

# Hansi Elorrieta Rondon

## ELORRIETA RONDON, HANSI-SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y LA CALIDAD DEL SERVI...

 Quick Submit

 Quick Submit

 Universidad Politécnica del Perú

---

### Detalles del documento

Identificador de la entrega

trn:oid:::1:3240855586

Fecha de entrega

5 may 2025, 10:06 p.m. GMT-5

Fecha de descarga

5 may 2025, 10:24 p.m. GMT-5

Nombre de archivo

IDAD\_DEL\_SERVICIO\_INFORM\_TICO\_EN\_LA\_UNIVERSIDAD\_NACIONAL\_DE.docx

Tamaño de archivo

1.2 MB

98 Páginas

16.629 Palabras

96.655 Caracteres

# 8% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

## Filtered from the Report




- ▶ Bibliography
- ▶ Quoted Text
- ▶ Small Matches (less than 20 words)

## Exclusions

- ▶ 1 Excluded Source

---


## Top Sources

- 8%  Internet sources
- 0%  Publications
- 4%  Submitted works (Student Papers)

---

## Integrity Flags

### 1 Integrity Flag for Review

-  **Hidden Text**  
5 suspect characters on 4 pages  
Text is altered to blend into the white background of the document.

Our system's algorithms look deeply at a document for any inconsistencies that would set it apart from a normal submission. If we notice something strange, we flag it for you to review.

A Flag is not necessarily an indicator of a problem. However, we'd recommend you focus your attention there for further review.

## Top Sources

- 8% Internet sources
- 0% Publications
- 4% Submitted works (Student Papers)

## Top Sources

The sources with the highest number of matches within the submission. Overlapping sources will not be displayed.

|   |                |                                  |     |
|---|----------------|----------------------------------|-----|
| 1 | Internet       | repositorio.ujcm.edu.pe          | 4%  |
| 2 | Internet       | repositorio.uap.edu.pe           | 2%  |
| 3 | Student papers | Universidad Politécnica del Perú | 2%  |
| 4 | Student papers | Universidad Alas Peruanas        | <1% |
| 5 | Internet       | ujcm.edu.pe                      | <1% |
| 6 | Internet       | repositorio.unjfsc.edu.pe        | <1% |
| 7 | Internet       | repositorio.upt.edu.pe           | <1% |
| 8 | Internet       | hdl.handle.net                   | <1% |

# UAP

**UNIVERSIDAD ALAS PERUANAS  
VICERRECTORADO ACADÉMICO  
ESCUELA DE POSGRADO**

**SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN  
Y LA CALIDAD DEL SERVICIO INFORMÁTICO EN LA  
UNIVERSIDAD NACIONAL DE MOQUEGUA-2024**

**PARA OPTAR EL GRADO ACADÉMICO DE:  
DOCTOR EN INGENIERÍA DE SISTEMAS  
E INFORMÁTICA**

**PRESENTADO POR:  
Mg. HANSI ELORRIETA RONDON  
CÓDIGO ORCID: <https://orcid.org/000-0002-9142-9368>**

**Asesor :  
Dr. RICHARD ROBERT RAFAEL RUTTE  
Codigo orcid: <https://orcid.org/0009-0005-2508-4823>**

**TACNA – PERÚ  
2024**

## **DEDICATORIA**

A Cristo Redentor por darme perseverancia en la culminación de mis estudios.

## **AGRADECIMIENTO**

A mi familia que siempre me dio aliento para continuar y culminar mis estudios doctorales.

## **RECONOCIMIENTO**

A mis docentes de la Escuela de  
Posgrado UAP.

## INTRODUCCIÓN

La información es fundamental para el funcionamiento de las organizaciones actuales. A partir de esto, se puede considerar a las organizaciones como entidades cohesionadas por el flujo de información, lo que otorga un valor crucial a la información y a los procesos de adquisición, procesamiento y conservación de esta. La protección de la información dentro de la organización es responsabilidad de la seguridad de la información, un campo clave dentro de los sistemas de información que desempeña diversas funciones esenciales, como la protección del funcionamiento organizacional, el aseguramiento de operaciones seguras y la protección de otros activos. Esto se conoce generalmente como la misión de la seguridad de la información, de la cual se deriva una definición amplia de la seguridad de los sistemas de información como el estado de estar libre de riesgos y, al mismo tiempo, no estar expuesto a posibles daños causados por ataques o accidentes.

El objetivo principal de esta investigación es implementar nuevos mecanismos de seguridad que mejoren el rendimiento organizacional en términos de exposición, integridad, disponibilidad y confidencialidad de la información. Además, se busca evaluar el nivel de conocimiento sobre seguridad de la información entre los empleados de la UNAM Filial Ilo.

En el capítulo I, titulado "Planteamiento del problema", se analiza la realidad problemática desde una perspectiva amplia del tema de estudio, basada en evidencias empíricas y documentales que guían la investigación. Posteriormente, en la definición del problema, se plantea la cuestión principal a resolver. A continuación, se identifican los objetivos de la investigación, se justifica su importancia y se abordan tanto la viabilidad como las limitaciones del estudio.

En el capítulo II, titulado "Marco Filosófico", se abordan los fundamentos epistemológicos y ontológicos del estudio.

En el capítulo III, se lleva a cabo el análisis de los antecedentes del problema de investigación, así como de las bases teóricas, las cuales deben ser pertinentes para una adecuada contextualización del problema investigado.

En el capítulo IV, se definen las hipótesis y variables, seguidas por las definiciones conceptual y operativa de dichas variables.

En el capítulo V, denominado "Metodología de la investigación", se describe el tipo y nivel de la investigación, así como su diseño. Además, se identifica la población y la muestra, se detallan las técnicas, instrumentos y fichas informativas utilizadas, y se explica el proceso de recolección y análisis de datos.

El Capítulo VI, "Resultados", se centra en los resultados descriptivos e inferenciales, luego se desarrolla la discusión de resultados, conclusiones, recomendaciones las referencias bibliográficas y anexos referentes a la matriz de consistencias, instrumentos, base de datos y autenticidad de la tesis.

# Índice

|   |           |
|---|-----------|
| DEDICATORIA .....   | ii        |
| AGRADECIMIENTO.....                                       | iii       |
| RECONOCIMIENTO .....                                      | iv        |
| INTRODUCCIÓN.....   | v         |
| INDICE DE TABLAS .....                                    | x         |
| INDICE DE FIGURAS .....                                   | xi        |
| RESUMEN .....   | 12        |
| ABSTRACT .....  | 13        |
| RIEPILOGO .....   | 14        |
| <b>1 CAPITULO I: PLANEAMIENTO DEL PROBLEMA.....</b>       | <b>15</b> |
| 1.1 Descripción de la Realidad Problemática .....         | 15        |
| 1.2 Delimitación de la Investigación.....                 | 19        |
| <b>1.2.1 Delimitación espacial .....</b>                  | <b>19</b> |
| <b>1.2.2 Delimitación social .....</b>                    | <b>19</b> |
| <b>1.2.3 Delimitación Temporal.....</b>                   | <b>19</b> |
| <b>1.2.4 Delimitación Conceptual .....</b>                | <b>19</b> |
| 1.3 Problemas de Investigación.....                       | 19        |
| <b>1.3.1 Problema General.....</b>                        | <b>19</b> |
| <b>1.3.2 Problemas Específicos .....</b>                  | <b>20</b> |
| 1.4 Objetivos de la Investigación .....                   | 20        |
| <b>1.1.1. Objetivo General.....</b>                       | <b>20</b> |
| <b>1.1.2. Objetivos Específicos .....</b>                 | <b>20</b> |
| 1.5 Justificación e Importancia de la Investigación ..... | 21        |
| <b>1.5.1 Justificación Teórica.....</b>                   | <b>21</b> |
| <b>1.5.2 Justificación Practica.....</b>                  | <b>21</b> |
| <b>1.5.3 Justificación Social.....</b>                    | <b>21</b> |
| <b>1.5.4 Justificación Metodológica.....</b>              | <b>21</b> |
| <b>1.5.5 Importancia .....</b>                            | <b>22</b> |
| 1.6 Factibilidad de la Investigación .....                | 23        |
| 1.7 Limitaciones del estudio .....                        | 23        |
| <b>2 CAPITULO II: MARCO FILOSOFICO .....</b>              | <b>24</b> |
| 2.1 Fundamentación Ontológica.....                        | 24        |
| 2.2 Fundamentación Epistemológica .....                   | 24        |
| <b>3 CAPITULO III: MARCO TEORICO CONCEPTUAL .....</b>     | <b>27</b> |
| 3.1 Antecedentes de la investigación .....                | 27        |
| <b>3.1.1 Antecedentes a nivel internacional.....</b>      | <b>27</b> |

|          |  |           |
|----------|--|-----------|
| 3.1.2    | <b>Antecedentes a nivel Nacional</b> .....   | <b>30</b> |
| 3.2      | Bases teóricas .....   | 33        |
| 3.2.1    | <b>La Norma ISO 17799</b> .....  | <b>33</b> |
| 3.2.2    | <b>Norma ISO/IEC 27001</b> .....   | <b>35</b> |
| 3.2.3    | <b>El modelo SERVQUAL</b> .....  | <b>36</b> |
| 3.2.4    | <b>ISO 9001 aplicado a los servicios</b> .....   | <b>38</b> |
| 3.3      | Definición de Términos Básico .....  | 39        |
| <b>4</b> | <b>CAPITULO IV: HIPOTESIS Y VARIABLES</b> .....  | <b>43</b> |
| 4.1      | Hipótesis General .....  | 43        |
| 4.2      | Hipótesis Específicas .....  | 43        |
| 4.3      | Definición conceptual y operacional de las variables .....                               | 43        |
| 4.3.1    | <b>VARIABLE 1</b> .....  | <b>43</b> |
| 4.3.2    | <b>VARIABLE 2</b> .....  | <b>44</b> |
| 4.4      | Cuadro de Operacionalización de Variables .....  | 45        |
| <b>5</b> | <b>CAPITULO V: METODOLOGIA DE LA INVESTIGACION</b> .....                                 | <b>49</b> |
| 5.1      | 5.1 ENFOQUE, TIPO Y NIVEL DE INVESTIGACION .....   | 49        |
| 5.1.1    | <b>5.1.1. ENFOQUE DE INVESTIGACION: CUANTITATIVO</b> .....                               | <b>49</b> |
| 5.1.2    | <b>TIPO DE INVESTIGACIÓN: BASICA</b> .....   | <b>50</b> |
| 5.1.3    | <b>NIVEL DE INVESTIGACION DESCRIPTIVO - CORRELACIONAL</b> .....                          | <b>51</b> |
| 5.2      | METODOS DE INVESTIGACION .....   | 52        |
| 5.2.1    | <b>METODO GENERAL: HIPÓTETICO- DEDUCTIVO</b> .....                                       | <b>52</b> |
| 5.2.2    | <b>METODO ESPECIFICO: ESTADISTICO</b> .....  | <b>53</b> |
| 5.2.3    | <b>DISEÑO DE LA INVESTIGACION</b> .....  | <b>53</b> |
| 5.3      | POBLACION Y MUESTRA DE LA INVESTIGACION .....  | 54        |
| 5.3.1    | <b>POBLACION</b> .....   | <b>54</b> |
| 5.3.2    | <b>MUESTRA: CENSAL</b> .....   | <b>54</b> |
| 5.4      | TECNICAS E INSTRUMENTOS DE RECOLECCION DE DATOS .....                                    | 55        |
| 5.4.1    | <b>TECNICAS</b> .....  | <b>55</b> |
| 5.4.2    | <b>INSTRUMENTOS</b> .....  | <b>56</b> |
| 5.4.3    | <b>VALIDEZ Y CONFIABILIDAD</b> .....   | <b>56</b> |
| 5.4.4    | <b>PROCESAMIENTO Y ANALISIS DE DATOS</b> .....   | <b>56</b> |
| 5.4.5    | <b>ETICA EN LA INVESTIGACION</b> .....   | <b>57</b> |
| <b>6</b> | <b>CAPITULO VI: RESULTADOS</b> .....   | <b>58</b> |
| 6.1      | ANÁLISIS DESCRIPTIVO .....   | 58        |
| 6.1.1    | <b>Variable Sistema de Gestión de la Seguridad de la Información (SGSI)</b><br><b>58</b> |           |
| 6.2      | ESTADÍSTICA INFERENCIAL .....  | 69        |

|          |   |           |
|----------|---|-----------|
| <b>7</b> | <b>CAPITULO VI: DISCUSIÓN DE LOS RESULTADOS</b>                                   | <b>75</b> |
|          | <b>CONCLUSIONES</b>   | <b>77</b> |
|          | <b>RECOMENDACIONES</b>  | <b>78</b> |
|          | <b>REFERENCIAS BIBLIOGRÁFICAS</b>   | <b>79</b> |
|          | <b>ANEXO 1: MATRIZ DE CONSISTENCIA</b>  | <b>84</b> |
|          | <b>ANEXO 2: CUESTIONARIOS</b>   | <b>86</b> |
|          | <b>ANEXO 3: FICHAS DE VALIDACIÓN DE EXPERTOS</b>                                  | <b>91</b> |
|          | <b>ANEXO 04. COPIA DE LA DATA PROCESADA</b>                                       | <b>94</b> |
|          | <b>ANEXO N°5: CONSENTIMIENTO INFORMADO</b>  | <b>96</b> |
|          | <b>ANEXO N°6: AUTORIZACIÓN DE LA ENTIDAD DONDE SE REALIZÓ EL TRABAJO DE CAMPO</b> | <b>97</b> |
|          | <b>ANEXO 7: DECLARATORIA DE AUTENTICIDAD DE TESIS</b>                             | <b>98</b> |

## INDICE DE TABLAS

|   |    |
|---|----|
| Tabla 1: Sistema de Gestión de la Seguridad de la Información .....                 | 58 |
| Tabla 2: D1 Principios de Seguridad de la Información .....                         | 60 |
| Tabla 3: D2 ISO/IEC 27001 .....   | 61 |
| Tabla 4: D3 Gestion de Seguridad de la Información .....                            | 62 |
| Tabla 5: D4 Implantación del Sistema de Gestion de Seguridad de la Información..... | 63 |
| Tabla 6: Variable: Calidad del Servicio Informático.....                            | 64 |
| Tabla 7: D1 Fiabilidad.....   | 65 |
| Tabla 8: D2 Capacidad de respuesta.....   | 66 |
| Tabla 9: D3 Capacitacion del personal.....  | 67 |
| Tabla 10: D4 Atención al Cliente .....  | 68 |
| Tabla 11: Prueba de Normalidad .....  | 69 |
| Tabla 12: Contrastación de Hipótesis General .....                                  | 70 |
| Tabla 13: Contrastación de Hipótesis Específica 1 .....                             | 71 |
| Tabla 14: Contrastación de Hipótesis Específica 2.....                              | 72 |
| Tabla 15: Contrastación de Hipótesis Específica 3.....                              | 73 |
| Tabla 16: Contrastación de Hipótesis Específica 3.....                              | 74 |

2

## INDICE DE FIGURAS

|  |    |
|--|----|
| Figura 1: Sistema de Gestión de la Seguridad de la Información .....                 | 58 |
| Figura 2: D1 Principios de Seguridad de la Información. ....                         | 60 |
| Figura 3: D2 ISO/IEC 27001 .....   | 61 |
| Figura 4: D3 Gestion de Seguridad de la Información.....                             | 62 |
| Figura 5: D4 Implantación del Sistema de Gestion de Seguridad de la Información .... | 63 |
| Figura 6: Calidad del Servicio Informático .....                                     | 64 |
| Figura 7: D1 Fiabilidad .....  | 65 |
| Figura 8: D2 Capacidad de respuesta .....  | 66 |
| Figura 9: D3 Capacitacion del personal .....   | 67 |
| Figura 10: D4 Atención al Cliente.....   | 68 |

## RESUMEN

5 El objetivo fue la relación entre Sistema de Gestión de Seguridad de la Información con la Calidad del Servicio Informático de la Universidad Nacional de Moquegua, Año 2024

Se desarrollaron los contenidos de las variables Sistema de Gestión de la Seguridad de la Información y la calidad de los servicios informáticos con sus dimensiones principios de la seguridad de la información, la norma ISO/TEC27001, el Sistema de Gestión de Seguridad de la Información y la Implantación de SGSI para la primera variable y las dimensiones fiabilidad del servicio, capacidad de respuesta, capacitación del personal y la atención al cliente de la segunda variable.

El estudio fue de tipo básico, nivel descriptivo correlacional, no experimental y método hipotético deductivo. La población estuvo conformada por 92 docentes y una muestra censal. Se aplicó la técnica de la encuesta y dos cuestionarios con 22 ítems cada uno.

3 Mediante la correlación de Pearson y con una significancia bilateral de 0,000 menor a  $p = 0,05$  nos permite rechazar la  $H_0$  y aceptar que El Sistema de Gestión de Seguridad de la Información se relaciona significativamente con la Calidad del Servicio Informático en la Universidad Nacional de Moquegua, Año 2,024, con un coeficiente positivo de nivel moderado de 0,545.

**PALABRAS CLAVE:** Sistema de gestión de seguridad de la información, calidad del servicio informático.

## ABSTRACT

The objective was the relationship between the Information Security Management System and the Quality of the Computer Service of the National University of Moquegua, Year 2024.

The contents of the Information Security Management System variables and the quality of computer services with their dimensions, principles of information security, the ISO/TEC27001 standard, the Information Security Management System and the Implementation of ISMS for the first variable and the dimensions service reliability, responsiveness, staff training and customer service of the second variable.

The study was of a basic type, correlational descriptive level, non-experimental and hypothetical-deductive method. The population was made up of 92 teachers and a census sample. The survey technique and two questionnaires with 22 items each were applied.

3 Using the Pearson correlation and with a bilateral significance of 0.000 less than  $p = 0.05$  allows us to reject the  $H_0$  and accept that the Information Security Management System is significantly related to the Quality of the Computer Service at the National University of Moquegua, Year 2,024, with a positive coefficient of moderate level of 0.545.

**KEYWORDS:** Information security management system, quality of computer service.

## RIEPILOGO

L'obiettivo era il rapporto tra il Sistema di Gestione della Sicurezza delle Informazioni e la Qualità del Servizio Informatico dell'Università Nazionale di Moquegua, Anno 2024.

Il contenuto delle variabili del Sistema di Gestione della Sicurezza delle Informazioni e la qualità dei servizi informatici con le loro dimensioni, i principi della sicurezza delle informazioni, lo standard ISO/TEC27001, il Sistema di Gestione della Sicurezza delle Informazioni e l'implementazione dell'ISMS per la prima variabile e le dimensioni affidabilità del servizio, la reattività, la formazione del personale e il servizio al cliente sono la seconda variabile.

Lo studio è stato di tipo base, di livello descrittivo correlazionale, non sperimentale e con metodo ipotetico-deduttivo. La popolazione era composta da 92 insegnanti e da un campione censito. Sono state applicate la tecnica del sondaggio e due questionari da 22 item ciascuno.

Utilizzando la correlazione di Pearson e con un significato bilaterale di 0,000 inferiore a  $p = 0,05$  ci permette di rifiutare l' $H_0$  e accettare che il Sistema di Gestione della Sicurezza delle Informazioni sia significativamente correlato alla Qualità del Servizio Informatico presso l'Università Nazionale di Moquegua, Anno 2024, con un coefficiente positivo di livello moderato pari a 0,545.

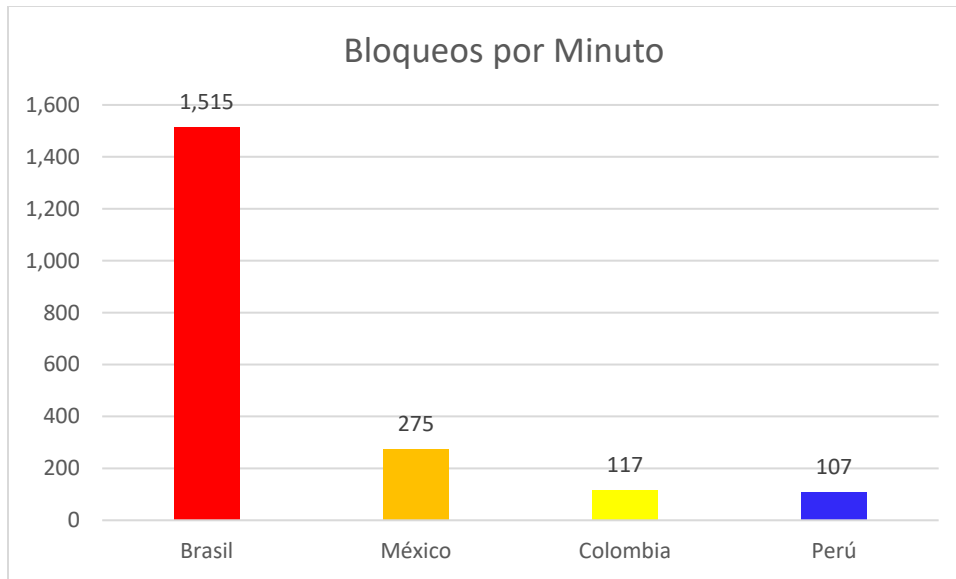
**PAROLE CHIAVE:** Sistema di gestione della sicurezza delle informazioni, qualità del servizio informatico.

## **1 CAPITULO I: PLANEAMIENTO DEL PROBLEMA**

### **1.1 Descripción de la Realidad Problemática**

El progreso continuo en tecnología permite a las empresas e instituciones superar las barreras previas en la protección de su activo más valioso, la información. Esto se logra a través de un enfoque de seguridad integral que fortalece la confianza de clientes internos y externos, proveedores y socios estratégicos, de manera eficiente y duradera.

Sudamérica enfrenta una de sus peores crisis de ciberseguridad, siendo los gobiernos, el sector financiero y los usuarios los más afectados por ataques de malware entre 2022 y mediados de 2023. Según Kaspersky, en este periodo se bloquearon 1,190 millones de ataques en esta zona del mundo, con un promedio de 37.9 intentos de ataque por segundo. Brasil lidera en ataques bloqueados, con 1,515 por minuto, seguido por México con 275 bloqueos por minuto, Colombia con 117 y Perú en el cuarto lugar con 107 bloqueos por minuto



*Figura 1. Ataques de malware bloqueados por minuto en países de sudamerica  
(2022-2023)*

Además de las amenazas tradicionales, las versiones avanzadas impulsadas por inteligencia artificial, como el phishing, están en aumento. Kaspersky predice que los atacantes podrán crear correos electrónicos más auténticos gracias a la GenIA, eliminando las barreras idiomáticas. Los objetos conectados también son vulnerables a ataques, como DDoS. Con el auge del trabajo híbrido, frente al aumento de ciberamenazas impulsadas por la inteligencia artificial, como el phishing avanzado y los ataques a dispositivos IoT, Fabio Assolini, Director del Equipo de Investigación y Análisis para América Latina en Kaspersky, enfatiza que las empresas deben adoptar sistemas de Inteligencia de Amenazas para anticipar riesgos. Además, recomienda mantener un inventario completo de los activos conectados y aplicar políticas de Confianza Cero, asignando privilegios de forma selectiva para reducir el riesgo. Esto es especialmente relevante en entornos de trabajo híbridos o remotos, donde la seguridad debe ser una prioridad constante.

En el Perú, se cuenta con la Norma Técnica Peruana NTP ISO/IEC 27001:2014, que se centra en las técnicas de seguridad de la información, la gestión de la seguridad de la información y el manejo de requisitos. Esta norma será de cumplimiento obligatorio para las entidades que forman parte del Sistema Nacional de Informática (SIN).

En Perú, las organizaciones, ya sean públicas o privadas, están enfrentando una creciente necesidad de implementar sistemas de gestión que aseguren la protección de la información que manejan, ya sea recibida, procesada o generada dentro de ellas. En este contexto, se ha emitido la Resolución Ministerial N.º 004-2016-PCM, que establece la obligatoriedad para las instituciones del Estado de adoptar un Sistema de Gestión de la Seguridad de la Información (SGSI).

Las universidades en Perú y alrededor del mundo enfrentan la misma necesidad de proteger sus recursos informáticos, dado que su administración se fundamenta en una variedad de sistemas de información y telecomunicaciones que contribuyen a la eficiencia de sus diversos procesos.

La UNAM dispone de departamentos especializados que facilitan la implementación, mejora y buen funcionamiento de soluciones tecnológicas para automatizar sus procesos. A pesar de esto, se han identificado tres problemas principales que podrían afectar a la institución, los cuales se explican a continuación:

En primer lugar, el área de sistemas se encuentra desarrollando varios proyectos, tanto con proveedores externos como con su equipo interno de desarrollo, lo que implica el uso compartido de información importante. Sin embargo, no se han implementado medidas como seudonimización, enmascaramiento de datos,

generación de datos ficticios o eliminación segura para proteger esta información. Como resultado, la información está expuesta en los entornos de prueba, muchos de los cuales son accesibles a través de enlaces públicos.

En segundo lugar, el proceso de implementación de proyectos sigue una serie de etapas que incluyen la identificación de requisitos, el diseño de procesos, el desarrollo de soluciones y la ejecución del proyecto. Sin embargo, debido a la falta de una fase específica o de un responsable que se encargue de evaluar la seguridad a lo largo del avance del proyecto, los desarrollos tecnológicos de la universidad carecen de controles rigurosos en materia de seguridad. Esto implica la ausencia de medidas como autenticación adecuada, protocolos seguros de transmisión como https, y encriptación de datos, lo que aumenta el riesgo de accesos no autorizados, transferencia insegura de información o exposición del código fuente.

En tercer lugar, los desarrolladores de sistemas no reciben formación adecuada sobre estándares y mejores prácticas de programación segura, lo que limita su capacidad para crear sistemas protegidos frente a amenazas. Ante esta problemática, la investigación que realizaremos sugiere el diseño de un Sistema de Gestión de Seguridad de la Información (SGSI), que podría ser implementado en la UNAM como un paso posterior.

En el caso de la Universidad Nacional de Moquegua (UNAM), es fundamental prestar atención especial a la protección de los activos de información mediante la implementación de Políticas y Planes que garanticen la seguridad, integridad, confiabilidad y disponibilidad de los datos. Esto se vuelve crucial dado que estudiantes, docentes, personal administrativo e incluso entidades gubernamentales dependen de la información generada por la UNAM.

Surge entonces la interrogante de si la UNAM evalúa la calidad de sus servicios informáticos a través de un Sistema de Gestión de Seguridad.

## **1.2 Delimitación de la Investigación**

### **1.2.1 Delimitación espacial**

La investigación se llevó a cabo en la filial de la UNAM en Ilo, localizada en la Región Moquegua, Provincia de Ilo, Distrito de Pacocha.

### **1.2.2 Delimitación social**

Los sujetos de análisis en esta investigación fueron los docentes de la filial de la UNAM en Ilo

### **1.2.3 Delimitación Temporal**

La investigación comenzó en mayo de 2024 y se extendió hasta diciembre 2024.

### **1.2.4 Delimitación Conceptual**

Esta investigación se basó en fundamentos bibliográficos y científicos, que se detallan en el marco teórico y la definición conceptual de las variables relacionadas con el Sistema de Gestión de Seguridad de la Información y la Calidad del Servicio Informático en la Universidad Nacional de Moquegua, año 2024, incluyendo sus dimensiones correspondientes.

## **1.3 Problemas de Investigación**

### **1.3.1 Problema General.**

¿Cuál es la relación entre el Sistema de Gestión de Seguridad de la Información con la Calidad del Servicio Informático en la Universidad Nacional de Moquegua, año 2024?

### 1.3.2 Problemas Específicos

- ¿Cuál es la relación entre el principio de seguridad de la información con la Calidad del Servicio Informático de la Universidad Nacional de Moquegua, Año 2024?
- ¿Cuál es la relación entre la Norma ISO/TEC con la calidad del servicio informático de la Universidad Nacional de Moquegua, Año 2024?
- ¿Cuál es la relación entre la gestión de seguridad de información con la calidad del servicio informático de la Universidad Nacional de Moquegua, Año 2024?
- ¿Cuál es la relación entre la implantación del sistema de gestión de seguridad informática con la calidad del servicio informático de la Universidad Nacional de Moquegua, Año 2024?

## 1.4 Objetivos de la Investigación

### 1.1.1. Objetivo General

Determinar la relación entre Sistema de Gestión de Seguridad de la Información con la Calidad del Servicio Informático de la Universidad Nacional de Moquegua, Año 2024

### 1.1.2. Objetivos Específicos

- a) Diagnosticar los principios de Seguridad de información en relación con la Calidad del Servicio Informático.
- b) Analizar la Norma ISO/IEC 27001 en relación con la Calidad del Servicio Informático.
- c) Evaluar la gestión de la seguridad de la información en relación con la Calidad del Servicio Informático
- d) Evaluar la implantación de la Norma ISO/IEC 27001 en relación con la Calidad del Servicio Informático.

## **1.5 Justificación e Importancia de la Investigación**

### **1.5.1 Justificación Teórica**

La tesis permite determinar el nivel de relación entre el Sistema de Gestión de Seguridad de la Información y la Calidad del Servicio Informático en la Universidad Nacional de Moquegua, año 2024. Para ello, se utilizaron fundamentos teóricos sólidos, como las normas ISOS de la serie 2700X, la Norma Técnica Peruana y el modelo de Calidad del Servicio Informático para realizar la evaluación. Además, se consideraron estudios previos tanto nacionales como internacionales que han investigado la seguridad de la información y su impacto en la calidad del servicio informático.

### **1.5.2 Justificación Practica**

La UNAM tiene la posibilidad de implementar mejoras en su Sistema de Gestión de Seguridad de la Información mediante la adopción de políticas, planes, procesos y procedimientos que garanticen la protección de sus activos de información.

### **1.5.3 Justificación Social**

Esta investigación es fundamental ya que permite avanzar en la mejora del Sistema de Gestión de Seguridad de la Información y su impacto en la Calidad del Servicio Informático en la Universidad Nacional de Moquegua. También proporciona una base sólida para que otros investigadores continúen explorando y contribuyendo con estudios relacionados con este tema.

### **1.5.4 Justificación Metodológica**

La tesis facilita la aplicación de la metodología de investigación y el método científico de manera detallada, con el objetivo de cuantificar los resultados

obtenidos a través del cuestionario. Además, se presentan los resultados en figuras, junto con sus interpretaciones, para ofrecer una comprensión más clara de los datos obtenidos.

### **1.5.5 Importancia**

Esta investigación es de gran relevancia ya que ayuda a mejorar el Sistema de Gestión de Seguridad de la Información y su impacto en la Calidad del Servicio Informático en la Universidad Nacional de Moquegua. La optimización de estos recursos requiere diseñar y ejecutar estrategias que aseguren la calidad de estos sistemas. Aprovechar al máximo el aumento de recursos disponibles, a pesar de la inversión continua en software, equipos tecnológicos y personal, solo será posible mediante este enfoque estratégico. Al adoptar esta estrategia para la calidad de la información, se asegurará un incremento en el nivel de calidad, exactitud y eficacia en su gestión. Los sistemas de información de alta calidad proporcionan un claro retorno de la inversión en diversos contextos, ya que unos datos bien gestionados y de alta calidad se convierten en uno de los activos más valiosos para la organización. En definitiva, estas capacidades se traducirán en numerosos beneficios que permitirán a la UNAM aprovechar las nuevas oportunidades del mercado. Entre las ventajas se incluyen mejoras en prestigio, marketing, difusión del conocimiento, eficiencia operativa, satisfacción del cliente, toma de decisiones, cumplimiento de normativas y un impacto positivo en los resultados financieros, entre otros aspectos favorables.

Para lograr una ventaja competitiva mediante la calidad, la implementación de este sistema de información necesitará un proceso continuo de mejora, que sea escalable y, en última instancia, que apoye el desarrollo de las diversas actividades de la UNAM en sus distintas áreas.

## 1.6 Factibilidad de la Investigación

La factibilidad de la investigación es un aspecto crucial en cualquier estudio, ya que garantiza su continuidad durante el período planificado. Por esta razón, se señala que la investigación se llevó a cabo en forma adecuada con fondos propios.

## 1.7 Limitaciones del estudio

La falta de disponibilidad de la Alta Gerencia, especialmente de la persona a cargo del área de TI en la UNAM. La cual fue superada mediante el recojo de datos vía virtual. La Ausencia de un especialista en seguridad de la información en la UNAM para apoyar y respaldar el diseño del proyecto. Aunque el área de TI se encarga de la seguridad de la información, este tema no es su principal prioridad en la actualidad. Por lo que el actual personal brindó la información respectiva.

Baja conciencia entre la alta dirección, funcionarios, docentes y estudiantes sobre la importancia de la seguridad de la información, lo que resulta en una falta significativa de apoyo organizacional, a pesar de ser un requerimiento legal. Se han propuesto soluciones para estas limitaciones, como asignar roles a funcionarios actuales y desarrollar programas de sensibilización y formación para la comunidad universitaria, dado que los usuarios son una fuente principal de amenazas. En el futuro, se enfrentan desafíos importantes para la implementación completa de la norma y la validación del modelo propuesto, siendo el principal reto cambiar la cultura de seguridad de la información, aumentar la conciencia y capacitación de los usuarios, y, como consecuencia, obtener el apoyo de la alta dirección y funcionarios, reconociendo adecuadamente la importancia de la seguridad de la información y la seguridad en general.

## 2 CAPITULO II: MARCO FILOSOFICO

### 2.1 Fundamentación Ontológica.

La calidad educativa es esencial para las instituciones de educación superior, abarcando tanto el proceso de aprendizaje como los aspectos de gestión. Para asegurar que el servicio educativo sea de alta calidad, es crucial que todos los procesos relacionados estén bien definidos, controlados y gestionados de manera eficiente. Esto se logra a través de la implementación de un Sistema de Gestión de la Calidad. En el contexto de esta investigación, centrada en el Sistema de Gestión de Seguridad de la Información y la Calidad del Servicio Informático en la Universidad Nacional de Moquegua, año 2024, se busca entender cómo un enfoque sistemático en la gestión de calidad y seguridad puede mejorar los servicios educativos y administrativos. La adecuada integración de estos sistemas permitirá optimizar la eficiencia operativa y garantizar la protección de la información, promoviendo así una educación de calidad y un entorno universitario más seguro y efectivo.

### 2.2 Fundamentación Epistemológica

Se pretende evaluar cómo el sistema de gestión de seguridad, basado en la Norma ISO 9001:2008, influye en la calidad del Servicio Informático. Para alcanzar este objetivo, se llevará a cabo un diagnóstico de la situación actual y se desarrollará

una propuesta que se ajuste a los estándares de la Norma ISO 9001:2008. Esto incluirá la identificación y el diseño de un proceso para investigar la calidad del Servicio Informático. El diseño del Sistema de Gestión de Seguridad se implementará inicialmente entre estudiantes, docentes y personal administrativo. Los resultados obtenidos servirán para validar las mejoras significativas en la participación de estos grupos en la investigación y en la calidad del servicio. Se espera que, al final del proceso, se pueda demostrar un alto nivel de satisfacción entre alumnos, docentes y personal administrativo con respecto al diseño del Sistema de Gestión de Calidad. Además, este enfoque permitirá identificar áreas de mejora y ajustar el sistema para maximizar su efectividad y beneficio para toda la comunidad universitaria.

En conclusión, será necesario validar la hipótesis de que la implementación de un sistema de gestión de calidad basado en la Norma ISO 9001:2008 tendrá un impacto positivo en la calidad del Servicio Informático de la UNAM. Para ello, se llevará a cabo una serie de pruebas y evaluaciones que medirán cómo la adopción de este sistema contribuye a la mejora en la eficiencia y efectividad del servicio. Se examinarán diversos indicadores de rendimiento y satisfacción para confirmar si la norma contribuye significativamente a la optimización de los procesos y la calidad general del servicio informático. Además, se analizará la respuesta de los usuarios y la adecuación del sistema en diferentes contextos dentro de la universidad. Este enfoque permitirá ajustar y perfeccionar el sistema de gestión, garantizando que cumpla con las expectativas y necesidades de la comunidad universitaria.

Fundamentando la Epistemología, el siglo XXI enfrenta un desafío significativo con el avance de los Sistemas de Información enfocados en la seguridad informática. Esta evolución exige una revisión profunda de los enfoques

epistemológicos tradicionales, cuestionando su capacidad para abordar y clasificar las nuevas problemáticas emergentes. La introducción de la seguridad informática plantea nuevamente el debate sobre la relación entre sentido e inteligencia, aunque en este caso no se trata de seres humanos, sino de máquinas que imitan procesos de pensamiento. Este fenómeno da lugar a un nuevo ámbito, que se podría denominar Epistemología de la Seguridad Informática. Esta perspectiva no debe considerarse descabellada, sino como una extensión lógica de la Inteligencia Artificial aplicada a la seguridad. Aunque la aplicación de estos conceptos puede ser adecuada o inadecuada en diferentes contextos, ofrece una visión renovada y crítica sobre los desafíos actuales en la protección de la información.

### 3 CAPITULO III: MARCO TEORICO CONCEPTUAL

#### 3.1 Antecedentes de la investigación

##### 3.1.1 Antecedentes a nivel internacional

Lanche (2015), en su tesis: “Diseño de sistemas de seguridad de la información de la empresa Acotecnic, con normas NTEINEN ISO/IEC 27002.”

Menciona que la información es un activo muy valioso, para todas las empresas y se debe proteger adecuadamente mediante procedimientos de seguridad para la información que nos faciliten una apropiada gestión sobre la seguridad de nuestros activos de información, empleando las TIC's, enfocados en una cultura de ética del manejo en la información, mediante el modelo administrativo de eficiencia, con objetivos claros dentro del marco legal vigente, asegurando también la continuidad del negocio. La finalidad del estudio fue identificar la factibilidad para implementar un SGI, en las pequeñas empresas, por tal motivo se estableció un esquema que apoye a la implementación, mejora y mantenimiento de un SGI, basados en las normas NTE INEN ISO/IEC 27002.

1 Rebolledo (2016), en su tesis: “Esquema de tareas para gobiernos de seguridad en la información para servicios aplicando computación en la nube”. Su problema de investigación está basado en la seguridad de la información y como esta interviene en la aceptación de las tecnologías informáticas, para poder frenar el descontrol de la organización sobre los activos de información, desarrollando una estrategia de gobernabilidad sobre la seguridad informática y su debido desarrollo. Además, se plantea un marco de trabajo alineado con los actuales estándares de seguridad, referente a las buenas prácticas aplicando una propuesta orientada a los procesos de la empresa mediante el programa SPEM 2.0, el cual ayudará a la implementación de los estándares mencionados. Finalmente, la tesis presenta un grupo de herramientas de apoyo, para facilitar los procesos y procedimientos de gobernabilidad respecto a la seguridad de la información.

Lascurain (2017), en su tesis: “Valoración y Ofrecimiento para el perfeccionamiento de calidad en el servicio de una empresa de energía eléctrica ininterrumpida”. El estudio de investigación se centró en la fidelización de los clientes, con el propósito de determinar las causas que contribuyen a la calidad de los servicios prestados.

7 Puentes (2021) Diseño de una guía de mejoramiento en los procesos del SGSI bajo la norma ISO 27002:2015, ítems, 6.1 en el área de infraestructura de la empresa corbeta S.A. Bogotá sede calle 31. Universidad Cooperativa de Colombia, Bogotá. <https://hdl.handle.net/20.500.12494/33981>

Señaló que, al proporcionar una guía de mejoramiento completa de implementación, esta normativa describirá cómo establecer los controles los mismos que serán elegidos basándose en una evaluación de riesgo de

1 aquellos activos mas significativos de la organización. Contrariamente a la creencia popular, la ISO 27002 alcanza a respaldar la implementación del SGSI en cualquier tipo de organización, pública o privada, pequeña o grande, con fines de lucro o no. Y no solo empresas de tecnología. La normativa ISO / IEC 27002: 2015 ITEM 6.1 es una guía que contiene la estructura de gestión necesaria para diseñar e implementar un sistema de gestión de seguridad de la información de acuerdo con los requisitos especificados en la ISO / IEC 27000, que gestiona la seguridad de la información de una organización. (pág.13)

Marín et al. (2021). La seguridad Informacional en el ministerio de transporte y obras públicas en Portoviejo. Revista Dominio de las Ciencias, 7(2), 835-857.

Define a la información como uno de los activos mas importantes en toda organización, por lo que se requiere que esta esté adecuadamente protegida y garantizada, incluso respaldada por los documentos legales e instruccionales, tanto a nivel nacional, empresarial y hasta personal.

Primero, es necesario enfatizar que a nivel internacional, la Organización Internacional de normas técnicas (ISO, International Organization for Standarization) en el año 2000, la norma ISO 17799 surge como una normativa técnica de seguridad en información, conocida a nivel mundial. Esto respalda las prácticas exitosas de seguridad de la información. En beneficio de esta ley, se pueden citar: protegiendo los activos de la compañía (información y operaciones), protegiendo la información de comunicación y software, protegiendo contra el acceso malicioso, prevención de cambios de comunicación entre las organizaciones, el procedimiento de la información de seguridad, mayor

1 seguridad en la sociedad, Planificación y gestión de seguridad, mayor creencia en las auditorías de seguridad del cliente, precisa y más confiable, menos responsabilidad civil, entre otros. En este contexto, apareció la norma internacional ISO/IEC 27002, centrándose en la información de la Gestión de la Gestión de la Buena Información. Hoy en día, es necesario fortalecer el Sistema de Gestión de Seguridad de la Información (SGSI), garantizar la continuidad y el mantenimiento de los procesos de seguridad, de acuerdo con los objetivos de la Organización. (P.846)

### 3.1.2 Antecedentes a nivel Nacional

1 Alfonso (2016), en su tesis: “Factores para la implementación del sistema de administración de seguridad de la información en las empresas públicas peruanas de acuerdo con la NTP-ISO/IEC 27001”. Se identifican las posibles causas para la ejecución del SGSI, en la gestión pública. Además, buscamos identificar las posibles restricciones que impiden implementar un adecuado SGSI en el estado, Mediante las entrevistas y análisis documental se obtuvo la información requerida para desarrollar el estudio de acuerdo con la NTP-ISO/IEC27001. Finalmente determinamos los factores relevantes que permiten evaluar el nivel de complejidad y la implementación de la NTP-ISO/IEC 27001.

1 Arrué (2017), tesis: “Análisis de calidad del servicio de atención en la Oficina de OSIPTEL Loreto desde la percepción del usuario periodo junio a setiembre de 2014”. Se desarrolló un estudio sobre la visión de la calidad para los servicios brindados por OSIPTEL Loreto, donde se realizó una investigación transversal descriptivo no experimental. Se midió la calidad y como recae en la calidad del servicio prestado. Las conclusiones obtenidas de la tesis determinan

que lo observado por el cliente respecto a la calidad del servicio es de 62%, que según la escala de calificación el resultado sería el adecuado, pero no suficiente.

Carranza et al. (2018). En su tesis: “Plan para perfeccionar el grado de estabilidad de reportes y seguida del centro de datos en la gerencia regional de Educación de la Libertad aplicando cada uno de los pasos ISO 27001 y buenas prácticas COBIT” Se planteo un objetivo principal que es la presentación del plan de mejora para seguridad informática en el centro de datos, mostrando los datos de la auditoría de sistemas empleando la metodología MAIGTI, con directrices en auditoría de lineamientos ISO 27001 y COBIT 4.0, Finalmente se determinan los procesos más adecuados para el control según los estándares con una evaluación y recomendaciones.

1 Polar (2021). Modelo para la valoración de activos de información basados en la norma ISO 27000 universidad Nacional Jorge Basadre Grohmann, Tacna, Perú.

Señaló que en la etapa de investigación y prueba de estándares, procedimientos, software y tesis, entre otros, se observó que no existe una metodología que permita la identificación precisa de los activos de información; La información existente se reduce a encuestas, inspecciones, observaciones, listas de verificación, técnicas de evaluación abierta e incluso el uso de una matriz DAFO; no se encontró nada que incluyera los requisitos, basados en los estándares de la Organización Internacional de Normalización (ISO) para la seguridad de la información. Este trabajo presenta un modelo que facilita la evaluación de los activos de información, basándose en los estándares de la familia ISO 27000; que combina nuestra experiencia laboral, investigación utilizada, herramientas creadas e investigación adicional, para proporcionar un prototipo útil, escalable y fácil de usar para los participantes en esta ruta de seguridad de la información aplicable a

**todo** tipo de organizaciones, independientemente de su tipo, tamaño o naturaleza.  
(pág. 4).

Choquehuayta (2021) “Modelo servqual para la evaluación del servicio de defensoría municipal del niño y el adolescente en la municipalidad distrital de Lluta, Caylloma 2019” Universidad Nacional de Arequipa, Perú.

Afirmó que a partir de este modelo desarrollaron una herramienta, de evaluación de la calidad del servicio, denominada SERVQUAL, por su abreviatura en inglés " service quality ", esta investigación es una de las primeras en cuestionarse sobre la satisfacción de los usuarios de los servicios municipales concluyendo que el índice de la calidad de servicio percibido esta muy por debajo de lo esperado por los usuarios.

Cáceres et al. (2021). calidad de servicio de la línea aérea Latam en Perú. Pontificia Universidad Católica del Perú. Surco -lima, Perú.

Hace referencia al campo de la aviación comercial afectada por la conciencia de la calidad de los servicios que los usuarios pueden tener y ser importantes hoy en día representa el 2,6% del PIB con un total de once millones de clientes que utilizan los servicios (MTC, 2019). Sin embargo, hasta ahora, ningún modelo se autentica en Perú para este campo de acuerdo con la calidad cognitiva. El objetivo principal es validar el modelo servqual en el campo de la aviación comercial y, con este propósito se evaluaron 5 dimensiones: (a) tangibilidad, (b) confiabilidad, (c) capacidad de respuesta, (d) seguridad; y (e) empatía. Estas dimensiones hacen posible determinar la calidad de acuerdo con la espera en comparación con la conciencia que los usuarios tienen. Latam Airlines en sus vuelos nacionales se consideró como objeto de investigación por ser la más representativa en el Perú con

1 una participación de mercado del 62% en 2019 (MTC, 2019) y se tomaron encuestas en el Aeropuerto Internacional Jorge Chávez de Lima se le ha otorgado a Metropolitana para patrocinar a los pasajeros que han usado aerolíneas al menos dos veces en el último año. (p.9).

## 3.2 Bases teóricas

### 3.2.1 La Norma ISO 17799

ISO 17799 (Myler & Broadbent, 2006) es una norma internacional que ofrece diversas directrices para la gestión de la seguridad de la información. Está destinada a los responsables de iniciar, implementar y mantener las medidas de seguridad de la información en una organización.

La información puede conceptualizarse como un conjunto estructurado de datos procesados y organizados que, al ser interpretados, generan conocimiento útil para la toma de decisiones. Dentro de una empresa, la información adquiere valor como un activo estratégico, ya que proporciona una base para acciones eficaces, fomenta la innovación y puede ser utilizada para obtener ventajas competitivas. Al ser intangible, su relevancia radica no solo en su contenido, sino también en su precisión, accesibilidad y seguridad, convirtiéndose en un recurso esencial para el funcionamiento eficiente y el éxito a largo plazo de la organización.

La seguridad de la información tiene como fin preservar este recurso, asegurar la continuidad operativa de la empresa, reducir posibles daños y maximizar el retorno de las inversiones realizadas.

Además, su protección se convierte en un elemento clave para garantizar la competitividad, la integridad operativa y la confianza tanto de los clientes como

de los socios comerciales. La correcta administración de la información impulsa el desarrollo estratégico y fortalece las bases de crecimiento de la empresa.

La seguridad de la información se basa en los siguientes principios fundamentales:

- **Confidencialidad:** Garantiza que solo las personas autorizadas puedan acceder a la información.
- **Integridad:** Asegura que la información se mantenga precisa, completa y que los procesos para su gestión sean adecuados.
- **Disponibilidad:** Asegura que los usuarios con los permisos correspondientes puedan acceder a la información y los recursos asociados cuando sea necesario.

La norma ISO 17799x ((ISO/IEC), 2000) establece un marco sólido para la creación de diversas normas de seguridad de la información en las organizaciones, promoviendo prácticas eficientes en la gestión de la seguridad.

La norma adaptada en Perú recibe el nombre de NTP-ISO/IEC 17799, a través de la cual se definen diez (10) dominios o áreas de control que abarcan por completo la gestión de la seguridad de la información.



Figura 2. NTP ISO 27799 – Áreas de Control

Se destaca que la norma ISO 17799x proporciona beneficios a las organizaciones, tales como:

- Mayor seguridad en los sistemas de información.
- Planificación eficiente en la gestión de la seguridad.
- Aseguramiento de la continuidad operativa del negocio.
- Mejora constante a través de auditorías internas.
- Incremento en la confianza de clientes y colaboradores.
- Mejora del valor empresarial y la reputación corporativa.

### 3.2.2 Norma ISO/IEC 27001

(Disterer, 2013), señala que el modelo SGSI se fundamenta en la gestión de riesgos, empleando controles apropiados para asegurar que el riesgo operativo se mantenga dentro de un rango aceptable.



Figura 3. Esquema del Sistema de Gestión de la Seguridad de la Información

En la imagen a continuación se ilustran los ámbitos de control y las medidas que cubren de manera integral los diversos aspectos relacionados con la empresa.

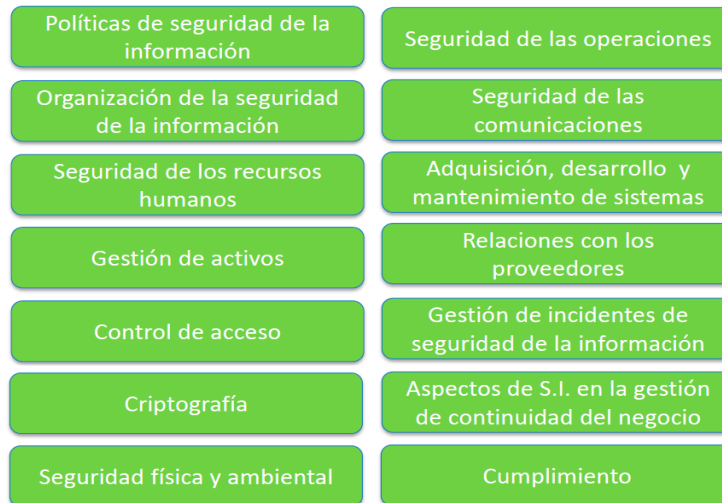


Figura 4. Áreas de control y medidas del Sistema de Gestión de la Seguridad de la Información (SGSI)

### Ventajas del SGSI

Ofrece un lenguaje común con conceptos universales para la seguridad de la información, fomentando la confianza entre los participantes del negocio que implementan un SGSI conforme a la norma. Esto es particularmente relevante para quienes buscan la certificación ISO/IEC 27001, ya que integra prácticas reconocidas globalmente y ajusta los controles a las necesidades específicas de cada empresa. Además, contribuye a cumplir con las demandas empresariales y los requisitos legales, contractuales y regulatorios.

### 3.2.3 El modelo SERVQUAL

(Scardina, 1994), Zeithaml, Parasuraman y Berry desarrollaron el concepto de calidad del servicio con el objetivo de gestionar y mejorar la calidad del servicio ofrecido por la empresa. Para evaluar esta calidad, se utiliza un cuestionario que mide y analiza el servicio en base a cinco dimensiones propuestas:

- **Fiabilidad:** La capacidad de la empresa para proporcionar un servicio consistente y exacto de acuerdo con las promesas hechas.
- **Capacidad de Respuesta:** La disposición y habilidad del personal para asistir a los clientes y resolver problemas de manera eficiente y oportuna.

- **Seguridad:** La confianza que los clientes tienen en que el servicio es seguro y que sus datos e información están protegidos de riesgos o vulnerabilidades.
- **Empatía:** La capacidad del personal para comprender y atender las necesidades y preocupaciones individuales de los clientes, mostrando atención y cuidado personalizado.
- **Elementos Tangibles:** Los aspectos físicos del servicio, como el entorno, el equipo y el personal, que afectan la percepción de la calidad del servicio ofrecido

El modelo SERVQUAL, que utiliza una escala de respuestas múltiples, fue diseñado para captar una variedad de perspectivas de los clientes sobre el servicio. Este enfoque permite a las empresas medir las expectativas y percepciones del cliente en relación con cada una de las dimensiones mencionadas. A continuación, se ilustra el flujo de estas dimensiones, proporcionando una visión clara de cómo se integran para evaluar la calidad del servicio.

Este modelo facilita una comprensión más profunda de las áreas de mejora necesarias para satisfacer mejor a los clientes.

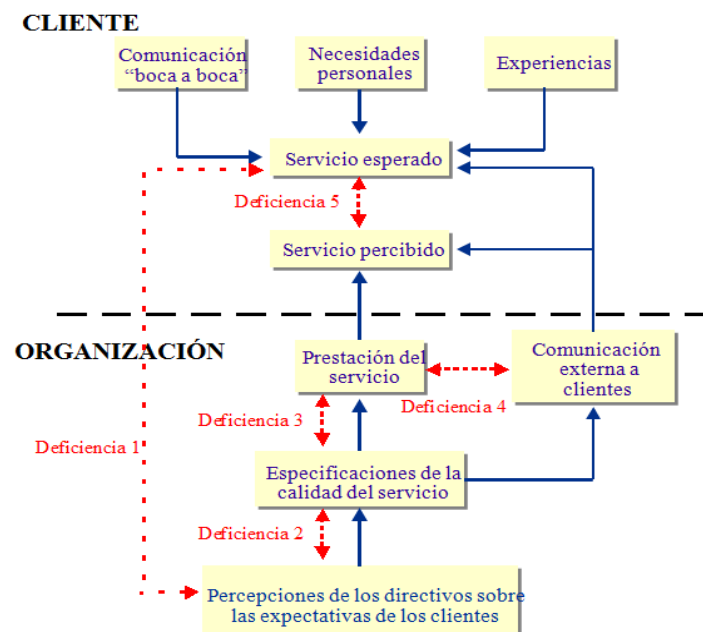


Figura 5. Diagrama del Modelo SERVQUAL para la Evaluación de la Calidad del Servicio

### 3.2.4 ISO 9001 aplicado a los servicios

Se refiere a un conjunto de características inherentes de un bien o servicio que buscan cumplir con las expectativas y necesidades de los clientes. La calidad es definida desde diversas perspectivas por diferentes autores. (Juran, 1989) describe la calidad como “la adecuación al uso” y también la considera como “las propiedades de un producto o servicio que le otorgan la capacidad de satisfacer las diversas necesidades de los clientes”. Por su parte, (Deming, 1986) señala que la calidad debe garantizarse en términos de capacidad para asegurar la satisfacción adecuada del cliente.

Al examinar las tecnologías aplicadas a los servicios, se observan ciertas características distintivas que pueden destacarse:

- 1 • Los servicios o productos ofrecidos por la empresa son intangibles, se proporcionan solo una vez y se consumen de manera simultánea.
- El proceso de apoyo del servicio juega un papel crucial para el cliente.
- Una vez que el servicio ha sido entregado, no es posible corregirlo.
- Es fundamental definir claramente las responsabilidades para cumplir con las características que satisfagan las expectativas del cliente.
- La personalización del servicio influye directamente en el nivel de satisfacción del cliente.
- Estandarizar el servicio resulta complejo debido a la variabilidad de las necesidades del cliente.
- El servicio se distingue por la interacción directa con el cliente durante las transacciones.

A continuación, presentamos el flujo del servicio en la imagen.

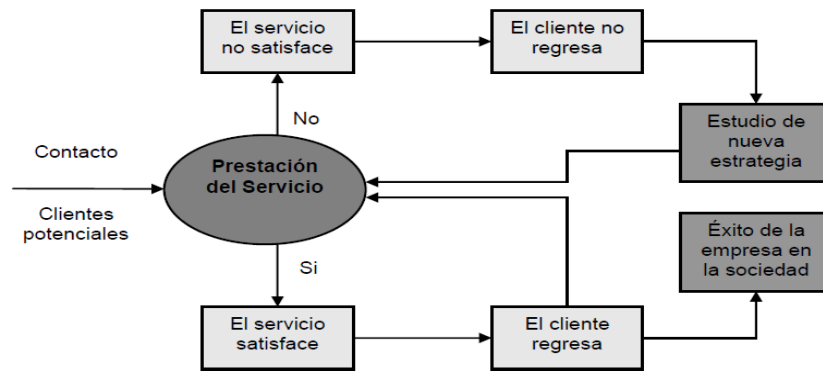


Figura 6. Factores que influyen en la entrega del servicio.

### 3.3 Definición de Términos Básico

**Sistema de Gestión de Seguridad de Información:** Es un sistema compuesto por capacidades, procesos, procedimientos, directrices, recursos y actividades que la empresa implementa de manera conjunta para salvaguardar los activos representados por la información ISO/IEC 27000:2016. (2016).

**Información:** La norma ISO 17799 considera la información como un recurso valioso para la organización, lo que hace necesario garantizar su protección. El propósito de la seguridad de la información es salvaguardar este recurso para asegurar la continuidad de las operaciones, reducir posibles daños a la empresa y optimizar tanto el retorno de las inversiones como las oportunidades de negocio.

UNE-ISO/IEC 17799

**Seguridad de información.** Entre sus partes principales: la confidencialidad, la disponibilidad y la integridad son relevantes para implementar un nivel de seguridad apropiado para garantizar el éxito y continuidad del negocio. UNE-ISO/IEC 17799

**Clasificación de las medidas de Seguridad.** La seguridad informática puede categorizarse de acuerdo con al menos tres criterios distintos. No obstante, cuando se trata de los elementos sobre los que se implementan estas medidas, se identifican tres tipos principales: seguridad del hardware, seguridad del software y seguridad de la red. <https://www.ceac.es/blog/tipos-de-seguridad-informatica>

**Características de Seguridad de la Información.** La seguridad informática sirve para garantizar la privacidad de la información y la continuidad del servicio, tratando de minimizar la vulnerabilidad de los sistemas y de la información contenida en ellos, así como de las redes privadas y sus recursos.

[https://www.ecured.cu/Seguridad\\_Inform%C3%A1tica](https://www.ecured.cu/Seguridad_Inform%C3%A1tica)

**Confidencialidad.** La información no es accesible ni se divulga a personas, organizaciones o procedimientos que no tienen autorización.  
<https://www.pais.gob.pe/sgsi/sgsi.html>

**Integridad.** Garantizar la precisión y la integridad de la información, así como los métodos empleados para su manejo. <https://www.pais.gob.pe/sgsi/sgsi.html>

**Disponibilidad.** Permitir que personas, organizaciones o procesos autorizados accedan y utilicen la información y los sistemas de tratamiento según sea necesario.  
<https://www.pais.gob.pe/sgsi/sgsi.html>

**Concepto de Calidad de Servicio.** El servicio es un término capaz de acoger significados muy diversos. En el caso que nos ocupa hay que entender el servicio como el conjunto de prestaciones accesorias de naturaleza cuantitativa o cualitativa que acompaña a la prestación principal, ya consista ésta en un producto o en un servicio.

Treviño (2021), la calidad del servicio es un elemento para ganar y mejorar la satisfacción del cliente; es decir, al renovar el servicio de acuerdo con las necesidades del cliente, se eleva su percepción positiva, lo que genera la retención de clientes y la obtención de mejores márgenes de ganancia. *Revista Científica de la UCSA. (2022).*

**Clasificación de los indicadores de calidad** A medida que las organizaciones enfrentan mayores retos para descubrir ventajas competitivas, será cada vez más necesario que centren sus esfuerzos en el servicio como un factor clave para lograr una diferenciación sostenible a largo plazo.

|                              | INTERNOS   | EXTERNOS  |
|------------------------------|--|---|
| CALIDAD DENTRO DE LA EMPRESA | <b>FINANCIEROS</b><br>- C. de Prevención<br>- C. de Evaluación<br>- C. de Fallos en la empresa<br><br><b>NO FINANCIEROS</b><br>- nº unidades defectuosas<br>- nº unidades reprocesadas<br>- Tiempos perdidos ... |   |
| SATISFACCIÓN DEL CLIENTE     | <b>FINANCIEROS</b><br>- C. de Fallos con clientes<br><br><b>NO FINANCIEROS</b><br>- nº de quejas<br>- nº facturas mal confeccionadas<br>- nº de clientes repiten compras   | <b>NO FINANCIEROS</b><br>- SEERVQUAL<br>- SERVPERF<br>- Desempeño Evaluado<br>- Calidad Normalizada |

Figura 7. Clasificación de indicadores de calidad.

**Clasificación** La administración y el perfeccionamiento de la calidad exigen seleccionar y aplicar un conjunto de indicadores que sea eficiente y relevante, por lo tanto, sugerimos la siguiente categorización:

**Indicadores internos:** Estos indicadores utilizan datos que ya están disponibles dentro de la empresa. La tarea consiste en organizar y analizar esta información para obtener las métricas requeridas.

**Indicadores externos:** Se enfocan en captar las percepciones directas de los clientes respecto al servicio recibido, reflejando su nivel de satisfacción o descontento. Generalmente, la empresa no cuenta con esta información de manera directa, por lo que es necesario emplear métodos como encuestas para obtenerla.

**Gestión de calidad del servicio:** La administración de la calidad del servicio requiere que la Contabilidad de Gestión, como componente esencial del sistema informativo de la empresa, se ajuste y responda a las nuevas demandas de información planteadas por los directivos debido a los continuos cambios tanto internos como externos. Esto permitirá apoyar de manera efectiva el proceso de toma de decisiones. Ruiz Olalla, C. (2001). "Gestión de la calidad del servicio "

**Características de los servicios de calidad** Los aspectos esenciales de los servicios se basan en su intangibilidad, la falta de separación entre producción y entrega, y la simultaneidad de producción y consumo (Parasuraman, Zeithaml y Berry, 1985).

Las distinciones clave entre productos tangibles y servicios influyen en cómo se evalúa la calidad del servicio. Por tanto, los servicios y los productos tangibles no se pueden evaluar con los mismos criterios. A continuación, se explican estas características con mayor profundidad:

**La intangibilidad** La mayoría de los servicios son intangibles (Lovelock, 1983). En lugar de ser objetos físicos, son el resultado de una acción o proceso. Esto implica que los consumidores no pueden verificar la calidad del servicio antes de adquirirlo, ni establecer especificaciones uniformes como ocurre con los productos tangibles. Debido a esta naturaleza intangible, las empresas de servicios a menudo enfrentan desafíos para entender cómo los clientes perciben la calidad de lo que ofrecen (Zeithaml, 1981)

**La heterogeneidad** Los servicios, en particular aquellos que requieren un alto grado de trabajo, muestran variabilidad significativa en sus resultados, que pueden fluctuar entre diferentes proveedores, clientes y días. Por lo tanto, mantener una calidad constante es complicado, ya que la percepción del cliente sobre lo que recibe puede diferir considerablemente de lo que la empresa cree ofrecer.

**La inseparabilidad** En numerosos servicios, la producción y el consumo ocurren de manera simultánea e indivisible (Grönroos, 1978). En servicios que dependen en gran medida de la intervención humana, suele haber una interacción directa entre el cliente y el representante de la empresa. Esta interacción tiene un impacto significativo en la calidad del servicio y en su evaluación. Según Parasuraman, Zeithaml y Berry (1985), estas características de los servicios conllevan cuatro implicaciones clave para el análisis de la calidad del servicio:

- La evaluación de la calidad de los servicios suele ser más compleja que la de los productos.
- La inherentemente variable naturaleza de los servicios provoca una mayor fluctuación en su calidad, resultando en un riesgo percibido por el cliente que generalmente es superior al asociado con la mayoría de los productos.
- La percepción del cliente sobre la calidad del servicio se basa en la comparación entre sus expectativas y los resultados obtenidos.
- Las valoraciones de la calidad consideran tanto los resultados finales como los procesos involucrados en la prestación del servicio.

## 4 CAPITULO IV: HIPOTESIS Y VARIABLES

### 4.1 Hipótesis General

El Sistema de Gestión de Seguridad de la Información y la Calidad del Servicio Informático se relacionan significativamente en la Universidad Nacional de Moquegua, Año 2,024

### 4.2 Hipótesis Específicas

- Los principios básicos del sistema de gestión de seguridad de la información ISO 27001 se relacionan significativamente con la Calidad del Servicio informático en la Universidad Nacional de Moquegua, Año 2,024.
- La Norma ISO/IEC 27001 se relaciona significativamente con la Calidad del Servicio. en la Universidad Nacional de Moquegua, Año 2,024.
- La Gestión de seguridad de la información se relaciona significativamente con la Calidad del Servicio. en la Universidad Nacional de Moquegua, Año 2,024.
- La implantación de la Norma ISO/IEC 27001 de la Gestión de seguridad de la información se relaciona significativamente con la Calidad del Servicio informático en la Universidad Nacional de Moquegua, Año 2,024

### 4.3 Definición conceptual y operacional de las variables

#### 4.3.1 VARIABLE 1

##### **Sistema de Gestión de Seguridad de la Información**

Con el creciente papel de la tecnología de la información, surge una necesidad urgente de implementar medidas adecuadas para proteger la información. La

gestión organizada de la seguridad de la información se ha convertido en una de las prioridades clave en la administración de TI. Desde que comenzaron a surgir informes sobre violaciones de la privacidad, prácticas contables fraudulentas y ataques a sistemas informáticos, las organizaciones han comenzado a reconocer la importancia de proteger tanto los activos físicos como la información. Los estándares de seguridad proporcionan directrices para desarrollar y mantener un sistema efectivo de gestión de seguridad de la información (SGSI). Normas como ISO/IEC 27000, 27001 y 27002 están ganando aceptación y reconocimiento internacional, siendo consideradas como un "lenguaje común" para la seguridad de la información a nivel global. Con la certificación ISO/IEC 27001, las empresas pueden demostrar a sus clientes que su SGSI cumple con estándares rigurosos a través de una validación externa.

Sistema de Gestión de Seguridad de la Información. Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for Information Security Management. *Journal of InformationSecurity*.

<https://www.scirp.org/journal/paperinformation.aspx?paperid=30059>

#### 4.3.2 VARIABLE 2

##### **Calidad del servicio informático**

Actualmente, las Instituciones de Educación Superior (IES) en Ecuador y otras naciones latinoamericanas a menudo carecen de una metodología administrativa básica para la formulación, evaluación, control y seguimiento sistemático de los Planes Institucionales a corto, mediano y largo plazo. Esto subraya la necesidad de desarrollar e implementar un Modelo de Gestión Estratégica y Operativa para la Universidad Estatal de Milagro (UNEMI) como parte de su Sistema Integral de

Planificación. Una evaluación estandarizada y continua es crucial para asegurar que los resultados sean de alta calidad, basados en metas y acciones cuantificables, y obtenidos a través de técnicas de medición efectivas. Además, se revela una carencia en la definición de procesos apoyados por Tecnologías de la Información y Comunicaciones (TIC) y sistemas de información que optimicen el monitoreo y control de programas y proyectos. La evaluación y el seguimiento del direccionamiento estratégico son esenciales para medir los resultados; sin herramientas de planificación como el POA (Plan Operativo Anual), PAT (Plan Anual de Tecnología), PAC (Plan Anual de Contrataciones) y PAI (Plan Anual de Inversión), sería difícil cuantificar con precisión el desempeño de la institución.

Calidad del servicio Informático. Vinueza et al. (2015). La Calidad en los Procesos Informáticos de las Universidades Ecuatorianas. *CIENCIA UNEMI*, 7(12), 58-68

#### 4.4 Cuadro de Operacionalización de Variables

| <b>VARIABLES</b>                                     | <b>DIMENSIONES</b>                            | <b>INDICADORES</b>   | <b>ITEMS</b>         | <b>ESCALA DE MEDICIÓN</b>                          |
|--|---|--|----------------------|--|
| X: Sistema de gestión de seguridad de la información | X1: Principios de seguridad de la información | -Principio de confidencialidad<br>-Principio de integridad<br>-Principio de disponibilidad | 1,2,3,4,5,6<br>7,8,9 | Ordinal<br>5=TA<br>4=A<br>3=NANDA<br>2=DA<br>1=TDA |

|  |   |   |                                 |  |
|--|---|---|---------------------------------|--|
|  | <p>X2: ISO/IEC 27001</p>  | <p>-Nivel de conocimiento de la Norma ISO</p> <p>- Nivel de capacitación de la Norma ISO</p>  | <p>10,11</p>                    |  |
|  | <p>X3: Sistema de Gestión de Seguridad de la información(GSI)</p> | <p>-Sistemas de gestión de seguridad de la información</p> <p>-Modelo PDCA</p> <p>-Evaluación y medición de la seguridad de la información.</p> | <p>12,13,14,15,16<br/>17,18</p> |  |
|  | <p>X3: Implantación de SGSI</p>                                   | <p>-Planificación del proyecto</p> <p>-Análisis de situación respecto a la norma</p> <p>-Política de seguridad</p>                              | <p>19,20,21,22</p>              |  |

|  |  |   |  |  |
|--|--|---|--|--|
|  |  | <p>-Enfoque para la evaluación de riesgos</p> <p>-Análisis de riesgos</p> <p>-Gestión de riesgos</p> <p>-Plan de tratamiento de riesgos</p> <p>-Sistema de métricas.</p> <p>-Elaboración de cuerpo documental</p> <p>-Formación y concienciación</p> <p>-Responsabilidad de la gerencia.</p> <p>-Auditorías internas del SGSI</p> <p>-Mantenimiento y mejora.</p> |  |  |
|--|--|---|--|--|

|                                     |                               |   |                   |
|-------------------------------------|-------------------------------|---|-------------------|
| Y: Calidad del servicio informático | Y1: Fiabilidad del servicio   | -Número de requerimientos atendidos<br>-Nivel de satisfacción del usuario por el servicio prestado. | 1,2,3,4,5,6       |
|                                     | Y2: Capacidad de respuesta    | -Tiempos de respuesta al usuario.   | 7,8,9,10,11       |
|                                     | Y3: Capacitación del personal | -Nivel de conocimiento para atender al usuario.   | 12,13,14,15,16    |
|                                     | Y4: Atención al cliente       | -Nivel de atención al usuario.  | 17,18,19,20,21,22 |

## **5 CAPITULO V: METODOLOGIA DE LA INVESTIGACION**

### **5.1 5.1 ENFOQUE, TIPO Y NIVEL DE INVESTIGACION**

#### **5.1.1 5.1.1. ENFOQUE DE INVESTIGACION: CUANTITATIVO**

Para este trabajo de investigación, adoptamos un enfoque cuantitativo. Según Roberto Hernández Sampieri, este enfoque se basa en la recolección y análisis de datos numéricos para evaluar hipótesis, establecer patrones de comportamiento y validar teorías mediante el uso de métodos estadísticos.

El enfoque cuantitativo sigue un proceso secuencial y riguroso. Cada fase debe completarse antes de pasar a la siguiente, sin omitir pasos, aunque es posible ajustar alguna etapa. Se inicia con una idea general que se va especificando. Una vez delimitada, se definen objetivos y preguntas de investigación, se revisa la literatura existente y se construye un marco teórico. A partir de las preguntas, se formulan hipótesis y se identifican variables; se elabora un plan para probarlas (diseño); se miden las variables en un contexto determinado; se utilizan métodos estadísticos para analizar los datos obtenidos, y se sacan conclusiones sobre las hipótesis. Este proceso está ilustrado en la figura 8.

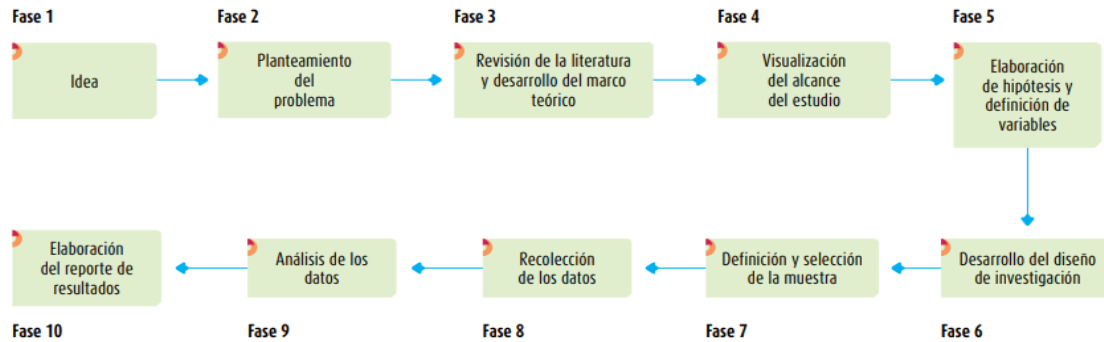


Figura 8. proceso cuantitativo

Sampieri, R. H. (2010). *Metodología de la investigación* (6.ª ed.). McGraw-Hill.

### 5.1.2 TIPO DE INVESTIGACIÓN: BÁSICA

El enfoque de investigación que utilizamos en este trabajo fue de tipo básica. La investigación básica o fundamental tiene como objetivo comprender la realidad o los fenómenos naturales para avanzar en el conocimiento y enfrentar mejor los desafíos que presenta la humanidad. Este tipo de investigación no está orientado a la aplicación inmediata de sus hallazgos, sino que se centra en expandir el conocimiento general, el cual puede servir como base para futuras investigaciones. La investigación básica ha transformado la manera en que entendemos el mundo, ha desarrollado nuevas técnicas y se ha convertido en una base esencial para el conocimiento y el aprendizaje. Según Roberto Hernández Sampieri, la investigación básica se describe como “un conjunto de procesos sistemáticos y empíricos aplicados al estudio de un fenómeno”

Sampieri, R. H. (2010). *Metodología de la investigación* (6.ª ed.). McGraw-Hill.

Alan Bryman sostiene que la investigación básica se centra en la ampliación del conocimiento teórico acerca de distintos aspectos del mundo natural o social, sin que su objetivo principal sea la aplicación práctica inmediata de sus hallazgos. Este

tipo de investigación juega un papel crucial en el desarrollo de teorías y conceptos que pueden servir como base para investigaciones posteriores (Bryman, 2016)

Bryman, A. (2016). *Social research methods* (5th ed.). Oxford University Press.

### 5.1.3 NIVEL DE INVESTIGACION DESCRIPTIVO -CORRELACIONAL

Dependiendo del enfoque de la investigación, el estudio puede clasificarse como Descriptivo-Correlacional.

**Estudios Descriptivos:** Estos se centran en detallar las propiedades, características y perfiles de personas, grupos, comunidades o cualquier fenómeno que se esté analizando. Su principal objetivo es recolectar información sobre las variables estudiadas, sin enfocarse en cómo estas variables se relacionan entre sí. La principal ventaja de estos estudios es su capacidad para ofrecer una visión clara de los diferentes aspectos de los fenómenos o situaciones analizadas.

**Estudios Correlacionales:** Estos estudios se orientan a medir la relación entre dos o más variables o conceptos. Se evalúa cada variable por separado y luego se cuantifica y analiza la relación entre ellas. Los estudios correlacionales se basan en hipótesis que se someten a prueba, buscando responder preguntas sobre cómo y en qué medida dos variables están interrelacionadas. Por ejemplo, se podría investigar si los niños que pasan más tiempo viendo televisión tienen un vocabulario más extenso en comparación con aquellos que ven menos televisión. Sin embargo, es importante tener en cuenta que una correlación entre variables no siempre implica una relación causal, y en algunos casos puede dar lugar a correlaciones espurias, donde las variables parecen estar relacionadas sin una conexión real.

Estos estudios, aunque útiles para entender las relaciones entre variables, ofrecen una explicación parcial, ya que solo revelan cómo se vinculan los conceptos sin necesariamente explicar por qué ocurre esa relación.

Sampieri, R. H. (2010). *Metodología de la investigación* (6.<sup>a</sup> ed.). McGraw-Hill.

## 5.2 METODOS DE INVESTIGACION

### 5.2.1 METODO GENERAL: HIPÓTETICO- DEDUCTIVO

El enfoque metodológico de esta investigación fue el método hipotético-deductivo. En este enfoque, se comienzan con hipótesis derivadas de principios teóricos o indicios empíricos. A partir de estas hipótesis, se generan predicciones que se verifican empíricamente. Si las predicciones coinciden con los datos observados, la hipótesis inicial se confirma; de lo contrario, si las predicciones resultan contradictorias, esto indica una posible inconsistencia en la hipótesis original, lo que lleva a su revisión o modificación.

Este método es frecuentemente utilizado en medicina, especialmente en el diagnóstico clínico. Como detalla León-Barúa (1999), el proceso empieza cuando el paciente describe sus síntomas al médico, quien realiza un examen físico para detectar alteraciones en el cuerpo. Basado en la historia clínica y el examen físico, el médico formula una o más hipótesis diagnósticas sobre la causa del problema del paciente. Estas hipótesis se evalúan mediante exámenes adicionales. Los resultados de estos exámenes confirman o refutan las hipótesis diagnósticas planteadas. Este procedimiento ilustra cómo el método hipotético-deductivo se aplica en la práctica, utilizando la veracidad de los enunciados iniciales para determinar la validez de las hipótesis. La metodología requiere de la prueba rigurosa de contraejemplos y la refutación de los mismos para validar las hipótesis (Behar, 2008).

Este enfoque permite la revisión y ajuste continuo del marco teórico, conceptual o metodológico de la investigación, y por ende, se puede considerar fundamentalmente como un método para el desarrollo del conocimiento. Behar (2008).

### 5.2.2 METODO ESPECIFICO: ESTADISTICO

Dependiendo del enfoque de la investigación, el estudio se clasifica como un análisis estadístico. Las hipótesis estadísticas son una forma de convertir las hipótesis de investigación en términos estadísticos, tanto nulas como alternativas.

Existen tres principales tipos de hipótesis estadísticas, que corresponden a distintas categorías de las hipótesis de investigación:

- **Hipótesis de estimación:** Estas se utilizan para evaluar suposiciones sobre el valor de una característica o variable en una muestra o población, basándose en información previa. En el contexto de hipótesis descriptivas, sirven para hacer previsiones sobre un dato específico.
- **Hipótesis de correlación:** Estas hipótesis buscan expresar estadísticamente la relación entre dos o más variables.
- **Hipótesis sobre diferencias de medias u otros valores:** Estas se centran en comparar estadísticas entre dos o más grupos para determinar si existen diferencias significativas. Sampieri. (2010).

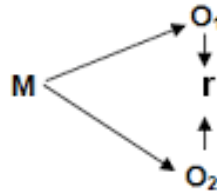
### 5.2.3 DISEÑO DE LA INVESTIGACION

El diseño de la investigación fue de tipo No Experimental y Transversal, según definición de Hernández Sampieri (2014):

a) **No Experimental:** En este enfoque, no se manipulan las variables causales para observar sus efectos. En lugar de ello, se limita a describir y analizar cómo inciden e interrelacionan las variables en un momento específico.

b) **Transversal:** Este diseño incorpora un enfoque Descriptivo-Correlacional para el análisis.

A continuación, se muestra el esquema correlacional:



Donde:

M = Muestra

O<sub>1</sub> = Observación de la V.1.

O<sub>2</sub> = Observación de la V.2.

r = Correlación entre dichas variables.

*Figura 9. Esquema Correlacional*

## 5.3 POBLACION Y MUESTRA DE LA INVESTIGACION

### 5.3.1 POBLACION

Según Hernández Sampieri, "una población es el conjunto completo de casos que cumplen con un conjunto de características específicas" (p. 174). Esta definición abarca el fenómeno total que se desea investigar, donde todas las unidades de la población comparten una característica que se examina y que origina los datos de la investigación. Sampieri. (2010).

La población del estudio estuvo conformada por 92 docentes.

### 5.3.2 MUESTRA: CENSAL

Oseña (2008, p. 121) define una muestra como una porción pequeña de la población que, aunque limitada en tamaño, refleja las principales características de la población total. De manera similar, Bernal (2010, p. 161) describe la muestra como

el segmento de la población del cual se recopila la información para el estudio, y sobre el cual se realizan las mediciones y observaciones de las variables de interés.

En el contexto de esta investigación, dado que la población estuvo compuesta por los 92 docentes, la muestra incluye a todos los individuos de la población, lo que la convierte en una muestra censal. Para este estudio, se utilizó un muestreo censal debido al tamaño reducido de la población.

López (1998, p. 123) señala que una muestra censal abarca toda la población. Por su parte, Hayes (1999, p. 24) identifica tres métodos de muestreo:

- **Censal:** En este método, la muestra representa a toda la población, y se usa cuando es necesario obtener datos de todos los participantes o cuando se tiene acceso completo a la base de datos.
- **Basado en criterio personal:** La muestra se selecciona según los intereses y objetivos del investigador.
- **Estadístico:** La muestra se elige como un subgrupo de la población con igual probabilidad de ser seleccionado.

## 5.4 5.4 TECNICAS E INSTRUMENTOS DE RECOLECCION DE DATOS

### 5.4.1 TECNICAS

Según Torres y Paz (2006), los métodos de recolección de datos son procesos y actividades que facilitan la obtención de información necesaria para alcanzar los objetivos de una investigación.

Para este estudio, se empleó la técnica de encuesta, que implica formular preguntas, ya sean orales o escritas, a una muestra específica con el fin de recolectar datos relevantes para el proyecto de investigación.

Campoy y Gómez (2015) indican que la encuesta es un método científico para recolectar datos que permite recoger información de los sujetos investigados sobre diversos temas.

#### 5.4.2 INSTRUMENTOS

Se empleó un cuestionario compuesto por una serie de preguntas (ítems) para obtener datos de los participantes en la encuesta (Corral, 2010).

#### 5.4.3 VALIDEZ Y CONFIABILIDAD

La validez fue realizada por medio de tres expertos quien realizaron la validación de los instrumentos con un resultado de 90 por ciento, de forma cualitativa de excelente, por lo que se aplicaron los mismo a la muestra del estudio.

Para el análisis de la confiabilidad se realizó mediante el Alfa de Cronbach, cuyos resultados son los siguientes:

| variables  | Alfa de Cronbach | N° de elementos |
|--|------------------|-----------------|
| Sistema de gestión de la seguridad de la información | 0.855            | 22              |
| Calidad del servicio informático                     | 0.823            | 22              |

#### 5.4.4 PROCESAMIENTO Y ANALISIS DE DATOS

Después de recolectar la información, se utilizó el software SPSS versión 25 para el procesamiento de los datos, así como para la creación de tablas y figuras que

mostraron los resultados de las variables estudiadas. Para organizar y clasificar los datos, se emplearon tablas de frecuencias y figuras estadísticas. Además, para evaluar las hipótesis generales y específicas, se aplicó el coeficiente de correlación Pearson.

#### **5.4.5 ETICA EN LA INVESTIGACION**

Los datos utilizados en esta investigación fueron obtenidos del grupo de estudio y procesados correctamente, sin alteraciones. Asimismo, el marco teórico se recopiló siguiendo los criterios establecidos para este tipo de estudio, asegurando originalidad y evitando la copia de otros trabajos, lo que permitió un uso efectivo de la investigación en beneficio de todos.

## 6 CAPITULO VI: RESULTADOS

### 6.1 ANÁLISIS DESCRIPTIVO

#### 6.1.1 Variable Sistema de Gestión de la Seguridad de la Información (SGSI)

Tabla 1.

Sistema de Gestión de la Seguridad de la Información

|        |                                | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|--------|--------------------------------|------------|------------|-------------------|----------------------|
| Válido | En desacuerdo                  | 1          | 1,1        | 1,1               | 1,1                  |
|        | Ni de acuerdo ni en desacuerdo | 33         | 35,9       | 35,9              | 37,0                 |
|        | De acuerdo                     | 56         | 60,9       | 60,9              | 97,8                 |
|        | Totalmente de acuerdo          | 2          | 2,2        | 2,2               | 100,0                |
|        | Total                          | 92         | 100,0      | 100,0             |                      |

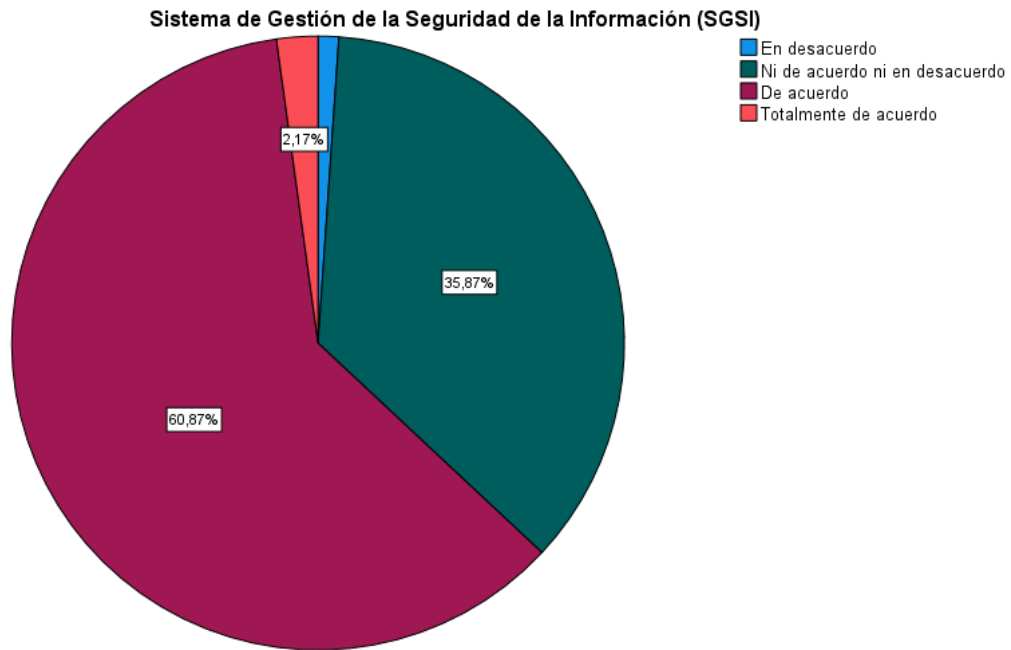


Figura 1

Sistema de Gestión de la Seguridad de la Información

**Interpretación:** El 60.9 % de los docentes consideraron que están de acuerdo que el Sistema de Gestión de la Seguridad de la Información es adecuado, seguido de 35.9 % que no están ni de acuerdo ni en desacuerdo.

Tabla 2.

D1 Principios de Seguridad de la Información

|        |                                | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|--------|--------------------------------|------------|------------|-------------------|----------------------|
| Válido | En desacuerdo                  | 9          | 9,8        | 9,8               | 9,8                  |
|        | Ni de acuerdo ni en desacuerdo | 23         | 25,0       | 25,0              | 34,8                 |
|        | De acuerdo                     | 56         | 60,9       | 60,9              | 95,7                 |
|        | Totalmente de acuerdo          | 4          | 4,3        | 4,3               | 100,0                |
|        | Total                          | 92         | 100,0      | 100,0             |                      |

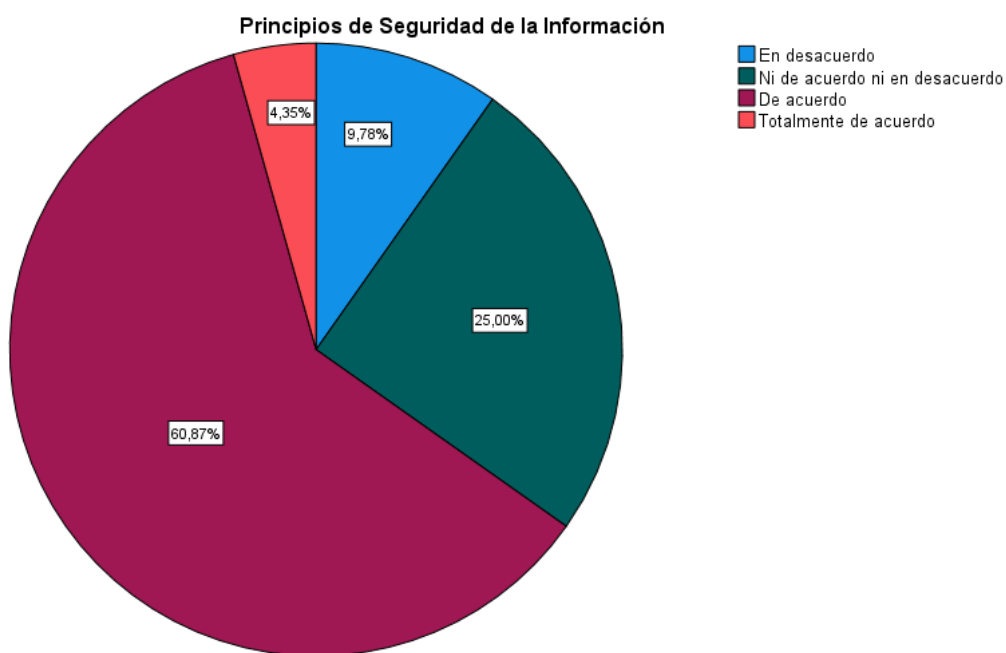


Figura 2

D1 Principios de Seguridad de la Información

**Interpretación:** El 60.9 % de los docentes consideraron que están de acuerdo que los principios de Seguridad de la Información son adecuados, seguido de 25 % que no están ni de acuerdo ni en desacuerdo.

Tabla 3

D2 ISO/IEC 27001

|        |                                | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|--------|--------------------------------|------------|------------|-------------------|----------------------|
| Válido | En desacuerdo                  | 10         | 10,9       | 10,9              | 10,9                 |
|        | Ni de acuerdo ni en desacuerdo | 24         | 26,1       | 26,1              | 37,0                 |
|        | De acuerdo                     | 45         | 48,9       | 48,9              | 85,9                 |
|        | Totalmente de acuerdo          | 13         | 14,1       | 14,1              | 100,0                |
|        | Total                          | 92         | 100,0      | 100,0             |                      |

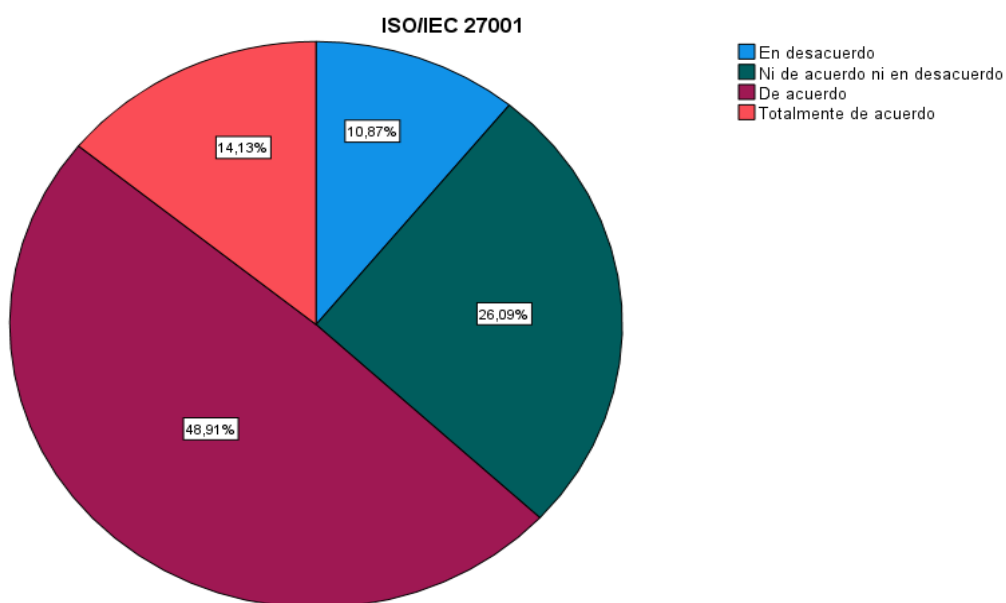


Figura 3  
D2 ISO/IEC 27001

**Interpretación:** El 48.9 % de los docentes consideraron que están de acuerdo que la aplicación de la ISO/IEC 27001 es adecuada, seguido de 26.1 % que no están ni de acuerdo ni en desacuerdo.

Tabla 4

D3 Gestión de Seguridad de la Información (SGSI)

|        |                                | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|--------|--------------------------------|------------|------------|-------------------|----------------------|
| Válido | En desacuerdo                  | 2          | 2,2        | 2,2               | 2,2                  |
|        | Ni de acuerdo ni en desacuerdo | 35         | 38,0       | 38,0              | 40,2                 |
|        | De acuerdo                     | 54         | 58,7       | 58,7              | 98,9                 |
|        | Totalmente de acuerdo          | 1          | 1,1        | 1,1               | 100,0                |
|        | Total                          | 92         | 100,0      | 100,0             |                      |

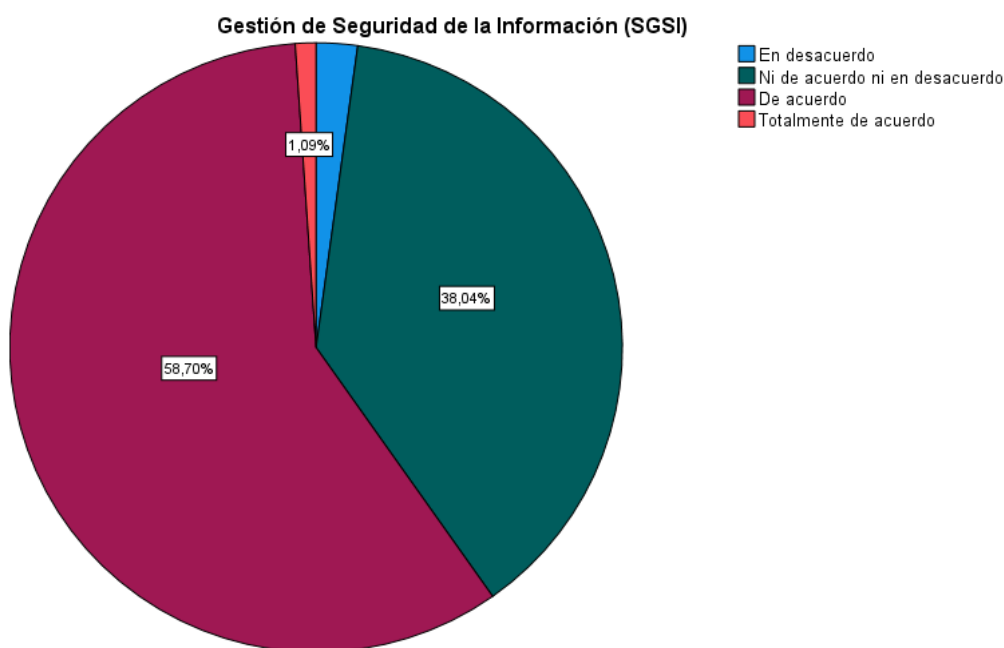


Figura 4

D3 Gestión de Seguridad de la Información (SGSI)

**Interpretación:** El 58.7 % de los docentes consideraron que están de acuerdo que la Gestión de la Seguridad de la Información es adecuada, seguido de 38 % que no están ni de acuerdo ni en desacuerdo.

Tabla 5

D4: Implantación del Sistema de Gestión de Seguridad de la Información

|        |                                | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|--------|--------------------------------|------------|------------|-------------------|----------------------|
| Válido | En desacuerdo                  | 12         | 13,0       | 13,0              | 13,0                 |
|        | Ni de acuerdo ni en desacuerdo | 12         | 13,0       | 13,0              | 26,1                 |
|        | De acuerdo                     | 54         | 58,7       | 58,7              | 84,8                 |
|        | Totalmente de acuerdo          | 14         | 15,2       | 15,2              | 100,0                |
|        | Total                          | 92         | 100,0      | 100,0             |                      |

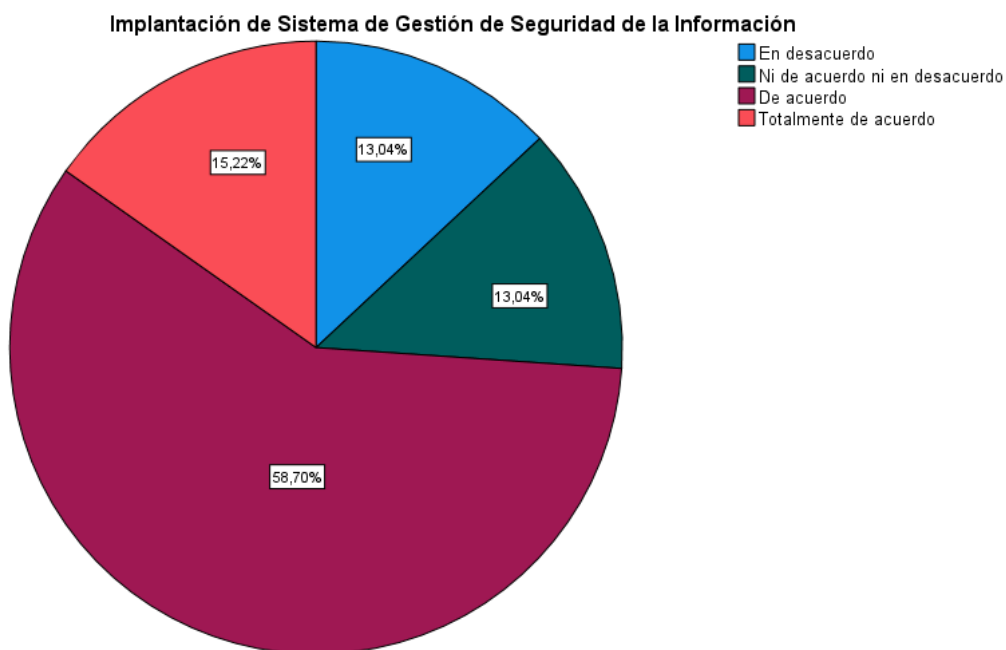


Figura 5

D4: Implantación del Sistema de Gestión de Seguridad de la Información

**Interpretación:** El 58.7 % de los docentes consideraron que están de acuerdo con la implantación del Sistema de Gestión de Seguridad de la Información, seguido de 15.2 % de totalmente de acuerdo.

Tabla 6

Variable: Calidad del Servicio Informático

|                                | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|--------------------------------|------------|------------|-------------------|----------------------|
| Válido En desacuerdo           | 1          | 1,1        | 1,1               | 1,1                  |
| Ni de acuerdo ni en desacuerdo | 39         | 42,4       | 42,4              | 43,5                 |
| De acuerdo                     | 51         | 55,4       | 55,4              | 98,9                 |
| Totalmente de acuerdo          | 1          | 1,1        | 1,1               | 100,0                |
| Total                          | 92         | 100,0      | 100,0             |                      |

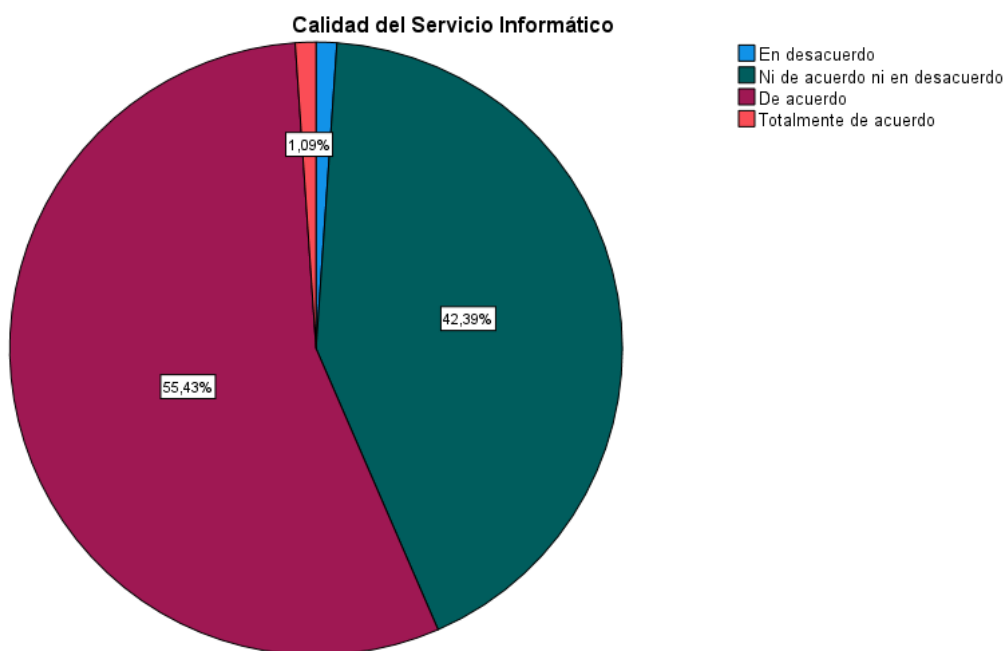


Figura 6

Calidad del Servicio Informático

**Interpretación:** El 55.4 % de los docentes consideraron que están de acuerdo que la calidad del servicio informático es adecuada, seguido del 42.4 % que no están ni de acuerdo ni en desacuerdo.

Tabla 7

D1: Fiabilidad

|        |                                | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|--------|--------------------------------|------------|------------|-------------------|----------------------|
| Válido | En desacuerdo                  | 8          | 8,7        | 8,7               | 8,7                  |
|        | Ni de acuerdo ni en desacuerdo | 15         | 16,3       | 16,3              | 25,0                 |
|        | De acuerdo                     | 61         | 66,3       | 66,3              | 91,3                 |
|        | Totalmente de acuerdo          | 8          | 8,7        | 8,7               | 100,0                |
|        | Total                          | 92         | 100,0      | 100,0             |                      |

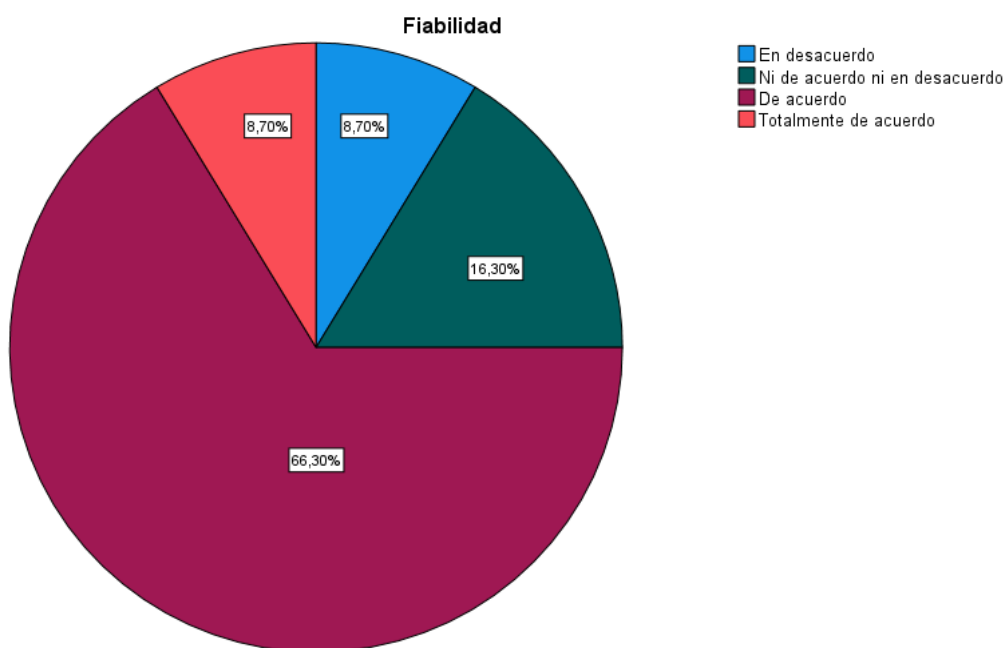


Figura 7

D1 Fiabilidad

**Interpretación:** El 66.3 % de los docentes consideraron que están de acuerdo que la fiabilidad de la calidad del servicio informático es adecuada, seguido de 16.3 % que no están ni de acuerdo ni en desacuerdo.

Tabla 8

D2: Capacidad de respuesta

|        |                                | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|--------|--------------------------------|------------|------------|-------------------|----------------------|
| Válido | En desacuerdo                  | 11         | 12,0       | 12,0              | 12,0                 |
|        | Ni de acuerdo ni en desacuerdo | 37         | 40,2       | 40,2              | 52,2                 |
|        | De acuerdo                     | 36         | 39,1       | 39,1              | 91,3                 |
|        | Totalmente de acuerdo          | 8          | 8,7        | 8,7               | 100,0                |
|        | Total                          | 92         | 100,0      | 100,0             |                      |

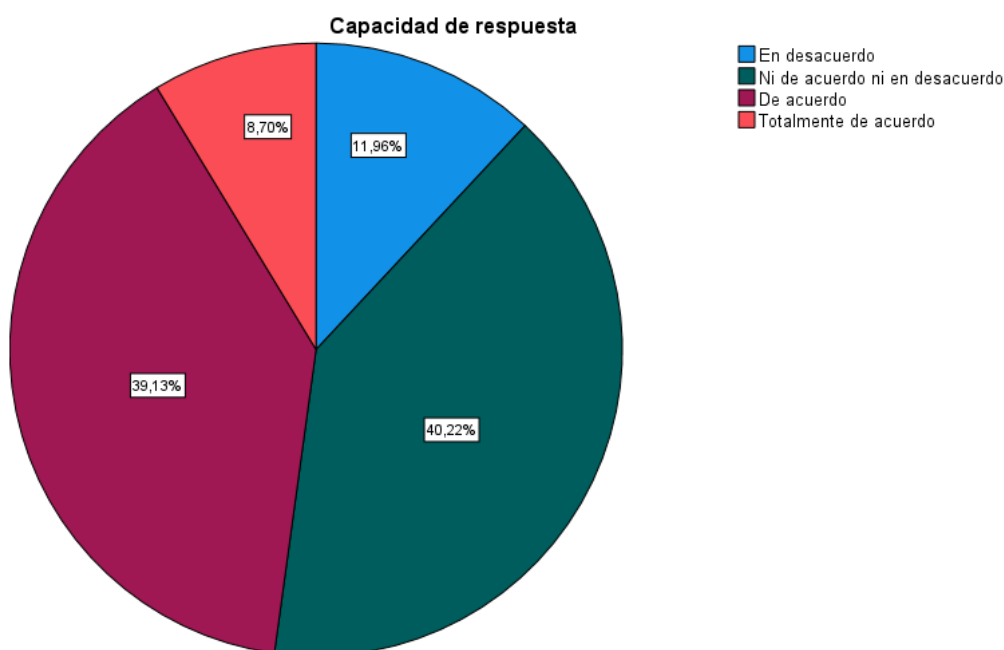


Figura 8

D2: Capacidad de respuesta

**Interpretación:** El 40.2 % de los docentes consideraron que no están ni de acuerdo ni de en desacuerdo con la capacidad de respuesta de la calidad del servicio informático, seguido del 39.1 % que estuvieron de acuerdo.

Tabla 9

D3: Capacitación del Personal

|        |                                | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|--------|--------------------------------|------------|------------|-------------------|----------------------|
| Válido | En desacuerdo                  | 8          | 8,7        | 8,7               | 8,7                  |
|        | Ni de acuerdo ni en desacuerdo | 26         | 28,3       | 28,3              | 37,0                 |
|        | De acuerdo                     | 51         | 55,4       | 55,4              | 92,4                 |
|        | Totalmente de acuerdo          | 7          | 7,6        | 7,6               | 100,0                |
|        | Total                          | 92         | 100,0      | 100,0             |                      |

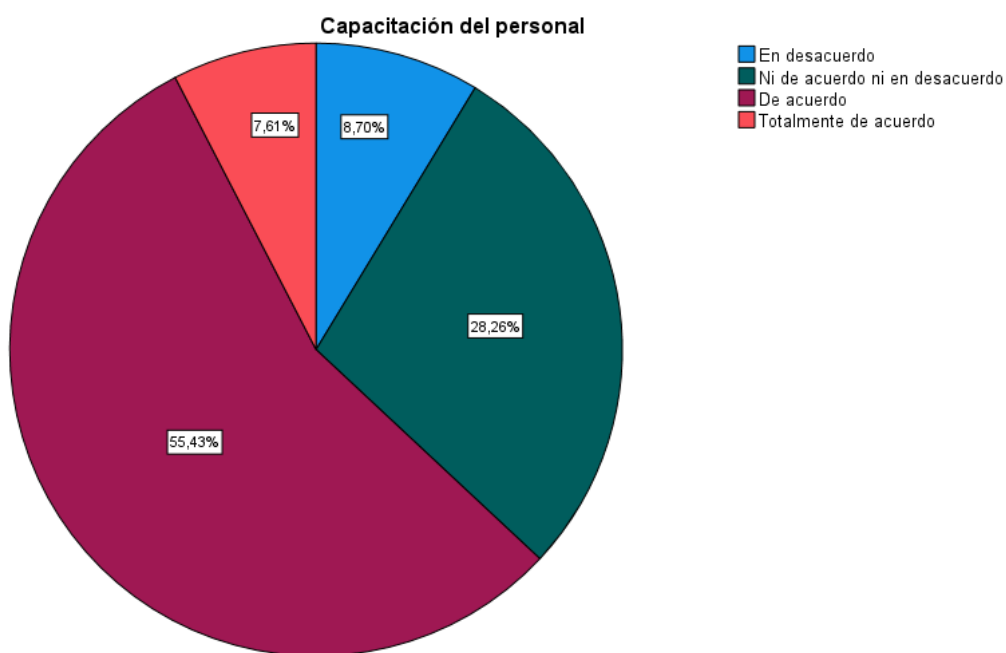


Figura 9

D3: Capacitación del Personal

**Interpretación:** El 55.4 % de los docentes consideraron que están de acuerdo con la realización de capacitación del personal, seguido de 28.3 % que no están ni de acuerdo ni en desacuerdo.

Tabla 10

D4: Atención al Cliente

|        |                                | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|--------|--------------------------------|------------|------------|-------------------|----------------------|
| Válido | En desacuerdo                  | 10         | 10,9       | 10,9              | 10,9                 |
|        | Ni de acuerdo ni en desacuerdo | 21         | 22,8       | 22,8              | 33,7                 |
|        | De acuerdo                     | 56         | 60,9       | 60,9              | 94,6                 |
|        | Totalmente de acuerdo          | 5          | 5,4        | 5,4               | 100,0                |
|        | Total                          | 92         | 100,0      | 100,0             |                      |

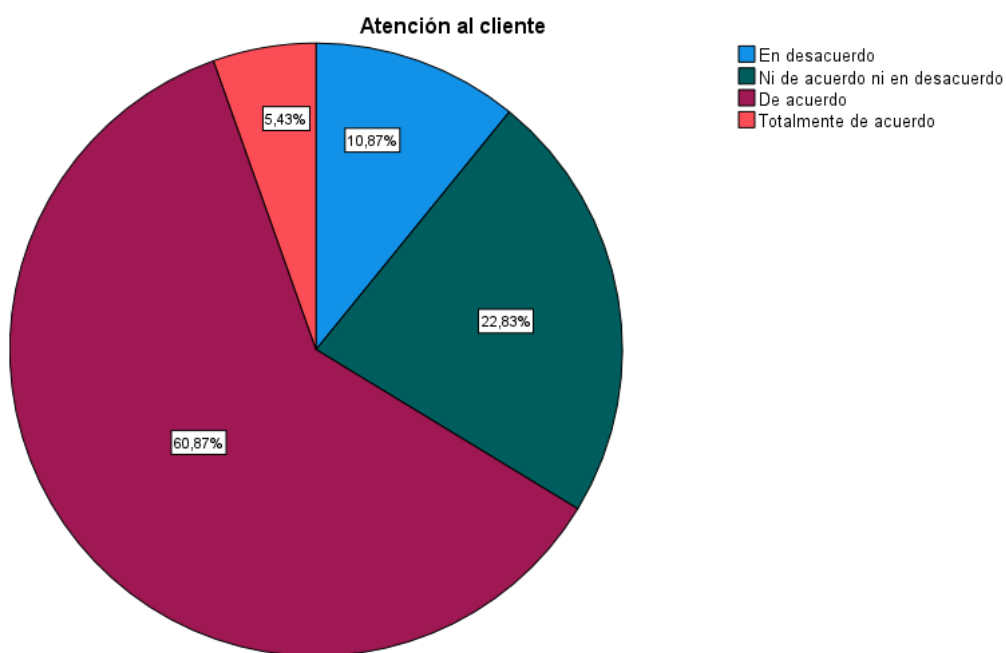


Figura 10

D4: Atención al Cliente

**Interpretación:** El 60.9 % de los docentes consideraron que están de acuerdo que la atención al cliente es adecuada, seguido de 22.8 % que no están ni de acuerdo ni en desacuerdo.

## 6.2 ESTADÍSTICA INFERENCIAL

### Prueba de Distribución normal:

**Ho:** Los datos tienen distribución normal.

**Ha:** Los datos no tienen distribución normal.

**Nivel de significancia:** 5%

### Prueba estadística:

Tabla 11

Prueba de Normalidad

|      | Calidad       | Seguridad | Kolmogorov-Smirnov <sup>a</sup> |     |         | Shapiro-Wilk |    |      |
|------|---------------|-----------|---------------------------------|-----|---------|--------------|----|------|
|      |               |           | Estadístico                     | gl  | Sig.    | Estadístico  | gl | Sig. |
|      | Informática   |           |                                 |     |         |              |    |      |
| SGSI | Nunca         |           | . 3                             |     | . 3     |              |    |      |
|      | Casi nunca    |           | ,111 3                          | ,08 | ,101  3 | ,09          |    |      |
|      | Algunas veces |           | ,223 20                         | ,08 | ,284 20 | ,09          |    |      |
|      | Casi siempre  |           | ,305 63                         | ,08 | ,355 63 | ,09          |    |      |
|      | Siempre       |           | . 3                             |     | . 3     |              |    |      |

a. Corrección de significación de Lilliefors

Según la muestra fue 92 y  $>$  a 50, se utilizó la prueba de Kolmogorov-Smirnov<sup>a</sup>, donde los resultados de la prueba estadística (sig.= 0.0) fueron mayor al 5% (0.05), por lo tanto, se rechazó la hipótesis alterna, los datos tienen una distribución normal, por lo que se empleó Pearson.

### Contrastación de hipótesis general

**Hi:** El Sistema de Gestión de Seguridad de la Información se relaciona significativamente con la Calidad del Servicio Informático en la Universidad Nacional de Moquegua, Año 2,024

**Ho:** El Sistema de Gestión de Seguridad de la Información no se relaciona significativamente con la Calidad del Servicio Informático en la Universidad Nacional de Moquegua, Año 2,024

Tabla 12

Contrastación Hipótesis General

#### Correlaciones

|   |                        | Sistema de Gestión de la Seguridad de la Información (SGSI) | Calidad del Servicio Informático |
|---|------------------------|---|----------------------------------|
| Sistema de Gestión de la Seguridad de la Información (SGSI) | Correlación de Pearson | 1   | ,545**                           |
|   | Sig. (bilateral)       |   | ,000                             |
|   | N                      | 92  | 92                               |
| Calidad del Servicio Informático                            | Correlación de Pearson | ,545**  | 1                                |
|   | Sig. (bilateral)       | ,000  |                                  |
|   | N                      | 92  | 92                               |

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

Según la significancia bilateral de 0,000 menor a  $p = 0,05$  nos permite rechazar la  $H_0$  y aceptar que El Sistema de Gestión de Seguridad de la Información se relaciona significativamente con la Calidad del Servicio Informático en la Universidad Nacional de Moquegua, Año 2,024, con un coeficiente positivo de nivel moderado de 0,545.

### Contrastación de hipótesis específica 1

Hi: Los principios básicos del sistema de gestión de seguridad de la información ISO 27001 se relacionan significativamente con la Calidad del Servicio informático en la Universidad Nacional de Moquegua, Año 2,024.

Ho: Los principios básicos del sistema de gestión de seguridad de la información ISO 27001 no se relacionan significativamente con la Calidad del Servicio informático en la Universidad Nacional de Moquegua, Año 2,024.

Tabla 13

Contrastación de Hipótesis Especifica 1

#### Correlaciones

|   |                        | Principios de Seguridad de la Información | Calidad del Servicio Informático |
|---|------------------------|---|----------------------------------|
| Principios de Seguridad de la Información | Correlación de Pearson | 1   | ,445**                           |
|   | Sig. (bilateral)       |   | ,000                             |
|   | N                      | 92  | 92                               |
| Calidad del Servicio Informático          | Correlación de Pearson | ,445**                                    | 1                                |
|   | Sig. (bilateral)       | ,000                                      |                                  |
|   | N                      | 92  | 92                               |

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

Según la significancia bilateral de 0,000 menor a  $p = 0,05$  nos permite rechazar la Ho y aceptar que: Los principios básicos del sistema de gestión de seguridad de la información ISO 27001 se relacionan significativamente con la Calidad del Servicio informático en la Universidad Nacional de Moquegua, Año 2,024, con un coeficiente de correlación positivo moderado de 0,445.

### Contrastación de hipótesis específica 2

Hi: La Norma ISO/IEC 27001 se relaciona significativamente con la Calidad del Servicio. en la Universidad Nacional de Moquegua, Año 2,024.

Ho: La Norma ISO/IEC 27001 no se relaciona significativamente con la Calidad del Servicio. en la Universidad Nacional de Moquegua, Año 2,024.

Tabla 14

Contrastación de Hipótesis Específica 2

#### Correlaciones

|                                  |                        | ISO/IEC 27001 | Calidad del Servicio Informático |
|----------------------------------|------------------------|---------------|----------------------------------|
| ISO/IEC 27001                    | Correlación de Pearson | 1             | ,488**                           |
|                                  | Sig. (bilateral)       |               | ,000                             |
|                                  | N                      | 92            | 92                               |
| Calidad del Servicio Informático | Correlación de Pearson | ,488**        | 1                                |
|                                  | Sig. (bilateral)       | ,000          |                                  |
|                                  | N                      | 92            | 92                               |

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

Según la significancia bilateral de 0,000 que es menor a  $P = 0,05$  nos permite rechazar la  $H_0$  y aceptar que: La Norma ISO/IEC 27001 se relaciona significativamente con la Calidad del Servicio. en la Universidad Nacional de Moquegua, Año 2,024, con un coeficiente de correlación positivo moderado de 0,488.

### Contrastación de hipótesis específica 3

Hi: La Gestión de seguridad de la información se relaciona significativamente con la Calidad del Servicio. en la Universidad Nacional de Moquegua, Año 2,024.

Ho: La Gestión de seguridad de la información no se relaciona significativamente con la Calidad del Servicio. en la Universidad Nacional de Moquegua, Año 2,024.

Tabla 15

Contrastación de Hipótesis Específica 3

#### Correlaciones

|   |                        | Gestión de Seguridad de la Información (SGSI) | Calidad del Servicio Informático |
|---|------------------------|---|----------------------------------|
| Gestión de Seguridad de la Información (SGSI) | Correlación de Pearson | 1   | ,455**                           |
|   | Sig. (bilateral)       |   | ,000                             |
|   | N                      | 92  | 92                               |
| Calidad del Servicio Informático              | Correlación de Pearson | ,455**  | 1                                |
|   | Sig. (bilateral)       | ,000  |                                  |
|   | N                      | 92  | 92                               |

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

Por la significancia bilateral de 0,000 que es  $< a P = 0,05$  se rechaza la Ho y aceptar que: La Gestión de seguridad de la información se relaciona significativamente con la Calidad del Servicio. en la Universidad Nacional de Moquegua, Año 2,024, con un coeficiente de correlación positivo moderado de 0,455.

### Contrastación de hipótesis específica 4

Hi: La implantación de la Norma ISO/IEC 27001 de la Gestión de seguridad de la información se relaciona significativamente con la Calidad del Servicio informático en la Universidad Nacional de Moquegua, Año 2,024

Ho: La implantación de la Norma ISO/IEC 27001 de la Gestión de seguridad de la información no se relaciona significativamente con la Calidad del Servicio informático en la Universidad Nacional de Moquegua, Año 2,024

Tabla 16

Contrastación de Hipótesis Específica 3

#### Correlaciones

|   |                        | Implantación de Sistema de Gestión de Seguridad de la Información | Calidad del Servicio Informático |
|---|------------------------|---|----------------------------------|
| Implantación de Sistema de Gestión de Seguridad de la Información | Correlación de Pearson | 1   | ,250                             |
|   | Sig. (bilateral)       |   | ,000                             |
|   | N                      | 92  | 92                               |
| Calidad del Servicio Informático                                  | Correlación de Pearson | ,250  | 1                                |
|   | Sig. (bilateral)       | ,000  |                                  |
|   | N                      | 92  | 92                               |

Por la significancia bilateral de 0,000 que es  $< \alpha = 0,05$  se rechaza la Ho y aceptar que: La implantación de la Norma ISO/IEC 27001 de la Gestión de seguridad de la información se relaciona significativamente con la Calidad del Servicio informático en la Universidad Nacional de Moquegua, Año 2,024, con un coeficiente de correlación positivo bajo de 0.250.

## 7 CAPITULO VI: DISCUSIÓN DE LOS RESULTADOS

Según la significancia bilateral de 0,000 menor a  $p = 0,05$  nos permite rechazar la  $H_0$  y aceptar que el Sistema de Gestión de Seguridad de la Información se relaciona significativamente con la Calidad del Servicio Informático en la Universidad Nacional de Moquegua, Año 2,024, con un coeficiente positivo de nivel moderado de 0,545.

Resultado similar tiene Carranza et al. (2018). En su trabajo titulado “Plan para perfeccionar el grado de estabilidad de reportes y seguida del centro de datos en la gerencia regional de Educación de la Libertad aplicando cada uno de los pasos ISO 27001 y buenas prácticas COBIT” Se planteo un objetivo principal que es la presentación del plan de mejora metodología MAIGTI, con directrices en auditoría de lineamientos ISO 27001 y COBIT 4.0, Finalmente se determinan los procesos más adecuados para el control según los estándares con una evaluación y recomendaciones.

También concuerda con la tesis de Polar (2021). Modelo para la valoración de activos de información basados en la norma ISO 27000 universidad Nacional Jorge Basadre Grohmann, Tacna, Perú. Este trabajo presenta un modelo que facilita la evaluación de los activos de información, basándose en los estándares de la familia

ISO 27000; que combina nuestra experiencia laboral, investigación utilizada, herramientas creadas e investigación adicional, para proporcionar un prototipo útil, escalable y fácil de usar para los participantes en esta ruta de seguridad de la información aplicable a todo tipo de organizaciones, independientemente de su tipo, tamaño o naturaleza.

Similar resultado tiene Choquehuayta (2021) “Modelo servqual para la evaluación del servicio de defensoría municipal del niño y el adolescente en la municipalidad distrital de Lluta, Caylloma 2019” Universidad Nacional de Arequipa, Perú.

Afirmó que a partir de este modelo desarrollaron una herramienta, de evaluación de la calidad del servicio, denominada SERVQUAL, por su abreviatura en inglés "service quality", esta investigación es una de las primeras en cuestionarse sobre la satisfacción de los usuarios de los servicios municipales concluyendo que el índice de la calidad de servicio percibido esta muy por debajo de lo esperado por los usuarios.

1 Finalmente concuerda con el trabajo de Puentes (2021) Diseño de una guía de mejoramiento en los procesos del SGSI bajo la norma ISO 27002:2015, ítems, 6.1 en el área de infraestructura de la empresa corbeta S.A. Bogotá sede calle 31. Universidad Cooperativa de Colombia, Bogotá.

1 La normativa ISO / IEC 27002: 2015 ITEM 6.1 es una guía que contiene la estructura de gestión necesaria para diseñar e implementar un sistema de gestión de seguridad de la información de acuerdo con los requisitos especificados en la ISO / IEC 27000, que gestiona la seguridad de la información de una organización.

## CONCLUSIONES

1.-El Sistema de Gestión de Seguridad de la Información se relaciona significativamente con la Calidad del Servicio Informático en la Universidad Nacional de Moquegua, Año 2,024, con un coeficiente positivo de nivel moderado de 0,545.

2.-Los principios básicos del sistema de gestión de seguridad de la información ISO 27001 se relacionan significativamente con la Calidad del Servicio informático en la Universidad Nacional de Moquegua, Año 2,024, con un coeficiente de correlación positivo moderado de 0,445.

3.-La Norma ISO/IEC 27001 se relaciona significativamente con la Calidad del Servicio. en la Universidad Nacional de Moquegua, Año 2,024, con un coeficiente de correlación positivo moderado de 0,488.

4.- La Gestión de seguridad de la información se relaciona significativamente con la Calidad del Servicio. en la Universidad Nacional de Moquegua, Año 2,024, con un coeficiente de correlación positivo moderado de 0,455.

5.- La implantación de la Norma ISO/IEC 27001 de la Gestión de seguridad de la información se relaciona significativamente con la Calidad del Servicio informático en la Universidad Nacional de Moquegua, Año 2,024, con un coeficiente de correlación positivo bajo de 0.250.

## RECOMENDACIONES

- 1.- Recomendar a la Jefatura de Tecnologías de Información contar con un presupuesto específico para llevar a cabo acciones y actividades relacionadas a la seguridad, gestión de vulnerabilidad, control de acceso que permita salvaguardar la información de la UNAM.
- 2.- Recomendar a la Jefatura de Tecnologías de información y Recursos Humanos se realicen actividades de sensibilización y capacitación con los usuarios a fin de realizar el empleo de la información en forma adecuada.
- 3.- Recomendar a la Jefatura de Tecnologías de Información, se realizan auditorias, a fin de lograr la certificación, acreditación y evaluaciones de seguridad.
- 4.- Recomendar a la Jefatura de Tecnologías de Información, se elaboren planes de contingencias, identificación, autenticación, gestión de incidentes y se socialicen con los usuarios.
- 5.- Recomendar a la Jefatura de Tecnologías de Información se realicen mantenimientos preventivos, protección de medios, seguridad física, seguridad personal, evaluación de riesgos, así de ser necesario la adquisición de activos y servicios a fin de optimizar el sistema de gestión de seguridad de la información en la UNAM.

## REFERENCIAS BIBLIOGRÁFICAS

- Arrué Flores, J. L. (2014). *Análisis de la calidad de servicio de atención en la oficina desconcentrada de OSIPTEL desde la percepción del usuario* [Tesis de maestría, Universidad Nacional de la Amazonía Peruana]. Universidad Nacional de la Amazonía Peruana. <https://repositorio.unapiquitos.edu.pe/bitstream/handle/20>.
- Behar, J. (2008). *Métodos científicos de indagación y de construcción del conocimiento*. <https://www.redalyc.org/pdf/206/20652069006.pdf>.
- Bernal, C. (2013). *Metodología de la investigación*. *Journal of Chemical Information and Modeling*. <https://doi.org/10.1017/CBO9781107415324.004>
- Bryman, A. (2016). *Social research methods* (5th ed.). Oxford University Press. [https://books.google.com.pe/books?hl=es&lr=&id=N2zQCgAAQBAJ&oi=fnd&pg=PP1&dq=Alan+Bryman+\(Bryman,+2016\).&ots=dqKvIPP3vh&sig=ObNo5Y13BiGNFObi\\_V0M4tuyqmU#v=onepage&q=Alan%20Bryman%20\(Bryman%2C%202016\).&f=false](https://books.google.com.pe/books?hl=es&lr=&id=N2zQCgAAQBAJ&oi=fnd&pg=PP1&dq=Alan+Bryman+(Bryman,+2016).&ots=dqKvIPP3vh&sig=ObNo5Y13BiGNFObi_V0M4tuyqmU#v=onepage&q=Alan%20Bryman%20(Bryman%2C%202016).&f=false)
- Campoy, T., & Gómez, E. (2015). Técnicas e instrumentos cualitativos de recogida de datos. In *Manual básico para la realización de tesinas, tesis y trabajos de investigación*. <https://dialnet.unirioja.es/servlet/libro?codigo=499550>
- Carranza, Y., & Zavala, C. (2016). *Plan de mejora de la seguridad de información y continuidad del centro de datos de la Gerencia Regional de Educación La Libertad aplicando lineamientos ISO 27001 y buenas prácticas COBIT* [Tesis de licenciatura, Universidad Privada Antenor Orrego]. Universidad Privada Antenor Orrego. <https://hdl.handle.net/20.500.12759/645>
- Corral, Y. (2010). *Diseño de cuestionarios para recolección de datos*. Revista de la Facultad de Ciencias Económicas y Sociales, Universidad de Carabobo. Recuperado de <http://servicio.bc.uc.edu.ve/educacion/revista/n36/art08.pdf>
- Deming, W. E. (1986). *The Deming Management Method. Notes*.

<https://doi.org/10.1007/s11249-006-9028-5>

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for Information Security Management. *Journal of Information Security*.  
<https://doi.org/10.4236/jis.2013.42011>

Disterer, G. (2013). *ISO/IEC 27000, 27001 y 27002 para la gestión de la seguridad de la información*. *Journal of Information Security*, 4, 92-100.  
<http://dx.doi.org/10.4236/jis.2013.42011>

Geraldi, J., & Lechter, T. (2012). Gantt charts revisited: A critical analysis of its roots and implications to the management of projects today. *International Journal of Managing Projects in Business*, 5(4), 578-594. Disponible en [https://www.researchgate.net/publication/263571905\\_Gantt\\_charts\\_revisited\\_A\\_critical\\_analysis\\_of\\_its\\_roots\\_and\\_implications\\_to\\_the\\_management\\_of\\_projects\\_to\\_day](https://www.researchgate.net/publication/263571905_Gantt_charts_revisited_A_critical_analysis_of_its_roots_and_implications_to_the_management_of_projects_to_day)

Hernández Sampieri, R. (2014). *Metodología de la investigación* (6.ª ed.). McGraw Hill Education.  
[https://apiperiodico.jalisco.gob.mx/api/sites/periodicooficial.jalisco.gob.mx/files/metodologia\\_de\\_la\\_investigacion\\_-\\_roberto\\_hernandez\\_sampieri.pdf](https://apiperiodico.jalisco.gob.mx/api/sites/periodicooficial.jalisco.gob.mx/files/metodologia_de_la_investigacion_-_roberto_hernandez_sampieri.pdf)

ISO/IEC. (2018). *ISO/IEC 27000:2018 Information technology — Security techniques — Information security management systems — Overview and vocabulary*. ISO.  
<https://www.iso.org/standard/84257.html>  
Juran, J. M. (1989). *Juran on Planning for Quality*. ASQ.  
<https://sistemasdecalidad6to.weebly.com/uploads/4/6/5/8/46581171/metodo-juran-an%C3%A1lisis-y-planeaci%C3%B3n-de-la-calidad-juran-5ta.pdf>

ISO/IEC. (2000). *ISO/IEC 17799:2000 - Information technology - Code of practice for information security management*. (ISO).  
<https://www.semanticscholar.org/paper/Information-Technology%3A-Code-of-Practice-for-Peltier/c0cbad7dd4021229bf25a8162973f2c57f3f78de>

ISO/IEC. (2014). *ISO/IEC 27000: Information technology - Security techniques - Information security management systems - Overview and vocabulary*. ISO/IEC.  
<https://www.iso.org/standard/73906.html>

- ISO/IEC 27000:2016. (2016). ISO/IEC 27000:2016 Information technology — Security techniques <https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-4:v1:en>
- Lascurain Gutiérrez, I. (2012). *Diagnóstico y propuesta de mejora de calidad en el servicio de una empresa de unidades de energía eléctrica ininterrumpida* (Tesis de maestría, Maestría en Ingeniería de Calidad). Universidad Iberoamericana. <https://ri.iber.mx/bitstream/handle/iber/561/015599s.pdf?sequence=1&isAllowed=y>
- López, P. L. (2004). Población, muestra y muestreo. *Punto Cero*, 9(8). <https://www.scielo.org.bo/pdf/rpc/v09n08/v09n08a12.pdf>
- Ludewig, C. (1998). Universo y muestra. En *Taller de metodología de la investigación*. [https://www.geocities.ws/ucla\\_investigacion/muestreo.pdf](https://www.geocities.ws/ucla_investigacion/muestreo.pdf)
- Méndez Ramírez, O. (2002). *La investigación científica*. Editorial Investigaciones Jurídicas. Retrieved from <https://books.google.com.pe/books?id=hlHQAQAACAAJ&dq=Méndez+investigación&hl=es-419&sa=X&ved=0ahUKEwiMsY--7sPhAhVnzlkKHWRgC8IQ6AEIKDAA>
- Myler, E., & Broadbent, G. (2006). ISO 17799: Standard for Security. *Information Management* <https://lloydscer.ir/Files/b2a73f13-8f75-4782-b57d-fa669ec48b04.pdf>
- Myler, E., & Broadbent, G. (2006). ISO 17799: Estándar para la seguridad. *Gestión de la información*, 40 (6), 43. <https://lloydscer.ir/Files/b2a73f13-8f75-4782-b57d-fa669ec48b04.pdf>
- Moquillaza Henríquez, S. D., & Carrillo Gomero, F. N. (2016). *Implementando la Norma Técnica Peruana NTP-ISO/IEC 27001:2014 en una entidad del estado [Implementing the Peruvian Technical Standard NTP-ISO/IEC 27001: 2014 in an entity state]*. *Electrónica – UNMSM*, 19(1), 1-10. [https://www.academia.edu/68874435/Implementando\\_la\\_Norma\\_T%C3%A9cnica\\_Peruana\\_NTP\\_ISO\\_IEC\\_27001\\_2014\\_en\\_una\\_Entidad\\_del\\_Estado?hb-sb-sw=18767764](https://www.academia.edu/68874435/Implementando_la_Norma_T%C3%A9cnica_Peruana_NTP_ISO_IEC_27001_2014_en_una_Entidad_del_Estado?hb-sb-sw=18767764)

- Muñoz Ñauta, J. D. (2016). *Diseño de políticas de seguridad informática para la Dirección de Tecnologías de la Información y Comunicación (DTIC) de la Universidad de Cuenca* (Proyecto de titulación, Maestría en Gestión Estratégica de Tecnologías de Información y Comunicación). Universidad de Cuenca. <https://dspace.ucuenca.edu.ec/bitstream/123456789/25646/1/Tesis.pdf>
- Rebolledo Martínez, O. (2014). Marco para el Gobierno de la Seguridad de la Información en servicios Cloud Computing. Retrieved from <https://ruidera.uclm.es/xmlui/handle/10578/4121>
- Revista Científica de la UCSA*. (2022). *Revista Científica de la UCSA*, 9(3), 23-35. <https://doi.org/10.18004/ucsa/2409-8752/2022.009.03.023>
- Rodríguez, G., Gil, J., & García, E. (1996). *Metodología de la investigación Cualitativa. Metodología de la investigación cualitativa* Málaga: Aljibe
- Rodríguez Peñuelas, M. A., & Universidad Autónoma de Sinaloa. (2010). *Métodos de investigación : diseño de proyectos y desarrollo de tesis en ciencias administrativas, organizacionales y sociales*. Universidad Autónoma de Sinaloa. [https://books.google.com.pe/books/about/Métodos\\_de\\_investigación.html?id=tsGyMwEACAAJ&redir\\_esc=y](https://books.google.com.pe/books/about/Métodos_de_investigación.html?id=tsGyMwEACAAJ&redir_esc=y)
- Ruiz Olalla, C. (2001). "Gestión de la calidad del servicio " <https://ciberconta.unizar.es/leccion/calidadserv/>
- Sampieri, R. H. (2010). *Metodología de la investigación* (6.ª ed.). McGraw-Hill. [https://apiperiodico.jalisco.gob.mx/api/sites/periodicooficial.jalisco.gob.mx/files/metodologia\\_de\\_la\\_investigacion\\_-\\_roberto\\_hernandez\\_sampieri.pdf](https://apiperiodico.jalisco.gob.mx/api/sites/periodicooficial.jalisco.gob.mx/files/metodologia_de_la_investigacion_-_roberto_hernandez_sampieri.pdf)
- Scardina, S. A. (1994). SERVQUAL. *Journal of Nursing Care Quality*. <https://doi.org/10.1097/00001786-199401000-00008>
- Seclén Arana, J. A. (2016). *Factores que afectan la implementación del sistema de gestión de seguridad de la información en las entidades públicas peruanas de acuerdo a la NTP-ISO/IEC 27001* (Tesis de maestría, Universidad Nacional Mayor de San Marcos). <https://cybertesis.unmsm.edu.pe/backend/api/core/bitstreams/e26db776-75bf-447d-93c4-6ba9cbcd505/content>

Torres, M., & Paz, K. (2006). Métodos de recolección de datos para una investigación. *Facultad de Ingeniería - Universidad Rafael Landívar.*

Treviño R. y E. Treviño (2021), la calidad del servicio

UNE-ISO/IEC 17799 <http://www.shutdown.es/ISO17799.pdf>

Vásquez Carrasco, R. E. de los M. (2015). *Efectividad de los métodos para medir calidad de servicio en universidades: Caso universidades privadas del departamento de Lambayeque* (Tesis doctoral, Universidad de Málaga, Departamento de Economía y Administración de Empresas). Universidad de Málaga. <https://educacion.gob.es/teseo/imprimirFicheroTesis.do?idFichero=UAhshR%2FwTug%3D>

Vinueza Martínez, J., & Correa Peralta, M. A. (2015). La Calidad en los Procesos Informáticos de las Universidades Ecuatorianas. *CIENCIA UNEMI*, 7(12), 58-68. <https://www.redalyc.org/pdf/5826/582663859008.pdf>

#### REVISTAS CIENTIFICAS VIRTUALES

<https://www.ceac.es/blog/tipos-de-seguridad-informatica>

[https://www.ecured.cu/Seguridad\\_Inform%C3%A1tica](https://www.ecured.cu/Seguridad_Inform%C3%A1tica)

<https://www.pais.gob.pe/sgsi/sgsi.html>

<https://www.pais.gob.pe/sgsi/sgsi.html>

<https://www.pais.gob.pe/sgsi/sgsi.html>

## ANEXO 1: MATRIZ DE CONSISTENCIA

### SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y LA CALIDAD DEL SERVICIO INFORMÁTICO DE LA UNAM-2024

| Problema General   | Objetivo general   | Hipótesis general   | Metodología  |   |   |
|--|--|---|--|---|---|
|  |  |   | Variable   | Dimensiones   |   |
| ¿Cuál es la relación entre el Sistema de Gestión de Seguridad de la Información y la Calidad del Servicio Informático en la UNAM-2024? | Determinar si la relación entre el Sistema de Gestión de Seguridad de la información y la Calidad del Servicio Informático de la UNAM-2024 | El Sistema de Gestión de Seguridad de la Información y la Calidad del Servicio Informático se relacionan significativamente en la UNAM-2024 | X: Sistema de Gestión de Seguridad de la Información | X1: Principios de seguridad de la información<br>X2: ISSO/IEC 27001<br>X3: GSI<br>X4: Implantación SGSI | <b>Tipo de investigación:</b><br>Básica<br><br><b>Nivel de investigación:</b><br>Descriptivo correlacional<br><br><b>Método de investigación:</b><br>hipotético-deductivo |
| Problemas específicos  | Objetivos específicos  | Hipótesis específicas   | Variable   | Dimensiones   | <b>Diseño de investigación:</b>   |

|  |   |   |  |   |  |
|--|---|---|--|---|--|
| <ul style="list-style-type: none"> <li>• ¿Cuál es la relación entre el principio de seguridad de la Información y la Calidad del Servicio Informático en la UNAM-2024?</li> <li>• ¿Cuál es la relación entre la Norma ISO/TEC 270001 con la Calidad del Servicio Informático en la UNAM-2024?</li> <li>• Cuál es la relación entre el Sistema de gestión de información y la Calidad del Servicio Informático en la UNAM-2024?</li> <li>• ¿Cuál es la relación entre la implantación del sistema de gestión de seguridad informática y la Calidad del Servicio Informático en la UNAM-2024?</li> </ul> | <ul style="list-style-type: none"> <li>• Diagnosticar los principios de seguridad de la Información en relación con el sistema de gestión de seguridad de la información y la calidad del servicio informático.</li> <li>• Analizar la Norma ISO/IEC 27001 en relación con la calidad del servicio informático.</li> <li>• Determinar la relación del sistema de gestión de seguridad de la información con la calidad del servicio informático.</li> <li>• Evaluar la implantación de la Norma ISO/IEC 270001 en relación con el sistema de gestión de seguridad de la información y la calidad del servicio informático.</li> </ul> | <ul style="list-style-type: none"> <li>• Los principios básicos del sistema de gestión de seguridad de la información ISO 27001 se relacionan significativamente con la calidad del servicio informático en la UNAM-2024.</li> <li>• La Norma ISO/IEC se relaciona significativamente con la calidad del servicio informático en la UNAM,-2024</li> <li>• La gestión de seguridad de la información se relaciona con la calidad del servicio informático en la UNAM,-2024</li> <li>• La implantación de la Norma ISO/IEC 27001 del SGI se relaciona significativamente con la calidad del servicio informático en la UNAM-2024</li> </ul> | <p>Y: Calidad del servicio informático</p> | <p>Y1: Fiabilidad del servicio<br/>Y2: Capacidad de respuesta<br/>Y3: Capacitación del personal<br/>Y4: Atención al cliente</p> | <p>diseño no experimental</p> <p><b>Población:</b> 92 docentes</p> <p><b>Muestra:</b> 92 docentes(censal).</p> <p><b>Técnica:</b> La encuesta</p> <p><b>Instrumento:</b> El cuestionario</p> |
|--|---|---|--|---|--|

## ANEXO 2: CUESTIONARIOS

### Sistema de Gestión de la Seguridad de la Información (SGSI)

Es un gusto ponerme en contacto con usted para hacerle llegar este cuestionario, que tiene como objetivo recopilar información sobre el Sistema de Gestión de seguridad de la información (SGSI), en la UNAM. Le aclaro que este cuestionario es anónimo.

Agradezco de su atención y colaboración. A continuación, encontrará una serie de preguntas; le solicito que las lea con atención y marque con una X en el casillero correspondiente, considerando la siguiente escala de valoración:

|                          |               |                                |            |                       |
|--------------------------|---------------|--------------------------------|------------|-----------------------|
| 1                        | 2             | 3                              | 4          | 5                     |
| Totalmente en desacuerdo | En desacuerdo | Ni de acuerdo Ni en desacuerdo | De acuerdo | Totalmente de acuerdo |

| <b>Variable:</b> Sistema de Gestión de la Seguridad de la Información (SGSI) |  |   |   |   |   |   |
|--|--|---|---|---|---|---|
| N°   | Dimensión: Principios de Seguridad de la Información   | 1 | 2 | 3 | 4 | 5 |
| 1  | ¿La Universidad cuenta con directrices, normativas o estándares establecidos para resguardar la información de los usuarios que emplean los sistemas informáticos?   |   |   |   |   |   |
| 2  | ¿La Universidad ha establecido un control adecuado y seguro para gestionar el acceso de los usuarios a sus sistemas informáticos?                                    |   |   |   |   |   |
| 3  | ¿La Universidad ha establecido un control adecuado para gestionar los niveles de autorización necesarios para acceder a la información en sus sistemas informáticos? |   |   |   |   |   |
| 4  | ¿La Universidad ha establecido controles efectivos para prevenir la modificación o pérdida parcial o total de la información en sus sistemas informáticos?           |   |   |   |   |   |
| 5  | ¿La Universidad ha establecido procesos o procedimientos para recuperar la información en caso   |   |   |   |   |   |

|   |   |  |  |  |  |  |
|---|---|--|--|--|--|--|
|   | de pérdida o modificación, ya sea intencional o accidental?   |  |  |  |  |  |
| 6   | ¿La Universidad ha establecido procesos o procedimientos para proteger la integridad de la información en sus sistemas informáticos?  |  |  |  |  |  |
| 7   | ¿La Universidad supervisa y evalúa el cumplimiento adecuado de las normas y procedimientos destinados a garantizar la continuidad del servicio en sus sistemas informáticos?  |  |  |  |  |  |
| 8   | ¿La Universidad ha establecido mecanismos para garantizar la continuidad y disponibilidad de los sistemas informáticos para sus usuarios?   |  |  |  |  |  |
| 9   | ¿La Universidad administra y evalúa de manera adecuada los tiempos de respuesta de los sistemas informáticos para los usuarios?   |  |  |  |  |  |
| <b>Dimensión: ISO/IEC 27001</b>                                 |   |  |  |  |  |  |
| 10  | ¿Cuál es su grado de conocimiento actual respecto a la norma ISO/IEC 27001 y la gestión de la seguridad de la información según la norma ISO/17799?   |  |  |  |  |  |
| 11  | ¿Estaría de acuerdo en que la Universidad le brinde capacitación sobre las normas ISO/IEC 27001 e ISO 17799, con el objetivo de conocer los requisitos que abarcan y aplicarlos en el desarrollo de sus actividades y en la gestión de los sistemas informáticos? |  |  |  |  |  |
| <b>Dimensión: Gestión de Seguridad de la Información (SGSI)</b> |   |  |  |  |  |  |
| 12  | ¿Los sistemas de gestión implementados por la Universidad han logrado cumplir los objetivos establecidos en relación con la seguridad de los sistemas informáticos?   |  |  |  |  |  |
| 13  | ¿Cree que los sistemas de gestión implementados para respaldar los procesos de la Universidad aplican la estrategia de mejora continua en lo que respecta a la seguridad de la información?   |  |  |  |  |  |

|  |   |  |  |  |  |  |
|--|---|--|--|--|--|--|
| 14   | ¿Cree usted que la implementación de un Sistema de Gestión de Seguridad de la Información contribuirá a gestionar la información y los recursos informáticos de forma óptima y segura en la Universidad?  |  |  |  |  |  |
| 15   | ¿Cree usted que al adaptar y aplicar la norma ISO/IEC 27001, basándose en los principios de la ISO 17799, se garantizará la integridad, confidencialidad y disponibilidad de la información en los sistemas informáticos?                                   |  |  |  |  |  |
| 16   | ¿Considera que a través de políticas de seguridad es posible asegurar niveles adecuados de protección de la información que cumplan con los requisitos de nuestros grupos de interés dentro de la Universidad?  |  |  |  |  |  |
| 17   | ¿Considera que es fundamental que la Universidad lleve a cabo el análisis y diseño de un Sistema de Gestión de Seguridad de la Información (SGSI) para proteger los activos informáticos?   |  |  |  |  |  |
| 18   | ¿Cree que la implementación de indicadores de seguridad de la información en la Universidad ayudará a medir el desempeño de los sistemas informáticos?  |  |  |  |  |  |
| <b>Dimensión:</b> Implantación de Sistema de Gestión de Seguridad de la Información. |   |  |  |  |  |  |
| 19   | ¿Percibe que hay un compromiso por parte de las autoridades universitarias para establecer un sistema de gestión de seguridad de la información?  |  |  |  |  |  |
| 20   | ¿Está al tanto de los riesgos que pueden presentarse durante el desarrollo de su trabajo en relación con la seguridad de la información en la Universidad?  |  |  |  |  |  |
| 21   | ¿Considera que la institución cuenta con los recursos necesarios para implementar un plan de tratamiento de riesgos de seguridad de la información si se establece un sistema de gestión de seguridad de la información en el proceso de registros civiles? |  |  |  |  |  |

|    |  |  |  |  |  |  |
|----|--|--|--|--|--|--|
| 22 | ¿Cree que la implementación de la declaración de aplicabilidad dentro del marco de seguridad de la información ayuda a validar los controles de seguridad de la información más adecuados para la Universidad? |  |  |  |  |  |
|----|--|--|--|--|--|--|

### Calidad del Servicio Informático

Es un gusto ponerme en contacto con usted para hacerle llegar este cuestionario, que tiene como objetivo recopilar información sobre la Calidad del Servicio Informático en la UNAM. Le aclaro que este cuestionario es anónimo.

Agradezco de su atención y colaboración. A continuación, encontrará una serie de preguntas; le solicito que las lea con atención y marque con una X en el casillero correspondiente, considerando la siguiente escala de valoración:

| 1  | 2   | 3                                    | 4          | 5                     |   |   |
|--|---|--------------------------------------|------------|-----------------------|---|---|
| Totalmente en desacuerdo                 | En desacuerdo   | Ni de acuerdo<br>Ni en<br>desacuerdo | De acuerdo | Totalmente de acuerdo |   |   |
| <b>Variable:</b> Calidad del Servicio    |   |                                      |            |                       |   |   |
| N°                                       | Dimensión: Fiabilidad   | 1                                    | 2          | 3                     | 4 | 5 |
| 1  | Cuando la empresa de servicios se compromete a realizar una tarea en un plazo determinado, lo cumple. |                                      |            |                       |   |   |
| 2  | Cuando un cliente enfrenta un problema, la empresa demuestra un genuino interés en resolverlo.        |                                      |            |                       |   |   |
| 3  | La empresa lleva a cabo el servicio correctamente desde el primer intento.                            |                                      |            |                       |   |   |
| 4  | La empresa finaliza el servicio dentro del plazo acordado.  |                                      |            |                       |   |   |
| 5  | La empresa de servicios se esfuerza por permanecer libre de errores.                                  |                                      |            |                       |   |   |
| 6  | La empresa de servicios cumple de forma constante con tus expectativas y compromisos.                 |                                      |            |                       |   |   |
| <b>Dimensión:</b> Capacidad de respuesta |   |                                      |            |                       |   |   |
| 7  | Los empleados informan a los clientes sobre cuándo se completará el servicio.                         |                                      |            |                       |   |   |

|   |  |  |  |  |  |  |
|---|--|--|--|--|--|--|
| 8   | Los empleados de la empresa brindan un servicio ágil a sus clientes.   |  |  |  |  |  |
| 9   | Los empleados de la empresa de servicios siempre están disponibles para asistir a sus clientes.  |  |  |  |  |  |
| 10  | Los empleados nunca están tan ocupados que no puedan atender las preguntas de sus clientes.  |  |  |  |  |  |
| 11  | Los empleados de la empresa de servicios aclaran tus preguntas y preocupaciones.   |  |  |  |  |  |
| <b>Dimensión: Capacitación del personal</b> |  |  |  |  |  |  |
| 12  | La actitud de los empleados de la empresa de servicios genera confianza en sus clientes.   |  |  |  |  |  |
| 13  | Los clientes se sienten confiados en sus interacciones con la empresa de servicios.  |  |  |  |  |  |
| 14  | Los empleados de la empresa de servicios son siempre corteses con los clientes.  |  |  |  |  |  |
| 15  | Los empleados poseen los conocimientos necesarios para responder a las preguntas de los clientes.  |  |  |  |  |  |
| 16  | Los empleados de la empresa de servicios crees que están preparados para manejar las situaciones que puedan surgir en el servicio informático. |  |  |  |  |  |
| <b>Dimensión: Atención al cliente</b>       |  |  |  |  |  |  |
| 17  | La empresa de servicios proporciona a sus clientes un servicio personalizado.  |  |  |  |  |  |
| 18  | La empresa de servicios cuenta con horarios accesibles para todos sus clientes.  |  |  |  |  |  |
| 19  | El personal de servicio fue amable en sus interacciones con los clientes.  |  |  |  |  |  |
| 20  | La empresa de servicios se interesa por las necesidades de sus clientes.   |  |  |  |  |  |
| 21  | La empresa de servicios entiende las necesidades particulares de sus clientes.   |  |  |  |  |  |
| 22  | La empresa de servicios te brinda atención de inmediato cuando solicitas ayuda.  |  |  |  |  |  |

## ANEXO 3: FICHAS DE VALIDACIÓN DE EXPERTOS

### FICHA DE VALIDACION DE INSTRUMENTO

#### I. DATOS GENERALES

- 1.1 Apellidos y nombres del experto: RAMIREZ JULCA MÁXIMO
- 1.2 Grado académico: DOCTOR
- 1.3 Cargo e institución donde labora: DTC UAP
- 1.4 Título de la Investigación: Sistema de Gestión de Seguridad de la Información y la Calidad del Servicio Informático de la Universidad Nacional de Moquegua-2024
- 1.5 Autor del instrumento: Mag. Hansi Elorrieta Rondón
- 1.6 Doctorado en Ingeniería de Sistemas
- 1.7 Nombre del instrumento: Cuestionario

| INDICADORES        | CRITERIOS CUALITATIVOS/CUANTITATIVOS                                | Deficiente 0-20% | Regular 21-40% | Bueno 41-60% | Muy Bueno 61-80% | Excelente 81-100% |
|--------------------|---|------------------|----------------|--------------|------------------|-------------------|
| 1. CLARIDAD        | Está formulado con lenguaje apropiado.                              |                  |                |              |                  | 90                |
| 2. OBJETIVIDAD     | Está expresado en conductas observables.                            |                  |                |              |                  | 90                |
| 3. ACTUALIDAD      | Adecuado al alcance de ciencia y tecnología.                        |                  |                |              |                  | 90                |
| 4. ORGANIZACION    | Existe una organización lógica.                                     |                  |                |              |                  | 90                |
| 5. SUFICIENCIA     | Comprende los aspectos de cantidad y calidad.                       |                  |                |              |                  | 90                |
| 6. INTENCIONALIDAD | Adecuado para valorar aspectos del estudio.                         |                  |                |              |                  | 90                |
| 7. CONSISTENCIA    | Basados en aspectos Teóricos-Científicos y del tema de estudio.     |                  |                |              |                  | 90                |
| 8. COHERENCIA      | Entre los índices, indicadores, dimensiones y variables.            |                  |                |              |                  | 90                |
| 9. METODOLOGIA     | La estrategia responde al propósito del estudio.                    |                  |                |              |                  | 90                |
| 10. CONVENIENCIA   | Genera nuevas pautas en la investigación y construcción de teorías. |                  |                |              |                  | 90                |
| <b>SUB TOTAL</b>   |   |                  |                |              |                  | 90                |
| <b>TOTAL</b>       |   |                  |                |              |                  | 90/10=90          |

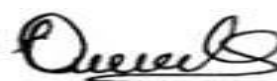
VALORACION CUANTITATIVA (Total x

0.20) : 18 VALORACION CUALITATIVA:

Excelente OPINIÓN DE APLICABILIDAD:

Aplicable

Lima, 14 setiembre 2024



.....  
Dr. Máximo Ramírez Julca

ORCID: 0000-0002-1385-3139

## FICHA DE VALIDACION DE INSTRUMENTO

### IDATOS GENERALES

- 1.1 Apellidos y nombres del experto: PEDRO SOLIS CESPEDES
- 1.2 Grado académico: DOCTOR
- 1.3 Cargo e institución donde labora: DTC UAP
- 1.4 Título de la Investigación: Sistema de Gestión de la Información y la Calidad del Servicio Informático de la Universidad Nacional de Moquegua-2024
- 1.5 Autor del instrumento: Mag. Hansi Elorrieta Rondón
- 1.6 Doctorado en Ingeniería de Sistemas
- 1.7 Nombre del instrumento: Cuestionario

| INDICADORES        | CRITERIOS CUALITATIVOS/CUANTITATIVOS                                | Deficiente 0-20% | Regular 21-40% | Bueno 41-60% | Muy Bueno 61-80% | Excelente 81-100% |
|--------------------|---|------------------|----------------|--------------|------------------|-------------------|
| 1. CLARIDAD        | Está formulado con lenguaje apropiado.                              |                  |                |              |                  | 90                |
| 2. OBJETIVIDAD     | Está expresado en conductas observables.                            |                  |                |              |                  | 90                |
| 3. ACTUALIDAD      | Adecuado al alcance de ciencia y tecnología.                        |                  |                |              |                  | 90                |
| 4. ORGANIZACIÓN    | Existe una organización lógica.                                     |                  |                |              |                  | 90                |
| 5. SUFICIENCIA     | Comprende los aspectos de cantidad y calidad.                       |                  |                |              |                  | 90                |
| 6. INTENCIONALIDAD | Adecuado para valorar aspectos del estudio.                         |                  |                |              |                  | 90                |
| 7. CONSISTENCIA    | Basados en aspectos Teóricos-Científicos y del tema de estudio.     |                  |                |              |                  | 90                |
| 8. COHERENCIA      | Entre los índices, indicadores, dimensiones y variables.            |                  |                |              |                  | 90                |
| 9. METODOLOGIA     | La estrategia responde al propósito del estudio.                    |                  |                |              |                  | 90                |
| 10. CONVENIENCIA   | Genera nuevas pautas en la investigación y construcción de teorías. |                  |                |              |                  | 90                |
| <b>SUB TOTAL</b>   |   |                  |                |              |                  | 900               |
| <b>TOTAL</b>       |   |                  |                |              |                  | 90/10=90          |

**VALORACION CUANTITATIVA (Total x 0.20) : 18**

**VALORACION CUALITATIVA: Excelente**

**OPINIÓN DE APLICABILIDAD: Aplicable**

Lima, 14 setiembre 2024



.....  
Dr. Pedro Solís Céspedes

ORCID: 0000-0002-7339-8721

## FICHA DE VALIDACION DE INSTRUMENTO

### IDATOS GENERALES

- 1.1 Apellidos y nombres del experto: **BRINGAS SALVADOR JORGE LUIS**
- 1.2 Grado académico: **DOCTOR**
- 1.3 Cargo e institución donde labora: **DTC UAP**
- 1.4 Título de la Investigación: **Sistema de Gestión de Seguridad de la información y la Calidad del Servicio Informático de la Universidad Nacional de Moquegua, año 2024**
- 1.5 Autor del instrumento: **Mag. Hansi Elorrieta Rondón**
- 1.6 Doctorado en Ingeniería de Sistemas
- 1.7 Nombre del instrumento: **Cuestionario**

| INDICADORES        | CRITERIOS CUALITATIVOS/CUANTITATIVOS                                | Deficiente 0-20% | Regular 21-40% | Bueno 41-60% | Muy Bueno 61-80% | Excelente 81-100% |
|--------------------|---|------------------|----------------|--------------|------------------|-------------------|
| 1. CLARIDAD        | Está formulado con lenguaje apropiado.                              |                  |                |              |                  | 90                |
| 2. OBJETIVIDAD     | Está expresado en conductas observables.                            |                  |                |              |                  | 90                |
| 3. ACTUALIDAD      | Adecuado al alcance de ciencia y tecnología.                        |                  |                |              |                  | 90                |
| 4. ORGANIZACIÓN    | Existe una organización lógica.                                     |                  |                |              |                  | 90                |
| 5. SUFICIENCIA     | Comprende los aspectos de cantidad y calidad.                       |                  |                |              |                  | 90                |
| 6. INTENCIONALIDAD | Adecuado para valorar aspectos del estudio.                         |                  |                |              |                  | 90                |
| 7. CONSISTENCIA    | Basados en aspectos Teóricos-Científicos y del tema de estudio.     |                  |                |              |                  | 90                |
| 8. COHERENCIA      | Entre los índices, indicadores, dimensiones y variables.            |                  |                |              |                  | 90                |
| 9. METODOLOGIA     | La estrategia responde al propósito del estudio.                    |                  |                |              |                  | 90                |
| 10. CONVENIENCIA   | Genera nuevas pautas en la investigación y construcción de teorías. |                  |                |              |                  | 90                |
| <b>SUB TOTAL</b>   |   |                  |                |              |                  | 900               |
| <b>TOTAL</b>       |   |                  |                |              |                  | 900/10=90         |

**VALORACION CUANTITATIVA (Total x 0.20) : 18**

**VALORACION CUALITATIVA: Excelente**

**OPINIÓN DE APLICABILIDAD: Aplicable**

**Lima, 04 octubre 2024**



.....  
**Dr. Jorge Bringas Salvador**

**ORCID: 0000-0003-2011-4964**

### ANEXO 04. COPIA DE LA DATA PROCESADA

| Encuestado | Sistema de Gestión de la Seguridad de la Información (SGSI) |    |    |    |    |    |    |    |    |               |   |     |     |     |     |     |                                       |            |     | Calidad del Servicio Informático |     |                        |     |     |    |                           |    |    |    |                     |    |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |   |   |
|------------|---|----|----|----|----|----|----|----|----|---------------|---|-----|-----|-----|-----|-----|---------------------------------------|------------|-----|----------------------------------|-----|------------------------|-----|-----|----|---------------------------|----|----|----|---------------------|----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|---|---|
|            | Principios de Seguridad de la Información                   |    |    |    |    |    |    |    |    | ISO/IEC 27001 | Gestión de Seguridad de la Información (SGSI) |     |     |     |     |     | Implantación de Sistema de Gestión de | Fiabilidad |     |                                  |     | Capacidad de respuesta |     |     |    | Capacitación del personal |    |    |    | Atención al cliente |    |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |   |   |
|            | P1  | P2 | P3 | P4 | P5 | P6 | P7 | P8 | P9 |               | P10   | P11 | P12 | P13 | P14 | P15 |                                       | P16        | P17 | P18                              | P19 | P20                    | P21 | P22 | P1 | P2                        | P3 | P4 | P5 | P6                  | P7 | P8  | P9  | P10 | P11 | P12 | P13 | P14 | P15 | P16 | P17 | P18 | P19 | P20 | P21 | P22 |   |   |
|            | P1  | P2 | P3 | P4 | P5 | P6 | P7 | P8 | P9 | P10           | P11   | P12 | P13 | P14 | P15 | P16 | P17                                   | P18        | P19 | P20                              | P21 | P22                    | P1  | P2  | P3 | P4                        | P5 | P6 | P7 | P8                  | P9 | P10 | P11 | P12 | P13 | P14 | P15 | P16 | P17 | P18 | P19 | P20 | P21 | P22 |     |     |   |   |
| 1          | 3   | 3  | 4  | 2  | 4  | 3  | 5  | 5  | 3  | 3             | 4   | 3   | 3   | 2   | 3   | 2   | 2                                     | 2          | 3   | 2                                | 2   | 2                      | 3   | 4   | 3  | 3                         | 2  | 3  | 5  | 4                   | 3  | 4   | 2   | 5   | 4   | 5   | 5   | 3   | 2   | 2   | 2   | 2   | 2   | 2   |     |     |   |   |
| 2          | 2   | 2  | 2  | 3  | 2  | 2  | 2  | 3  | 2  | 2             | 2   | 2   | 2   | 3   | 2   | 4   | 3                                     | 4          | 5   | 5                                | 2   | 4                      | 2   | 2   | 2  | 2                         | 3  | 2  | 2  | 2                   | 2  | 2   | 2   | 2   | 2   | 2   | 2   | 4   | 2   | 4   | 2   | 2   | 3   | 4   |     |     |   |   |
| 3          | 3   | 3  | 4  | 3  | 5  | 3  | 4  | 5  | 4  | 5             | 3   | 5   | 2   | 4   | 3   | 4   | 5                                     | 3          | 3   | 3                                | 5   | 3                      | 5   | 3   | 5  | 2                         | 4  | 3  | 5  | 3                   | 2  | 4   | 2   | 3   | 5   | 5   | 3   | 2   | 4   | 4   | 4   | 2   | 4   | 3   |     |     |   |   |
| 4          | 4   | 5  | 3  | 3  | 3  | 5  | 3  | 3  | 5  | 2             | 4   | 3   | 2   | 3   | 4   | 3   | 3                                     | 4          | 2   | 5                                | 4   | 2                      | 2   | 4   | 3  | 2                         | 3  | 4  | 2  | 3                   | 4  | 2   | 4   | 4   | 4   | 4   | 2   | 4   | 4   | 3   | 5   | 3   | 4   | 4   | 5   |     |   |   |
| 5          | 4   | 4  | 2  | 3  | 3  | 4  | 5  | 4  | 2  | 4             | 4   | 3   | 5   | 5   | 2   | 2   | 2                                     | 3          | 2   | 2                                | 2   | 4                      | 4   | 3   | 5  | 5                         | 2  | 5  | 5  | 3                   | 4  | 4   | 4   | 4   | 4   | 4   | 5   | 3   | 2   | 2   | 2   | 2   | 2   | 2   |     |     |   |   |
| 6          | 5   | 4  | 3  | 5  | 5  | 4  | 4  | 2  | 5  | 4             | 5   | 4   | 5   | 5   | 4   | 4   | 3                                     | 4          | 5   | 5                                | 2   | 4                      | 4   | 5   | 4  | 5                         | 5  | 4  | 5  | 5                   | 4  | 3   | 5   | 4   | 5   | 4   | 4   | 2   | 4   | 2   | 4   | 2   | 2   | 3   | 4   |     |   |   |
| 7          | 5   | 5  | 2  | 2  | 5  | 3  | 2  | 2  | 3  | 2             | 2   | 4   | 3   | 4   | 4   | 5   | 3                                     | 3          | 5   | 3                                | 5   | 3                      | 5   | 3   | 2  | 2                         | 4  | 3  | 4  | 4                   | 3  | 3   | 4   | 4   | 4   | 4   | 3   | 4   | 4   | 4   | 4   | 4   | 2   | 4   | 3   |     |   |   |
| 8          | 3   | 2  | 3  | 4  | 5  | 5  | 2  | 5  | 5  | 3             | 5   | 2   | 5   | 4   | 3   | 3   | 4                                     | 5          | 2   | 5                                | 2   | 4                      | 3   | 5   | 2  | 5                         | 4  | 3  | 5  | 5                   | 5  | 5   | 5   | 5   | 5   | 5   | 5   | 4   | 4   | 2   | 5   | 5   | 4   | 3   | 4   | 2   | 4 |   |
| 9          | 4   | 2  | 4  | 2  | 3  | 5  | 5  | 5  | 2  | 2             | 4   | 4   | 3   | 3   | 3   | 2   | 4                                     | 4          | 5   | 4                                | 5   | 4                      | 2   | 4   | 4  | 3                         | 3  | 3  | 2  | 3                   | 4  | 5   | 2   | 2   | 2   | 2   | 5   | 4   | 4   | 5   | 5   | 5   | 4   | 5   | 4   |     |   |   |
| 10         | 3   | 3  | 5  | 2  | 4  | 4  | 5  | 5  | 3  | 4             | 5   | 2   | 4   | 5   | 3   | 5   | 2                                     | 2          | 2   | 3                                | 3   | 3                      | 4   | 5   | 2  | 4                         | 5  | 2  | 5  | 5                   | 5  | 5   | 5   | 5   | 5   | 5   | 3   | 4   | 3   | 5   | 3   | 2   | 5   | 3   | 5   | 3   | 2 |   |
| 11         | 3   | 4  | 3  | 3  | 4  | 2  | 2  | 4  | 5  | 3             | 5   | 5   | 5   | 3   | 3   | 5   | 3                                     | 3          | 4   | 2                                | 5   | 3                      | 5   | 5   | 5  | 3                         | 3  | 5  | 5  | 3                   | 4  | 2   | 5   | 5   | 2   | 5   | 4   | 2   | 3   | 3   | 3   | 2   | 4   |     |     |     |   |   |
| 12         | 5   | 4  | 4  | 4  | 5  | 5  | 4  | 5  | 4  | 4             | 5   | 2   | 5   | 4   | 3   | 2   | 2                                     | 3          | 2   | 2                                | 2   | 4                      | 5   | 2   | 5  | 4                         | 3  | 5  | 4  | 3                   | 2  | 2   | 4   | 5   | 5   | 2   | 3   | 2   | 2   | 2   | 2   | 2   | 2   | 2   | 2   |     |   |   |
| 13         | 5   | 5  | 5  | 5  | 3  | 5  | 4  | 4  | 5  | 2             | 4   | 5   | 5   | 5   | 2   | 3   | 3                                     | 4          | 3   | 5                                | 3   | 4                      | 2   | 4   | 5  | 5                         | 5  | 2  | 2  | 5                   | 3  | 4   | 4   | 4   | 3   | 5   | 3   | 4   | 2   | 3   | 5   | 5   | 3   | 5   |     |     |   |   |
| 14         | 5   | 5  | 4  | 5  | 4  | 5  | 5  | 2  | 2  | 5             | 4   | 4   | 5   | 2   | 5   | 4   | 5                                     | 3          | 3   | 3                                | 5   | 3                      | 5   | 4   | 4  | 5                         | 2  | 5  | 5  | 5                   | 5  | 4   | 5   | 4   | 5   | 4   | 5   | 4   | 5   | 2   | 4   | 4   | 4   | 2   | 4   | 3   |   |   |
| 15         | 2   | 2  | 2  | 2  | 3  | 2  | 2  | 2  | 2  | 2             | 2   | 2   | 2   | 2   | 3   | 4   | 4                                     | 2          | 3   | 3                                | 4   | 5                      | 2   | 2   | 2  | 2                         | 2  | 3  | 3  | 2                   | 2  | 3   | 5   | 2   | 2   | 2   | 2   | 4   | 4   | 4   | 4   | 4   | 5   | 3   |     |     |   |   |
| 16         | 2   | 5  | 3  | 4  | 2  | 4  | 5  | 3  | 2  | 4             | 3   | 2   | 4   | 2   | 3   | 5   | 4                                     | 3          | 5   | 5                                | 4   | 4                      | 4   | 3   | 2  | 4                         | 2  | 3  | 3  | 2                   | 3  | 3   | 3   | 2   | 5   | 3   | 3   | 4   | 3   | 5   | 4   | 5   | 4   | 4   |     |     |   |   |
| 17         | 3   | 3  | 3  | 5  | 5  | 3  | 5  | 4  | 3  | 4             | 2   | 4   | 3   | 5   | 2   | 5   | 5                                     | 2          | 2   | 5                                | 3   | 2                      | 4   | 2   | 4  | 3                         | 5  | 2  | 3  | 3                   | 5  | 3   | 4   | 5   | 4   | 3   | 2   | 4   | 4   | 3   | 4   | 3   | 4   | 4   |     |     |   |   |
| 18         | 3   | 2  | 3  | 3  | 5  | 5  | 5  | 4  | 3  | 3             | 4   | 3   | 3   | 5   | 4   | 3   | 2                                     | 3          | 4   | 5                                | 2   | 3                      | 4   | 3   | 3  | 5                         | 4  | 5  | 4  | 5                   | 2  | 3   | 4   | 4   | 5   | 3   | 4   | 2   | 5   | 2   | 2   | 2   | 2   | 2   |     |     |   |   |
| 19         | 5   | 5  | 5  | 2  | 5  | 2  | 5  | 4  | 3  | 5             | 5   | 5   | 4   | 5   | 4   | 2   | 4                                     | 2          | 3   | 5                                | 5   | 3                      | 5   | 5   | 5  | 4                         | 5  | 5  | 3  | 3                   | 4  | 2   | 5   | 4   | 5   | 5   | 5   | 3   | 4   | 2   | 5   | 2   | 2   | 5   | 4   | 4   |   |   |
| 20         | 2   | 2  | 2  | 3  | 2  | 2  | 2  | 2  | 2  | 2             | 2   | 2   | 3   | 5   | 2   | 3   | 3                                     | 5          | 2   | 4                                | 4   | 5                      | 2   | 2   | 2  | 3                         | 5  | 2  | 2  | 2                   | 2  | 2   | 2   | 2   | 2   | 2   | 2   | 2   | 2   | 2   | 2   | 3   | 5   | 5   |     |     |   |   |
| 21         | 3   | 4  | 5  | 2  | 5  | 2  | 4  | 5  | 4  | 4             | 2   | 4   | 5   | 5   | 5   | 3   | 4                                     | 3          | 3   | 4                                | 2   | 2                      | 4   | 2   | 4  | 2                         | 4  | 5  | 5  | 5                   | 3  | 2   | 5   | 5   | 4   | 3   | 4   | 2   | 4   | 2   | 5   | 5   | 2   | 5   | 5   |     |   |   |
| 22         | 2   | 4  | 4  | 5  | 4  | 5  | 4  | 4  | 3  | 5             | 2   | 4   | 4   | 5   | 2   | 5   | 4                                     | 4          | 5   | 5                                | 4   | 5                      | 2   | 4   | 4  | 5                         | 2  | 5  | 4  | 4                   | 4  | 5   | 5   | 5   | 4   | 5   | 2   | 2   | 4   | 5   | 5   | 2   | 2   | 2   |     |     |   |   |
| 23         | 3   | 5  | 2  | 2  | 2  | 3  | 3  | 2  | 2  | 5             | 5   | 2   | 3   | 2   | 5   | 5   | 5                                     | 5          | 5   | 3                                | 5   | 4                      | 5   | 5   | 2  | 3                         | 2  | 5  | 3  | 4                   | 2  | 3   | 2   | 5   | 3   | 5   | 3   | 4   | 4   | 4   | 3   | 5   | 3   | 5   |     |     |   |   |
| 24         | 5   | 3  | 3  | 3  | 4  | 2  | 5  | 4  | 3  | 4             | 4   | 4   | 3   | 2   | 5   | 5   | 4                                     | 5          | 4   | 5                                | 5   | 4                      | 4   | 3   | 2  | 5                         | 5  | 2  | 3  | 4                   | 2  | 3   | 3   | 3   | 2   | 4   | 5   | 4   | 5   | 4   | 5   | 4   | 5   | 4   |     |     |   |   |
| 25         | 3   | 4  | 5  | 5  | 5  | 2  | 5  | 3  | 5  | 5             | 5   | 5   | 5   | 2   | 2   | 2   | 2                                     | 2          | 3   | 2                                | 2   | 5                      | 3   | 4   | 3  | 4                         | 5  | 5  | 5  | 5                   | 5  | 5   | 5   | 5   | 5   | 5   | 5   | 3   | 5   | 2   | 2   | 2   | 2   | 2   |     |     |   |   |
| 26         | 5   | 5  | 4  | 4  | 5  | 4  | 2  | 3  | 4  | 3             | 4   | 3   | 4   | 3   | 4   | 2   | 5                                     | 3          | 4   | 2                                | 4   | 5                      | 3   | 4   | 3  | 4                         | 3  | 4  | 5  | 5                   | 4  | 4   | 5   | 5   | 4   | 4   | 5   | 4   | 5   | 3   | 4   | 3   | 3   | 2   | 5   | 3   | 3 | 2 |
| 27         | 4   | 4  | 3  | 4  | 2  | 5  | 4  | 5  | 5  | 4             | 4   | 4   | 2   | 5   | 2   | 3   | 3                                     | 3          | 5   | 5                                | 3   | 5                      | 4   | 4   | 4  | 2                         | 5  | 2  | 5  | 3                   | 2  | 4   | 5   | 4   | 5   | 4   | 5   | 3   | 4   | 5   | 4   | 3   | 2   | 4   |     |     |   |   |
| 28         | 2   | 2  | 2  | 5  | 2  | 2  | 4  | 3  | 3  | 3             | 4   | 3   | 5   | 4   | 2   | 3   | 2                                     | 3          | 3   | 5                                | 5   | 5                      | 3   | 4   | 3  | 5                         | 4  | 2  | 2  | 3                   | 2  | 2   | 3   | 3   | 5   | 4   | 5   | 2   | 3   | 4   | 4   | 5   | 3   | 3   |     |     |   |   |
| 29         | 3   | 2  | 5  | 3  | 2  | 3  | 2  | 4  | 3  | 2             | 5   | 2   | 5   | 3   | 3   | 3   | 3                                     | 4          | 2   | 5                                | 4   | 2                      | 2   | 5   | 2  | 5                         | 3  | 3  | 3  | 4                   | 5  | 5   | 4   | 5   | 2   | 5   | 5   | 4   | 3   | 5   | 3   | 4   | 4   | 5   |     |     |   |   |
| 30         | 3   | 2  | 4  | 4  | 3  | 2  | 4  | 5  | 4  | 4             | 4   | 4   | 4   | 3   | 5   | 2   | 2                                     | 2          | 3   | 2                                | 2   | 2                      | 4   | 4   | 4  | 4                         | 3  | 5  | 2  | 3                   | 5  | 2   | 2   | 4   | 4   | 2   | 5   | 3   | 2   | 2   | 2   | 2   | 2   | 2   |     |     |   |   |
| 31         | 2   | 5  | 3  | 2  | 2  | 2  | 5  | 3  | 3  | 3             | 4   | 5   | 2   | 4   | 4   | 3   | 4                                     | 5          | 5   | 2                                | 4   | 3                      | 3   | 4   | 5  | 2                         | 4  | 2  | 3  | 4                   | 3  | 4   | 2   | 3   | 2   | 4   | 4   | 2   | 4   | 2   | 4   | 2   | 3   | 4   |     |     |   |   |
| 32         | 5   | 3  | 5  | 5  | 5  | 5  | 5  | 5  | 5  | 5             | 5   | 5   | 5   | 5   | 4   | 5   | 3                                     | 3          | 3   | 5                                | 3   | 5                      | 5   | 5   | 5  | 5                         | 5  | 5  | 5  | 4                   | 5  | 3   | 5   | 5   | 4   | 4   | 5   | 2   | 4   | 4   | 4   | 2   | 4   | 3   |     |     |   |   |
| 33         | 2   | 4  | 4  | 4  | 4  | 3  | 3  | 4  | 2  | 3             | 2   | 3   | 5   | 4   | 4   | 3   | 4                                     | 5          | 2   | 5                                | 2   | 4                      | 3   | 2   | 3  | 5                         | 4  | 4  | 5  | 3                   | 4  | 4   | 5   | 3   | 3   | 4   | 2   | 5   | 5   | 4   | 3   | 4   | 2   | 4   |     |     |   |   |
| 34         | 4   | 3  | 5  | 5  | 5  | 2  | 4  | 4  | 3  | 4             | 3   | 4   | 5   | 5   | 2   | 2   | 4                                     | 4          | 5   | 4                                | 5   | 4                      | 4   | 3   | 4  | 5                         | 5  | 2  | 4  | 4                   | 3  | 5   | 5   | 4   | 5   | 4   | 4   | 4   | 4   | 5   | 5   | 5   | 4   | 5   | 4   |     |   |   |
| 35         | 4   | 3  | 4  | 4  | 2  | 4  | 4  | 5  | 4  | 3             | 4   | 5   | 2   | 5   | 5   | 3   | 5                                     | 2          | 2   | 2                                | 3   | 3                      | 4   | 5   | 2  | 5                         | 5  | 5  | 4  | 4                   | 5  | 2   | 4   | 3   | 5   | 4   | 3   | 2   | 5   | 3   | 5   | 3   | 2   |     |     |     |   |   |
| 36         | 5   | 4  | 4  | 2  | 5  | 3  | 3  | 4  | 4  | 3             | 4   | 3   | 5   | 3   | 5   | 3   | 3                                     | 4          | 2   | 5                                | 3   | 4                      | 3   | 3   | 5  | 3                         | 5  | 4  | 5  | 5                   | 3  | 5   | 4   | 5   | 5   | 4   | 5   | 5   | 4   | 2   | 3   | 3   | 3   | 2   | 4   |     |   |   |
| 37         | 3   | 3  | 4  | 2  | 5  | 4  | 2  | 5  | 5  | 3             | 3   | 5   | 5   | 3   | 2   | 2   | 2                                     | 3          | 2   | 2                                | 2   | 3                      | 3   | 5   | 5  | 5                         | 3  | 4  | 3  | 2                   | 4  | 3   | 5   | 3   | 4   | 4   | 3   | 2   | 2   | 2   | 2   | 2   | 2   | 2   |     |     |   |   |
| 38         | 2   | 2  | 2  | 3  | 2  | 2  | 2  | 3  | 2  | 2             | 2   | 2   | 2   | 3   | 2   | 3   | 4                                     | 3          | 5   | 3                                | 4   | 2                      | 2   | 2   | 2  | 3                         | 2  | 2  | 2  | 2                   | 2  | 2   | 2   | 2   | 2   | 2   | 2   | 2   | 2   | 2   | 2   | 4   | 2   | 3   | 5   | 5   | 3 | 5 |
| 39         | 4   | 3  | 4  | 5  | 5  | 2  | 4  | 4  | 5  | 4             | 4   | 4   | 4   | 5   | 5   | 4   | 5                                     | 3          | 3   | 3                                | 5   | 3                      | 4   | 4   | 4  | 4                         | 5  | 5  | 4  | 3                   | 2  | 4   | 2   | 4   | 2   | 4   | 2   | 2   | 3   | 2   | 4   | 4   | 4   | 2   | 4   | 3   |   |   |
| 40         | 4   | 5  | 3  | 3  | 3  | 5  | 3  | 3  | 5  | 2             | 4   | 3   | 2   | 3   | 4   | 4   | 4                                     | 2          | 3   | 3                                | 4   | 5                      | 2   | 4   | 3  | 2                         | 3  | 4  | 2  | 3                   | 4  | 2   | 3   | 4   | 2   | 4   | 4   | 4   |     |     |     |     |     |     |     |     |   |   |

|    |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
|----|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 47 | 4 | 4 | 3 | 4 | 2 | 5 | 4 | 5 | 5 | 4 | 4 | 4 | 2 | 5 | 2 | 3 | 5 | 2 | 4 | 3 | 3 | 4 | 4 | 4 | 4 | 2 | 5 | 2 | 5 | 3 | 2 | 4 | 5 | 4 | 5 | 4 | 5 | 2 | 4 | 3 | 3 | 4 | 2 | 2 |   |   |   |
| 48 | 2 | 2 | 2 | 5 | 2 | 2 | 4 | 3 | 3 | 3 | 4 | 3 | 5 | 4 | 2 | 5 | 4 | 4 | 2 | 4 | 5 | 5 | 3 | 4 | 3 | 5 | 4 | 2 | 2 | 3 | 2 | 2 | 3 | 3 | 5 | 4 | 5 | 4 | 2 | 4 | 5 | 5 | 5 | 5 |   |   |   |
| 49 | 3 | 2 | 5 | 3 | 2 | 3 | 2 | 4 | 3 | 2 | 5 | 2 | 5 | 3 | 3 | 4 | 3 | 5 | 2 | 4 | 5 | 2 | 2 | 5 | 2 | 5 | 3 | 3 | 4 | 5 | 5 | 4 | 5 | 2 | 5 | 5 | 5 | 2 | 4 | 5 | 2 | 5 | 4 |   |   |   |   |
| 50 | 3 | 2 | 4 | 4 | 3 | 2 | 4 | 5 | 4 | 4 | 4 | 4 | 3 | 5 | 2 | 2 | 5 | 5 | 2 | 2 | 5 | 4 | 4 | 4 | 4 | 3 | 5 | 2 | 3 | 5 | 2 | 2 | 4 | 4 | 2 | 5 | 5 | 5 | 2 | 2 | 5 | 3 | 3 |   |   |   |   |
| 51 | 2 | 5 | 3 | 2 | 2 | 2 | 2 | 5 | 3 | 3 | 3 | 4 | 5 | 2 | 4 | 4 | 3 | 4 | 4 | 4 | 2 | 5 | 3 | 3 | 4 | 5 | 2 | 4 | 2 | 3 | 4 | 3 | 4 | 2 | 3 | 2 | 4 | 4 | 4 | 2 | 5 | 5 | 4 |   |   |   |   |
| 52 | 5 | 3 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 3 | 2 | 2 | 2 | 2 | 3 | 2 | 5 | 5 | 5 | 5 | 5 | 5 | 4 | 5 | 3 | 5 | 5 | 4 | 4 | 5 | 2 | 2 | 2 | 3 | 2 | 2 | 3 |   |   |   |   |   |
| 53 | 2 | 4 | 4 | 4 | 4 | 3 | 3 | 4 | 2 | 3 | 2 | 3 | 5 | 4 | 4 | 5 | 3 | 5 | 4 | 3 | 3 | 2 | 3 | 5 | 4 | 4 | 5 | 3 | 4 | 4 | 5 | 3 | 3 | 4 | 2 | 5 | 3 | 5 | 4 | 3 | 5 | 4 |   |   |   |   |   |
| 54 | 4 | 3 | 5 | 5 | 5 | 2 | 4 | 4 | 3 | 4 | 3 | 4 | 5 | 5 | 2 | 3 | 5 | 2 | 4 | 3 | 3 | 4 | 4 | 3 | 4 | 5 | 5 | 2 | 4 | 4 | 3 | 5 | 5 | 4 | 5 | 4 | 2 | 4 | 3 | 3 | 4 | 2 | 2 |   |   |   |   |
| 55 | 4 | 3 | 4 | 4 | 2 | 4 | 4 | 5 | 4 | 3 | 4 | 5 | 2 | 5 | 5 | 4 | 2 | 4 | 4 | 3 | 5 | 2 | 3 | 4 | 5 | 2 | 5 | 5 | 4 | 4 | 5 | 2 | 4 | 3 | 5 | 4 | 4 | 4 | 3 | 5 | 2 | 5 | 4 |   |   |   |   |
| 56 | 5 | 4 | 4 | 2 | 5 | 3 | 3 | 4 | 4 | 3 | 4 | 3 | 3 | 5 | 3 | 2 | 5 | 4 | 5 | 4 | 5 | 4 | 3 | 4 | 3 | 3 | 5 | 3 | 5 | 4 | 5 | 5 | 3 | 5 | 4 | 5 | 5 | 4 | 5 | 4 | 5 | 4 | 5 | 4 |   |   |   |
| 57 | 3 | 3 | 4 | 2 | 5 | 4 | 2 | 5 | 5 | 3 | 3 | 5 | 5 | 5 | 3 | 2 | 3 | 2 | 2 | 4 | 4 | 4 | 3 | 3 | 5 | 5 | 5 | 3 | 4 | 3 | 2 | 4 | 3 | 5 | 3 | 4 | 4 | 2 | 2 | 4 | 4 | 3 | 4 |   |   |   |   |
| 58 | 2 | 2 | 2 | 3 | 2 | 2 | 2 | 3 | 2 | 2 | 2 | 2 | 2 | 2 | 3 | 2 | 5 | 5 | 3 | 5 | 2 | 4 | 3 | 2 | 2 | 2 | 2 | 3 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 3 | 5 | 2 | 4 | 3 | 5 | 5 |   |   |   |   |
| 59 | 4 | 3 | 4 | 5 | 5 | 2 | 4 | 4 | 5 | 4 | 4 | 4 | 4 | 5 | 5 | 5 | 2 | 2 | 4 | 4 | 3 | 3 | 4 | 4 | 4 | 4 | 5 | 5 | 4 | 3 | 2 | 4 | 2 | 4 | 2 | 2 | 3 | 2 | 4 | 4 | 3 | 3 | 2 | 5 |   |   |   |
| 60 | 4 | 5 | 3 | 3 | 5 | 3 | 5 | 2 | 4 | 3 | 2 | 3 | 4 | 5 | 5 | 3 | 4 | 5 | 4 | 5 | 2 | 3 | 4 | 2 | 3 | 4 | 2 | 3 | 4 | 2 | 4 | 4 | 4 | 2 | 4 | 3 | 4 | 4 | 3 | 4 | 5 | 4 | 5 | 2 | 5 |   |   |
| 61 | 3 | 3 | 4 | 2 | 5 | 4 | 2 | 5 | 5 | 3 | 3 | 5 | 5 | 3 | 4 | 5 | 3 | 5 | 5 | 3 | 3 | 3 | 3 | 5 | 5 | 3 | 4 | 3 | 2 | 4 | 3 | 5 | 3 | 4 | 3 | 2 | 4 | 3 | 5 | 5 | 3 | 3 | 5 | 4 |   |   |   |
| 62 | 2 | 2 | 2 | 3 | 2 | 2 | 2 | 3 | 2 | 2 | 2 | 2 | 2 | 3 | 2 | 5 | 4 | 4 | 5 | 2 | 4 | 3 | 2 | 2 | 2 | 2 | 3 | 2 | 2 | 2 | 2 | 2 | 3 | 2 | 2 | 2 | 2 | 2 | 4 | 5 | 2 | 4 | 3 | 5 | 2 |   |   |
| 63 | 4 | 3 | 4 | 5 | 5 | 2 | 4 | 4 | 5 | 4 | 4 | 4 | 4 | 5 | 5 | 4 | 5 | 2 | 4 | 5 | 5 | 2 | 4 | 4 | 4 | 4 | 5 | 5 | 4 | 3 | 2 | 4 | 2 | 4 | 2 | 2 | 3 | 2 | 4 | 5 | 5 | 2 | 2 | 4 |   |   |   |
| 64 | 4 | 5 | 3 | 3 | 3 | 5 | 3 | 3 | 5 | 2 | 4 | 3 | 2 | 3 | 4 | 2 | 2 | 5 | 4 | 4 | 2 | 5 | 2 | 4 | 3 | 2 | 3 | 4 | 2 | 3 | 4 | 2 | 3 | 4 | 2 | 4 | 4 | 4 | 2 | 4 | 5 | 4 | 4 | 2 | 5 | 5 | 4 |
| 65 | 3 | 4 | 5 | 2 | 5 | 2 | 4 | 5 | 4 | 4 | 2 | 4 | 5 | 5 | 5 | 2 | 2 | 2 | 2 | 3 | 4 | 2 | 4 | 5 | 5 | 5 | 5 | 3 | 2 | 5 | 5 | 4 | 3 | 4 | 2 | 4 | 5 | 4 | 2 | 2 | 2 | 2 | 3 | 3 | 3 |   |   |
| 66 | 2 | 4 | 4 | 5 | 4 | 5 | 4 | 4 | 3 | 5 | 2 | 4 | 4 | 5 | 2 | 3 | 2 | 4 | 3 | 2 | 2 | 3 | 5 | 2 | 4 | 4 | 5 | 2 | 5 | 4 | 4 | 4 | 5 | 5 | 5 | 4 | 5 | 4 | 3 | 2 | 2 | 3 | 3 | 3 |   |   |   |
| 67 | 3 | 5 | 2 | 2 | 2 | 3 | 3 | 2 | 2 | 5 | 5 | 2 | 3 | 2 | 5 | 4 | 3 | 4 | 2 | 4 | 5 | 2 | 5 | 5 | 2 | 3 | 2 | 5 | 3 | 4 | 2 | 3 | 2 | 5 | 3 | 5 | 3 | 4 | 2 | 4 | 5 | 2 | 3 | 3 |   |   |   |
| 68 | 5 | 3 | 3 | 3 | 4 | 2 | 5 | 4 | 3 | 4 | 4 | 4 | 3 | 2 | 5 | 4 | 3 | 3 | 4 | 3 | 5 | 4 | 4 | 4 | 4 | 3 | 2 | 5 | 5 | 2 | 3 | 4 | 2 | 3 | 3 | 3 | 2 | 3 | 4 | 3 | 5 | 4 | 5 | 2 |   |   |   |
| 69 | 3 | 4 | 5 | 5 | 5 | 2 | 5 | 3 | 5 | 5 | 5 | 5 | 5 | 5 | 2 | 5 | 5 | 3 | 3 | 5 | 5 | 3 | 5 | 5 | 5 | 5 | 5 | 5 | 2 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 3 | 3 | 5 | 5 | 3 | 4 | 4 |   |
| 70 | 5 | 5 | 4 | 4 | 5 | 4 | 2 | 3 | 4 | 3 | 4 | 3 | 4 | 3 | 4 | 3 | 2 | 2 | 2 | 3 | 2 | 3 | 4 | 3 | 4 | 3 | 4 | 5 | 5 | 5 | 4 | 4 | 5 | 3 | 4 | 3 | 2 | 2 | 2 | 2 | 3 | 2 | 2 | 3 |   |   |   |
| 71 | 4 | 4 | 3 | 4 | 2 | 5 | 4 | 5 | 5 | 4 | 4 | 4 | 2 | 5 | 2 | 4 | 5 | 4 | 4 | 4 | 5 | 5 | 4 | 4 | 4 | 2 | 5 | 2 | 5 | 3 | 2 | 4 | 5 | 4 | 5 | 4 | 5 | 4 | 4 | 4 | 5 | 5 | 4 | 4 |   |   |   |

|    |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
|----|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 72 | 2 | 2 | 2 | 5 | 2 | 2 | 4 | 3 | 3 | 3 | 4 | 3 | 5 | 4 | 2 | 3 | 5 | 2 | 4 | 3 | 3 | 4 | 4 | 3 | 5 | 4 | 2 | 2 | 3 | 2 | 2 | 3 | 3 | 5 | 4 | 5 | 2 | 4 | 3 | 3 | 4 | 2 | 2 |   |   |   |   |
| 73 | 3 | 2 | 5 | 3 | 2 | 3 | 2 | 4 | 3 | 2 | 5 | 2 | 5 | 3 | 3 | 5 | 4 | 4 | 2 | 4 | 5 | 5 | 2 | 5 | 2 | 5 | 3 | 3 | 4 | 5 | 5 | 4 | 5 | 2 | 5 | 5 | 4 | 2 | 4 | 5 | 5 | 5 | 5 | 5 |   |   |   |
| 74 | 3 | 2 | 4 | 4 | 3 | 2 | 4 | 5 | 4 | 4 | 4 | 4 | 3 | 5 | 4 | 3 | 5 | 2 | 4 | 5 | 2 | 4 | 4 | 4 | 4 | 3 | 5 | 2 | 3 | 5 | 2 | 2 | 4 | 4 | 2 | 5 | 5 | 2 | 4 | 5 | 2 | 5 | 4 | 4 |   |   |   |
| 75 | 2 | 5 | 3 | 2 | 2 | 2 | 2 | 5 | 3 | 3 | 3 | 4 | 5 | 2 | 4 | 2 | 2 | 5 | 5 | 2 | 2 | 5 | 3 | 3 | 4 | 5 | 2 | 4 | 2 | 3 | 4 | 3 | 4 | 2 | 3 | 2 | 4 | 5 | 5 | 2 | 2 | 5 | 3 | 3 |   |   |   |
| 76 | 5 | 3 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 4 | 3 | 4 | 4 | 4 | 4 | 2 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 4 | 5 | 3 | 5 | 5 | 4 | 4 | 5 | 4 | 4 | 4 | 2 | 5 | 5 | 4 |   |   |   |
| 77 | 2 | 4 | 4 | 4 | 4 | 3 | 3 | 4 | 2 | 3 | 2 | 3 | 5 | 4 | 4 | 3 | 2 | 2 | 2 | 3 | 2 | 3 | 2 | 3 | 5 | 4 | 4 | 5 | 3 | 4 | 4 | 5 | 3 | 3 | 4 | 2 | 2 | 2 | 2 | 3 | 2 | 2 | 3 |   |   |   |   |
| 78 | 4 | 3 | 5 | 5 | 5 | 2 | 4 | 4 | 3 | 4 | 3 | 4 | 5 | 5 | 2 | 5 | 4 | 5 | 3 | 5 | 4 | 3 | 4 | 3 | 4 | 5 | 5 | 2 | 4 | 4 | 3 | 5 | 5 | 4 | 5 | 4 | 4 | 5 | 3 | 5 | 4 | 3 | 5 | 4 |   |   |   |
| 79 | 3 | 3 | 4 | 2 | 5 | 4 | 2 | 5 | 5 | 3 | 3 | 5 | 5 | 3 | 3 | 5 | 2 | 4 | 3 | 3 | 4 | 3 | 3 | 5 | 5 | 5 | 3 | 4 | 3 | 2 | 4 | 3 | 5 | 3 | 4 | 4 | 2 | 4 | 3 | 3 | 4 | 2 | 2 |   |   |   |   |
| 80 | 2 | 2 | 2 | 3 | 2 | 2 | 2 | 3 | 2 | 2 | 2 | 2 | 2 | 3 | 2 | 4 | 2 | 4 | 4 | 3 | 5 | 2 | 2 | 2 | 2 | 2 | 3 | 2 | 2 | 2 | 2 | 3 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 4 | 4 | 3 | 5 | 2 | 5 | 4 |   |
| 81 | 4 | 3 | 4 | 5 | 5 | 2 | 4 | 4 | 5 | 4 | 4 | 4 | 4 | 5 | 5 | 2 | 3 | 2 | 2 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 5 | 5 | 4 | 3 | 2 | 4 | 2 | 4 | 2 | 2 | 3 | 2 | 2 | 4 | 4 | 4 | 3 | 4 |   |   |   |
| 82 | 4 | 5 | 3 | 3 | 3 | 5 | 3 | 3 | 5 | 2 | 4 | 3 | 2 | 3 | 4 | 5 | 5 | 3 | 5 | 2 | 4 | 3 | 2 | 4 | 3 | 2 | 4 | 3 | 2 | 3 | 4 | 2 | 3 | 4 | 2 | 4 | 4 | 4 | 2 | 4 | 3 | 5 | 2 | 4 | 3 | 5 | 5 |
| 83 | 3 | 3 | 4 | 2 | 5 | 4 | 2 | 5 | 5 | 3 | 3 | 5 | 5 | 5 | 3 | 5 | 2 | 2 | 4 | 4 | 3 | 3 | 3 | 3 | 5 | 5 | 5 | 3 | 4 | 3 | 2 | 4 | 3 | 5 | 3 | 4 | 4 | 2 | 4 | 4 | 3 | 3 | 2 | 5 | 4 |   |   |
| 84 | 2 | 2 | 2 | 3 | 2 | 2 | 2 | 3 | 2 | 2 | 2 | 2 | 2 | 3 | 2 | 5 | 5 | 3 | 4 | 5 | 4 | 5 | 2 | 2 | 2 | 2 | 3 | 2 | 2 | 2 | 2 | 3 | 2 | 2 | 2 | 2 | 2 | 2 | 3 | 4 | 5 | 4 | 5 | 2 | 5 |   |   |
| 85 | 4 | 3 | 4 | 5 | 5 | 2 | 4 | 4 | 5 | 4 | 4 | 4 | 4 | 5 | 5 | 4 | 5 | 3 | 5 | 5 | 3 | 3 | 4 | 4 | 4 | 4 | 5 | 5 | 4 | 3 | 2 | 4 | 2 | 4 | 2 | 4 | 2 | 2 | 3 | 5 | 5 | 3 | 5 | 4 |   |   |   |
| 86 | 4 | 5 | 3 | 3 | 3 | 5 | 3 | 3 | 5 | 2 | 4 | 3 | 2 | 3 | 4 | 5 | 4 | 4 | 5 | 2 | 4 | 3 | 2 | 4 | 3 | 2 | 4 | 3 | 2 | 3 | 4 | 2 | 3 | 4 | 2 | 4 | 4 | 4 | 2 | 4 | 4 | 5 | 2 | 4 | 3 | 5 | 2 |
| 87 | 3 | 4 | 5 | 2 | 5 | 2 | 4 | 5 | 4 | 4 | 2 | 4 | 5 | 5 | 5 | 4 | 5 | 2 | 4 | 5 | 5 | 2 | 4 | 2 | 4 | 5 | 5 | 5 | 3 | 2 | 5 | 5 | 4 | 3 | 4 | 2 | 2 | 4 | 5 | 5 | 2 | 2 | 4 | 4 | 5 | 4 |   |
| 88 | 2 | 4 | 4 | 5 | 4 | 5 | 4 | 4 | 3 | 5 | 2 | 4 | 4 | 5 | 2 | 2 | 2 | 5 | 4 | 4 | 2 | 5 | 4 | 4 | 2 | 5 | 5 | 2 | 4 | 4 | 5 | 5 | 5 | 4 | 4 | 5 | 5 | 5 | 4 | 5 | 5 | 4 | 4 | 2 | 5 | 5 | 4 |
| 89 | 3 | 5 | 2 | 2 | 2 | 3 | 3 | 2 | 2 | 5 | 5 | 2 | 3 | 2 | 5 | 4 | 2 | 4 | 4 | 3 | 5 | 2 | 5 | 5 | 2 | 3 | 2 | 5 | 3 | 4 | 2 | 3 | 2 | 5 | 3 | 5 | 3 | 4 | 4 | 3 | 5 | 2 | 5 | 4 |   |   |   |
| 90 | 5 | 3 | 3 | 3 | 4 | 2 | 5 | 4 | 3 | 4 | 4 | 4 | 3 | 2 | 5 | 2 | 5 | 4 | 5 | 4 | 5 | 4 | 4 | 4 | 3 | 2 | 5 | 5 | 2 | 3 | 4 | 2 | 3 | 3 | 2 | 4 | 5 | 4 | 5 | 4 | 5 | 4 | 5 | 4 |   |   |   |
| 91 | 2 | 2 | 2 | 3 |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |

## ANEXO N°5: CONSENTIMIENTO INFORMADO

(Debe ser redactado por el investigador de acuerdo con la estructura de su investigación y los principios éticos correspondiente)

### TÍTULO DE LA INVESTIGACIÓN

**NO APLICABLE**

### PROPÓSITO DEL ESTUDIO

(Para que se va a realizar el estudio)

### PROCEDIMIENTO PARA LA TOMA DE INFORMACIÓN

(Metodología a seguir para la toma de información)

### RIESGOS

(Riesgos que se podrían presentar para el que brinda información)

### BENEFICIOS

(Beneficios que se podrían presentar para la institución del que brinda información). No representa ningún tipo de beneficio económico para el encuestado)

### COSTOS

(Costos que se podrían presentar para el que brinda información). No representa ningún costo para el encuestado ni para su institución.

### INCENTIVOS O COMPENSACIONES

(Incentivos o compensaciones que se le podrían dar a el que brinda información)

### TIEMPO

(Duración de la toma de información)

### CONFIDENCIABILIDAD

(Participación voluntaria y anónima, de ser el caso). Los datos recabados serán utilizados estrictamente en la presente investigación respetando su estrictamente su confidencialidad, los cuales serán eliminados al término del estudio.

**CONSENTIMIENTO:** Acepto voluntariamente participar en esta investigación. Tengo pleno conocimiento de este y entiendo que puedo decidir no participar y que puedo retirarme del estudio si los acuerdos establecidos se incumplen.

En fe de lo cual firmo a continuación:

-----

**Apellidos y Nombres**

**DNI N°** \_\_\_\_\_

## **ANEXO N°6: AUTORIZACIÓN DE LA ENTIDAD DONDE SE REALIZÓ EL TRABAJO DE CAMPO**

Los cuestionarios fueron aplicados a los docentes, en forma directa cuando transitaban por inmediaciones de la zona de los centros de compra, mercados de abastos, instituciones públicas ingresaban o salían de la universidad, los cuales lo realizaron en forma voluntaria, por lo que no se requirió autorización de alguna entidad para el trabajo de campo.

## ANEXO 7: DECLARATORIA DE AUTENTICIDAD DE TESIS

Yo, Hansi ELORRIETA Rondón, alumno de la Escuela de Posgrado del Doctorado en Ingeniería de Sistemas, de la Universidad Alas Peruanas, identificado con DNI N° 04648155 y con la tesis titulada:

**“SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y LA CALIDAD DEL SERVICIO INFORMÁTICO EN LA UNIVERSIDAD NACIONAL DE MOQUEGUA, REGION TACNA, AÑO 2024”**

Declaro bajo juramento que:

-La tesis es de mi autoría.

-Se ha respetado las normas internacionales de citas y referencias bibliográficas.

Tacna, 05 de diciembre del 2024



---

Ing. Hansi Elorrieta Rondón  
DNI 04648155



---

Hansi Elorrieta Rondón  
DNI 04648155