a) Laravel

Laravel es un framework que nos permite optimizar código, facilitando el desarrollo de distintas funcionalidades, asimismo cumple con los estándares de seguridad en cuestión de gestión de usuarios. Laravel trabaja en un entorno PHP (Laravel, s.f.).

b) PHP (Hypertext Preprocessor)

Es un lenguaje de programación de código abierto muy popular de hace muchos años atrás, muy trabajado en entornos web (PHP, s.f.).

c) Composer (Software)

Esta herramienta es un administrador de paquetes para lenguaje de programación PHP, lo cual facilita la administración de dependencias PHP (Composer, s.f.).

d) Servidor HTTP Apache

Servidor web HTTP para plataformas Linux, Microsoft Windows, Macintosh y otras plataformas y/o sistema operativo.

e) MySQL

Es un sistema de gestión de Base de Datos, lo cual nos permitirá el almacenamiento de información requerida para el sistema a desarrollar.

f) XAMPP

Herramienta que almacena distintos módulos como Apache, MySQL, FileZilla, Mercury y Tomcat.

g) Sublime Text 3

Plataforma para codificar lenguaje de programación PHP, estilos CSS, javascript, entre otros.

1.3.2 Metodología de desarrollo de Software (RUP)

Metodología RUP (Rational Unified Process) Es un proceso de ingeniería de software que garantiza un proceso de desarrollo de software de calidad asimismo suministra un enfoque para asignar tareas y responsabilidades dentro de una organización de desarrollo. Su objetivo es asegurar la producción de software de alta y de mayor calidad para satisfacer las necesidades de los usuarios que tienen un cumplimiento al final dentro de un límite de tiempo y presupuesto previsible. Es una metodología de desarrollo iterativo que es enfocada hacia "diagramas de los casos de uso, y manejo de los riesgos y el manejo de la arquitectura".

RUP consta de 4 fases: Inicio, énfasis en el alcance del sistema; Elaboración, énfasis en la arquitectura; Construcción, énfasis en el desarrollo; Transición, énfasis en la aplicación. El Sistema Web "Control de amenazas y vulnerabilidades" está desarrollado en base a la metodología de desarrollo RUP.

a) Fase inicio

En esta primera fase vamos a enfocarnos al periodo de elaboración del sistema y los procesos para la mitigación de amenazas y vulnerabilidades.

1) Cronograma de actividades

Nombre de tarea	Duración	Comienzo	Fin
Sistema Web "Control de amenazas y vulnerabilidades"	**20 días**	**lun 21/03/22**	**vie 15/04/22**
1. Fase Inicio	**3 días**	**lun 21/03/22**	**mié 23/03/22**
Cronograma de Actividades	1 día	lun 21/03/22	lun 21/03/22
Requerimientos del Administrador Responsable	1 día	mar 22/03/22	mar 22/03/22
Diagramas	1 día	mié 23/03/22	mié 23/03/22
2. Fase Elaboración	**6 días**	**jue 24/03/22**	**jue 31/03/22**
Requerimientos del Sistema	1 día	jue 24/03/22	jue 24/03/22
Especificación de Caso de Uso	3 días	vie 25/03/22	mar 29/03/22
Arquitectura Laravel MVC	1 día	mié 30/03/22	mié 30/03/22
Diagrama Entidad Relación	1 día	jue 31/03/22	jue 31/03/22
3. Fase Desarrollo	**9 días**	**vie 1/04/22**	**mié 13/04/22**
Estructura del Sistema	9 días	vie 1/04/22	mié 13/04/22
4. Fase Transición	**2 días**	**jue 14/04/22**	**vie 15/04/22**
Manual de Instalación	1 día	jue 14/04/22	jue 14/04/22
Manual de Usuario	1 día	vie 15/04/22	vie 15/04/22

Tabla 10: Cronograma de actividades

Fuente: Elaboración propia

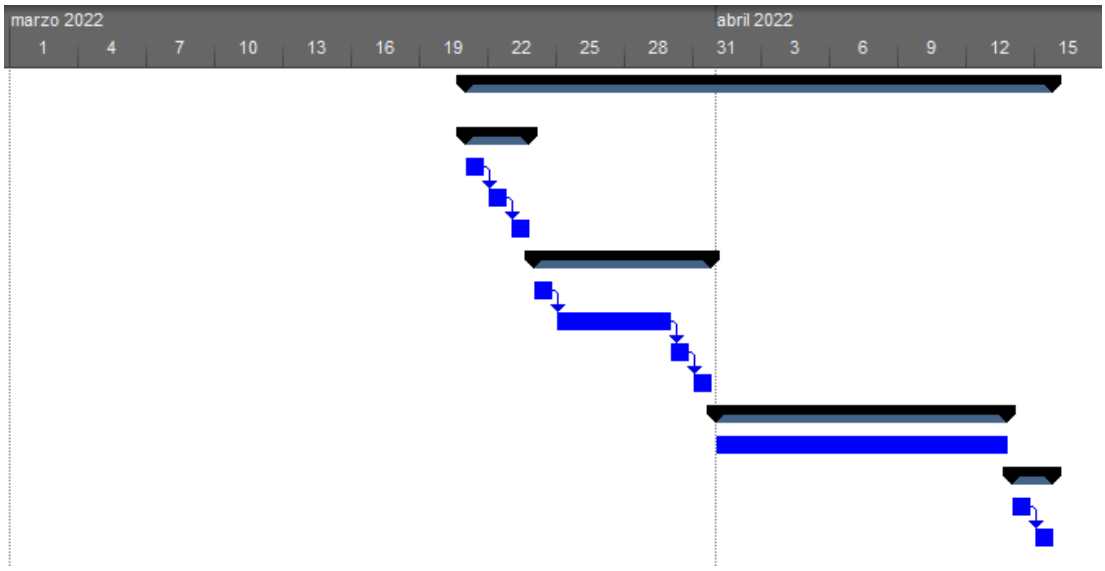


Figura 02: Cronograma de actividades grafica

Fuente: Elaboración propia

Interpretación: La Figura 19 y 20 muestra el cronograma de actividades a desarrollar el sistema de control de amenazas y vulnerabilidades.

2) Requerimientos del Administrador Responsable

A continuación, se muestra el listado de requerimientos generales dados por parte del administrador responsable en los procesos del sistema web control de amenazas y vulnerabilidades.

- ✓ Opción para poder registrar usuarios.
- ✓ Opción para poder registrar componentes.
- ✓ Opción para poder registra nivel de probabilidad.
- ✓ Opción para poder registrar impacto.
- ✓ Opción para poder registrar efectividad de control.

3) Diagrama de procesos

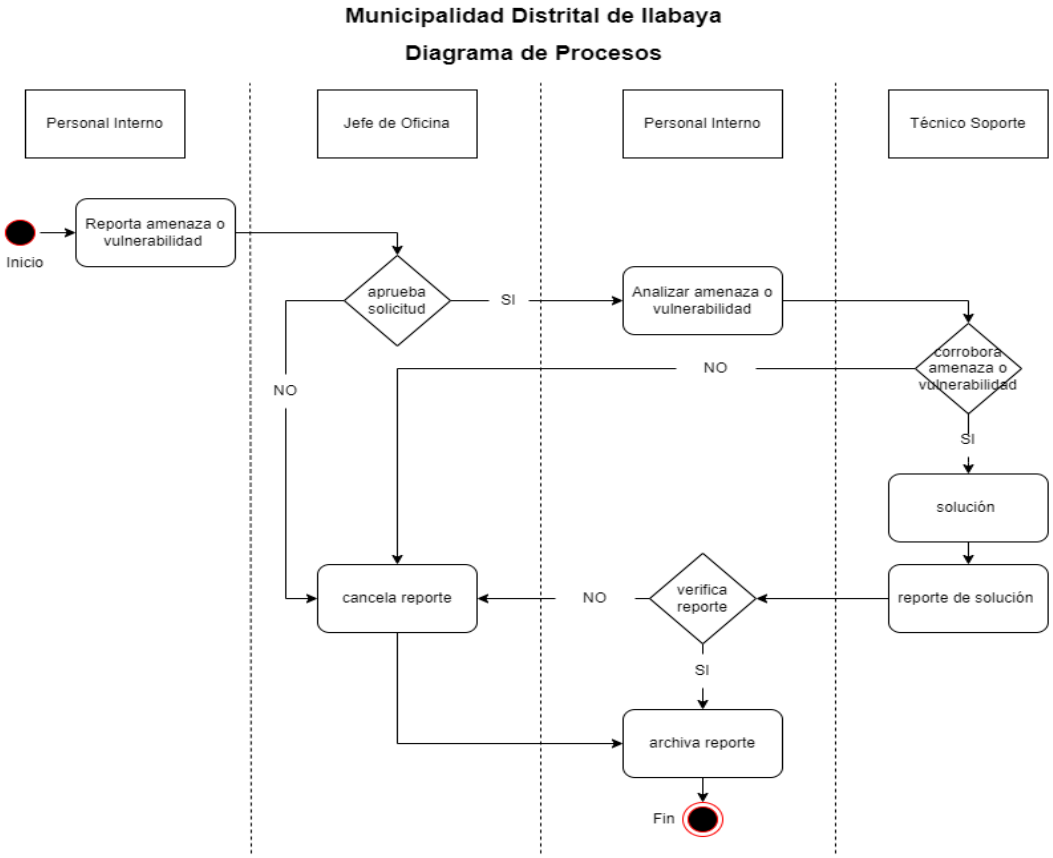


Figura 03: Diagrama de procesos

Fuente: Elaboración propia

4) Diagrama de secuencia

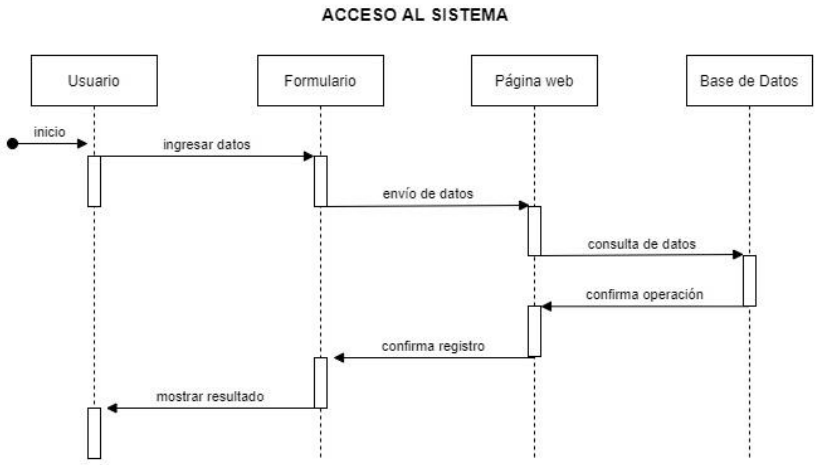


Figura 04: Acceso al sistema

Fuente: Elaboración propia

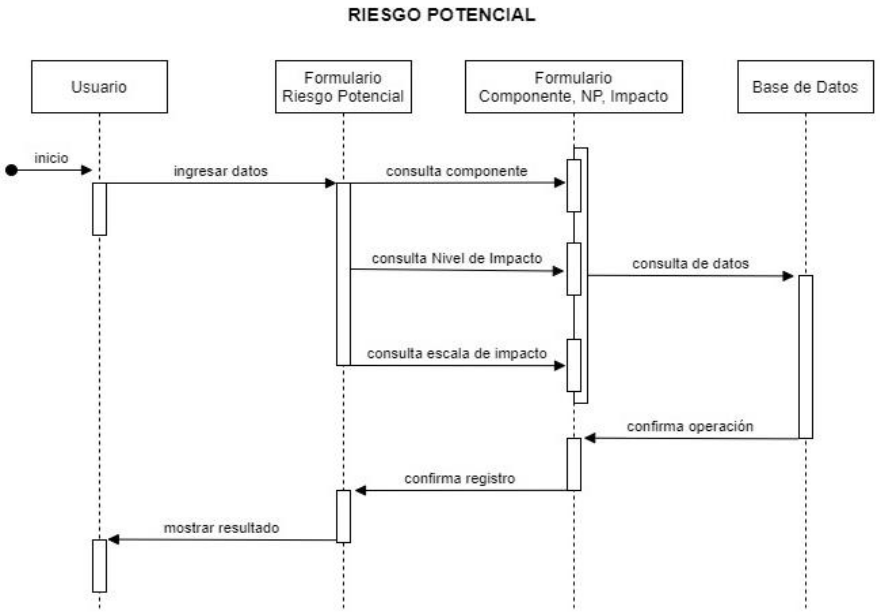


Figura 05: Riesgo Potencial

Fuente: Elaboración propia

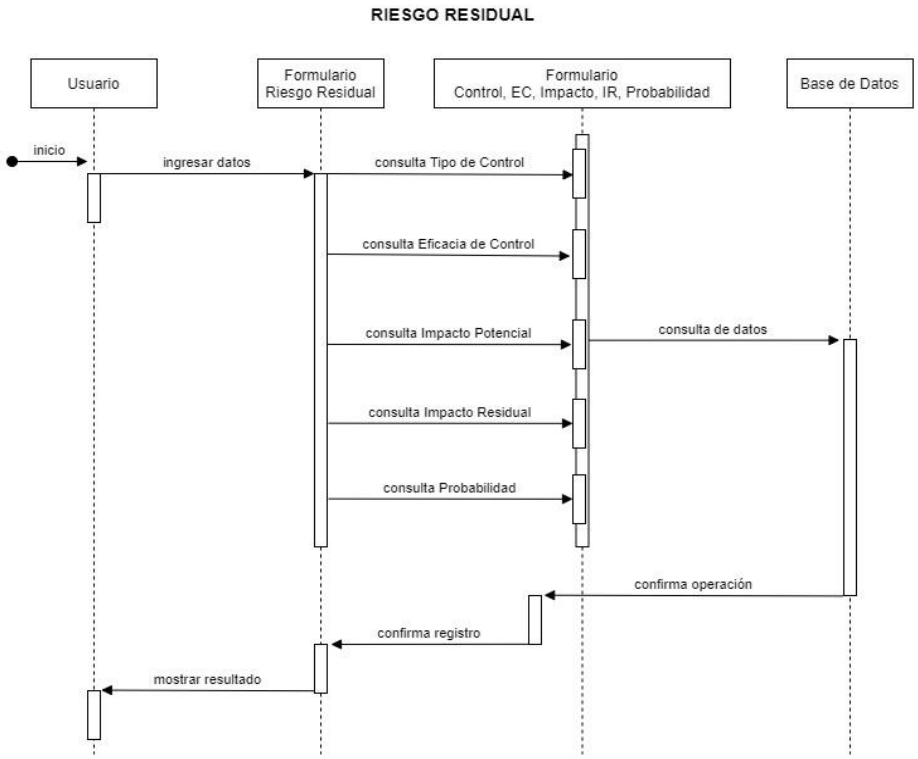


Figura 06: Riesgo residual

Fuente: Elaboración propia

5) Diagrama de componentes

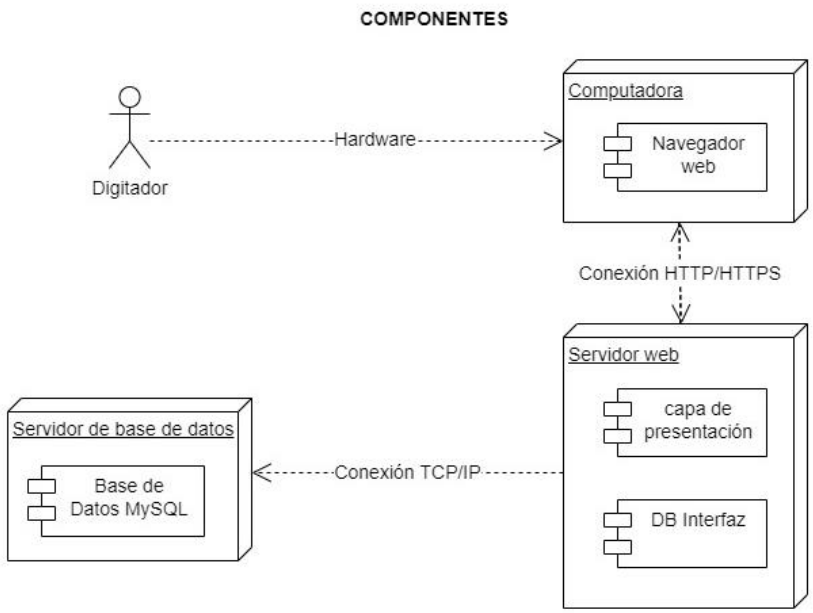


Figura 07: Diagrama de componente

Fuente: Elaboración propia

b) Fase elaboración

Requerimientos funcionales

Tabla 11: Requerimientos funcionales

MÓDULO	CÓDIGO	DESCRIPCIÓN
Módulo seguridad	R001	Gestionar usuario
Módulo control	R002	Gestionar componentes
	R003	Gestionar nivel de probabilidad
	R004	Gestionar impacto
	R005	Gestionar efectividad de control
	R006	**Gestionar riesgo potencial**
	R007	**Gestionar riesgo residual**

Fuente: Elaboración propia

Requerimientos no funcionales

Tabla 12: Requerimientos no funcionales

CÓDIGO	DESCRIPCIÓN
RNF001	El sistema web "Control de amenazas y vulnerabilidades" debe ser fácil de usar.
RNF002	El sistema web "Control de amenazas y vulnerabilidades" debe mostrar información correcta.
RNF003	El sistema web "Control de amenazas y vulnerabilidades" debe ser registrado por un personal con vínculo laboral.
RNF004	El sistema web "Control de amenazas y vulnerabilidades" debe ser capaz de funcionar en varios navegadores web.
RNF005	El sistema web "Control de amenazas y vulnerabilidades" debe ser capaz de ser adaptable a cualquier pantalla (responsive web design).
RNF006	El sistema web "Control de amenazas y vulnerabilidades" debe marcar los campos que han causado error al realizar algún procedimiento de guardado, modificado, etc.
RNF007	El sistema web "Control de amenazas y vulnerabilidades" debe mostrar alertas cuando las operaciones han sido realizadas con éxito o fracaso.
RNF008	El sistema web "Control de amenazas y vulnerabilidades" debe mostrar un tiempo de respuesta aceptable.
RNF009	El sistema web "Control de amenazas y vulnerabilidades" solo debe ser usado por los siguientes usuarios: a) Jefe responsable del SGSI b) Administrador c) Responsable asignado por el administrador

Fuente: Elaboración propia

c) Fase desarrollo

En la fase desarrollo nos vamos a enfocar en el desarrollo de la base de dato en MySQL, la estructura pre establecidas y/o la creación de carpetas y archivos a utilizar en Laravel 9, y el diseño del sistema web "control de amenazas y vulnerabilidades", al ser un sistema de administración se tiene como objetivo la fluidez y la capacidad de respuesta aceptable para una capacidad de respuesta inmediata.

Fase técnica del sistema a implementar. Según la base de datos Figura 26, se puede identificar las tablas a utilizar en nuestro sistema siendo la tabla amevuls (Amenazas y vulnerabilidades) y residuals (Riesgos residuales) siendo las tablas principales para identificar el grado de amenaza, vulnerabilidad y riesgo, las tablas que no están relacionadas cumplen la función de inicio de sesión, contraseña, usuarios, permisos y personas que agregaremos para cumplir funciones de administrador o usuario estándar, las tablas no relacionadas las crea el propio Framework a través de la tabla migración lo cual facilita el uso de login al sistema que se está planteando.

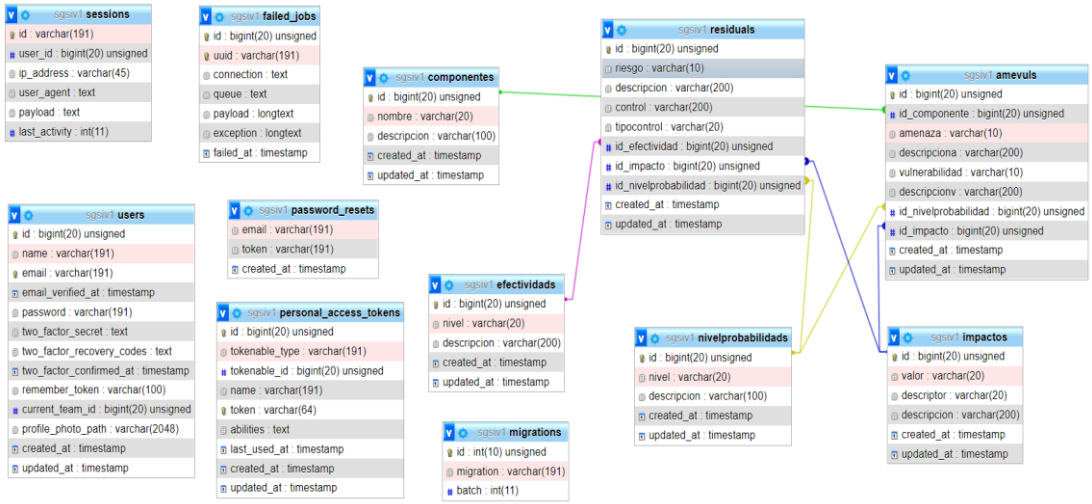


Figura 08: Base de Datos

Fuente: Elaboración propia

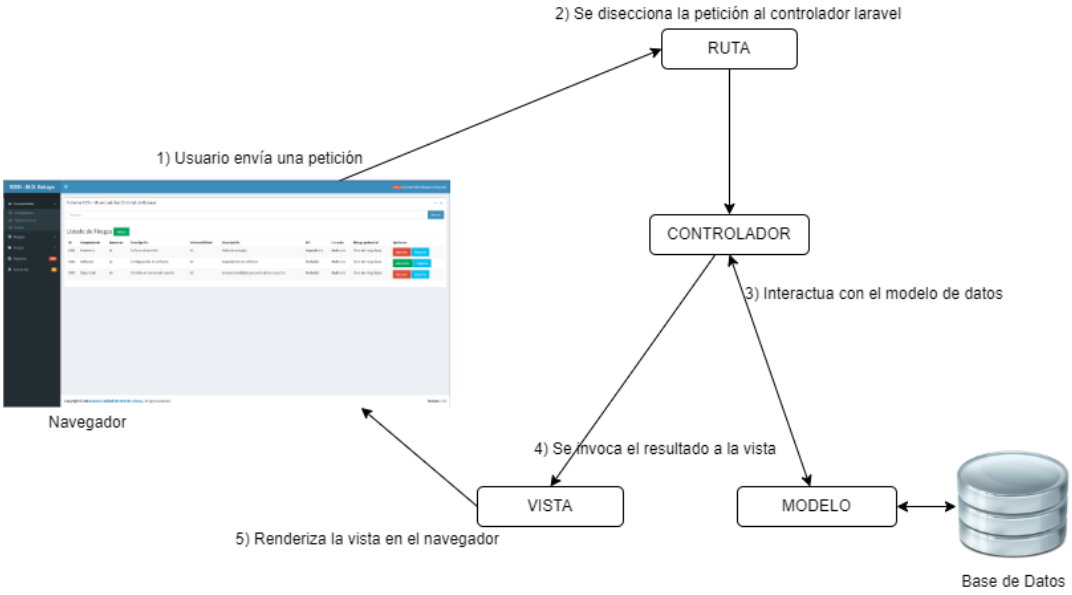


Figura 09: Arquitectura Laravel

Fuente: Elaboración propia

Estructura del sistema:

El sistema web "control de amenazas y vulnerabilidades" está generado automáticamente con Laravel 9 mediante comandos ejecutados en el símbolo del sistema de Windows, el proyecto es agrupado en una carpeta denominada SGSI_CONTROL a quien definimos al ejecutar el proyecto.

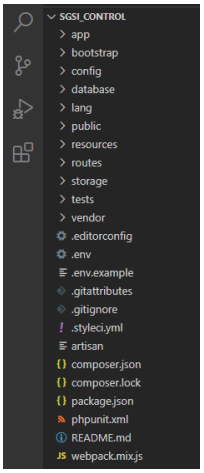


Figura 10: Estructura del sistema

Fuente: Elaboración propia

A continuación, daremos a conocer de los directorios y su funcionalidad de un entorno general y el cumplimiento que tienen para el funcionamiento del sistema web control de amenazas y vulnerabilidades, asimismo es necesario mencionar que todas las carpetas tienen una funcionalidad lo que hace intuitivo los proyectos realizados en Laravel.

- ✓ **Directorio app**

App es usado para ofrecer un hogar por defecto a todo el código personal del proyecto. Eso incluye clases que puedan ofrecer funcionalidades a la aplicación, archivos de configuración y más. Es considerado como el directorio más importante del proyecto ya que es donde se encuentra la codificación más relevante. Dentro de ello encontramos los siguientes directorios, Console, Exceptions, Http, Models y Providers. En esta versión de Laravel 9 los módulos se alojan en la carpeta Models y no como las versiones anteriores que se creaban en la raíz del directorio app, siendo en este directorio la carpeta más relevante los módulos.

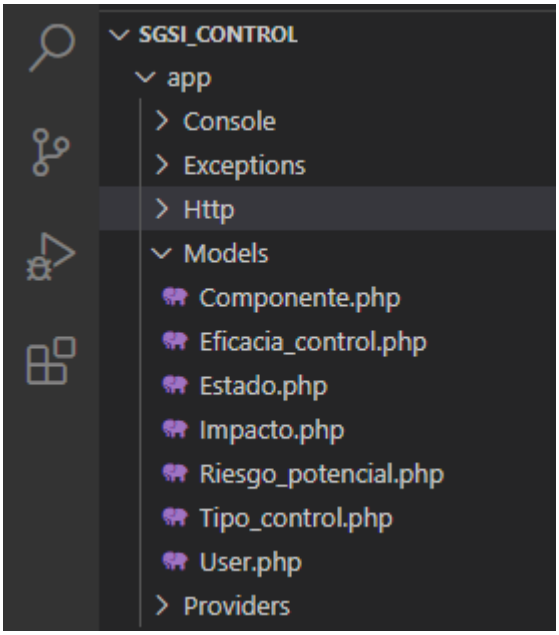


Figura 11: Directorio app

Fuente: Elaboración propia

- ✓ **Directorio Bootstrap**

Bootstrap es un frameworks de estilos lo cual permite un diseño lo que facilita la aplicación de estilos en el proyecto.

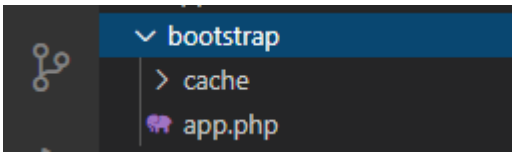


Figura 12: Directorio Bootstrap

Fuente: Elaboración propia

✓ **Directorio config**

App es usado para ofrecer un hogar por defecto a todo el código personal de tu proyecto. Eso incluye clases que puedan ofrecer funcionalidad a la aplicación, archivos de configuración y más. Es considerado el directorio más importante de nuestro proyecto ya que es en el que más trabajaremos.

La configuración tanto para el framework como para tu aplicación se mantiene en este directorio. La configuración de Laravel existe como un conjunto de archivos PHP que contienen matrices clave-valor. Entre los archivos más usados del directorio config se encuentran:

- app.php: En este archivo nos puede interesar configurar el lenguaje de nuestra aplicación, la zona horaria, los providers y aliases de las clases más comunes.
- database.php: En este archivo podemos configurar principalmente el motor de base de datos al cuál deseamos conectarnos.

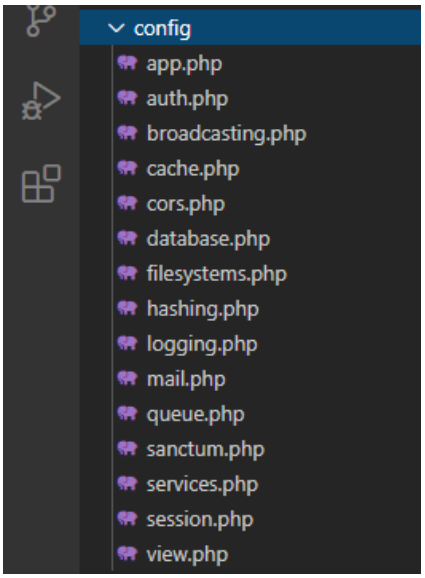


Figura 13: Directorio config

Fuente: Elaboración propia

✓ **directorio database**

Aquí se encontrarán los archivos relacionados con el manejo de la base de datos. Dentro de este directorio se encuentran los subdirectorios:

- factories: Aquí escribiremos nuestros model factories.
- migrations: Todas las migraciones que creamos se ubican en este subdirectorio.
- seeds: Contiene todas las clases de tipo seed.

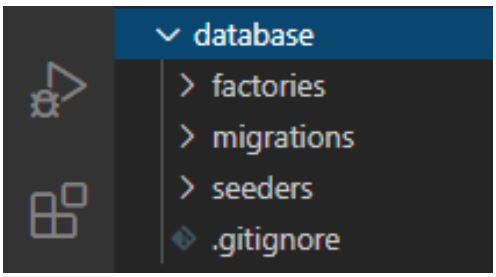


Figura 14: Directorio database

Fuente: Elaboración propia

✓ **directorio public**

Dentro de este directorio colocaremos todos los recursos estáticos de nuestra aplicación, es decir, archivos css, js, imágenes y fuentes.

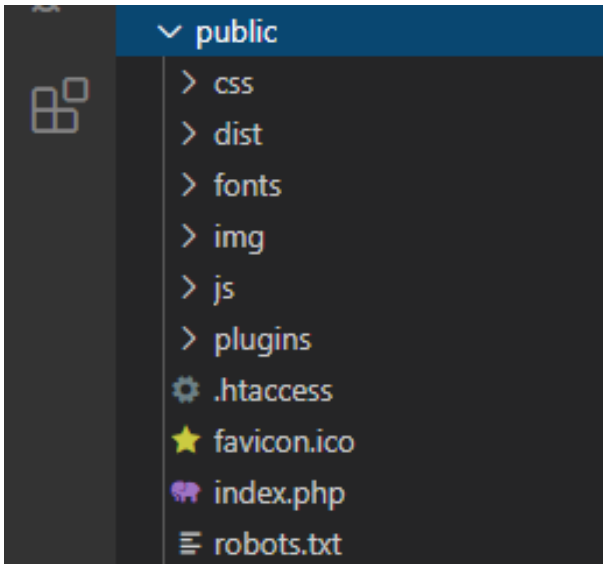


Figura 15: Directorio public

Fuente: Elaboración propia

✓ **directorio resources**

Dentro de este directorio se encuentran los subdirectorios:

- **assets**: Aquí se ubican todos los archivos less de nuestra aplicación (útil para desarrolladores front-end).
- **lang**: Aquí se encuentran todos los archivos de internacionalización, es decir, los archivos para poder pasar nuestro proyecto de un idioma a otro. Normalmente habrá una carpeta por cada idioma, ejemplo:
  - en: idioma inglés
  - es: idioma español
- **views**: Aquí ubicaremos nuestras vistas en formato php o php.blade, es recomendable crear una carpeta por cada controlador, además agregar una carpeta templates para las plantillas. Una plantilla es una vista general, que tiene segmentos que pueden ser reemplazados mediante la herencia de plantillas, más adelante se hablará de este tema.

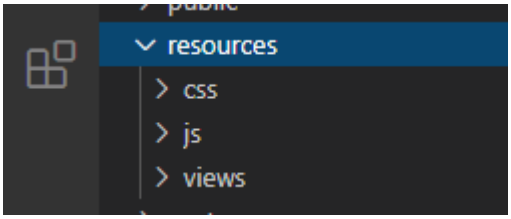


Figura 16: Directorio resources

Fuente: Elaboración propia

d) Fase transición

✓ **Iniciación del servicio Apache y MySQL**

Para la ejecución del sistema web "Control de amenazas y vulnerabilidades" tenemos que iniciar dos servicios de suma importancia, Apache y MySQL ya que el sistema está desarrollado con php y MySQL.

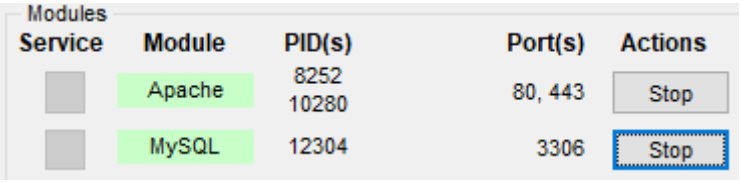


Figura 17: XAMPP panel de control

Fuente: (XAMPP, s.f.)

✓ **Cargar la base de datos**

Una vez iniciado los servicios de Apache y MySQL cargamos la base de datos donde serán almacenados toda la información registrada en el sistema web "Control de amenazas y vulnerabilidades".

Figura 18: Base de datos en Heidi

Fuente: Elaboración propia

✓ **Iniciar el sistema web control de amenazas y vulnerabilidades**

Con los servicios iniciados y con la base de datos cargado correctamente digitamos el siguiente comando: php artisan serve para poner en marcha el sistema web "Control de amenazas y vulnerabilidades", cabe resaltar que los comandos se ejecutan en la ruta del proyecto.

```
JEFF@DESKTOP-TGVEQ2B MINGW64 /c/xampp/htdocs/sgsi_control
$ php artisan serve
```

Figura 19: Comando a ejecutar

Fuente: Elaboración propia

✓ **Sistema web control de amenazas y vulnerabilidades**

En primera instancia el sistema web "Control de amenazas y vulnerabilidades" mostrará el formulario de acceso al sistema donde colocaremos el usuario jeff@munilabaya.gob.pe y la contraseña 123456 respectivamente. Para una mejor experiencia revisar el Anexo 04.

Figura 20: Acceso al sistema web

Fuente: Elaboración propia

✓ Página principal

Al iniciar el sistema web mostrará el listado de los riesgos ingresados, el sistema es desarrollado con un interfaz amigable y de fácil administración para los usuarios de la Municipalidad Distrital de Ilabaya.

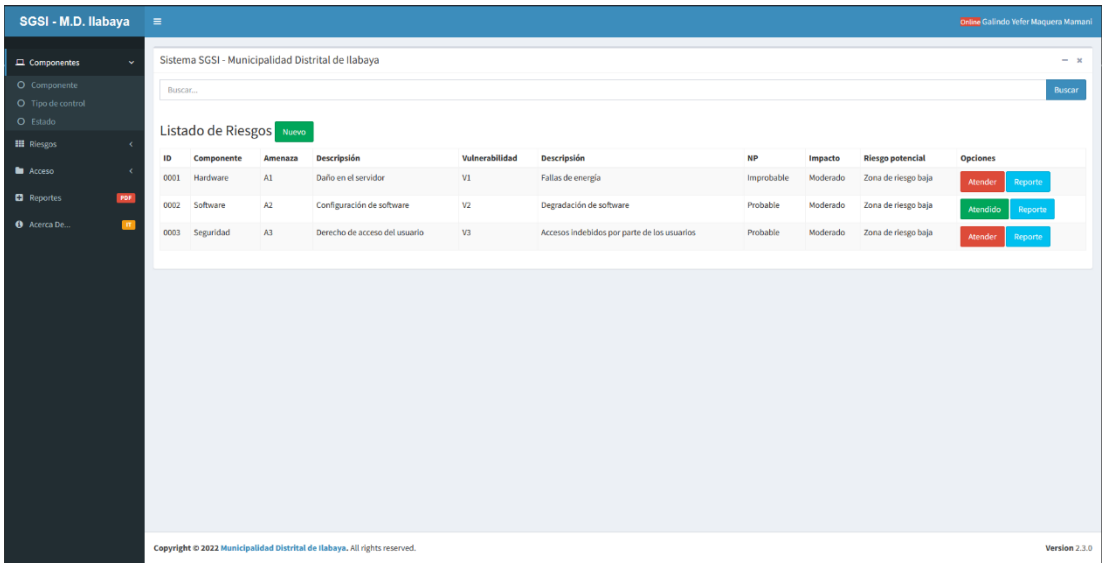


Figura 21: Página principal

Fuente: Elaboración propia

- ✓ **Listado de componentes**

Para agregar un nuevo registro es necesario en primera instancia agregar componentes tales como Componente, Tipo de control y Estado, esto con la finalidad de agilizar el llenado de campos en el registro de riesgos.

Figura 22: Listado de componentes

Fuente: Elaboración propia

- ✓ **Nuevo riesgo potencial**

Una vez agregado los componentes procedemos agregar un nuevo registro de riesgo potencial.

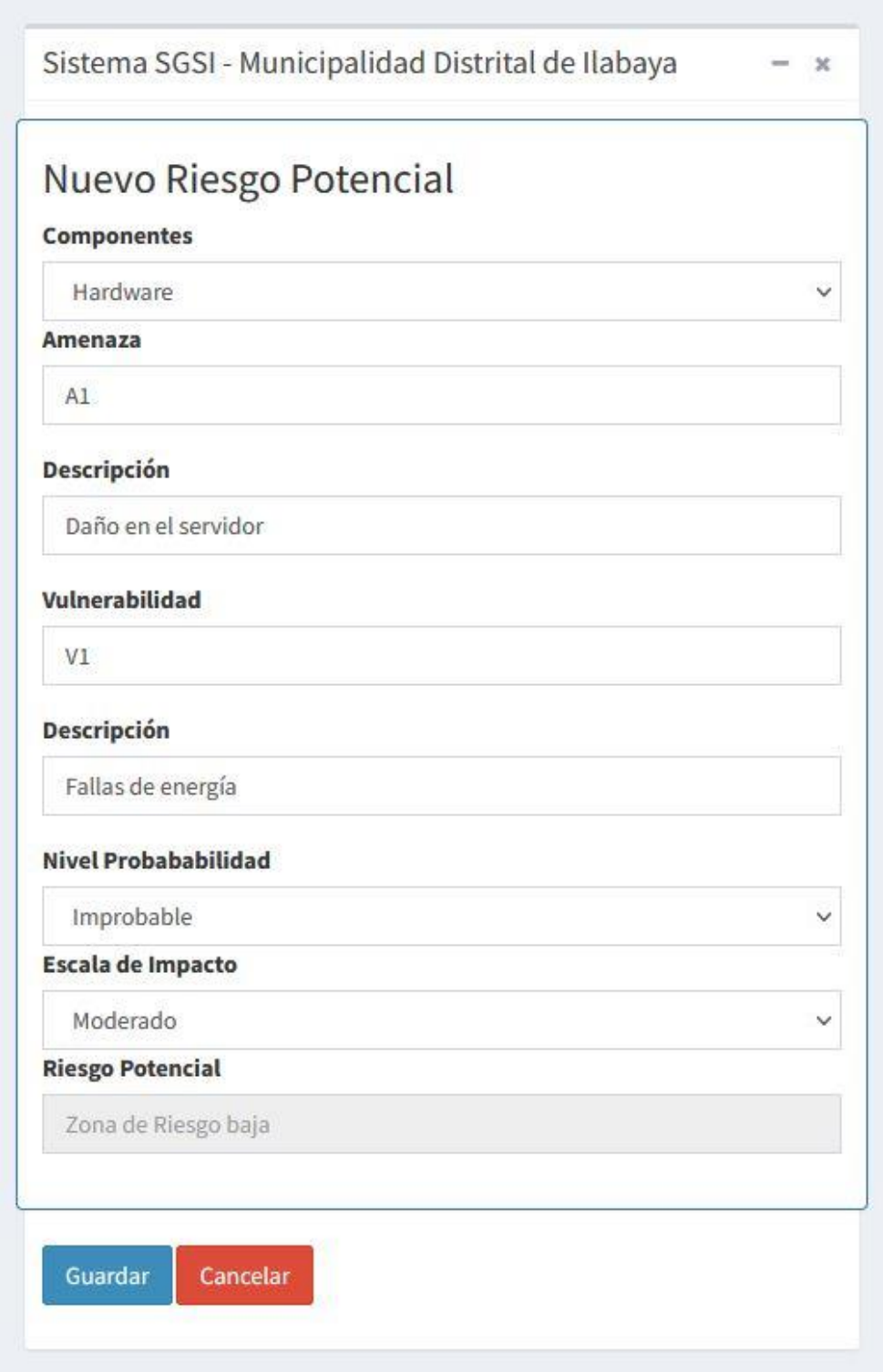


Figura 23: Nuevo registro de riesgo potencial

Fuente: Elaboración propia

✓ **Listado de riesgo potencial**

Después de agregar un nuevo riesgo el sistema muestra un listado de riesgos agregados, en donde tendremos la opción de atender los riesgos ingresados.

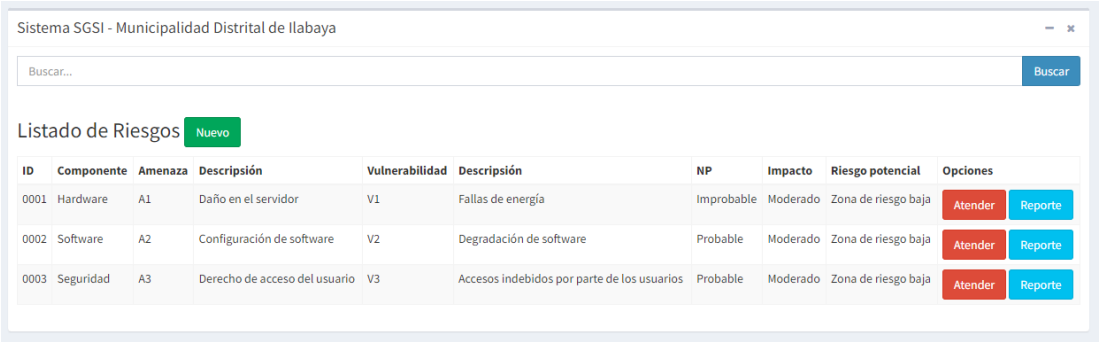


Figura 24: Listado de riesgo potencial

Fuente: Elaboración propia

✓ **Nuevo riesgo residual**

Después de agregar riesgo potencial en el listado de riesgos nos muestra una opción para atender, al ingresar procedemos atender el riesgo como se muestra en la Figura 43.

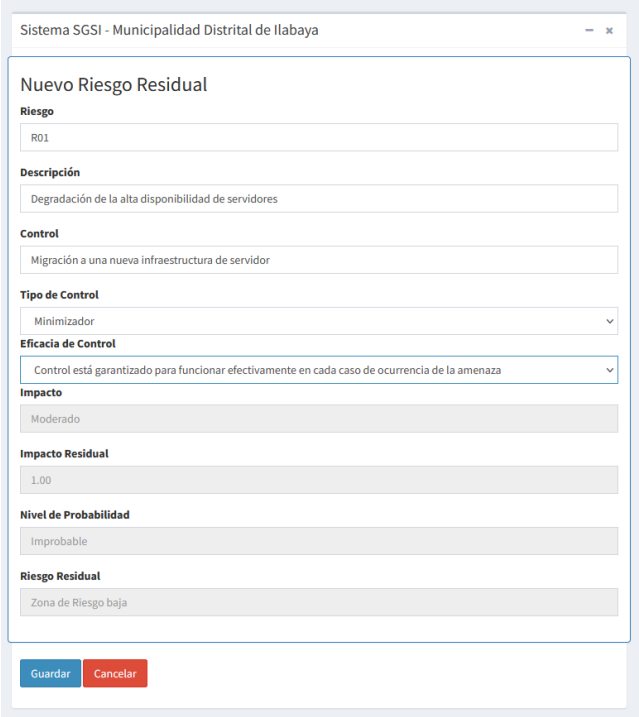


Figura 25: Atención de riesgo

Fuente: Elaboración propia

- ✓ **Listado de riesgo residual**

Una vez atendido el riesgo el sistema muestra un listado de riesgos en donde se puede mostrar detalle o generar reporte para los trámites correspondientes si lo amerita.

Figura 26: Listado de riesgos atendidos

Fuente: Elaboración propia

Luego de ser atendido el riesgo el sistema mostrará el botón Atendido de color verde en la sección de Opciones.

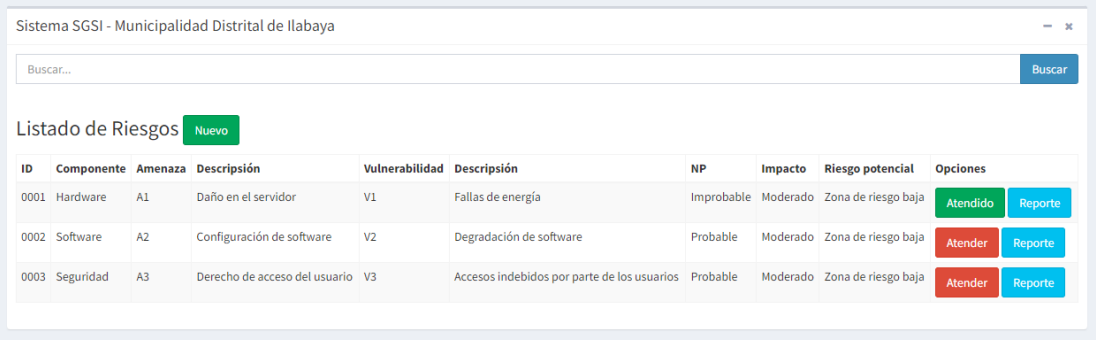


Figura 27: Listado de riesgo

Fuente: Elaboración propia

1.4 Cronograma de actividades

El cronograma de actividades esta desarrollado de acuerdo al tiempo establecido por el curso de investigación a su vez serán secuenciales y graduales según la siguiente tabla.

Tabla 13: Cronograma de actividades

Actividades / Semanas	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16
Identificación y acceso a la información	x	x														
Revisión y ajustes de los instrumentos de investigación			x	x												
Marco teórico				x	x	x										
Planteamiento y despliegue de datos					x	x	x									
Obtención de datos							x	x	x	x						
Resultados y conclusiones										x	x	x				

Desarrollo del informe final					x	x	x	x			
Interpretación preliminar								x			
Presentación y sustentación de tesis								x	x	x	

Fuente: Elaboración propia

1.5 Recursos humanos. Bienes y servicios

Asesor (1)

Estadístico (1)

Asistente (1)

1.6 Fuentes de financiamiento y presupuesto

El presupuesto estimado de todo el proyecto para la implementación de un sistema de gestión de seguridad de la información está estimado de la siguiente manera:

Tabla 14: Fuente de financiamiento y presupuesto

ÍTEM	DESCRIPCIÓN	UNIDAD	Nº DE UNIDADES	COSTO UNITARIO	COSTO TOTAL
1.0.	**RECURSOS HUMANOS**				
1.1.	Asesor	Hora	100	16	1,600.00
1.2.	Estadístico	Hora	50	13	650.00
1.3.	Asistente 1	Hora	480	13	6,240.00
	SUBTOTAL				8,490.00
2.0.	**RECURSOS MATERIALES**				
2.1.	Papel Bond	Millar	5	23	115.00
2.2	Útiles de oficina	Unidad	1	300	300.00
2.3	Computadora	Unidad	1	3000	3,000.00
	SUBTOTAL				3,415.00
3.0.	**SERVICIOS**				
3.1.	Fotocopias	Unidad	800	0.2	160.00
3.2.	Empastado	Unidad	6	30	180.00
3.3	Internet	Hora	100	2	200.00
3.4	Imprevistos	Varios	1	700	700.00
SUBTOTAL					1,240.00
TOTAL					**13,145.00**

Fuente: Elaboración propia

Anexo 3. Resolución

Resolución Ministerial

N° 004-2016-PCM

Lima, - 8 ENE. 2016

CONSIDERANDO:

Que, mediante Resolución Ministerial Nº 246-2007-PCM se aprobó el uso de la Norma Técnica Peruana "NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información. 2ª. Edición", en todas las entidades del Sistema Nacional de Informática;

Que, mediante Resolución Ministerial Nº 197-2011-PCM, se estableció el plazo para que determinadas entidades de la Administración Pública implementen el Plan de Seguridad de la Información dispuesto en la Norma Técnica Peruana antes señalada; posteriormente, mediante Resolución Ministerial Nº 129-2012-PCM se estableció un nuevo cronograma y la incorporación del rol del oficial de seguridad para el proceso de implementación de la Norma Técnica Peruana "NTP-ISO /IEC 27001:2008;

Que, la Norma Técnica Peruana "NTP ISO/IEC 27001:2008 EDI Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de seguridad de la Información. Requisitos", aprobada mediante Resolución Nº 42-2008/INDECOPI-CNB, por la Comisión de Normalización y de Fiscalización de Barreras Comerciales No Arancelarias del Instituto Nacional de Defensa de la Competencia y de Protección de la Propiedad Intelectual (INDECOPI) ha sido reemplazada por la nueva versión de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de seguridad de la Información. Requisitos.2ª Edición" aprobada por Resolución Nº 129-2014/DNB-INDECOPI;

Que, de acuerdo a lo establecido en el numeral 4.8 del artículo 4 y el artículo 49 del Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros, aprobado por el Decreto Supremo Nº 063-2007-PCM, la Presidencia del Consejo de Ministros actúa como ente rector del Sistema Nacional de Informática a través de la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI), siendo ésta la encargada de implementar la Política Nacional de Gobierno Electrónico e Informática;

Que, el "Plan de Desarrollo de la Sociedad de la Información en el Perú - La Agenda Digital Peruana 2.0" aprobado mediante Decreto Supremo Nº 066-2011-PCM, establece en su Objetivo Nº 7, la necesidad de promover una Administración Pública de calidad orientada a la población, determinando como parte de su Estrategia Nº 4, la implementación de mecanismos para mejorar la seguridad de la información, la necesidad de contar con una Estrategia Nacional de Ciberseguridad con el objetivo de minimizar los riesgos en caso de sufrir algún tipo de incidente en los recursos informáticos del Estado, así como, la disuasión del crimen cibernético, que se producen mediante el uso de redes teleinformáticas, entre otros;

Que, la actual Política Nacional de Gobierno Electrónico 2013 – 2017, aprobada mediante el Decreto Supremo N° 081-2013-PCM, prevé determinados Lineamientos

Estratégicos para el Gobierno Electrónico en el Perú, entre otros, el relacionado con la Seguridad de la Información, el mismo que busca velar por la integridad, seguridad y disponibilidad de los datos debiendo establecerse lineamientos de seguridad de la información a fin de mitigar el riesgo de exposición de información sensible del ciudadano, correspondiendo que en uso de las funciones atribuidas al ente rector del Sistema Nacional de Informática, para el caso ONGEI-PCM, a cargo de implementar dicha Política Nacional, articular la implementación efectiva del acotado lineamiento por parte de los distintos entes del sector público;

Que, estando a lo indicado en los considerando precedentes la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) de la Presidencia del Consejo de Ministros a través del Memorando N° 152-2015-PCM/ONGEI, recomienda la aplicación y uso de la Norma Técnica Peruana "NTP-ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de seguridad de la Información. Requisitos. 2ª Edición", en todas las entidades del Sistema Nacional de Informática, con la finalidad de coadyuvar con la infraestructura de Gobierno Electrónico, por considerar a la seguridad de la información, como un componente crucial para dicho objetivo;

De conformidad con lo dispuesto en la Ley N° 29158, Ley Orgánica del Poder Ejecutivo; la Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado; y, el Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros aprobado mediante Decreto Supremo N° 063-2007-PCM y sus modificatorias;

SE RESUELVE:

Artículo 1.- De la aprobación

Apruébese el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2ª Edición", en todas las entidades integrantes del Sistema Nacional de Informática.

Artículo 2.- Publicación

La Norma Técnica Peruana NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2ª Edición" será publicada en el Portal de la Presidencia del Consejo de Ministros (www.pcm.gob.pe) y en el Portal de la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) (www.ongei.gob.pe) el mismo día de la publicación de la presente resolución en el Diario Oficial El Peruano.

Artículo 3.- De la implementación

Las entidades integrantes del Sistema Nacional de Informática, tendrán un plazo máximo de dos (2) años para la implementación y/o adecuación de la presente norma.

Dichas entidades públicas tendrán un plazo de 60 días contados a partir de la fecha de publicación de la presente norma, para la presentación del cronograma de

Resolución Ministerial

implementación y/o adecuación del sistema de gestión de la Seguridad de la Información, que deberá ser presentado a la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) de la Presidencia del Consejo de Ministros.

La ONGEI brindará asistencia técnica a las entidades que lo requieran. Las entidades públicas que a la fecha cuenten con la certificación ISO 27001, están exoneradas del presente proceso de implementación.

Artículo 4.- De la certificación de la norma

Las entidades que requieran certificarse de acuerdo a lo establecido en la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2 Edición"; podrán realizar dicha certificación de forma opcional y con recursos propios de cada entidad.

Artículo 5.- Del Comité de Gestión de Seguridad de la Información

Cada entidad designará un Comité de Gestión de Seguridad de la Información, conformado por:

- El/la titular de la entidad;
- El/la responsable de administración o quien haga sus veces;
- El/la responsable de planificación o quien haga sus veces;
- El/la responsable del área de informática o quien haga sus veces;
- El/la responsable de área legal o quien haga sus veces y
- El/la oficial de seguridad de la información.

Las funciones del Comité de Gestión de Seguridad de la Información, serán establecidas por cada entidad de acuerdo a la norma que se aprueba mediante el Artículo 1° de la presente Resolución Ministerial.

Artículo 6.- De la responsabilidad de la implementación

La responsabilidad de la implementación de la presente norma será del titular de cada entidad.

Artículo 7.- Déjese sin efecto

Deróguese la Resolución Ministerial N° 129-2012-PCM.

Regístrese, comuníquese y publíquese

PEDRO CATERIANO BELLIDO
Presidente del Consejo de Ministros

Anexo 4. Instrumento Encuesta

CUESTIONARIO

Estimado (a):

La siguiente encuesta es de uso exclusivo para el proyecto de investigación, titulada Sistema de Gestión de Seguridad de la Información y su relación con la calidad de servicio de las redes LAN en la Municipalidad Distrital de Ilabaya, 2022.

*A continuación, encontrará una serie de enunciados con relación a su trabajo. Se solicita su opinión sincera al respecto. Después de leer cuidadosamente cada enunciado, marque con una **X** la alternativa que corresponda a su opinión; en base a la siguiente Leyenda:*

N°	Leyenda
1	Nunca
2	Casi Nunca
3	A veces
4	Casi Siempre
5	Siempre

Gerencia / Unidad: ..... Periodo Laboral: ….....

Cargo: …… Sexo: ..... Edad: ……..

Variable independiente: Sistema de Gestión de Seguridad de la Información							
Dimensión	N°	Preguntas	1	2	3	4	5
Confidencialidad		Seguridad de Personal					
	1	¿Se definen funciones y roles para la seguridad de la información?					
	2	¿Se definen procedimientos en caso de cese de personal, que incluyan la confidencialidad de la información en la entidad?					
		Privacidad de la información					
	3	¿Existen políticas de seguridad de la información?					
	4	¿Se han adoptado controles que ayuden a resguardar la privacidad de la información?					
Integridad		Seguridad lógica					
	5	¿Se realizan evaluaciones periódicas a los accesos concedidos de los usuarios?					
	6	¿Ud. cuenta con identificación única, en caso de posibles responsabilidades que puedan ser					

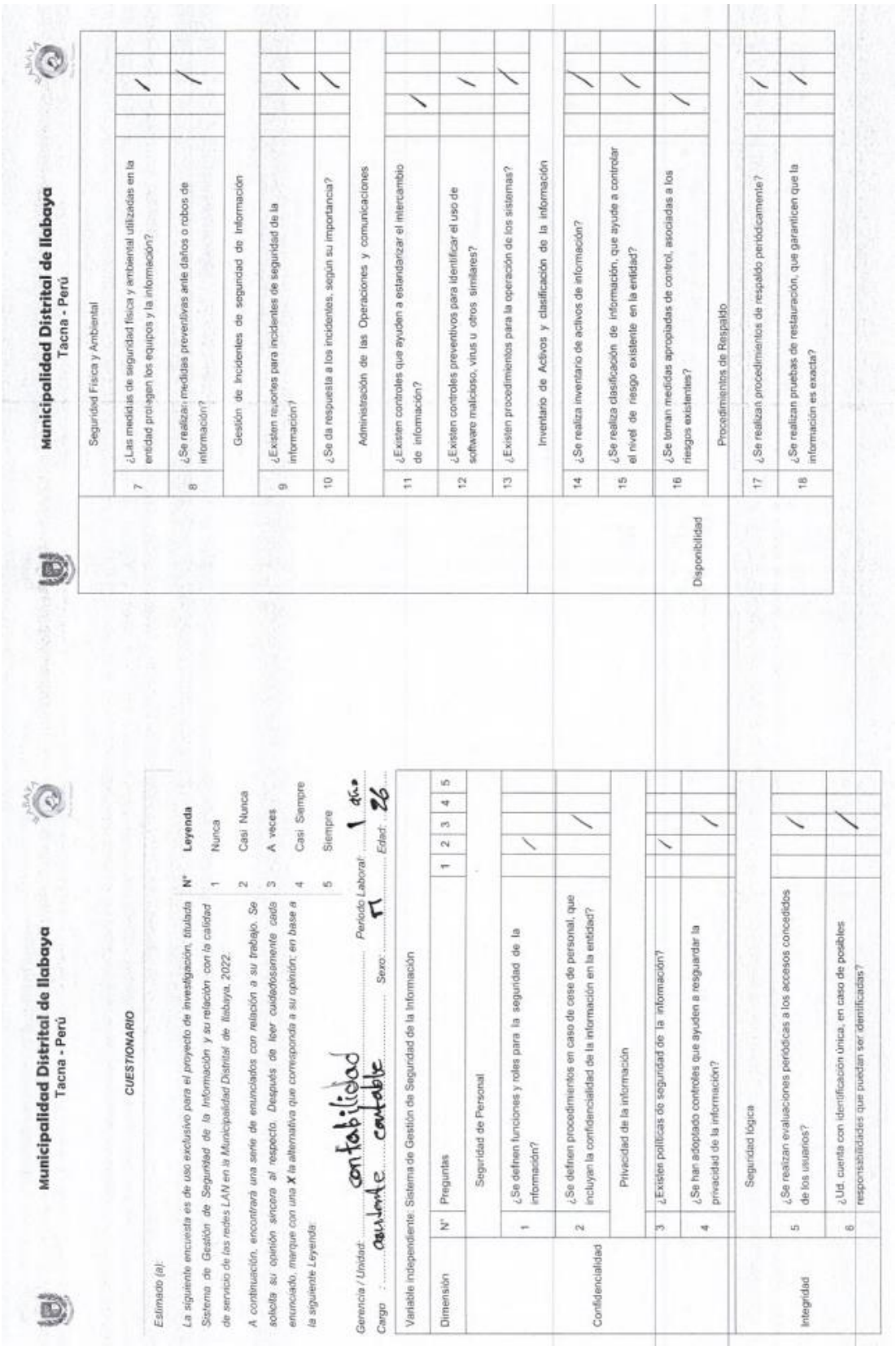
		identificadas?					
		Seguridad Física y Ambiental					
	7	¿Las medidas de seguridad física y ambiental utilizadas en la entidad protegen los equipos y la información?					
	8	¿Se realizan medidas preventivas ante daños o robos de información?					
		Gestión de Incidentes de seguridad de Información					
	9	¿Existen reportes para incidentes de seguridad de la información?					
	10	¿Se da respuesta a los incidentes, según su importancia?					
		Administración de las Operaciones y comunicaciones					
	11	¿Existen controles que ayuden a estandarizar el intercambio de información?					
	12	¿Existen controles preventivos para identificar el uso de software malicioso, virus u otros similares?					
	13	¿Existen procedimientos para la operación de los sistemas?					
Disponibilidad		Inventario de Activos y clasificación de la información					
	14	¿Se realiza inventario de activos de información?					
	15	¿Se realiza clasificación de información, que ayude a controlar el nivel de riesgo existente en la entidad?					
	16	¿Se toman medidas apropiadas de control, asociadas a los riesgos existentes?					
		Procedimientos de Respaldo					
	17	¿Se realizan procedimientos de respaldo periódicamente?					

	18	¿Se realizan pruebas de restauración, que garanticen que la información es exacta?					

Variable dependiente: Calidad de servicio de las redes LAN							
Dimensión	N°	Preguntas	1	2	3	4	5
Confiabilidad		Eficiencia					
	1	¿La calidad de servicio de redes es eficiente en la Municipalidad Distrital de Ilabaya?					
	2	¿Considera que la eficiencia de las redes es primordial en la Municipalidad Distrital de Ilabaya?					
		Efectividad					
	3	¿Los accesos a la información por medio de la Red son efectivas?					
	4	¿EL acceso a los servidores de los sistemas integrados de la entidad es estable?					
Aseguramiento		Confianza					
	5	¿La atención que se le da vía telefónica en cuanto a fallas tecnológicas y/o red solucionan sus problemas?					
	6	¿La capacidad de respuesta cuando usted utiliza cualquier servicio tecnológico por intermedio de la Red es inmediata?					
		Credibilidad					
	7	¿Los datos consultados por medio de la Red tienen un alto grado de fiabilidad?					
	8	¿La disponibilidad de la Red en la Municipalidad Distrital de Ilabaya es garantizada por equipo de respaldo?					
Capacidad de respuesta		Tiempo de respuesta					
	9	¿El tiempo de respuesta en atención a requerimientos					

		de redes influye en la seguridad de la información?					
	10	¿El tiempo de respuesta de información de calidad es considerable?					
		Mejora continua					
	11	¿Existen medios por donde el cliente interno podría realizar algunos comentarios sobre la calidad de servicio de la Red de la entidad?					
	12	¿Se lanzan encuestas y/o cuestionarios para saber la perspectiva desde el usuario interno sobre la calidad de servicio de la red en la Municipalidad Distrital de Ilabaya?					

Anexo 5. Encuestas Desarrolladas



Municipalidad Distrital de Ilabaya
Tacna - Perú

CUESTIONARIO

Estimado (a):

La siguiente encuesta es de uso exclusivo para el proyecto de investigación, titulada Sistema de Gestión de Seguridad de la Información y su relación con la calidad de servicio de las redes LAN en la Municipalidad Distrital de Ilabaya, 2022.

A continuación, encontrará una serie de enunciados con relación a su trabajo. Se solicita su opinión sincera al respecto. Después de leer cuidadosamente cada enunciado, marque con una X la alternativa que corresponda a su opinión; en base a la siguiente Leyenda:

N°	Leyenda
1	Nunca
2	Casi Nunca
3	A veces
4	Casi Siempre
5	Siempre

Gerencia / Unidad: contabilidad Periodo Laboral: 1 año

Cargo : asistente contable Sexo: F Edad: 26

Variable independiente: Sistema de Gestión de Seguridad de la Información

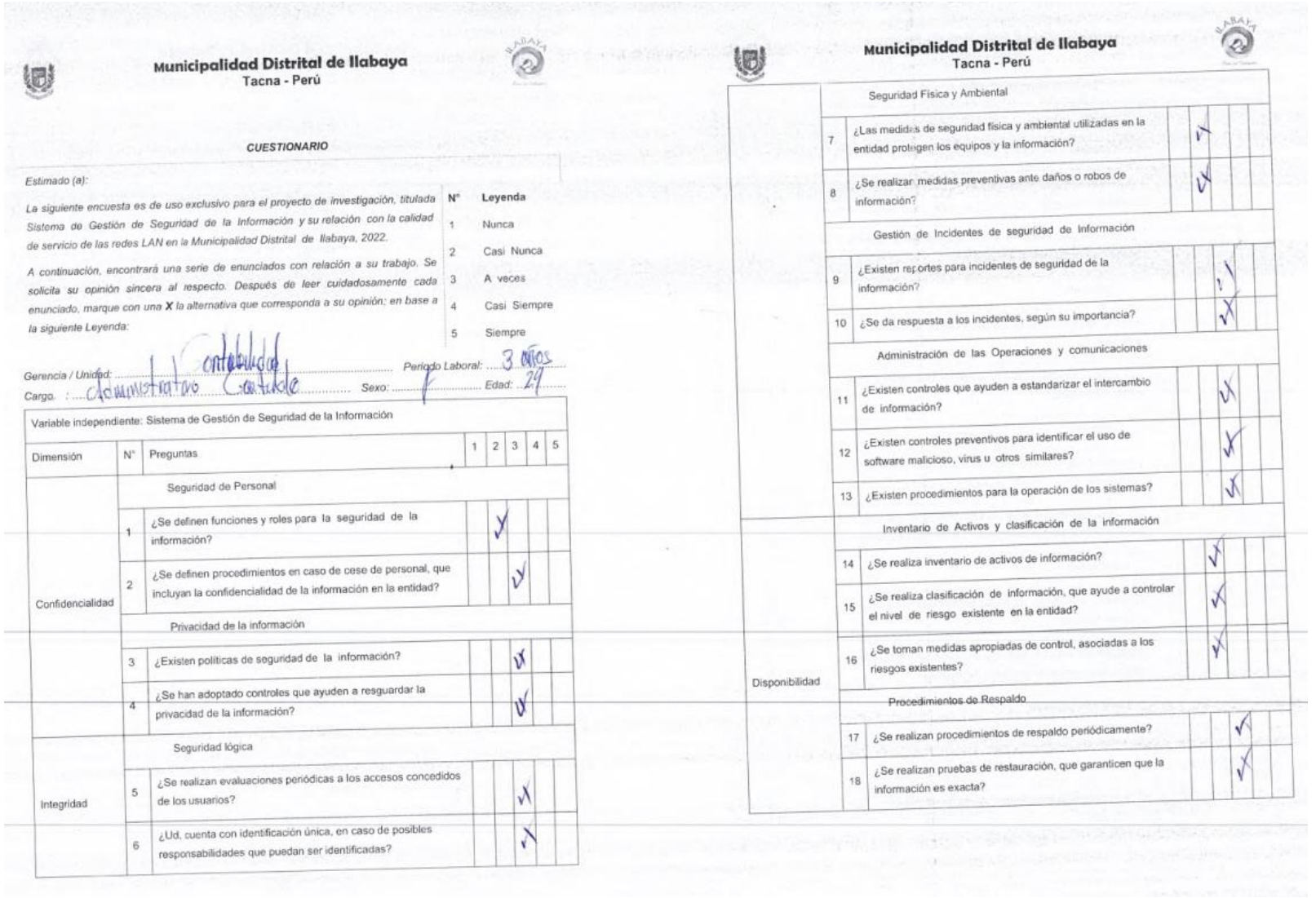
Dimensión	N°	Preguntas	1	2	3	4	5
		Seguridad de Personal					
Confidencialidad	1	¿Se definen funciones y roles para la seguridad de la información?		/			
	2	¿Se definen procedimientos en caso de cese de personal, que incluyan la confidencialidad de la información en la entidad?			/		
		Privacidad de la información					
	3	¿Existen políticas de seguridad de la información?		/			
	4	¿Se han adoptado controles que ayuden a resguardar la privacidad de la información?			/		
		Seguridad lógica					
Integridad	5	¿Se realizan evaluaciones periódicas a los accesos concedidos de los usuarios?			/		
	6	¿Ud. cuenta con identificación única, en caso de posibles responsabilidades que puedan ser identificadas?			/		
	7	¿Las medidas de seguridad física y ambiental utilizadas en la entidad protegen los equipos y la información?				/	
	8	¿Se realizan medidas preventivas ante daños o robos de información?				/	
		Gestión de Incidentes de seguridad de Información					
	9	¿Existen reportes para incidentes de seguridad de la información?				/	
	10	¿Se da respuesta a los incidentes, según su importancia?				/	
		Administración de las Operaciones y comunicaciones					
	11	¿Existen controles que ayuden a estandarizar el intercambio de información?				/	
	12	¿Existen controles preventivos para identificar el uso de software malicioso, virus u otros similares?				/	
	13	¿Existen procedimientos para la operación de los sistemas?				/	
		Inventario de Activos y clasificación de la información					
Disponibilidad	14	¿Se realiza inventario de activos de información?				/	
	15	¿Se realiza clasificación de información, que ayude a controlar el nivel de riesgo existente en la entidad?				/	
	16	¿Se toman medidas apropiadas de control, asociadas a los riesgos existentes?				/	
		Procedimientos de Respaldo					
	17	¿Se realizan procedimientos de respaldo periódicamente?				/	
	18	¿Se realizan pruebas de restauración, que garanticen que la información es exacta?				/	

Municipalidad Distrital de Ilabaya
Tacna - Perú

Variable dependiente: Calidad de servicio de las redes LAN								
Dimensión	N°	Preguntas	1	2	3	4	5	
Confiabilidad		Eficiencia						
	1	¿La calidad de servicio de redes es eficiente en la Municipalidad Distrital de Ilabaya?			✓			
	2	¿Considera que la eficiencia de las redes es primordial en la Municipalidad Distrital de Ilabaya?			✓			
		Efectividad						
	3	¿Los accesos a la información por medio de la Red son efectivas?		✓				
	4	¿EL acceso a los servidores de los sistemas integrados de la entidad es estable?		✓				
Aseguramiento		Confianza						
	5	¿La atención que se le da vía telefónica en cuanto a fallas tecnológicas y/o red solucionan sus problemas?		✓				
	6	¿La capacidad de respuesta cuando usted utiliza cualquier servicio tecnológico por intermedio de la Red es inmediata?		✓				
		Credibilidad						
	7	¿Los datos consultados por medio de la Red tienen un alto grado de fiabilidad?		✓				
	8	¿La disponibilidad de la Red en la Municipalidad Distrital de Ilabaya es garantizada por equipo de respaldo?		✓				
Capacidad de respuesta		Tiempo de respuesta						
	9	¿El tiempo de respuesta en atención a requerimientos de redes influye en la seguridad de la información?		✓				
	10	¿El tiempo de respuesta de información de calidad es considerable?		✓				

Municipalidad Distrital de Ilabaya
Tacna - Perú

		Mejora continua						
	11	¿Existen medios por donde el cliente interno podría realizar algunos comentarios sobre la calidad de servicio de la Red de la entidad?	✓					
	12	¿Se lanzan encuestas y/o cuestionarios para saber la perspectiva desde el usuario interno sobre la calidad de servicio de la red en la Municipalidad Distrital de Ilabaya?	✓					



Municipalidad Distrital de Ilabaya
Tacna - Perú

CUESTIONARIO

Estimado (a):

La siguiente encuesta es de uso exclusivo para el proyecto de investigación, titulada Sistema de Gestión de Seguridad de la Información y su relación con la calidad de servicio de las redes LAN en la Municipalidad Distrital de Ilabaya, 2022.

A continuación, encontrará una serie de enunciados con relación a su trabajo. Se solicita su opinión sincera al respecto. Después de leer cuidadosamente cada enunciado, marque con una ***X*** *la alternativa que corresponda a su opinión; en base a la siguiente Leyenda:*

N°	Leyenda
1	Nunca
2	Casi Nunca
3	A veces
4	Casi Siempre
5	Siempre

Gerencia / Unidad: contabilidad *Periodo Laboral:* 3 años

Cargo: Administrativo Contable *Sexo:* F *Edad:* 29

Variable independiente: Sistema de Gestión de Seguridad de la Información							
Dimensión	N°	Preguntas	1	2	3	4	5
Confidencialidad		Seguridad de Personal					
	1	¿Se definen funciones y roles para la seguridad de la información?				✓	
	2	¿Se definen procedimientos en caso de cese de personal, que incluyan la confidencialidad de la información en la entidad?				✓	
		Privacidad de la información					
	3	¿Existen políticas de seguridad de la información?				✓	
	4	¿Se han adoptado controles que ayuden a resguardar la privacidad de la información?				✓	
Integridad		Seguridad lógica					
	5	¿Se realizan evaluaciones periódicas a los accesos concedidos de los usuarios?				✓	
	6	¿Ud. cuenta con identificación única, en caso de posibles responsabilidades que puedan ser identificadas?				✓	

Municipalidad Distrital de Ilabaya
Tacna - Perú

		Seguridad Física y Ambiental					
	7	¿Las medidas de seguridad física y ambiental utilizadas en la entidad protegen los equipos y la información?				✓	
	8	¿Se realizan medidas preventivas ante daños o robos de información?				✓	
		Gestión de Incidentes de seguridad de Información					
	9	¿Existen reportes para incidentes de seguridad de la información?				✓	
	10	¿Se da respuesta a los incidentes, según su importancia?				✓	
		Administración de las Operaciones y comunicaciones					
	11	¿Existen controles que ayuden a estandarizar el intercambio de información?				✓	
	12	¿Existen controles preventivos para identificar el uso de software malicioso, virus u otros similares?				✓	
	13	¿Existen procedimientos para la operación de los sistemas?				✓	
Disponibilidad		Inventario de Activos y clasificación de la información					
	14	¿Se realiza inventario de activos de información?					✓
	15	¿Se realiza clasificación de información, que ayude a controlar el nivel de riesgo existente en la entidad?					✓
	16	¿Se toman medidas apropiadas de control, asociadas a los riesgos existentes?					✓
		Procedimientos de Respaldo					
	17	¿Se realizan procedimientos de respaldo periódicamente?				✓	
	18	¿Se realizan pruebas de restauración, que garanticen que la información es exacta?				✓	

Municipalidad Distrital de Ilabaya

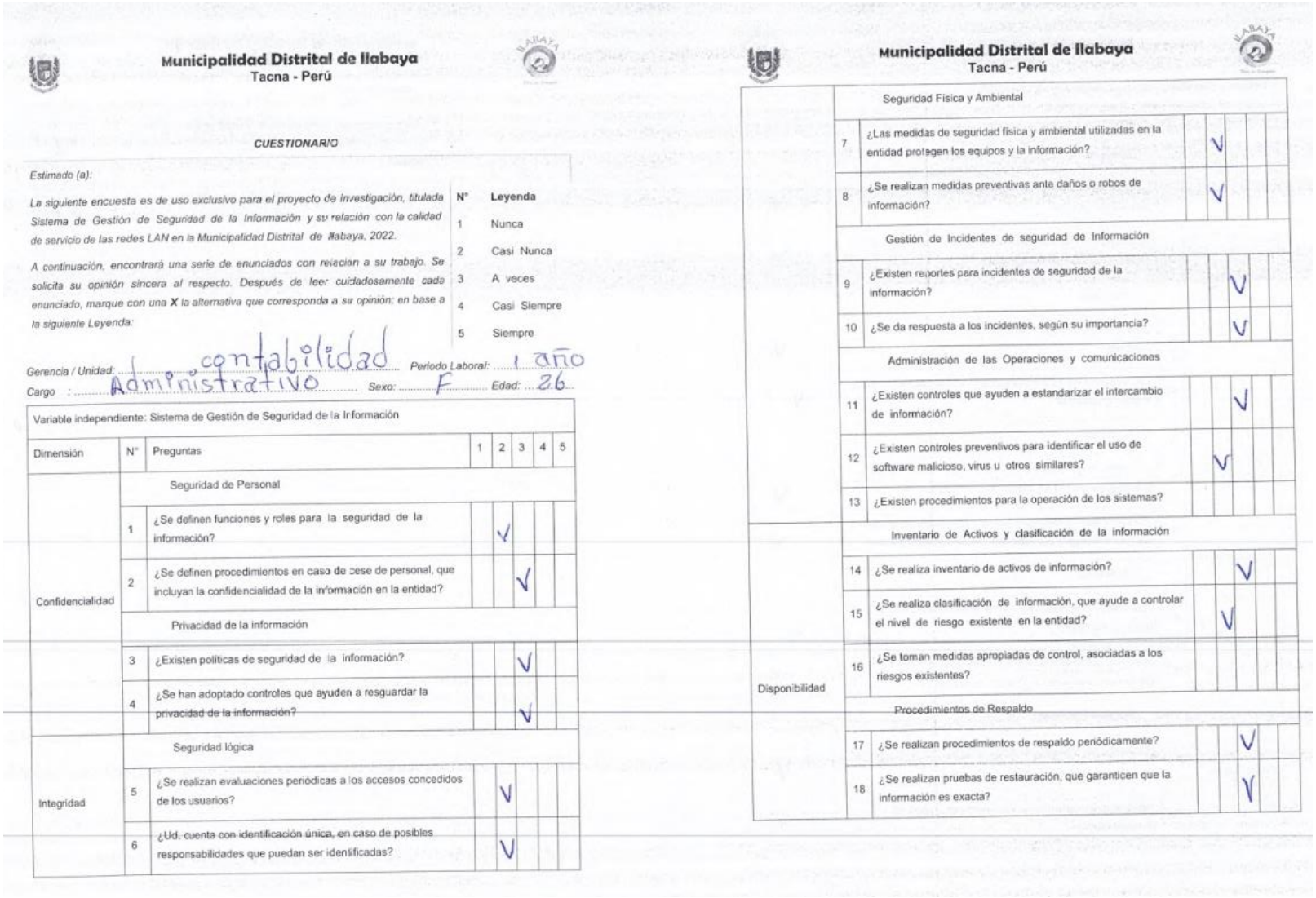
"Año del Fortalecimiento de la Soberanía Nacional"

Municipalidad Distrital de Ilabaya
Tacna - Perú

Variable dependiente: Calidad de servicio de las redes LAN								
Dimensión	N°	Preguntas	1	2	3	4	5	
Confiabilidad		Eficiencia						
	1	¿La calidad de servicio de redes es eficiente en la Municipalidad Distrital de Ilabaya?			✓			
	2	¿Considera que la eficiencia de las redes es primordial en la Municipalidad Distrital de Ilabaya?				✓		
		Efectividad						
	3	¿Los accesos a la información por medio de la Red son efectivas?			✓			
	4	¿EL acceso a los servidores de los sistemas integrados de la entidad es estable?			✓			
Aseguramiento		Confianza						
	5	¿La atención que se le da vía telefónica en cuanto a fallas tecnológicas y/o red solucionan sus problemas?			✓			
	6	¿La capacidad de respuesta cuando usted utiliza cualquier servicio tecnológico por intermedio de la Red es inmediata?			✓			
		Credibilidad						
	7	¿Los datos consultados por medio de la Red tienen un alto grado de fiabilidad?			✓			
	8	¿La disponibilidad de la Red en la Municipalidad Distrital de Ilabaya es garantizada por equipo de respaldo?			✓			
Capacidad de respuesta		Tiempo de respuesta						
	9	¿El tiempo de respuesta en atención a requerimientos de redes influye en la seguridad de la información?			✓			
	10	¿El tiempo de respuesta de información de calidad es considerable?			✓			

Municipalidad Distrital de Ilabaya
Tacna - Perú

		Mejora continua						
	11	¿Existen medios por donde el cliente interno podría realizar algunos comentarios sobre la calidad de servicio de la Red de la entidad?			✓			
	12	¿Se lanzan encuestas y/o cuestionarios para saber la perspectiva desde el usuario interno sobre la calidad de servicio de la red en la Municipalidad Distrital de Ilabaya?			✓			



Municipalidad Distrital de Ilabaya
Tacna - Perú

CUESTIONARIO

Estimado (a):

La siguiente encuesta es de uso exclusivo para el proyecto de investigación, titulada Sistema de Gestión de Seguridad de la Información y su relación con la calidad de servicio de las redes LAN en la Municipalidad Distrital de Ilabaya, 2022.

A continuación, encontrará una serie de enunciados con relacion a su trabajo. Se solicita su opinión sincera al respecto. Después de leer cuidadosamente cada enunciado, marque con una X la alternativa que corresponda a su opinión; en base a la siguiente Leyenda:

N°	Leyenda
1	Nunca
2	Casi Nunca
3	A veces
4	Casi Siempre
5	Siempre

Gerencia / Unidad: contabilidad *Periodo Laboral:* 1 año
Cargo : Administrativo *Sexo:* F *Edad:* 26

Variable independiente: Sistema de Gestión de Seguridad de la Información

Dimensión	N°	Preguntas	1	2	3	4	5
		Seguridad de Personal					
Confidencialidad	1	¿Se definen funciones y roles para la seguridad de la información?		√			
	2	¿Se definen procedimientos en caso de cese de personal, que incluyan la confidencialidad de la información en la entidad?			√		
		Privacidad de la información					
	3	¿Existen políticas de seguridad de la información?			√		
	4	¿Se han adoptado controles que ayuden a resguardar la privacidad de la información?			√		
Integridad		Seguridad lógica					
	5	¿Se realizan evaluaciones periódicas a los accesos concedidos de los usuarios?		√			
	6	¿Ud. cuenta con identificación única, en caso de posibles responsabilidades que puedan ser identificadas?		√			
		Seguridad Física y Ambiental					
	7	¿Las medidas de seguridad física y ambiental utilizadas en la entidad protegen los equipos y la información?		√			
	8	¿Se realizan medidas preventivas ante daños o robos de información?		√			
		Gestión de Incidentes de seguridad de Información					
	9	¿Existen reportes para incidentes de seguridad de la información?			√		
	10	¿Se da respuesta a los incidentes, según su importancia?			√		
		Administración de las Operaciones y comunicaciones					
	11	¿Existen controles que ayuden a estandarizar el intercambio de información?			√		
	12	¿Existen controles preventivos para identificar el uso de software malicioso, virus u otros similares?		√			
	13	¿Existen procedimientos para la operación de los sistemas?					
		Inventario de Activos y clasificación de la información					
	14	¿Se realiza inventario de activos de información?			√		
	15	¿Se realiza clasificación de información, que ayude a controlar el nivel de riesgo existente en la entidad?		√			
Disponibilidad	16	¿Se toman medidas apropiadas de control, asociadas a los riesgos existentes?					
		Procedimientos de Respaldo					
	17	¿Se realizan procedimientos de respaldo periódicamente?			√		
	18	¿Se realizan pruebas de restauración, que garanticen que la información es exacta?			√		

Municipalidad Distrital de Ilabaya
Tacna - Perú

Variable dependiente: Calidad de servicio de las redes LAN								
Dimensión	N°	Preguntas	1	2	3	4	5
Confiabilidad		Eficiencia					
	1	¿La calidad de servicio de redes es eficiente en la Municipalidad Distrital de Ilabaya?			√		
	2	¿Considera que la eficiencia de las redes es primordial en la Municipalidad Distrital de Ilabaya?			√		
		Efectividad					
	3	¿Los accesos a la información por medio de la Red son efectivas?			√		
	4	¿EL acceso a los servidores de los sistemas integrados de la entidad es estable?		√			
Aseguramiento		Confianza					
	5	¿La atención que se le da vía telefónica en cuanto a fallas tecnológicas y/o red solucionan sus problemas?			√		
	6	¿La capacidad de respuesta cuando usted utiliza cualquier servicio tecnológico por intermedio de la Red es inmediata?			√		
		Credibilidad					
	7	¿Los datos consultados por medio de la Red tienen un alto grado de fiabilidad?		√			
	8	¿La disponibilidad de la Red en la Municipalidad Distrital de Ilabaya es garantizada por equipo de respaldo?			√		
Capacidad de respuesta		Tiempo de respuesta					
	9	¿El tiempo de respuesta en atención a requerimientos de redes influye en la seguridad de la información?			√		
	10	¿El tiempo de respuesta de información de calidad es considerable?			√		

Municipalidad Distrital de Ilabaya
Tacna - Perú

	Mejora continua						
	11	¿Existen medios por donde el cliente interno podría realizar algunos comentarios sobre la calidad de servicio de la Red de la entidad?			√		
	12	¿Se lanzan encuestas y/o cuestionarios para saber la perspectiva desde el usuario interno sobre la calidad de servicio de la red en la Municipalidad Distrital de Ilabaya?			√		

Municipalidad Distrital de Ilabaya
Tacna - Perú

CUESTIONARIO

Estimado (a):

La siguiente encuesta es de uso exclusivo para el proyecto de investigación, titulada Sistema de Gestión de Seguridad de la Información y su relación con la calidad de servicio de las redes LAN en la Municipalidad Distrital de Ilabaya, 2022.

*A continuación, encontrará una serie de enunciados con relación a su trabajo. Se solicita su opinión sincera al respecto. Después de leer cuidadosamente cada enunciado, marque con una **X** la alternativa que corresponda a su opinión; en base a la siguiente Leyenda:*

N°	Leyenda
1	Nunca
2	Casi Nunca
3	A veces
4	Casi Siempre
5	Siempre

Gerencia / Unidad: contabilidad *Periodo Laboral:* 8 años
Cargo : Especialista *Sexo:* f *Edad:* 34

Variable independiente: Sistema de Gestión de Seguridad de la Información

Dimensión	N°	Preguntas	1	2	3	4	5
Confidencialidad		Seguridad de Personal					
	1	¿Se definen funciones y roles para la seguridad de la información?			X		
	2	¿Se definen procedimientos en caso de cese de personal, que incluyan la confidencialidad de la información en la entidad?			X		
		Privacidad de la información					
	3	¿Existen políticas de seguridad de la información?				X	
	4	¿Se han adoptado controles que ayuden a resguardar la privacidad de la información?			X		
Integridad		Seguridad lógica					
	5	¿Se realizan evaluaciones periódicas a los accesos concedidos de los usuarios?		X			
	6	¿Ud. cuenta con identificación única, en caso de posibles responsabilidades que puedan ser identificadas?			X		

Municipalidad Distrital de Ilabaya
Tacna - Perú

		Seguridad Física y Ambiental					
	7	¿Las medidas de seguridad física y ambiental utilizadas en la entidad protegen los equipos y la información?			X		
	8	¿Se realizan medidas preventivas ante daños o robos de información?			X		
		Gestión de Incidentes de seguridad de Información					
	9	¿Existen reportes para incidentes de seguridad de la información?		X			
	10	¿Se da respuesta a los incidentes, según su importancia?			X		
		Administración de las Operaciones y comunicaciones					
	11	¿Existen controles que ayuden a estandarizar el intercambio de información?			X		
	12	¿Existen controles preventivos para identificar el uso de software malicioso, virus u otros similares?		X			
	13	¿Existen procedimientos para la operación de los sistemas?			X		
Disponibilidad		Inventario de Activos y clasificación de la información					
	14	¿Se realiza inventario de activos de información?			X		
	15	¿Se realiza clasificación de información, que ayude a controlar el nivel de riesgo existente en la entidad?			X		
	16	¿Se toman medidas apropiadas de control, asociadas a los riesgos existentes?		X			
		Procedimientos de Respaldo					
	17	¿Se realizan procedimientos de respaldo periódicamente?	X				
	18	¿Se realizan pruebas de restauración, que garanticen que la información es exacta?	X				

Municipalidad Distrital de Ilabaya
Tacna - Perú

Variable dependiente: Calidad de servicio de las redes LAN								
Dimensión	N°	Preguntas	1	2	3	4	5
Confiabilidad		Eficiencia					
	1	¿La calidad de servicio de redes es eficiente en la Municipalidad Distrital de Ilabaya?			X		
	2	¿Considera que la eficiencia de las redes es primordial en la Municipalidad Distrital de Ilabaya?					X
		Efectividad					
	3	¿Los accesos a la información por medio de la Red son efectivas?			X		
	4	¿EL acceso a los servidores de los sistemas integrados de la entidad es estable?			X		
Aseguramiento		Confianza					
	5	¿La atención que se le da vía telefónica en cuanto a fallas tecnológicas y/o red soluconan sus problemas?			X		
	6	¿La capacidad de respuesta cuando usted utiliza cualquier servicio tecnológico por intermedio de la Red es inmediata?		X			
		Credibilidad					
	7	¿Los datos consultados por medio de la Red tienen un alto grado de fiabilidad?		X			
	8	¿La disponibilidad de la Red en la Municipalidad Distrital de Ilabaya es garantizada por equipo de respaldo?			X		
Capacidad de respuesta		Tiempo de respuesta					
	9	¿El tiempo de respuesta en atención a requerimientos de redes influye en la seguridad de la información?			X		
	10	¿El tiempo de respuesta de información de calidad es considerable?			X		

Municipalidad Distrital de Ilabaya
Tacna - Perú

	Mejora continua						
	11	¿Existen medios por donde el cliente interno podría realizar algunos comentarios sobre la calidad de servicio de la Red de la entidad?	X				
	12	¿Se lanzan encuestas y/o cuestionarios para saber la perspectiva desde el usuario interno sobre la calidad de servicio de la red en la Municipalidad Distrital de Ilabaya?	X				

Municipalidad Distrital de Ilabaya
Tacna - Perú

CUESTIONARIO

Estimado (a):

La siguiente encuesta es de uso exclusivo para el proyecto de investigación, titulada Sistema de Gestión de Seguridad de la Información y su relación con la calidad de servicio de las redes LAN en la Municipalidad Distrital de Ilabaya, 2022.

*A continuación, encontrará una serie de enunciados con relación a su trabajo. Se solicita su opinión sincera al respecto. Después de leer cuidadosamente cada enunciado, marque con una **X** la alternativa que corresponda a su opinión; en base a la siguiente Leyenda:*

N°	Leyenda
1	Nunca
2	Casi Nunca
3	A veces
4	Casi Siempre
5	Siempre

Gerencia / Unidad: Contabilidad *Periodo Laboral:* 2 años

Cargo : Asistente Contable *Sexo:* F *Edad:* 37

Variable independiente: Sistema de Gestión de Seguridad de la Información

Dimensión	N°	Preguntas	1	2	3	4	5
		Seguridad de Personal					
	1	¿Se definen funciones y roles para la seguridad de la información?		X			
Confidencialidad	2	¿Se definen procedimientos en caso de cese de personal, que incluyan la confidencialidad de la información en la entidad?		X			
		Privacidad de la información					
	3	¿Existen políticas de seguridad de la información?		X			
	4	¿Se han adoptado controles que ayuden a resguardar la privacidad de la información?		X			
		Seguridad lógica					
Integridad	5	¿Se realizan evaluaciones periódicas a los accesos concedidos de los usuarios?		X			
	6	¿Ud. cuenta con identificación única, en caso de posibles responsabilidades que puedan ser identificadas?			X		

Municipalidad Distrital de Ilabaya
Tacna - Perú

		Seguridad Física y Ambiental					
	7	¿Las medidas de seguridad física y ambiental utilizadas en la entidad protegen los equipos y la información?		X			
	8	¿Se realizan medidas preventivas ante daños o robos de información?		X			
		Gestión de Incidentes de seguridad de Información					
	9	¿Existen reportes para incidentes de seguridad de la información?		X			
	10	¿Se da respuesta a los incidentes, según su importancia?		X			
		Administración de las Operaciones y comunicaciones					
	11	¿Existen controles que ayuden a estandarizar el intercambio de información?			X		
	12	¿Existen controles preventivos para identificar el uso de software malicioso, virus u otros similares?			X		
	13	¿Existen procedimientos para la operación de los sistemas?		X			
		Inventario de Activos y clasificación de la información					
	14	¿Se realiza inventario de activos de información?			X		
	15	¿Se realiza clasificación de información, que ayude a controlar el nivel de riesgo existente en la entidad?		X			
Disponibilidad	16	¿Se toman medidas apropiadas de control, asociadas a los riesgos existentes?			X		
		Procedimientos de Respaldo					
	17	¿Se realizan procedimientos de respaldo periódicamente?		X			
	18	¿Se realizan pruebas de restauración, que garanticen que la información es exacta?		X			

Municipalidad Distrital de Ilabaya
Tacna - Perú

Variable dependiente: Calidad de servicio de las redes LAN								
Dimensión	N°	Preguntas	1	2	3	4	5
Confiabilidad		Eficiencia					
	1	¿La calidad de servicio de redes es eficiente en la Municipalidad Distrital de Ilabaya?			X		
	2	¿Considera que la eficiencia de las redes es primordial en la Municipalidad Distrital de Ilabaya?					X
		Efectividad					
	3	¿Los accesos a la información por medio de la Red son efectivas?			X		
	4	¿EL acceso a los servidores de los sistemas integrados de la entidad es estable?			X		
Aseguramiento		Confianza					
	5	¿La atención que se le da vía telefónica en cuanto a fallas tecnológicas y/o red solucionan sus problemas?		X			
	6	¿La capacidad de respuesta cuando usted utiliza cualquier servicio tecnológico por intermedio de la Red es inmediata?			X		
		Credibilidad					
	7	¿Los datos consultados por medio de la Red tienen un alto grado de fiabilidad?			X		
	8	¿La disponibilidad de la Red en la Municipalidad Distrital de Ilabaya es garantizada por equipo de respaldo?			X		
Capacidad de respuesta		Tiempo de respuesta					
	9	¿El tiempo de respuesta en atención a requerimientos de redes influye en la seguridad de la información?			X		
	10	¿El tiempo de respuesta de información de calidad es considerable?			X		

Municipalidad Distrital de Ilabaya
Tacna - Perú

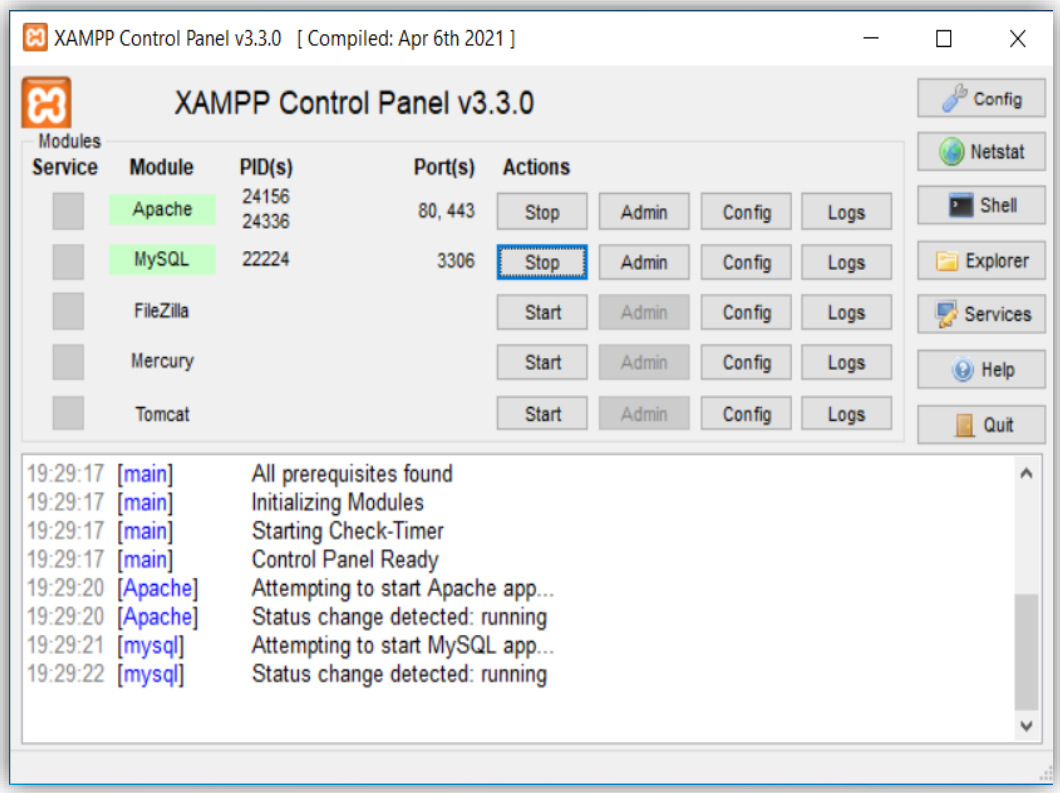
	Mejora continua						
	11	¿Existen medios por donde el cliente interno podría realizar algunos comentarios sobre la calidad de servicio de la Red de la entidad?			X		
	12	¿Se lanzan encuestas y/o cuestionarios para saber la perspectiva desde el usuario interno sobre la calidad de servicio de la red en la Municipalidad Distrital de Ilabaya?	X				

Anexo 6. Manual de Instalación

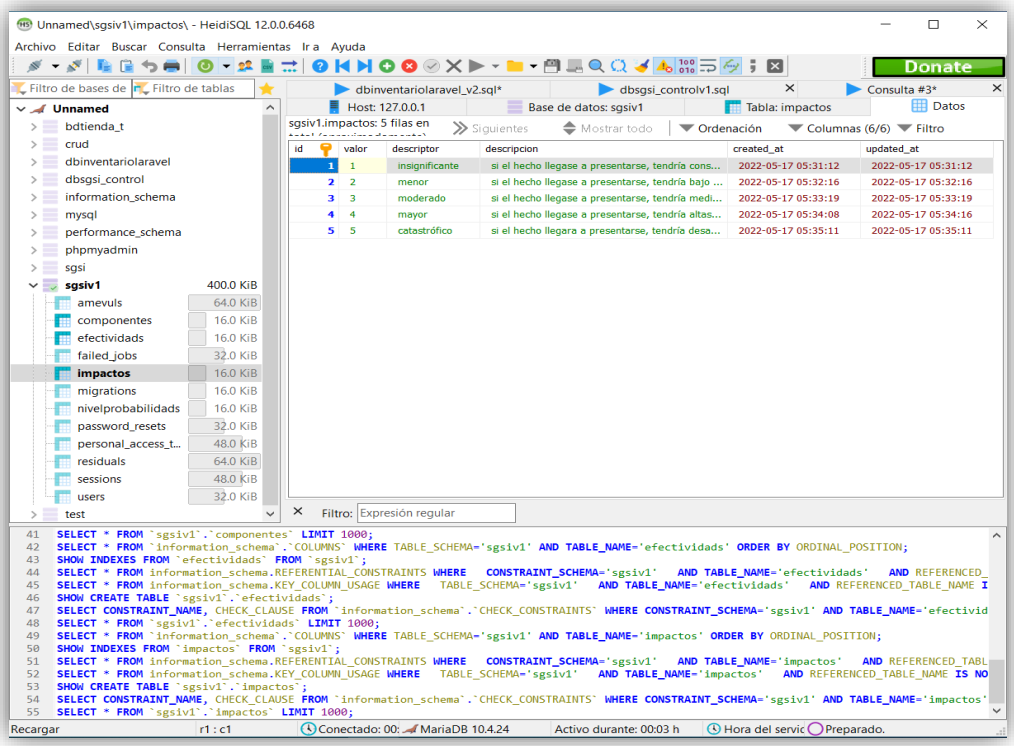
MANUAL DE INSTALACION

El sistema web "Control de Amenazas y vulnerabilidades" está desarrollado para agilizar el proceso de identificación de amenazas y vulnerabilidades y posteriormente ser tratados los riesgos identificados respectivamente en la Municipalidad Distrital de Ilabaya.

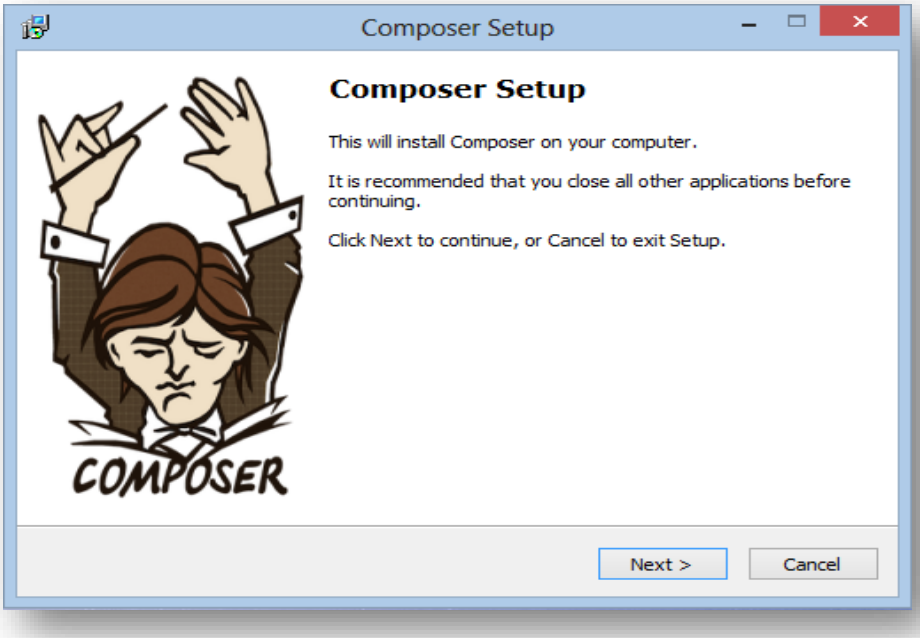
1. Instalar **XAMPP Control Panel v3.3.2** e iniciar **Apache** y **MySQL.**



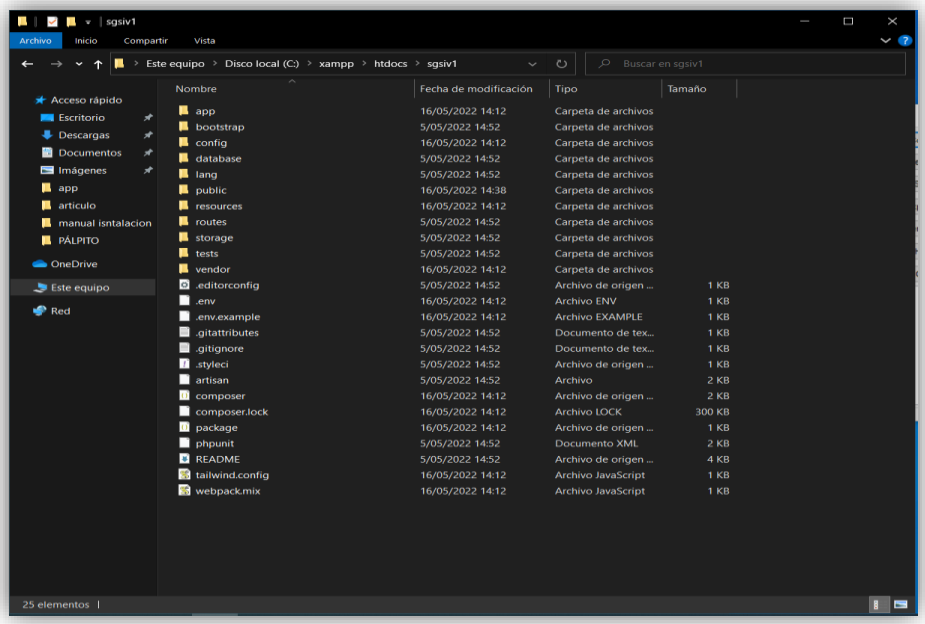
2. Instalar **HidiSQL 12.0.0.6468** e importar la base de datos.



3. Instalar **Composer**, la función de esta herramienta es la actualización de versión de Laravel o la conexión requerida en distintas computadoras a instalar el proyecto Sistema Web "Control de Amenazas y Vulnerabilidades" desarrollada para la Municipalidad Distrital de Ilabaya.



4. Copiar la carpeta **sgsiv1** a la unidad C:\xampp\htdocs\ ruta creada automáticamente al instalar xampp, en esta carpeta se alojan todos los proyectos desarrollados en Laravel o php de forma local.



5. Ejecutar cmd.

   Con comados cmd dirijase a la carpeta **C:\xampp\htdocs\sgsiv1.**

   Ejecutar el siguiente comando para iniciar Laravel.

   php artisan serve

   comando que permite la inicialización de los proyectos desarrollados en Framework Laravel de distintas versiones.

6. En el navegador de su preferencia inicie local host. http://127.0.0.1:8000, mencionada ruta mostrará en primera instancia el login de acceso al Sistema Web "Control de Amenazas y Vulnerabilidades" desarrollada para la entidad pública mencionada con anterioridad.

Anexo 7. Manual de Usuario

MANUAL DE USUARIO

El sistema web "Control de Amenazas y vulnerabilidades" está desarrollado para agilizar el proceso de identificación de amenazas y vulnerabilidades y posteriormente ser tratados los riesgos identificados respectivamente en la Municipalidad Distrital de Ilabaya.

1. Ingrese usuario y contraseña

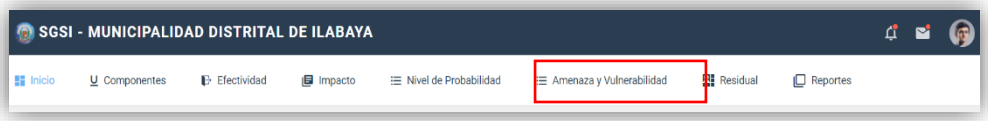
2. En primera instancia el Sistema web "Control de Amenazas y Vulnerabilidades" para la Municipalidad Distrital de Ilabaya muestra la plaza principal del Distrito como bienvenida y el nombre del usuario que ingresó al sistema.

3. Para el registro de un riesgo es necesario ingresar **Componentes**, **Efectividad**, **Impacto** y **Nivel de Probabilidad**, lo cual el ingreso de registro es similar respectivamente.

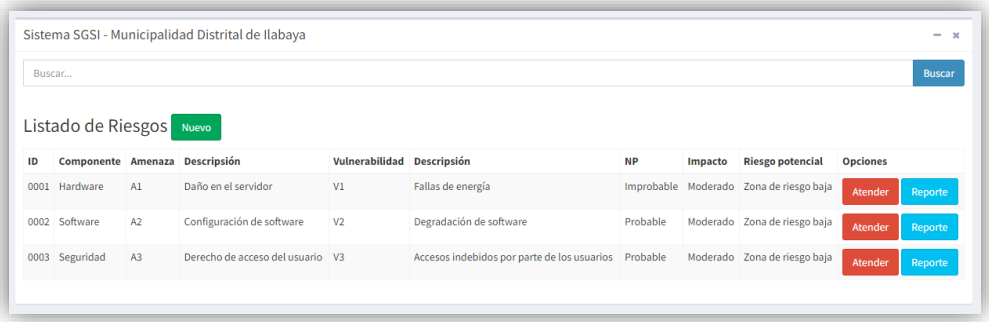
Iniciaremos ingresando un nuevo registro haciendo click en botón **Nuevo**.

4. Ingresar el nombre **Componentes**, **Efectividad**, **Impacto** o **Nivel de Probabilidad**, según corresponda y la descripción de esta, seguidamente hacer click en **Guardar**.

5. Una vez registrado los **Componentes**, **Efectividad**, **Impacto** y **Nivel de Probabilidad** procedemos a registrar la **Amenaza y Vulnerabilidad** respectivamente.

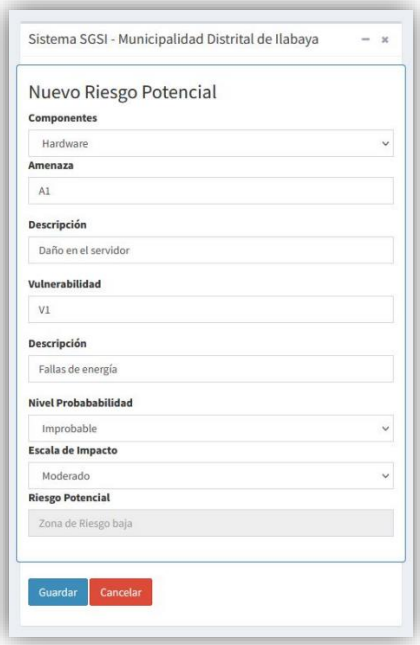


Para el ingreso de un nuevo ingreso de **Amenazas y Vulnerabilidades** hacer click en botón **Nuevo**.

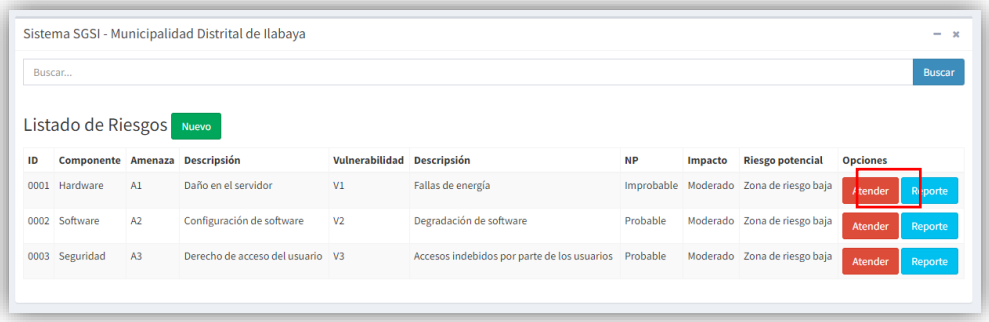


Para el registro de Amenazas y Vulnerabilidades vamos a seleccionar los campos ya registrados como son **Componentes**, **Efectividad**, **Impacto** y

Nivel de Probabilidad, posteriormente rellenar los campos en blanco, el campo **Riesgo Potencial** se encuentra bloqueado ya que es el resultado de la multiplicación de **Nivel de Probabilidad** por el **Impacto,** multiplicación que el Sistema web "Control de Amenazas y Vulnerabilidad" lo realiza automáticamente. Finalmente haga clic en **Guardar**.

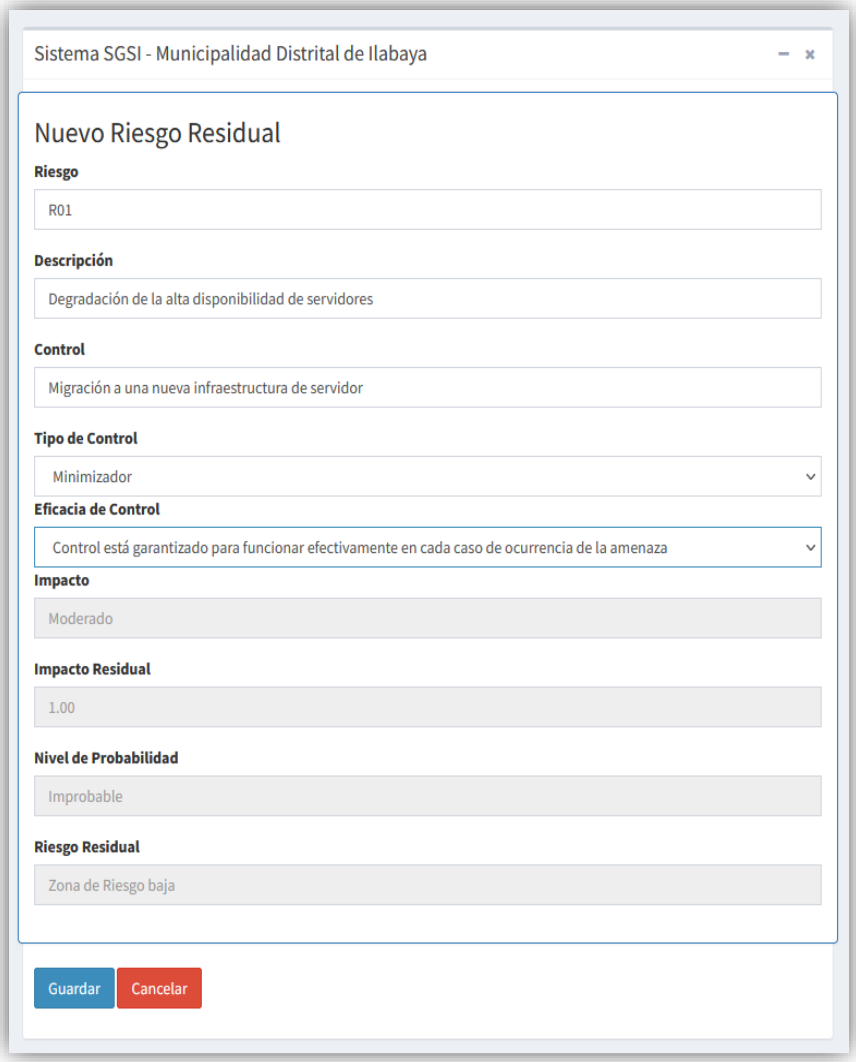


6. Luego del registro de la Amenaza y Vulnerabilidades procederemos atender dicho riesgo haciendo click en botón **Atender**.

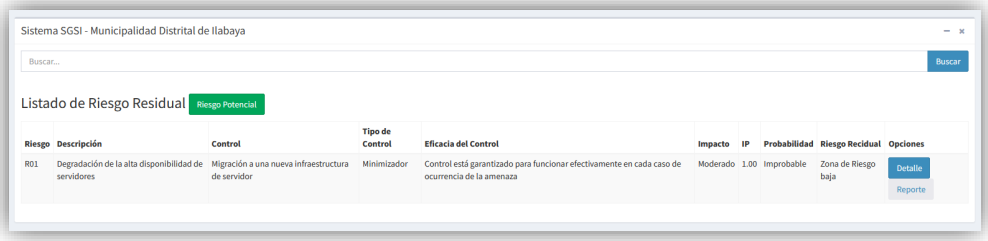


A continuación, el sistema mostrar los campos a ingresar, como se puede apreciar hay capos bloqueados por que ya han sido registrados en el formulario **Amenazas y Vulnerabilidades** en el caso del campo residual es la división de los campos **Eficacia de Control** entre **Impacto**, en el caso del

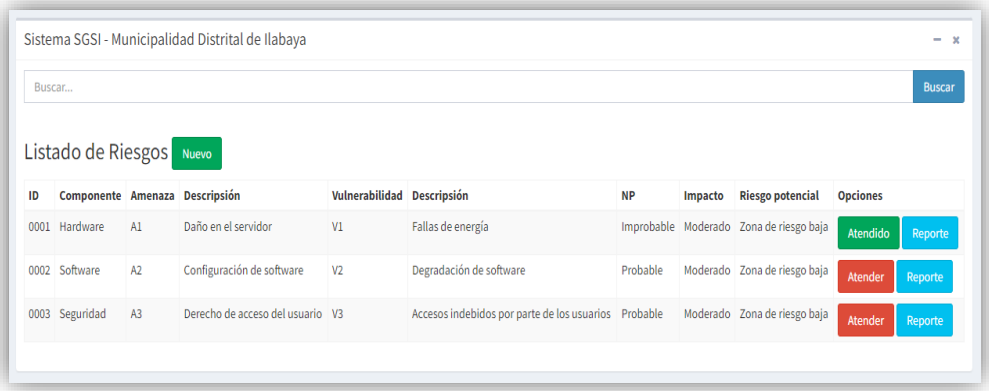
campo **Riesgo Residual** es el resultado de la multiplicación de **Impacto** por **Nivel de Probabilidad**.



7. Después de haber ingresado los espacios requeridos en el formulario **Riesgo Residual** se guarda un listado de estos, para su reporte y detalle respectivamente.



En el caso de **Amenazas y Vulnerabilidades** muestra el botón **Atendido.**



Anexo 8. Políticas de Seguridad MDI

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LA MUNICIPALIDAD DISTRITAL DE ILABAYAL

CONTROL DE VERSIONES			
Fecha	Descripción	Creado por	Versión
11/04/2022	Políticas de Seguridad de la Información	Yefer Maquera	0.1

INTRODUCCIÓN

La falta de políticas de seguridad es uno de los mayores problemas que enfrentan las entidades públicas en el Perú, exponiendo su información ante riesgos y vulnerabilidades que se pueden presentar en situaciones menos esperados, es por ello que se realiza una guía para la implementación de políticas de seguridad en la Municipalidad Distrital de Ilabaya.

La política de seguridad son instrucciones y orientaciones para manejar la seguridad de la información en la entidad en base a un plan para la implantación efectiva de medidas de protección tales como: identificación y control de acceso, respaldo de datos, planes de contingencia y detección de intrusos.

A menudo las políticas van acompañadas de normas, instrucciones y procedimientos. Las políticas son obligatorias, mientras que las recomendaciones o directrices son más bien opcionales. De hecho, las declaraciones de políticas de seguridad pueden transformarse fácilmente en recomendaciones reemplazando la palabra "debe" con la palabra "debería".

DECLARACIÓN DE CONFIDENCIALIDAD

La presente política contiene información confidencial y deberá estar disponible sólo para personas y entes debidamente autorizados para el desarrollo de sus funciones, así como para los trabajadores de la Municipalidad Distrital de Ilabaya. Todo requerimiento de acceso al presente documento deberá ser evaluado por la Oficina de Seguridad de la Información con la autorización expresa de la Gerencia de Administración y Finanzas, y Gerencia Municipal.

Si por error o cualquier otro motivo usted accede a este documento no estando autorizado, deberá mantener en reserva y no divulgar la información de su contenido, no copiar, transcribir, distribuir o utilizar de forma alguna dicha información, en tal sentido deberá devolver a la Municipalidad Distrital de Ilabaya el presente documento.

El uso del presente documento fuera de las instalaciones de la Municipalidad Distrital de Ilabaya podría denotar su uso irregular.

INDICE

I. OBJETIVOS 140

1. OBJETIVO GENERAL 140
2. OBJETIVOS ESPECÍFICOS 140

II. ALCANCE 140

III. BASE LEGAL 140

IV. APROBACIÓN.....141

V. DEFINICIONES 141

VI. CONTENIDO 142

1. DE LA SEGURIDAD DE LA INFORMACIÓN..... 142
2. METODOLOGÍA PARA EL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN 144
3. POLÍTICAS PARA LA ADMINISTRACIÓN DE SEGURIDAD DE LA INFORMACIÓN (NOMBRE DE LA ORGANIZACIÓN). 145
   - 3.1..... RESPECTO A LA SEGURIDAD LÓGICA 145
   - 3.2..... RESPECTO A LA SEGURIDAD DE PERSONAL..... 149
   - 3.3.....RESPECTO A LA SEGURIDAD FÍSICA Y AMBIENTAL:..... 151
   - 3.4.....RESPECTO AL INVENTARIO DE ACTIVOS Y CLASIFICACIÓN DE LA INFORMACIÓN 159
   - 3.5.....RESPECTO A LA ADMINISTRACIÓN DE LAS OPERACIONES Y LAS COMUNICACIONES..... 160
   - 3.6..RESPECTO AL DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN 167
   - 3.7..... RESPECTO DE LA SEGURIDAD DE LA COMPUTACIÓN MÓVIL Y TELETRABAJO 170
4. NORMAS Y POLÍTICAS EN EL USO DE SERVICIOS DE CORREO Y ACCESO A INTERNET 172
   - 4.1 CORREO ELECTRÓNICO 172
   - 4.2 ACCESO A INTERNET 173
5. SANCIONES 174

OBJETIVOS

1. OBJETIVO GENERAL

Lograr un nivel razonable de seguridad de la información como característica esencial para soportar los procesos del negocio que aseguren cumplir con los criterios de confidencialidad, integridad y disponibilidad de la información de la Municipalidad Distrital de Ilabaya en forma eficiente y eficaz cumpliendo con la normativa de los entes reguladores.

2. OBJETIVOS ESPECÍFICOS

a) Proporcionar una visión general de los requerimientos de seguridad de la información.
b) Definir las responsabilidades y conducta esperada de los individuos que tendrán acceso a la información.
c) Maximizar la generación de valor de los procesos internos a fin de satisfacer la expectativa de las partes interesadas.
d) Asegurar los activos de información de la Municipalidad Distrital de Ilabaya.

I. ALCANCE

El presente documento abarca el análisis de la información de todos los procesos de la Entidad identificando los activos de información, los riesgos a los que están expuestos y las medidas de seguridad a través de la selección de controles adecuados que los protejan razonablemente dando confianza a los clientes y grupos de interés así como proveer un marco de gestión de riesgos de Seguridad de la Información a la Entidad en cumplimiento de la Norma Técnica Peruana NTP ISO/IEC 27001:2014 y la Norma Técnica Peruana NTP – ISO/IEC 17799:2008, Tecnología de la información, código de buenas prácticas para la gestión de la seguridad de la información" tomando como referencia los estándares internacionales ISO/IEC 27001 e ISO/IEC 27002.

II. BASE LEGAL

1. Resolución de Contraloría Nº 320-2006-CG – Aprueban las Normas de Control Interno (en esta norma existe unas secciones relacionadas a TI, son obligatorias).
2. Resolución Ministerial No. 073-2004-PCM: "Guía para la Administración eficiente del Software Legal en la Administración Pública".
3. Resolución Ministerial No. 073-2004-PCM y carta 198-2004/PRE-INDECOPI.
4. Resolución INEI Nº 088-2003 Directiva sobre "Normas para el uso del servicio de correo electrónico en las entidades de la Administración Pública".
5. Norma Técnica Peruana NTP ISO/IEC 27001:2009. "Sistema de gestión de seguridad de la información".
6. Norma Técnica Peruana-ISO/IEC 17799:2007, "Código de Buenas Prácticas para la gestión de la seguridad de la información".
7. Norma Técnica Peruana-ISO/IEC 12207, Procesos de Ciclo de Vida del Software.

III. APROBACIÓN

- Aprobado en sesión de concejo de la Municipalidad Distrital de Ilabaya.

IV. DEFINICIONES

1. **Información**: Cualquier forma de registro electrónico, óptico, magnético o en otros medios similares, susceptible de ser procesada, y almacenada.
2. **Activo**: Cualquier cosa que tenga valor para la organización (ISO/IEC 13335-1:2004)
3. **Seguridad de la Información**: Característica de la información que se logra mediante la adecuada combinación de políticas, procedimientos, estructura organizacional y herramientas informáticas especializadas a efectos que dicha información cumpla los criterios de confidencialidad, integridad y disponibilidad, definidos de la siguiente manera:
   - **Confidencialidad**: La información debe ser accesible sólo a aquellos que se encuentren debidamente autorizados.
   - **Integridad**: La información debe ser completa, exacta y válida
   - **Disponibilidad**: La información debe estar disponible en forma organizada para los usuarios autorizados cuando sea requerida.

4. **Incidente de Seguridad de Información:** Evento asociado a una posible falla en la política de seguridad, una falla en los controles, o una situación previamente desconocida relevante para la seguridad, que tiene una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información
5. **Sistema de Gestión de Seguridad de la Información (SGSI):** Parte del sistema de gestión global, basada en una orientación a riesgo de negocio, para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información.
6. **Amenaza:** Una causa potencial de un incidente no-deseado, el cual puede resultar en daño a un sistema u organización (ISO/IEC 13335-1:2004)
7. **Vulnerabilidad:** La debilidad de un activo o grupo de activos que puede ser explotada por una o más amenazas (ISO/IEC 13335-1:2004).
8. **Control:** Medios para manejar el riesgo; incluyendo políticas, procedimientos, lineamientos, practicas o estructuras organizacionales, las cuales pueden ser administrativas, técnicas, de gestión o de naturaleza legal. El control también se utiliza como sinónimo de salvaguarda o contramedida.
9. **Terceros:** Persona u organismo que es reconocido como independiente de las partes involucradas, con relación al ítem en cuestión.

V. CONTENIDO

1. DE LA SEGURIDAD DE LA INFORMACIÓN

1.1 IMPORTANCIA

La información es uno de los activos más importantes de toda organización por lo que está constantemente bajo amenaza de muchas fuentes, estas pueden ser personas, procesos internos, tecnológicos, eventos externos y otros. Con el uso creciente de la nueva tecnología, almacenar, transmitir y recuperar la información, han originado un gran número y tipo creciente de amenazas.

La Municipalidad Distrital de Ilabaya cataloga a la información almacenada, distribuida, procesada en la ejecución de sus procesos como el activo más importante, así como los recursos que la apoyan.

Por ello, el Sistema de Gestión de Seguridad de la Información sirve para definir, realizar, mantener y mejorar la gestión integral del riesgo del que es

parte, como esencia para mantener la competitividad, flujo de liquidez, rentabilidad, cumplimiento de la legalidad y de reputación.

La seguridad de información no se puede lograr en su totalidad, pero con la aplicación de metodologías que permitan la mejora continua se podrá llegar a un nivel de riesgo aceptable. La gestión de la seguridad de la información necesita como mínimo, la participación de todos los miembros de la organización. Así como también la participación de los principales proveedores y clientes.

1.2 REQUERIMIENTOS PARA LA SEGURIDAD DE LA INFORMACIÓN

a) La primera fuente procede de la evaluación de los riesgos de la Seguridad de la Información de la organización, tomando en cuenta los procesos, objetivos y estrategias generales del negocio. Con ella se identifican las amenazas o riesgos a los activos de información, se evalúa la vulnerabilidad y la probabilidad de su ocurrencia y se estima su posible impacto.
b) La segunda fuente es el conjunto de requisitos legales, estatutos, regulaciones y contratos que debería satisfacer la organización, sus socios comerciales, los contratistas y los proveedores de servicios.
c) La tercera fuente está formada por los principios, objetivos y requisitos que forman parte del tratamiento de la información que la organización ha desarrollado para apoyar sus operaciones.
d) Compromiso por parte del Directorio y la Gerencia Municipal para apoyar activamente la seguridad dentro de la organización. La Gerencia Municipal debe invertir en seguridad, y verlo como un aspecto relevante. Algunas veces la seguridad requiere inversión económica, y parte del compromiso de la Gerencia Municipal implica tener un presupuesto especial para seguridad, de una forma razonable.
e) La asignación de responsabilidades sobre cada uno de los actores deberá ser de forma clara y determinada formalmente.
f) La concienciación y capacitación de todos los miembros de la organización en la búsqueda de una cultura diligente respecto a la seguridad de la Información.

1.3 RESPONSABILIDAD DEL CONSEJO DE ALCADIA RESPECTO A LA SEGURIDAD DE LA INFORMACIÓN

Las responsabilidades del consejo de alcaldía establecen:

a) Aprobar las políticas generales que guíen las actividades de la empresa en la gestión de los diversos riesgos que enfrenta.
b) Aprobar los recursos necesarios para el adecuado desarrollo de la Gestión Integral de Riesgos, a fin de contar con la infraestructura, metodología y personal apropiado.
c) Aprobar los manuales de organización y funciones, de políticas y procedimientos y demás manuales de la empresa.
d) Conocer los principales riesgos afrontados por la entidad estableciendo, cuando ello sea posible, adecuados niveles de tolerancia y apetito por el riesgo.
e) Obtener aseguramiento razonable que la empresa cuenta con una efectiva gestión de los riesgos a que está expuesta, y que los principales riesgos se encuentran bajo control dentro de los límites que han establecido.

2. METODOLOGÍA PARA EL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Los sistemas informáticos y la Información que en ellos se contienen, son activos críticos para la Entidad. Por ello se debe contar con controles apropiados a su verdadero valor. Se debe evitar sobreproteger algunos componentes, mientras otros no tengan la protección adecuada.

Para lograr el nivel de cobertura apropiado se requiere el desarrollo e implementación de un Sistema de Gestión de Seguridad de Información que define los controles que la Entidad considera necesarios para cubrir los distintos riesgos a los que los activos de Información están expuestos.

Asimismo, se ha planteado como punto fundamental la identificación de nuestros activos para su valoración, es así que toda área tiene la

responsabilidad de comunicar a la Oficina de Seguridad de la Información para la incorporación o eliminación de cualquier activo de información.

La metodología establecida para la Planificación y Establecimiento, Implementación y Operación, Monitoreo y Revisión y Mantenimiento y Mejora, estará basada en el enfoque PDCA (círculo de la calidad total, Deming) establecido en el Manual de Gestión del Sistema de Seguridad de la Información de la Municipalidad Distrital de Ilabaya

3. POLÍTICAS PARA LA ADMINISTRACIÓN DE SEGURIDAD DE LA INFORMACIÓN MUNICIPALIDAD DISTRITAL DE ILABAYA

3.1 RESPECTO A LA SEGURIDAD LÓGICA

a. Todo equipo de cómputo sean computadoras, estaciones de trabajo, y equipo accesorio, etc. que esté o sea conectado a la Red, o aquel que se tenga en forma autónoma y que sea propiedad de la Entidad debe sujetarse a las normas y procedimientos de la Municipalidad Distrital de Ilabaya.
b. El personal que hace uso de programas sistemas o aplicaciones propiedad de la Municipalidad Distrital de Ilabaya deberá tener las consideraciones de seguridad, para garantizar la integridad, confidencialidad y disponibilidad de la información guardada, procesada, transmitida y propagada por dichas aplicaciones.
c. Todo usuario que recibe una cuenta de acceso, firmará un documento donde declara conocer las políticas y procedimientos de seguridad, y acepta sus responsabilidades con relación al uso de la misma.
d. Los intentos de violación a los sistemas de seguridad y control de acceso que originen o no algún perjuicio, se consideran violatorias a la presente política de Seguridad, pudiendo ser casual de despido.
e. Las áreas responsables que administran y/o ejercen control sobre los sistemas informáticos deberán revisar periódicamente los derechos y perfiles de usuarios.
f. La única forma de acceder a los sistemas informáticos que la Entidad provea para el desarrollo de actividades es mediante una única cuenta

de acceso personal llamada también User_Id, Login, cuenta de acceso o Identificación y su clave de acceso, contraseña, palabra de paso o password respectiva.

g. Se deberá implementar un esquema de autenticación basado en dos factores como mínimo, para casos en los cuales el usuario tenga que acceder a los sistemas de información críticos desde fuera de la entidad a través de Internet.
h. Los usuarios deberán proteger, administrar y no compartir sus cuentas de acceso y contraseñas.
i. Está prohibido el uso de cuentas anónimas o de invitado (Guest) o aprovechar de vulnerabilidades o fallas en la seguridad de los sistemas para obtener acceso no autorizado o dañar el sistema.
j. Las cuentas se suspenderán automáticamente después de un cierto periodo de inactividad.
k. Los usuarios de la Municipalidad Distrital de Ilabaya usarán como única cuenta de correo aquella que haya sido asignada por el Administrador del Servicio.
l. Está prohibido realizar actividad alguna con una cuenta de acceso perteneciente a otro usuario.
m. Las claves de acceso serán cambiadas periódicamente, la cual deberá ser actualizada con el respectivo celo, cuidado y responsabilidad.
n. El uso de claves de acceso obtenido por medios ilegales y/o irregulares constituye una falta grave y está sujeta a sanción disciplinaria.
o. Programar auditorias periódicas y chequeos aleatorios, para controlar las áreas o funciones críticas con respecto a la seguridad de la información de la Entidad, documentando la ejecución y los resultados de dichas pruebas.
p. Se efectuarán revisiones de otorgamientos de accesos sobre cuentas de usuarios de los sistemas más importantes de la Entidad, manteniendo especial cuidado sobre las cuentas con privilegios especiales, estableciendo para ello un procedimiento y periodicidad.
q. Se deberán efectuar revisiones de la información crítica almacenada en la base de datos para poder detectar operaciones fraudulentas o actividades no autorizadas.
r. Se deberá elaborar procedimientos para la revisión de la información que incluya cambios en campos sensibles de tablas críticas.

s. El propietario de la información en coordinación con el Área de Tecnología de la Información y Comunicaciones y la Oficina de Seguridad de la Información deberán de establecer perfiles de acceso para los usuarios de los sistemas informáticos de la Municipalidad Distrital de Ilabaya tomando como referencia los puestos y funciones existentes en cada área organizativa. Los factores a considerarse en los perfiles de acceso deberán basarse en:

   i. Control de accesos a la información mediante la creación de roles de acceso en los sistemas
   ii. Segregación de Tareas
   iii. Acceso a información justificado en el principio de necesidad.
   iv. Considerando el principio Caso por Caso

   Asimismo, deberá comunicarse a la Gerencia Municipal para la implementación de los perfiles de acceso de cada sistema de información dentro del alcance de su competencia.

t. El Área de Tecnología de la Información y Comunicaciones es responsable de proporcionar a los usuarios el acceso a los recursos informáticos.

u. Dado el carácter unipersonal del acceso a la red de datos, así como a los sistemas informáticos de la Municipalidad Distrital de Ilabaya, el Área de Tecnologías de la Información y Comunicaciones y la Oficina de Seguridad de la Información verificarán su uso responsable, de acuerdo a las normativas existentes establecidas por la Entidad.

v. El acceso lógico y físico de equipos especializados de cómputo como servidores, enrutadores, base de datos, equipo de servidores centralizado y distribuido, etc. conectado a la red es administrado por el área de Tecnología de la Información y Comunicaciones, dicho acceso debe ser restringido para personal no autorizado.

w. Todo el equipo de cómputo que esté conectado a la red de la Municipalidad Distrital de Ilabaya o aquella que se tenga en forma autónoma y que sea de propiedad de la Entidad, debe de sujetarse a los procedimientos de acceso que emite el Área de Tecnología de la Información y Comunicaciones.

x. El Área de Tecnología de la Información y Comunicaciones es el responsable de proporcionar el servicio de acceso remoto a nuestros servidores y las normas de acceso a los recursos informáticos disponibles.

y. Para el caso especial de acceso a los recursos de cómputo a externos y/o terceros, deberán ser autorizados formalmente por la Gerencia Municipal.

z. Los usuarios externos y/o terceros deberán sujetarse a las políticas y reglamentos que establezca la Municipalidad Distrital de Ilabaya.

aa. El acceso remoto que realicen personas ajenas a la Entidad deberá de cumplir las normas y/o estándares establecidos para salvaguardar la seguridad de la información, asimismo dicho acceso deberá contar con la autorización formal de la Gerencia Municipal.

bb. Tendrá acceso a los sistemas informáticos solo el personal de la Municipalidad Distrital de Ilabaya que es titular de una cuenta de acceso o bien tenga autorización del responsable si se trata de personal de apoyo administrativo o técnico.

cc. El manejo de información de la Entidad que se considere de uso restringido deberá ser cifrada con el objeto de garantizar su integridad y confidencialidad.

dd. La instalación y uso de los sistemas de información se rigen por las políticas de uso de la red de la Municipalidad Distrital de Ilabaya y por las normas y procedimientos establecidos por el área de Tecnología de la Información y Comunicaciones.

ee. Los recursos y servicios disponibles a través de la red de la Municipalidad Distrital de Ilabaya serán de uso exclusivo para asuntos relacionados al desarrollo de las actividades laborales asignadas vinculadas.

ff. Se establecerán responsables para elaborar propuestas de mejoras a la política de seguridad lógica.

gg. Se establecerán responsables para desarrollar actividades y seguimiento de cumplimiento de la política de seguridad lógica.

hh. La Entidad implementará medidas a fin de tratar el riesgo de fuga de información respetando las expectativas de los Entes de Control y la normatividad vigente.

3.2 RESPECTO A LA SEGURIDAD DE PERSONAL:

3.2.1 Respecto a la Seguridad del Personal antes del Empleo

a) Todo proceso de selección de personal para la Municipalidad Distrital de Ilabaya debe hacerse mediante un proceso formal asegurándose la idoneidad del recurso humano para el rol o función que desempeñará.

b) Debe realizarse comprobaciones en el momento de la solicitud de trabajo, incluyendo:

- La verificación de referencias personales y/o comerciales.
- La comprobación de los datos completos y precisos del currículo vitae del candidato.
- La confirmación de las certificaciones académicas y profesionales.
- Una comprobación independiente de la identificación con pasaporte o documento similar.
- Una comprobación del crédito del candidato.
- Verificación de Antecedentes Judiciales y Policiales

c) Todos los miembros de la Municipalidad Distrital de Ilabaya, directores, funcionarios, trabajadores y practicantes que tenga acceso a información sensitiva, confidencial o restringida, deben firmar un acuerdo de confidencialidad o no divulgación antes de otorgarles acceso a los medios de procesamiento de la información.

d) Las cláusulas de confidencialidad deben revisarse cuando cambien los términos del empleo o contrato, especialmente cuando los empleados dejen la organización o sus contratos terminen.

e) El personal externo a la Entidad deberá firmar cuando la Entidad lo estime pertinente un compromiso de confidencialidad dentro del marco legal vigente.

f) Los términos y las condiciones de empleo deberían establecer la responsabilidad del empleado en materia de seguridad de la información. Dicha responsabilidad debería continuar durante un periodo definido tras la finalización del contrato.

3.2.2 Respecto a la Seguridad del Personal durante el Empleo.

a) Todos los empleados de la organización y, cuando sea relevante, los contratistas y terceros, deben recibir el apropiado conocimiento, capacitación y actualizaciones regulares de las políticas y procedimientos organizacionales, incluyendo requisitos de seguridad, responsabilidades legales, prácticas del uso correcto de los recursos de tratamiento de información, conforme sean relevantes para su función.

b) Se debe tener un proceso de inducción formal diseñado para introducir las políticas y expectativas de seguridad de la organización antes de otorgar acceso a la información o servicios.

c) La evaluación del personal en la Municipalidad Distrital de Ilabaya se realiza cada 06 meses y/o cuando las circunstancias lo requieran.

d) Se debe realizar una comprobación periódica de crédito, a personal que trate la información sensible como información financiera o confidencial.

e) Las incidencias que identifiquen los usuarios deben informarse a la Jefatura del área de Tecnología de la Información y Comunicaciones y a la Oficina de Seguridad de la Información lo más rápidamente posible.

f) Todo personal externo deberá identificarse y portar un carnet que lo identifique como visitante.

g) El personal externo a la Entidad como el personal con honorarios profesionales, proveedores, consultores-asesores, visitas, etc. están sujetas a las normativas y directivas establecidas por la Entidad durante el periodo que desarrollen sus actividades, al igual que el personal interno.

h) Todo personal externo deberá acatar las disposiciones emitidas por la Entidad, en lo pertinente al resguardo y seguridad de los activos de información en temas de encriptación, resguardo de material magnético e impreso y restricción de salida de material que contenga información crítica del negocio.

3.2.3 Respecto a la Seguridad al Término o Cambio del Empleo.

a) El personal interno y externo a la Entidad deberá entregar al término de su contrato todo el material, información y equipos que hubiesen sido proporcionados por la Entidad para el cumplimiento de sus actividades.

b) Los derechos de acceso de todos los usuarios empleados, contratistas y terceras personas a la información y los medios de procesamiento de información deben ser retirados a la terminación de su empleo, contrato o acuerdo, o debieran ser reajustados de acuerdo al cambio.

3.3 RESPECTO A LA SEGURIDAD FÍSICA Y AMBIENTAL:

3.3.1 Perímetro de seguridad física.

a) Se debe dar protección física mediante una serie de barreras físicas en torno a los locales de la Entidad y a los recursos de tratamiento de la información, teniendo en cuenta que el perímetro debe estar claramente definido, así como los muros del lugar deben ser sólidos y todas las puertas exteriores deben estar protegidas contra accesos no autorizados.

b) Las ventanas y puertas deben permanecer cerradas cuando la instalación este vacía. Se debe tener protección externa en las ventanas, sobre todo en las de planta baja.

c) Se debe instalar sistemas de detección de intrusos y probarse regularmente para cubrir todas las puertas externas y las ventanas accesibles. Se deben cubrir otras áreas como las salas de cómputo o de comunicaciones.

d) Las visitas a las áreas seguras deben ser supervisadas y ordenadas, registrando mínimamente la fecha, hora de entrada, hora de salida, motivo / justificación de visita, nombre del visitante, tipo de vínculo con la Entidad. Los visitantes solo tendrán acceso para propósitos específicos y autorizados, proporcionándoles instrucciones sobre los requisitos de seguridad del área y los procedimientos de emergencia.

e) Se debe controlar y restringir solo al personal autorizado el acceso a la información sensible y a los recursos de su tratamiento.

f) Se debe mantener un rastro auditable de todos los accesos, con las debidas medidas de seguridad.

g) Se debe exigir a todo el personal que lleve puesta alguna forma de identificación visible, así como a las personas visitantes.

h) Se debe revisar y actualizar regularmente los derechos de acceso a las áreas de seguridad.

i) Las visitas internas o externas podrán acceder a las áreas restringidas siempre y cuando se encuentren acompañadas cuando menos por un responsable del área con permiso de la autoridad correspondiente.

j) Se deberán establecer horarios de acceso a instalaciones físicas, especificando los procedimientos y en qué casos se deberá hacer excepciones.

k) Bajo condiciones de emergencia o de situaciones de urgencia manifiesta, el acceso a las áreas de servicio crítico estará sujeto a las que especifiquen las autoridades superiores de la Entidad.

l) Los recursos críticos deben situarse fuera de áreas de acceso público.

m) El público no debería acceder automáticamente a los ambientes de información personal de la Entidad que identifiquen lugares con recursos de tratamiento de información sensible.

n) Los materiales peligrosos y combustibles se deben almacenar en algún lugar distante de las áreas seguras.

o) El equipo y los medios de respaldo deben estar a una distancia de seguridad conveniente para evitar que se dañen por un desastre en el área principal.

p) No se debe permitir la presencia de equipos de fotografía, video, audio u otras formas de registro salvo autorización especial.

q) Se debe definir que personal está autorizado para mover, cambiar o extraer equipo del área de Tecnología de la Información y

Comunicaciones a través de identificaciones y formatos de E/S; y se debe informar de estas disposiciones a personal de seguridad.

r) El Área de Tecnología de la Información y Comunicaciones deberá proveer de la infraestructura de seguridad requerida con base en los requerimientos específicos de cada área.

s) La sala de Procesamiento de Información y comunicaciones del área de Tecnología de la Información y Comunicaciones, así como de las agencias debe:

i. Recibir limpieza al menos una vez por semana, que permita mantenerse libre de polvo.
ii. Ser un área restringida.
iii. Estar libre de contactos e instalaciones eléctricas en mal estado.
iv. Contar por lo menos con un extintor de incendio adecuado y cercano a la sala de comunicaciones.
v. La sala de comunicaciones deberá seguir los estándares vigentes para una protección adecuada de los equipos de comunicaciones y servidores.
vi. Los sistemas de tierra física, sistemas de protección e instalaciones eléctricas de la sala de comunicaciones deberán recibir mantenimiento anual con el fin de determinar la efectividad del sistema.
vii. Cada vez que se requiera conectar un equipo de cómputo, se deberá comprobar la carga de las tomas de corriente.
viii. Contar con algún esquema que asegure la continuidad del servicio.
ix. Se deberá tener fácil acceso a los procedimientos de contingencias.
x. Se deberá contar con rutas de evacuación y sus señalamientos correspondientes.
xi. Se programarán simulacros de evacuación en casos de contingencias.
xii. Se deberá de mantener un orden en la distribución de los medios de Procesamiento de Información, equipos y cableado.

3.3.2 Seguridad contra incendios.

a) Toda sede de la Municipalidad Distrital de Ilabaya debe contar con sensores de humo colocados de manera estratégica para cubrir un mayor radio de acción.
b) Toda dependencia de la Municipalidad Distrital de Ilabaya debe contar con extintores ubicados en lugares visibles y con la señalización respectiva.
c) Todo el personal de la Municipalidad Distrital de Ilabaya debe estar capacitado para hacer uso de los extintores durante cualquier contingencia.

3.3.3 Seguridad de los equipos.

a) Todo equipo de la Municipalidad Distrital de Ilabaya que sea de propósito especifico y de misión crítica asignada, requiere estar ubicado en un área que cumpla con las medidas de seguridad física, las condiciones ambientales, la alimentación eléctrica estabilizada y con equipos de respaldo de energía y será manipulado solo por el personal del Área de Tecnología de Información y Comunicaciones.
b) El área responsable del mantenimiento de los equipos deberá definir procedimientos para el inventario físico, entrega de equipos a personal autorizado, así como la custodia de toda documentación relacionada.
c) No fumar, beber y comer cerca de los equipos de cómputo.
d) Se debe vigilar las condiciones ambientales que puedan afectar negativamente al funcionamiento de los equipos de cómputo.
e) Todos los equipos de la Entidad deben contar con sistemas de contingencia para alimentación eléctrica en caso de caída de la red pública de energía.
f) Se tiene prohibido conectar a la red eléctrica de cómputo, cualquier dispositivo ajeno a las actividades de la Entidad como electrodomésticos, cargador de baterías, etc.
g) Cada agencia de la Municipalidad Distrital de Ilabaya debe contar con un pozo a tierra, el cual recibirá mantenimiento cada seis meses para garantizar su operatividad a niveles permisibles.

h) Se debe instalar interruptores de emergencia cerca de las puertas de emergencia de la sala de equipos para facilitar una desconexión rápida en caso de emergencia.

i) Los equipos informáticos principales y de contingencia como servidores de dominio o aplicación, equipos de comunicación, etc. de la sede principal deben estar protegidos por medios climáticos artificiales.

j) Se debe contar con un plan de mantenimiento preventivo para mantener adecuadamente la disponibilidad e integridad de los equipos, teniendo en cuenta los siguientes controles:

   i. Solo el personal de mantenimiento debidamente autorizado debe realizar la reparación y servicio de los equipos.

   ii. Se debe registrar documentalmente todos los fallos, reales o sospechados, así como el mantenimiento preventivo y correctivo.

   iii. Se deben adoptar medidas adecuadas cuando se envíen los equipos fuera de las instalaciones para su mantenimiento.

k) En el caso de los equipos atendidos por terceros, el Área responsable deberá normar al respecto.

l) Corresponde al área de Tecnología de Información y Comunicaciones dar a conocer las listas de las personas, que puedan tener acceso a los equipos y brindar los servicios de mantenimiento básico, a excepción de los atendidos por terceros.

m) Queda estrictamente prohibido dar mantenimiento a equipos de cómputo que no sean propiedad de la Entidad.

n) Los equipos de fotocopiado, faxes e impresión deben situarse adecuadamente en un área segura que evite el acceso de personal no autorizado.

o) El uso de cualquier equipo de cómputo, agendas electrónicas, teléfonos móviles fuera de los locales de la Entidad, que son de propiedad de la Municipalidad Distrital de Ilabaya y asignados al trabajador para el cumplimiento de sus funciones, debe ser autorizado por la Gerencia Municipal, previa evaluación de riesgos como daño físico, robo, intercepción o cualquier otro resultado de trabajar fuera de la Entidad.

p) El uso de una nueva funcionalidad de hardware, software, servicios y otros que procese, transfiera o almacene información de la Entidad, debe ser revisada y autorizada por la Oficina de Seguridad de La Información y la Gerencia Municipal con el fin de asegurar que son compatibles con otros componentes del sistema.

q) La información confidencial contenida en medios de almacenamiento debe de eliminarse de manera segura, utilizando técnicas y herramientas avanzadas de borrado o sobre escritura; podrá considerarse la destrucción de medios de almacenamiento como una alternativa.

r) Se debe elaborar procedimientos para la gestión de los medios removibles.

s) Si el contenido del medio removible no es requerido, deberá ser eliminado y no deberá ser recuperable.

t) Se deberá eliminar la información considerada confidencial o reservado contenida en el medio removible.

u) En caso de existir personal técnico de apoyo del área de Tecnología de la Información y Comunicaciones, éste notificará a la Jefatura de TIC de los cambios, tanto físicos como de software que realice en el área donde efectuó la atención, cumpliendo con los procedimientos formales establecidos por la Entidad.

v) Todo equipo de cómputo de la Municipalidad Distrital de Ilabaya a ser reubicado, se hará únicamente bajo la autorización del Área de Tecnología de Información y Comunicaciones.

w) Todos y cada uno de los equipos son asignados a un responsable, por lo que es de su competencia hacer buen uso de los mismos.

x) Las áreas donde se tiene equipo de propósito general cuya misión es crítica (servidores, equipos de comunicación) estarán sujetas a los requerimientos que el área de Tecnología de la Información y Comunicaciones emita.

y) Dada la naturaleza insegura de los sistemas operativos y su conectividad en la red, el Área de Tecnología de la Información y Comunicaciones tiene la facultad de acceder a cualquier equipo de cómputo que no estén bajo su supervisión.

z) Toda computadora asignada al personal de la Municipalidad Distrital de Ilabaya cuenta con medidas de protección de información como

la desactivación de las unidades de diskettes, y de Cd-Rom, USB, excepto las PC's asignadas a los funcionarios y personal de la Municipalidad Distrital de Ilabaya que cuenten con la debida autorización.

aa) Medidas para garantizar el correcto uso de los recursos de la PC y evitar Riesgos

i. Restringir el acceso a las configuraciones del sistema.
ii. Fondo de pantalla predefinido: (Para aceptación del usuario, será planteado con diversas opciones por áreas, mediante encuesta).
iii. Propiedades de pantalla, solo el page de configuración, para ajuste de tamaño.
iv. Restringir propiedades del sistema del panel de control.
v. Eliminar el entorno de red para todos los usuarios de red que tengan derecho a las aplicaciones para fines operacionales.
vi. Eliminar el acceso directo al DOS, para imposibilitar el mapeo desde DOS.
vii. Restringir el botón de ejecutar del menú de Inicio.
viii. Restringir el acceso al Registro de Windows.
ix. Deshabilitar autoboot de arranque del sistema operativo sobre lectoras y USB.
x. Restringir el acceso a la configuración de tareas programadas.
xi. Ejecución de copias de seguridad.

3.3.4 Controles generales.

a) Se debe adoptar una política de "Escritorio Limpio" o puesto de trabajo despejado de papeles y medios de almacenamiento removibles, ya que la información que se deja sobre las mesas, adicionalmente a riesgos de robo, sustracción, también pueden dañarse o destruirse en un desastre como un incendio, una inundación o una explosión.

b) Todo medio físico de almacenamiento de información como (disquetes, CD's, memorias USB, incluso papeles y documentos, debe guardarse bajo ciertas medidas de seguridad, para evitar riesgos, especialmente cuando contienen información importante, que podría ser mal usada en manos desconocidas.

c) Los usuarios deben de eliminar sus accesos directos en desuso creados en el escritorio, para esto pueden utilizar herramientas incluidas en los sistemas operativos como la denominada "Asistente de Limpieza del Escritorio".

d) Cuando el usuario deje de utilizar la estación de computo, es decir lo deje desatendido se debe bloquear la pantalla, con el objeto de reducir los riesgos de acceso no autorizado, perdidas o daños de la información dentro o fuera del horario normal de trabajo.

e) Se deben proteger los puntos de entrada y salida de correo, así como las máquinas de fax no atendidas.

f) Las fotocopiadoras deben de apagarse fuera de las horas de trabajo.

3.3.5 Instalación de los equipos de cómputo.

a) Todo equipo de cómputo como computadoras, estaciones de trabajo, servidores y equipos accesorios que estén conectados a la red de la Municipalidad Distrital de Ilabaya debe ajustarse a las normas dictadas por el área de Tecnología de Información y Comunicaciones y la Oficina de Seguridad de la Información, de acuerdo a la función que desempeñara el equipo.

b) Los responsables de las diferentes gerencias, áreas y agencias deberán conjuntamente con el responsable del área de Tecnología de Información y Comunicaciones y del Área de Logística dar cabal cumplimiento con las normas de instalación, y notificaciones correspondientes de actualización, reubicación, reasignación, y todo aquello que implique movimientos en su ubicación, de adjudicación, sistema y misión.

3.3.6 Seguridad en la instalación de software.

a) La Municipalidad Distrital de Ilabaya ha realizado las siguientes acciones como medidas preventivas para que el usuario no instale programas no autorizados. Estas son las siguientes:

   i. Deshabilitación de unidades lectoras de CD
   ii. Deshabilitación de unidades de disquete.
   iii. Deshabilitación de USB.

b) Las unidades de red o carpetas compartidas que contengan instaladores de software serán de acceso restringido.

c) El Área usuaria deberá coordinar con el área de Tecnología de la Información y Comunicaciones para la instalación de cualquier software.

3.3.7 Responsabilidad de los equipos.

a) La protección física de los equipos corresponde a los usuarios a los cuales se les asigna y corresponde notificar al jefe del Área de Tecnología de Información y Comunicaciones y al Área de Logística, los movimientos de equipos en caso se produzcan.

3.3.8 Actualización de equipos.

a) Todo equipo de cómputo (computadoras personales, estaciones de trabajo, servidores y demás equipos relacionados) y los de telecomunicaciones debe procurar ser actualizados tendiendo a conservar e incrementar la calidad del servicio que prestan en la Municipalidad Distrital de Ilabaya

3.4 RESPECTO AL INVENTARIO DE ACTIVOS Y CLASIFICACIÓN DE LA INFORMACIÓN

3.4.1 INVENTARIO DE ACTIVOS

Un activo de Información es algo que tiene valor o utilidad para la Entidad, sus operaciones y su continuidad, por esta razón, los activos necesitan tener protección para asegurar una correcta operación del negocio y una continuidad en las operaciones. Para nuestra Entidad son de vital importancia la gestión y la responsabilidad por los activos. En tal sentido se deben identificar con claridad los activos de información y mantener un inventario de activos, el mismo que debe incluir información necesaria para que la Entidad pueda recuperarse de un desastre; incluyendo el propietario, el custodio, tipo de activo, formato, ubicación, información de respaldo así como el tasado por cada activo de información con el fin de identificar su impacto en la Entidad por su deterioro, por sus fallas o perdidas en base a los criterios de: Confidencialidad, integridad y Disponibilidad.

Asimismo, los activos se identifican en la matriz de Activos siguiendo el procedimiento Oficina de Seguridad de la Información "Levantamiento de

información para la caracterización de los activos y la caracterización de las amenazas del sistema de gestión de seguridad de la información".

3.4.2 CLASIFICACIÓN DE LA INFORMACIÓN

Es el ordenamiento que se otorga a la información contenida en documentos, ya sea en soporte electrónico o físico, determinando si la misma es pública, reservada, confidencial o sensitiva. En tal sentido la entidad cuenta con la normativa interna Oficina de Seguridad de la Información "Clasificación y Tramite de la Información" donde se establece el procedimiento para la clasificación de la Información.

3.5 RESPECTO A LA ADMINISTRACIÓN DE LAS OPERACIONES Y LAS COMUNICACIONES

3.5.1 Procedimientos y responsabilidades de operación.

a) Se debe establecer la periodicidad para la revisión de los procedimientos de operación para las actividades de administración del sistema asociadas a los recursos de tratamiento y comunicación de la información.
b) Los programas operativos deberían estar sujetos a un control estricto de cambios, conservando un registro de auditoria conteniendo la información importante, teniendo en cuenta los siguientes controles:
    i. La identificación y registro de cambios significativos
    ii. La evaluación del posible impacto de los cambios.
    iii. Un procedimiento formal de aprobación de los cambios propuestos.
    iv. La comunicación de los detalles de cambio a todas las personas que corresponda.
    v. Procedimientos que identifiquen las responsabilidades de abortar y recuperar los cambios sin éxito.
c) Se debe contar con responsabilidades y procedimientos de gestión de incidencias para asegurar una respuesta rápida, eficaz y ordenada a las incidencias en materia de seguridad.
d) Se debe establecer procedimientos para cubrir todos los tipos posibles de incidencias de seguridad, teniendo en cuenta:

i. Fallos del sistema de información y pérdidas de servicio.
ii. Denegación de servicio.
iii. Errores que resultan de datos del negocio inexactos o incompletos.
iv. Violaciones de confidencialidad

e) Se debe establecer procedimientos adicionales a los planes de continuidad, normales, para recuperar sistemas o servicios tan rápidamente como sea posible, teniendo en cuenta:
   i. El análisis e identificación de la causa de la incidencia.
   ii. La planificación e implantación de medidas para evitar su repetición, si fuera necesario.
   iii. La recogida de pistas de auditoría y otras evidencias similares.
   iv. La comunicación con los afectados o implicados en la recuperación de la incidencia.
   v. La comunicación de las acciones realizadas a la autoridad apropiada.
   vi. Se deben proteger y asegurar las pistas de auditoria y evidencias similares.
   vii. Debe controlarse cuidadosa y formalmente la acción para recuperarse de los efectos de los fallos de seguridad y corregir los fallos del sistema, documentándose detalladamente todas las acciones realizadas por emergencia.

f) Se debe considerar la separación de la gestión o ejecución de tareas o áreas de responsabilidad para reducir las oportunidades de modificación no autorizada o de mal uso de la información o los servicios.

g) Se debe definir y documentar las reglas para transferir el software del entorno de desarrollo y certificación al de producción.

h) Se debe implementar una separación entre las funciones de desarrollo y certificación, manteniendo un entorno conocido y estable para poder realizar las pruebas significativas y evitar el acceso inapropiado del personal de desarrollo.

i) La segregación de los recursos de desarrollo, certificación y producción es conveniente para reducir el riesgo de cambios accidentales o del acceso no autorizado al software de producción y

a los datos de la organización, considerándose los siguientes controles:

i. El software de desarrollo y el de producción deben funcionar en procesadores diferentes, o en dominios o directorios distintos.
ii. Las tareas de desarrollo y certificación deben separarse tanto como sea posible.
iii. Los compiladores, editores y otros servicios del sistema no deben ser accesibles desde los sistemas de producción.
iv. Se debe usar procedimientos 'log-on' en los sistemas de producción y certificación para reducir el riesgo de confusión. Se debe indicar a los usuarios para que empleen contraseñas diferentes para estos dos sistemas y los menús deben exhibir los mensajes de identificación apropiados.
v. Los medios de desarrollo, prueba / certificación y producción deberán estar separados para reducir los riesgos de acceso no autorizado o cambios en los sistemas de producción.

3.5.2 Planificación y aceptación del sistema.

a) El Área de Tecnología de Información y Comunicaciones en coordinación con la Unidad de Seguridad de la Información y con la Gerencia Municipal, debe implementar la "Gestión de la Capacidad", proceso en el cual se monitorea y afina el uso de los recursos, comprobando las demandas actuales y las proyecciones de los futuros requisitos de capacidad tomando en cuenta los requerimientos del negocio, sistemas nuevos y las tendencias actuales, para asegurar la disponibilidad de capacidad de procesamiento y almacenamiento adecuados para la Entidad.
b) Se debe prestar atención a cualquier recurso con tiempo de espera largo de abastecimiento o costos altos, en tal sentido la Gerencia Municipal deberá monitorear la utilización de estos recursos claves del sistema.
c) Los administradores de los sistemas deben monitorear el uso de los recursos críticos del sistema, incluyendo los procesadores, el almacenamiento principal y el de archivos, las impresoras, otros dispositivos de salida y los sistemas de comunicaciones. Los

administradores de los sistemas deben usar esta información para identificar y evitar los posibles cuellos de botella que puedan representar una amenaza a la seguridad del sistema o a los servicios al usuario, para planificar la acción correctora apropiada.

d) Se deben establecer criterios de aceptación para nuevos sistemas de información y versiones nuevas o mejoradas y se deben desarrollar con ellos las pruebas adecuadas antes de su aceptación.
e) Los administradores de los sistemas se deben asegurar que los requisitos y criterios de aceptación de los nuevos sistemas están claramente definidos, acordados, documentados y probados, considerándose lo siguiente:
    i. Los requisitos de rendimiento y capacidad de las computadoras.
    ii. Los procedimientos de recuperación de errores y reinicio, así como los planes de contingencia.
    iii. La preparación y prueba de procedimientos operativos de rutina según las normas definidas.
    iv. Un conjunto acordado de controles y medidas de seguridad instalados.
    v. Manual de procedimiento eficaz
    vi. Plan de continuidad del negocio.
    vii. La formación en la operatividad o utilización de los sistemas nuevos.

3.5.3 Protección contra software malicioso.

a) Se debe implantar controles para detectar el software malicioso y prevenirse contra él, junto con procedimientos adecuados para sensibilizar a los usuarios, considerándose:
    i. El cumplimiento de las licencias de software y la prohibición del uso de software no autorizado.
    ii. Instalación y actualización frecuente de software de detección y reparación de virus.
    iii. Realización de revisiones regulares del software y de los datos contenidos en los sistemas que soportan procesos críticos de la organización.
    iv. Verificación de todo archivo adjunto a un correo electrónico.

v. Planes de continuidad del negocio apropiados para recuperarse de los ataques de virus.

b) La actualización de los antivirus se debe realizar en forma diaria y automática.

c) Todos los archivos obtenidos de fuente externa por medio magnético, óptico, etc. antes de ser instalados y/o ejecutados deberán ser previamente revisados por el Área de Tecnología de Información y Comunicaciones para prevenir infección por software malicioso.

d) Se debe implementar controles para la actualización de parches y otros del Sistema Operativo del computador.

3.5.4 Gestión interna de respaldo de la información.

a) El respaldo del Sistema Informático de la Municipalidad Distrital de Ilabaya se debe realizar de forma centralizada con procedimientos formales y responsables de la gestión de backups.

b) El proceso de restauración de la información lo realiza el personal autorizado del Área de Tecnología de Información y Comunicaciones utilizando los controles de seguridad respectivos para asegurar que el proceso fue satisfactorio.

c) Generar copias de resguardo sobre toda la información y programas necesarios para las operaciones de la organización, almacenando las copias generadas en un lugar seguro externo del CPD.(Centro de Procesamiento de Datos).

d) Se debe establecer la periodicidad de la generación de backups de información para su resguardo.

e) Se debe contar con adecuadas medidas de seguridad en los lugares de respaldo, sin estar expuestos a las mismas contingencias que el centro de cómputo principal, y serán transportados en un medio resistente que los proteja. Se designará un responsable y un suplente encargados de su custodia.

f) Se debe contar con una bitácora de registro de fallos en la generación de backups y restauración de los mismos, así como las acciones adoptadas para corregirlas.

3.5.5 Control de red.

a) Poner en conocimiento las normas y responsabilidades de cada usuario, para el uso correcto de la red.
b) Se prohíbe el uso de los sistemas de comunicación de la Municipalidad Distrital de Ilabaya para actividades comerciales privadas o para propósitos de entretenimiento y diversión.
c) La información enviada a través de la red de comunicaciones de la Municipalidad Distrital de Ilabaya se considera privada y es propiedad de la Entidad.
d) Se debe elaborar procedimientos para la autorización de los accesos a redes y servicios de red, los mismos que deberán ser elaborados por el Área de Tecnología de Información y Comunicaciones en coordinación con la Oficina de Seguridad de la Información.
e) Se debe elaborar procedimientos para protección del acceso a las conexiones de la red y los servicio en red, los mismos que deberán ser elaborados por el Área de Tecnología de Información y Comunicaciones en coordinación con la Oficina de Seguridad de la Información.

3.5.6 Confidencialidad y privacidad.

a) La Municipalidad Distrital de Ilabaya implementa las acciones a fin de asegurar la protección y seguridad de datos conforme a la legislación y regulación aplicable respecto a sus clientes y usuarios de servicios.
b) El personal no autorizado de la Entidad no debe interceptar las comunicaciones o divulgar su contenido.
c) Es política de la Entidad monitorear regularmente las comunicaciones, para lo cual es necesario realizar actividades de mantenimiento, seguridad o auditoria.
d) Respetar y guardar confidencialidad de toda la información de los clientes, infringir esta disposición será causal de despido.
e) No dejar las impresoras desatendidas, sobre todo si se está imprimiendo (o se va a imprimir) información confidencial.

3.5.7 Intercambio de Información.

a) Se debe establecer procedimientos para proteger el intercambio de información de la intercepción, copiado, modificación, routing equivocado y destrucción, los mismos que deberán ser implementados por el Área de Tecnología de Información y Comunicaciones en coordinación con la Oficina de Seguridad de la Información.

b) Todo el personal deberá hacer uso aceptable de los medios de comunicación electrónicos, los mismos que deberán estar debidamente reglamentados y aprobados por el Directorio.

c) Se debe establecer procedimientos y estándares para la comunicación inalámbrica, tomando en cuenta los riesgos particulares de este medio.

d) Se debe establecer procedimientos y estándares relacionados con el uso de técnicas de codificación para proteger la confidencialidad, integridad y autenticidad de la información, los mismos que deberán ser implementados por el Área de Tecnología de Información y Comunicaciones en coordinación con la Oficina de Seguridad de la Información.

e) Se debe concientizar al personal sobre buenas prácticas de seguridad en el intercambio de información.

f) Se debe elaborar procedimientos donde se establezca el manejo de las responsabilidades para el control y notificación de la transmisión, así como para el despacho y recepción de información.

g) Se debe implementar un proceso formal para el uso de etiquetado para la información confidencial o reservada, asegurando que el significado de las etiquetas sea entendido inmediatamente y que la información sea adecuadamente protegida.

h) Se debe elaborar procedimientos para el manejo y protección de los medios que contienen información, evitando así accesos no

autorizados, mal uso o corrupción durante el transporte más allá de los límites físicos de una organización.

3.6 RESPECTO AL DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN

3.6.1 Análisis de los Requerimientos de Información.

a) Todo desarrollo de cualquier nuevo sistema de información o modificación de los mismos requiere que esté debidamente justificado que a su vez será soportado por un sistema de gestión documental formal y con la participación explicita de los propietarios de la información.

b) El desarrollo y/o actualización de los Sistemas de Información es competencia del Comité de Gerencia Municipal, para lo cual se tomará en cuenta los requerimientos de los diversos usuarios, normatividad vigente y se conformará grupos de trabajo multidisciplinarios nombrados por la Gerencia Municipal.

c) La definición de requerimientos y la recopilación de información para el desarrollo del nuevo aplicativo o modificación de los existentes es responsabilidad del jefe de Proyecto o de los analistas responsables del desarrollo que deben realizar las coordinaciones con el o los usuarios del Área solicitante.

d) El jefe de proyecto y sus analistas o analista responsable en coordinación con los usuarios solicitantes determinaran los procesos de entrada de datos, el diseño de los formularios, tipos de campos a utilizar, y las etiquetas a utilizar.

e) El jefe del Área de Tecnología de Información y Comunicaciones establecerá un estándar de programación para el desarrollo de sistemas, a fin de garantizar un adecuado control de cambios de modificaciones sobre los aplicativos.

f) Definir estándares de configuración de acceso para perfiles de usuario requeridos en los sistemas.

g) Revisar periódicamente la data a fin de detectar inexactitud, cambios no autorizados e integridad de la información.

h) Toda modificación o desarrollo de un aplicativo nuevo deberá estar documentado, para que en otra oportunidad de ser necesario nuevas modificaciones se puedan realizar de una manera rápida, dado que

el analista ya cuenta con una información previa que le sirve de base para realizar el mantenimiento futuro del módulo y el usuario podrá conocer toda la funcionalidad del aplicativo.

3.6.2 Procesamiento correcto de las Aplicaciones.

a) Se debe tener un mecanismo para garantizar la integridad de datos a ser procesado, utilizando las validaciones de los campos de entrada de información, así como el manejo de una tabla de errores.
b) Se deben implementar los mecanismos de control de datos que garanticen la integridad de los mismos al ser procesados, para obtener información confiable.
c) Todo proceso de validación de datos debe complementarse con los mecanismos de ayuda necesarios para orientar a los usuarios sobre qué hacer ante cualquier eventualidad.
d) El analista responsable debe implementar los procedimientos de control de calidad respectivos, así como los mensajes de ayuda para que el usuario este informado.
e) Los controles de manejo de la salida de datos estarán bajo la responsabilidad del analista responsable del desarrollo del aplicativo y del propietario de la información que valida los resultados.
f) El analista responsable del desarrollo del aplicativo y el usuario del área de negocio designado son los encargados de hacer las revisiones y validaciones respectivas.
g) Se debe tener un medio único para la generación de los reportes emitidos, así como tener un registro de los reportes emitidos.
h) El responsable de monitorear la integridad de los datos almacenados en la base de datos es el DBA o el analista encargado del Desarrollo de la aplicación y debe adoptar las medidas de seguridad para la protección de la información que reside en ella para que no sea accedida por usuarios no autorizados.
i) Antes de la puesta en producción el equipo de certificación debe realizar las pruebas del aplicativo en coordinación con los usuarios del Área solicitantes para dar la conformidad del aplicativo.

3.6.3 Seguridad de los archivos del sistema.

a) El Analista Administrador de Base de Datos es el responsable de implementar las medidas de protección de la información en

coordinación con la Jefatura de Tecnología de la Información y Comunicaciones.

b) La Jefatura de Tecnología de la Información y Comunicaciones designara al responsable de la administración de las versiones y del almacenamiento de los programas fuentes de los Sistemas de Información existentes.

3.6.4 Política de Mantenimiento y Actualización.

a) El mantenimiento es responsabilidad del área de Tecnología de la Información y Comunicaciones, la cual debe documentar las acciones ejecutadas y cumplir con lo establecido por los controles existentes y la normativa vinculada

3.6.5 Respaldo y restauración.

a) Los procesos de respaldo y restauración deben de realizarse de manera automática con horarios definidos, las pruebas de control sobre las copias de respaldos y restauraciones de base de datos y programas fuentes deben de realizarse periódicamente por el personal de Desarrollo y el DBA.

b) Se debe tener respaldo de todos los objetos de la base de datos, así como los programas fuentes del o los sistemas de información usados por la Municipalidad Distrital de Ilabaya.

c) Los programas fuentes como la información de la base de datos debe ser almacenada y administrada de una manera centralizada mediante la utilización de los equipos y software adecuados para esta función.

d) Las operaciones realizadas deben estar debidamente registradas, para lo que se deben considerar la implementación de pistas de Auditoria para el control de las operaciones.

3.6.6 Controles Criptográficos.

a) Todas las transacciones electrónicas que se empleen deben de contemplar las medidas de seguridad de datos (encriptación de datos), tener las identificaciones de terminales emisor como receptor, el tipo de operaciones a realizar, otra información adicional.

3.6.7 Gestión de la Vulnerabilidad Técnica.

a) El área de Tecnología de la Información y Comunicaciones en coordinación con la Unidad de Seguridad y Continuidad del Negocio, deberá tomar la acción apropiada y oportuna en respuesta a la

identificación de vulnerabilidades técnicas potenciales, incluyendo el monitoreo de la vulnerabilidad, evaluación del riesgo de la vulnerabilidad y monitoreo de activos.

b) La evaluación de vulnerabilidades técnicas podrá ser ejecutada por personal de la Entidad o por entes externos especializados por lo menos una vez al año, asimismo, dicha evaluación deberá ser supervisada por el Área de Tecnologías de la Información y Comunicaciones.

c) El proceso de gestión de vulnerabilidad técnica deberá abarcar aplicativos relacionados con la atención a clientes, especialmente los utilizados en los canales electrónicos.

d) El proceso de gestión de vulnerabilidad técnica debe ser monitoreado y evaluado regularmente para asegurar su efectividad y eficacia.

e) Una vez que se identifique la vulnerabilidad técnica potencial, se debe identificar los riesgos asociados y las acciones a tomarse, conjuntamente con la definición del tiempo para reaccionar a las notificaciones de vulnerabilidades técnicas potencialmente relevantes

f) Se debe mantener un registro de todos los procedimientos realizados en la gestión de vulnerabilidades.

3.7 RESPECTO DE LA SEGURIDAD DE LA COMPUTACIÓN MÓVIL Y TELETRABAJO

3.7.1 Computación Móvil

a) En caso de utilizarse equipos móviles para el procesamiento de información, éste deberá de contar con un sistema de conexión remota segura VPN o mediante el uso de conexiones SSL para garantizar el flujo seguro de información.

b) Se debe implementar procedimientos para proteger la información sensible de la Entidad en ambientes desprotegidos, para evitar el acceso no autorizado o divulgación de la información almacenada y procesada por estos medios.

c) Todo usuario que realiza computación móvil debe cumplir con los controles de acceso a los sistemas y la información determinados en este documento.

d) Se debe establecer procedimientos contra los softwares maliciosos y se deben mantener actualizados.
e) Se debe implementar procedimientos de protección de la información en caso de robo o pérdida de equipos, como el respaldo de información de forma periódica.
f) Se debe planificar capacitación para el personal que utiliza computación móvil para elevar el nivel de conciencia sobre los riesgos adicionales resultantes de esta forma de trabajo y los controles que se debieran implementar.

3.7.2 Teletrabajo

El teletrabajo, o trabajo a distancia, permite trabajar en un lugar diferente a la oficina. La utilización de los medios informáticos permite mejor comunicación de forma remota, lo que permite trabajar de forma no presencial.

a) Se debe considerar la seguridad física en el lugar del tele-trabajo, tomando en cuenta la seguridad física del edificio y el ambiente del local.
b) La seguridad de las comunicaciones debe ser una prioridad, tomando en cuenta la necesidad de acceso remoto a los sistemas internos de la Entidad, la confidencialidad de la información a la cual se tendrá acceso y el vínculo de comunicación y confidencialidad del sistema interno.
c) Se debe implementar procedimientos para minimizar los riesgos relacionados a amenazas de acceso no autorizado a la información o recursos por parte de otras personas que utilizan el medio; por ejemplo, familia y amigos.
d) El Área de Tecnología de Información y Comunicaciones es responsable de la provisión de soporte y mantenimiento del hardware y software de propiedad de la Entidad, utilizados para el teletrabajo.
e) Se debe implementar procedimientos para el respaldo (backup) y la continuidad de negocio.
f) Se debe firmar un documento formal en el cual se estipule el acuerdo de teletrabajo de carácter voluntario y puede ser terminado por el empleado o por la Municipalidad Distrital de Ilabaya, con o sin razón.

g) Las funciones, compromisos, responsabilidades y la situación del empleado dentro de la empresa, así como su salario u otros beneficios deben ser los mismos.

h) El empleado debe cumplir con los horarios y las horas de trabajo establecidos por los términos del acuerdo de trabajo entre el empleado y la Entidad, si por alguna razón se requiere horas adicionales será con autorización de la Gerencia Municipal.

i) Se debe inspeccionar el lugar de teletrabajo empleado con el fin de determinar si el sitio es adecuado para las responsabilidades del empleado. La Entidad también deberá de inspeccionar y verificar las horas trabajadas por el empleado.

j) El empleado debe proteger los datos, documentos, archivos, software y equipos proporcionados por la Entidad, así como a respetar todas las políticas, reglamentos y normativa relativos a la seguridad de la información confidencial.

4. NORMAS Y POLÍTICAS EN EL USO DE SERVICIOS DE CORREO Y ACCESO A INTERNET

Es responsabilidad de todo miembro personal de la Municipalidad Distrital de Ilabaya utilizar el correo electrónico y el acceso a Internet de forma eficiente, eficaz, ética y diligente respetando las buenas costumbres, el orden público, el derecho a la intimidad y de acuerdo cumplir con las normas, reglamentos y procedimientos establecidos por la Entidad y respetando los aspectos legales vigentes, con el fin de proporcionar seguridad a la información de la Entidad.

Asimismo, la Entidad establecerá reglamentos conteniendo obligaciones y responsabilidades del uso del Correo Electrónico y Acceso a Internet.

4.1 CORREO ELECTRÓNICO

Su principal propósito es servir como herramienta para agilizar las comunicaciones que apoyen al sistema de comunicación de la gestión de control interno existente en la Entidad.

a) Los mensajes de correo electrónico son documentos formales, los cuales deben respetar todos los lineamientos referentes al uso apropiado del lenguaje.

b) Está prohibido suplantar a otra persona al enviar mensajes de correo.

c) No debe violarse la privacidad del personal, pero deben tomarse las medidas técnicas de resguardo y detección de información, para que en caso de una conducta ilícita, pueda realizarse la investigación correspondiente a fin de determinar la responsabilidad y posibilitar la obtención de las pruebas necesarias.

d) La Municipalidad Distrital de Ilabaya a través del Área Responsable, se reserva el derecho a auditar, vigilar, detectar y fiscalizar los sistemas de correspondencia electrónica para garantizar que los recursos informáticos de su propiedad sean utilizados sólo para propósitos y gestiones relacionadas con el trabajo. Estas auditorías se realizarán periódicamente, o de forma inopinada o cuando exista una investigación sobre una situación en particular. Al personal de la Entidad no le alberga expectativa de intimidad con relación a cualquier información, documento, mensaje creado, recibido o enviado a través del sistema de correo electrónico (E-mail) del servidor de la Municipalidad Distrital de Ilabaya.

e) La Municipalidad Distrital de Ilabaya, definirá un reglamento de uso de correo electrónico a fin de regular su funcionamiento y manejo, así como establecer las responsabilidades y obligaciones de los usuarios respecto a este servicio, dicho reglamento será puesto en conocimiento de los miembros de la organización.

4.2 **ACCESO A INTERNET**

Internet es una herramienta de consulta y acceso de información global cuyo uso autoriza explícitamente la Gerencia Municipal en forma extraordinaria, puesto que su utilización nos expone a amenazas.

a) El acceso a internet debe ser de uso exclusivamente para el desarrollo de las funciones asignadas al puesto bajo el criterio de Necesidad.

b) El acceso a Internet debe ser monitoreado y se debe tener registros de todos los sitios visitados por equipo y por usuario.

c) Debe existir un procedimiento formal de solicitud, autorización y entrega del permiso de acceso a Internet.

d) Los usuarios que hacen uso de este servicio no deben acceder a páginas de entretenimiento, pornografía, de contenido ilícito que atenten contra la dignidad e integridad humana: aquellas que realizan

apología del terrorismo, páginas con contenido xenófobo, racista etc. o que estén fuera del contexto laboral.

e) Los trabajadores autorizados tendrán acceso solo a la información necesaria para el desarrollo de sus actividades.

f) La Municipalidad Distrital de Ilabaya, definirá un reglamento de uso de internet a fin de regular su funcionamiento y manejo, así como establecer las responsabilidades y obligaciones de los usuarios respecto a este servicio, dicho reglamento será puesto en conocimiento de los miembros de la organización.

g) La política adoptada para el uso de Internet debe ser revisada periódicamente en caso de que surjan nuevas necesidades, únicas y particulares de la Municipalidad Distrital de Ilabaya.

5. **SANCIONES**

a) Cualquier violación a las políticas y normas de seguridad de la información deberá ser sancionada de acuerdo al reglamento interno emitido por la Entidad.

b) Las sanciones pueden ser desde una llamada de atención o informar al usuario hasta la suspensión del vínculo laboral del servicio dependiendo de la gravedad de la falta y de la malicia o perversidad que esta manifiesta.

c) También corresponderá a la Oficina de Seguridad de la Información hacer las propuestas finales sobre las sanciones a quienes violen las disposiciones en materia de seguridad de la información y continuidad de negocio de la Entidad.

d) Todas las acciones en las que se comprometa la seguridad de la información de la red, base de datos, sistemas informáticos, registros físicos y otros medios, de la Municipalidad Distrital de Ilabaya y que no estén previstas en esta política, deberán ser revisadas por la Gerencia Municipal, Oficina de Seguridad de la Información y el Área de Tecnología de la Información y Comunicaciones para dictar una resolución sujetándose al estado de derecho.

Anexo 9. Sistema SGSI_MDI

Ingresar al siguiente link para acceder al Sistema.

https://drive.google.com/drive/folders/1-wuNtrwFLIuHJsDO29T23eBDfzU4jhoX?usp=sharing