UNIVERSIDAD PRIVADA DE TACNA

FACULTAD DE INGENIERÍA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

TESIS

"NORMA TÉCNICA PERUANA 27001:2014 ISO-IEC Y SEGURIDAD EN SISTEMAS DE INFORMACIÓN DE LA MUNICIPALIDAD GREGORIO ALBARRACÍN, TACNA 2022"

PARA OPTAR:

TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS

PRESENTADO POR

Bach. JOSÉ JHONATAN ROJAS BUSTAMANTE

Bach. ANTHONY WASHINGTON CHURA CHURA

TACNA - PERÚ

2022

UNIVERSIDAD PRIVADA DE TACNA

FACULTAD DE INGENIERÍA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

TESIS

"NORMA TÉCNICA PERUANA 27001:2014 ISO-IEC Y SEGURIDAD EN SISTEMAS DE INFORMACIÓN DE LA MUNICIPALIDAD GREGORIO ALBARRACÍN, TACNA 2022"

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

PRESIDENTE	**:**	**Msc. LUIS ALFREDO FERNÁNDEZ VIZCARRA**
SECRETARIO	**:**	**Mtro. HUGO MANUEL BARRAZA VIZCARRA**
VOCAL	**:**	**Mag. RICARDO EDUARDO VALCÁRCEL ALVARADO**
ASESOR	**:**	**Mag. OSCAR JUAN JIMENEZ FLORES**

DECLARACIÓN DE ORIGINALIDAD

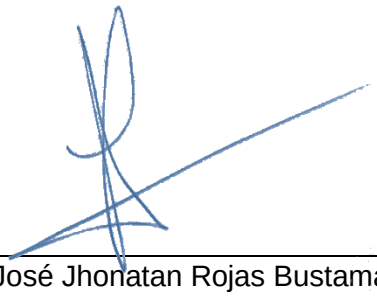
Nosotros, José Jhonatan Rojas Bustamante identificado con documento de identidad 46748024 y Anthony Washington Chura Chura identificado con documento de identidad 70432211, en calidad de: Bachilleres de la Escuela Profesional de Ingeniería de Sistemas de la Facultad de Ingeniería de la Universidad Privada de Tacna.
Declaramos bajo juramento que:

1. Somos autores de la tesis titulada:
"Norma Técnica Peruana 27001:2014 ISO-IEC Y Seguridad en Sistemas de Información de la Municipalidad Gregorio Albarracín, Tacna 2022", la misma que presento para optar:
Título de ingeniero de sistemas.
2. El documento no está plagiado en su totalidad o en parte, y cumple con los estándares internacionales de citas y los estándares de citas de referencia.
3. El trabajo presentado no infringe los derechos de terceros.
4. La disertación nunca ha sido publicada o ha publicado una disertación que haya obtenido una licenciatura o título profesional.
5. Los datos presentados en los resultados son reales, no han sido manipulados, copiados, copiados.

Sujeto a lo anterior, aceptamos toda responsabilidad frente a la universidad que pudiera derivarse de los derechos de autor, la originalidad y autenticidad del contenido de la tesis, así como de los derechos sobre la obra y/o la invención presentada. Soy por tanto responsable frente a la universidad y frente a terceros de los daños y perjuicios que puedan causarse por el incumplimiento de lo expuesto o que pueda encontrarse en la fuente del trabajo presentado, asumiendo todos los cargos pecuniarios que puedan derivarse a favor de terceros como consecuencia de ello. De acciones, reclamaciones o conflictos derivados del incumplimiento de lo declarado o que hayan encontrado la causa en el contenido de la tesis, libro y/o invención.

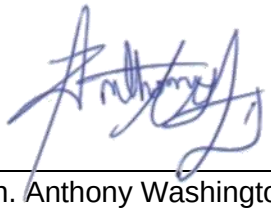
Si se identifica fraude, infracción de derechos de autor, plagio, falsificación o investigación publicada anteriormente; Asumo todas las consecuencias y sanciones que se deriven de mis actos, con sujeción a la normativa aplicable de la Universidad Privada de Tacna.

Tacna, 25 de junio de 2022



Bach. José Jhonatan Rojas Bustamante

DNI:46748024



Bach. Anthony Washington Chura Chura

DNI: 70432211

DEDICATORIA

Dedico el presente trabajo de investigación primeramente a mi madre Elena, mi hermana Shirley y sobre todo a mi novia Claudia que con su apoyo incondicional me guían para ser una mejor persona y un gran profesional.

Bach. José Jhonatan Rojas Bustamante

DEDICATORIA

Dedico el presente trabajo de investigación en primer lugar a mi madre Cayetana, tío Andrés y tía Sofia que son un pilar fundamental de apoyo y a quienes estaré eternamente agradecido por su estar en esta etapa de mi vida.

Bach. Anthony Washington Chura Chura

AGRADECIMIENTO

Agradecen en primer lugar a Dios por la vida y la salud que nos brinda para llegar a concluir el final de la carrera profesional.

Al Mag. Oscar Juan Jimenez Flores por su dedicada labor como asesor para que este trabajo de investigación sea posible.

Y agradecimiento a los trabajadores de la Municipalidad Gregorio Albarracín, por su colaboración de las diferentes Gerencias y Sub Gerencias por su colaboración en este trabajo de investigación.

Bach. José Jhonatan Rojas Bustamante

Bach. Anthony Washington Chura Chura

ÍNDICE DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE ANEXOS

RESUMEN

El presente trabajo de investigación titulado: “Norma Técnica Peruana 27001:2014 ISO-IEC y Seguridad en Sistemas de Información de la Municipalidad Gregorio Albarracín, Tacna 2022” tiene como objetivo evaluar la Norma Técnica Peruana 27001:2014 ISO-IEC y su correlación con la seguridad en sistemas de información de la Municipalidad Gregorio Albarracín, Tacna 2022. En donde se aplicó el enfoque cuantitativo con el tipo de investigación básica de diseño no experimental, por tanto, no se manipularon las variables, siendo el diseño de investigación correlacional, debido a que se buscó evaluar la relación entre las variables del estudio, teniendo como población 100 trabajadores los cuales son los que utilizan los sistemas informáticos en la institución, se consideró una muestra de 80 personas al aplicar la fórmula de población finita. El instrumento utilizado fue el cuestionario y así garantizar la confiabilidad de la investigación, esto comprobó que si existe relación entre la Norma Técnica Peruana 27001:2014 ISO-IEC y seguridad en sistemas de información. Finalmente, dejando como conclusión que la evaluación de la Norma Técnica Peruana 27001:2014 ISO-IEC es necesaria para la seguridad en sistema de información de nivel informático.

Palabras clave: NTP ISO/IEC 27001, Seguridad de la información, SGSI, Sistemas informáticos.

ABSTRACT

The present research work entitled: "Peruvian Technical Standard 27001: 2014 ISO-IEC and Security in Information Systems of the Municipality Gregorio Albarracín, Tacna 2022" aims to evaluate the Peruvian Technical Standard 27001: 2014 ISO-IEC and its correlation with security in information systems of the Gregorio Albarracín Municipality, Tacna 2022. Where the quantitative approach was applied with the type of basic research of non-experimental applied research, therefore the variables were not manipulated, being the correlational research design, because it sought to evaluate the relationship between the variables of the study, having as a population 100 people which are the ones that use the computer systems in the institution, a sample of 80 people was considered. The instrument used was the questionnaire and thus guarantee the reliability of the investigation, this verified that there is a relationship between the Peruvian Technical Standard 27001: 2014 ISO-IEC and security in information systems. Finally, leaving as a conclusion that the evaluation of the Peruvian Technical Standard 27001: 2014 ISO-IEC is necessary for the security of the information system at the computer level.

Keywords: NTP ISO/IEC 27001, Information security, ISMS, Computer systems.

INTRODUCCIÓN

En la actualidad las instituciones públicas del estado peruano, se ha visto inmersa en el desarrollo tecnológico de sistemas de información para continuar brindando sus servicios en los diferentes niveles del estado debido al COVID-19, motivo por el cual existe desde hace años la Norma Técnica Peruana ISO/IEC 27001:2014, en donde detalla los aspectos técnicos y funcionales a incluir y evaluar en los sistemas de información, ello con la finalidad de evitar intrusiones y vulnerabilidades en la institución. A fin de elaborar la descripción de los resultados se emplearon varias tablas al igual que gráficos estadísticos con sus interpretaciones en cada una de ellas, seguidamente de procedimientos de inferencias estadística, reducción de hipótesis y el software SPSS Versión 25.

El propósito es evaluar la seguridad en los sistemas de información mediante la Norma Técnica Peruana 27001:2014 ISO-IEC así mismo se determina su correlación.

Un sistema el cual se encarga de la gestión de seguridad de la información faculta en resguardar la información garantizando su disponibilidad, integridad y confidencialidad, brindando con ello confiabilidad para la organización, empleados, clientes; permitiendo una respuesta rápida ante situaciones que afecten los activos de la institución, el personal especializado debe identificar los posibles riesgos, en algunos casos tales como el acceso no deseado a ciertos usuarios, para evitar posibles robo de datos, documentos y/o modificación de estos. Un punto crítico es que se pueda llegar a perder las copias de seguridad, afectando los tres pilares de la seguridad de la información.

En el capítulo I, Planteamiento del problema, se realiza una descripción de la problemática y los diferentes factores o causas que generaron el problema, así como sus efectos, posteriormente se formula el problema de investigación, al igual que los objetivos y sus hipótesis, justificando la importancia del estudio en sus diferentes niveles.

En el capítulo II, Marco Teórico, se desarrollan los antecedentes del estudio tanto Internacionales como Nacionales, también las bases teóricas para conocer más a fondo a las variables del estudio y la definición de términos para comprender mejor los conceptos usados en la investigación.

En el capítulo III, Marco Metodológico, se presenta el tipo y el nivel de la investigación usado, se muestra la población y muestra del estudio usada, también se detalla el cuadro de Operacionalización de las variables para conocer mejor las dimensiones y sus indicadores.

En el capítulo IV, Resultados, se constatan los resultados generados a partir del análisis e interpretación de las variables de estudio luego del desarrollo del proyecto, así como la realización del contraste de la hipótesis que se consideró en la investigación.

En el capítulo V, Discusión, se muestra la discusión de resultados, donde se realiza el contraste entre los hallazgos encontrados de las tesis e investigaciones utilizadas las cuales se encuentran concordantes a los objetivos de la investigación.

Finalmente, el último apartado de la tesis se da con las conclusiones y recomendaciones, las mismas que dan razón del logro de los objetivos, demostrando las hipótesis que responden a los problemas identificados, siendo las recomendaciones producto de los hallazgos en los resultados, los que objetivamente nos permiten proponer mejoras en la municipalidad.

CAPÍTULO I: PLANTEAMIENTO DEL PROBLEMA

1.1. Descripción del problema

En el mundo la seguridad en los sistemas de información se ha visto afectada por la alta demanda de usuarios que requieren conectividad a sus centros de trabajo de manera virtual, haciendo uso de todos los recursos informáticos inhouse y otros servicios cloud; este incremento debido a la Pandemia ha generado una serie de problemas en torno a la seguridad de los sistemas de información de las organizaciones, mismos que no se preocupaban en gran medida de la seguridad informática. Renteria Echeverry (2016) menciona que las organizaciones actualmente están en una etapa de uso intensivo de las TIC, pero que sus empleados o colaboradores aún no cuentan con todas las destrezas para emplear sistemas de información de manera segura lo cual los hace poco fiables, ello que origina múltiples riesgos informáticos a nivel tangible e intangible.

En Latinoamérica el informe anual de Kaspersky del 2021, muestra una serie de estadísticas y tipos de ciberataques en la región, la cual tuvo un incremento del 24 % respecto al año anterior; esto trajo consecuencias a todas las organizaciones respecto a la seguridad en los sistemas de información, puesto que su capacidad de respuesta se vio amenazada por estos posibles ciberataques, como medida preventiva los especialistas recomiendan realizar planes de seguridad de la información basadas en estándares internacionales, acompañados de presupuestos que les permitan proteger sus activos más valiosos en términos de información mediante sus sistemas. Para Dmitry Bestuzhev (2021) la tendencia de uso de sistemas de información online de la mayoría de los negocios e instituciones gubernamentales se mantendrá en los próximos años, esto conlleva al escenario perfecto para que estas empresas inicien sus procesos internos de implementación en materia de seguridad.

En el Perú, que no es ajeno a la problemática mundial y latinoamericana, para Dávila Villanueva (2018), la mayoría de las municipalidades en el Perú no cuentan con la seguridad debida en sus sistemas de información, lo cual permita manejar la infraestructura tecnológica es decir sus elementos tangibles para resguardar los activos de la misma. Es por ello que través de la NTP ISO 27001:2014 se asegura

la capacidad de respuesta de la información para así garantizar la fiabilidad de la misma.

A nivel local en la Municipalidad de Gregorio Albarracín Lanchipa, los sistemas de información han sufrido en reiteradas ocasiones problemas debido a la infraestructura tecnológica (Elementos tangibles), por falta de mantenimiento y otros elementos importantes que no son incluidos en un plan seguridad de la información. Así mismo la fiabilidad de la información se ven vulnerables, debido a los diferentes ciberataques que sufrió la municipalidad, ocasionando alteración de la información al no contar con un plan de contingencia el cual permita saber cómo reaccionar frente a estos ataques para así minimizar los daños y mantener la información íntegra. Por último, la capacidad de respuesta, se ve constantemente interrumpida por lo antes mencionado, pero también se debe a la falta de mantenimiento de los sistemas informáticos, sumado a una infraestructura que no se encuentra adecuada para brindar un servicio eficiente.

Por tanto, es indispensable asegurar los sistemas de información de tipo informático de cada una de las gerencias de la municipalidad Gregorio Albarracín bajo la Norma Técnica Peruana 27001:2014 ISO-IEC, Además de considerar el modelo guía de la seguridad de la información en la organización las cuales son: la confidencialidad, la integridad y la disponibilidad. Para asegurar así la seguridad en sistemas de información informática que ofrece el área de la Sub Gerencia de Tecnologías de la Información y Comunicación (SGTIC) en la municipalidad, siendo el alcance de la misma el diseño de un prototipo de tablero control del SGSI basado en la Norma Técnica Peruana 27001:2014 ISO-IEC exclusivamente en el nivel informático de la seguridad en sistema de información.

1.2. Formulación del problema

1.2.1. Problema General

¿Cómo se correlaciona la Norma Técnica Peruana 27001:2014 ISO-IEC y la seguridad en sistemas de información de la Municipalidad Gregorio Albarracín, Tacna 2022?

1.2.2. Problemas Específicos

a. ¿Cómo se correlaciona la Norma Técnica Peruana 27001:2014 ISO-IEC y los elementos tangibles de la Municipalidad Gregorio Albarracín, Tacna 2022?

b. ¿Cómo se correlaciona la Norma Técnica Peruana 27001:2014 ISO-IEC y la fiabilidad de la Municipalidad Gregorio Albarracín, Tacna 2022?

c. ¿Cómo se correlaciona la Norma Técnica Peruana 27001:2014 ISO-IEC y la capacidad de respuesta de la Municipalidad Gregorio Albarracín, Tacna 2022?

1.3. Justificación e importancia

El presente trabajo de investigación se justifica en la evaluación de la Norma Técnica Peruana 27001:2014 ISO-IEC y su relación con la seguridad en sistemas de información de la Municipalidad Gregorio Albarracín, Tacna 2022. Todo ello debido a que instituciones públicas, en específico municipalidades en Tacna no estarían aplicando correctamente la norma técnica peruana y como consecuencia de ello se producen fallos en la seguridad de los sistemas de información, pérdidas importantes en las copias de seguridad, políticas desactualizadas por falta de interpretación de la norma actual. Por tanto, la investigación dará como resultado el diseño de un prototipo de tablero control del SGSI basado en la Norma Técnica Peruana 27001:2014 ISO-IEC.

1.3.1. Justificación Práctica:

Carrasco Diaz (2019) señala que al desarrollar la investigación tiene como fin la solución de un problema o propone indicaciones para su pronta aplicación y puedan solucionarlo dentro de la justificación correspondiente.

Por tanto, la justificación se da en torno a uno de los resultados que benefician a la organización y que es la evaluación de la Norma Técnica Peruana 27001:2014 ISO-IEC en la Municipalidad Gregorio Albarracín, Tacna 2022. Esta evaluación de la seguridad con base en estándares peruanos da pie a formular un plan de implementación del SGSI a futuro.

1.3.2. Justificación Teórica:

Carrasco Diaz (2019) menciona que el resultado de manera positiva de la investigación podría usarse en el campo de la ciencia referente al tema de la gnoseología, en cuanto esta sea demostrada la validez y la confiabilidad podrían ser usados en futuros trabajos de investigación.

Por tanto, la justificación en este punto se da debido a la escasa bibliografía referente a la evaluación y aplicación de la norma técnica peruana en instituciones públicas, en especial Municipalidades. Es así que la presente investigación aporta al conocimiento con respecto a la seguridad, principalmente en los sistemas concernientes a la información aplicando la NTP en el sector público con foco en Municipalidades.

1.3.3. Justificación Metodológica:

Carrasco Diaz (2019) señala que los métodos empleados, técnicas que se aplicarán y procedimientos e instrumentos ejecutados en la investigación, permita demostrar la confianza y validez podrán ser empleados en otros proyectos de investigación.

En esta justificación el aporte se da por el uso de la norma técnica peruana en el sector de las municipalidades, debido a que estas no evalúan correctamente la seguridad el cual es parte fundamental dentro de un sistema de información y no suelen proponer planes de acción para mejorar sus SGSI.

Los instrumentos empleados inicialmente son cuestionarios producto de la NTP y basado en la normativa vigente, por ello son una novedad para evaluar a este tipo de instituciones públicas.

1.4. Objetivos

1.4.1. Objetivo General

Evaluar la correlación entre Norma Técnica Peruana 27001:2014 ISO-IEC y la seguridad en sistemas de información de la Municipalidad Gregorio Albarracín, Tacna 2022.

1.4.2. Objetivos Específicos

a. Medir la correlación entre la Norma Técnica Peruana 27001:2014 ISO-IEC y los elementos tangibles de la Municipalidad Gregorio Albarracín, Tacna 2022.

b. Medir la correlación entre la Norma Técnica Peruana 27001:2014 ISO-IEC y la fiabilidad de la Municipalidad Gregorio Albarracín, Tacna 2022.

c. Medir la correlación entre la Norma Técnica Peruana 27001:2014 ISO-IEC y la capacidad de respuesta de la Municipalidad Gregorio Albarracín, Tacna 2022.

1.5. Hipótesis

1.5.1. Hipótesis General

Existe correlación significativa entre la Norma Técnica Peruana 27001:2014 ISO-IEC y la seguridad en sistemas de información de la Municipalidad Gregorio Albarracín, Tacna 2022

1.5.2. Hipótesis Específicas

a. Existe correlación significativa entre la Norma Técnica Peruana 27001:2014 ISO-IEC y los elementos tangibles de la Municipalidad Gregorio Albarracín, Tacna 2022.

b. Existe correlación significativa entre la Norma Técnica Peruana 27001:2014 ISO-IEC y la fiabilidad de la Municipalidad Gregorio Albarracín, Tacna 2022.

c. Existe correlación significativa entre la Norma Técnica Peruana 27001:2014 ISO-IEC y la capacidad de respuesta de la Municipalidad Gregorio Albarracín, Tacna 2022.

CAPÍTULO II: MARCO TEÓRICO

2.1. Antecedentes del estudio

2.1.1. Antecedentes Internacionales

En Ecuador el autor Zapata Chasiguasin (2020) en su tesis *"Sistema de gestión de seguridad de la información basado en las normas ISO/IEC 27001, En El departamento de tecnologías de la información del gobierno autónomo descentralizado de la Municipalidad de Ambato",* menciona como problemática la cual es la seguridad concerniente a la información, el escaso conocimiento y que estas no se han examinado a fondo, aunque son básicas para toda organización, aunque son puntos importantes deben ser considerados para cualquier empresa, agencia u organización donde aplique el uso de sistemas de información. Esta investigación tuvo como finalidad la implantación de un Sistema de Gestión de Seguridad de la Información (SGSI) bajo una de las normas internacionales más utilizada a nivel internacional es la ISO 27001, dentro del área o departamento de tecnologías de la información de la Municipalidad de Ambato. Tiene como metodología Investigar, analizar y obtener resultados reales de la información, luego analizarla y finalmente recomendar acciones a tomar para mejorar la seguridad informática, el personal del departamento de TIC se tomó como la población del estudio con una muestra menor de 100, se realizó la aplicación de entrevistas y encuestas. Dando como resultado la existencia de algunas vulnerabilidades en el sistema, siempre se desarrollan nuevos métodos, pero estos a su vez también afectan a la seguridad informática, por ello es preciso realizar una indagación acerca de las amenazas actuales y así poder definir un SGSI la cual reducirá el riesgo para el sistema de forma no autorizada reduciendo así el porcentaje de riesgo. Se concluyó en que han resaltado deficiencias en la seguridad informática, los servidores a través de los cuales gestiona información importante de la organización están vulnerables a diversos ataques y amenazas de seguridad, por la cuales se aplicaran medidas de remediación para evitar que se vulnere la confidencialidad de la información. Por ello se ha diseñado el SGSI en la cual se ejecuta la norma internacional ISO 27001 de acuerdo a sus estándares para así brindar una

seguridad, a la información que posee la institución, así como la disponibilidad, confidencialidad y por último la integridad.

En Chile los autores Burgos Salazar, Jorge & Campos G., Pedro (2008) en su trabajo de *"Modelo para Seguridad de la Información en TIC".* Indica que: Actualmente existen muchos riesgos referentes a los equipos y sistemas informáticos los cuales no cuentan con políticas de seguridad y si cuentan no ofrecen una protección eficaz. Lo cual es muy preocupante debido a que están conscientes tanto las grandes, medianas y pequeñas organizaciones que corren el riesgo de ser atacados y perder sus sistemas centrales de información. Y no solo se tiene que estar consciente de los peligros, sino contar con un plan de seguridad, de este modo se puede prever las fallas y pérdidas en los sistemas. También se toma en cuenta que los ataques no son solo externos sino también internos (dentro de la institución), la cual es un riesgo que no debe ser considerado de baja prioridad, este riesgo puede conllevar a pérdidas de los datos, activos valiosos que pongan en duda la confiabilidad de parte de los usuarios y accionistas de la organización. Según un informe Chile sus empresas el 99 % de ellas ignoran el asunto de la seguridad en la información, así mismo el 96 % de ellas no logran detectar una intromisión o ataque en sus sistemas cuyo 99 % no cuentan con las herramientas para la detección del fraude informático.

En Ecuador el autor Christian Damián (2020) en su trabajo "Plan de Seguridad Informática basado en la Norma ISO 27001, para proteger la información y activos de la empresa privada Megaprofer S.A". Menciona que la falta de políticas adecuada, así como controles pertinentes que de alguna manera mantenga la integridad de la información y correctamente protegida. Además, que la institución precedente de perdida de información, por su falta de implementación de políticas. Por lo cual el objetivo es la implementación de un SGSI, de esta forma permita una mejora con respecto a la gestión de la seguridad. Para lo cual se empleó una entrevista la cual permita recoger los datos y proceder con su análisis, para desarrollar una propuesta de un Sistema de Gestión de Seguridad de la Información. A través de las encuentras se evidencio la falta de conocimiento por parte del personal del área de TIC con respecto a la seguridad de la información, así como la falta de medidas de control para garantizar una infraestructura adecuada para asegurar la información almacenada dentro de los servidores. Se concluyó que la falta de conocimiento con respecto a la seguridad de la información es un punto muy

importante, además que cuentan con antecedentes de perdida de información por la falta de implementación de políticas de seguridad. Por lo cual un plan de seguridad basado en la norma ISO 27001 correctamente implementado permita el desarrollo de políticas y controles correctamente adecuados según la norma ISO 27001, para así minimizar los riesgos a los cuales se vean expuestos la información de la empresa.

En Ecuador la Autora Crespo Chávez (2018) en su tesis "La aplicación de las normas ISO 27001 y 27002 y su incidencia en la seguridad de las bases de datos de las Instituciones de Educación Superior", menciona como problemática la falta de talento humano y el inadecuado manejo de protocolos de seguridad que permitan asegurar la información, para que pueda preservar su integridad. Esta investigación tuvo como finalidad la implementación de la normativa, así como los debidos procedimientos de seguridad que serían de gran utilidad, debido que así se pueda permitir la integridad de la información que se utiliza. Tiene como metodología el investigar, analizar los datos obtenido por medio de encuestas, para así brindar las recomendaciones para mejorar la seguridad de la información que se encuentran en las bases de datos; se seleccionó como muestra a estudiantes y docentes de la UNACH, se empleó entrevistas y encuestas. Lo cual permitido obtener como resultado la existencia de una falta de conocimiento y capacitación por parte de los docentes y estudiantes. Además de que los sistemas no se encuentran correctamente protegidos, esto se suma la falta de políticas o medidas de protección de datos. Se concluyó en que han resaltado la falta de implementación de un procedimiento y a su vez su respectiva documentación la cual permita el monitoreo, evaluación y mejora con respecto a la seguridad de la información, esto evidencio el grado de riesgo al que están expuesto los datos de la Institución. Por ello la implementación de planes de capacitación y a su vez concientización sobre la importancia de la seguridad de la información, para los usuarios que hacen uso de los sistemas de información.

En Ecuador la autora Puentes Sánchez (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”,* señala que, al proporcionar una guía integral para mejorar el desempeño, esta norma describirá cómo establecer controles los cuales se seleccionarán con base en una evaluación de riesgos para los activos más importantes de la organización.

Contrariamente a la creencia popular, la norma ISO 27002 está destinada a respaldar la implementación de SGSI en cualquier organización ya sea pequeña o grande, pública o privada, con o sin fines de lucro. La ISO/IEC 27002:2015 es una guía que contiene la estructura de gestión requerida para el diseño e implementación de un SGSI de acuerdo con los requisitos establecidos en la norma ISO/IEC 27000, que gestiona la seguridad en sistemas de la información en la organización. Esta investigación tuvo como finalidad la mejora en los procesos de permisos y los accesos que se pueden asignar al personal de la empresa.

Para protegernos de los ataques se debe tener una correcta administración de la seguridad en sistemas de información y tener presente los tres requerimientos de mayor importancia: la Integridad, la disponibilidad. Y la confidencialidad. Además, se puede apoyar en estándares como: ISO 17799, COBIT e ITIL V3, entre otros para reforzar la seguridad, pero siempre enfocándolos a los tres requerimientos antes mencionados.

2.1.2. Antecedentes Nacionales

Según los autores Mendoza Silva, Luis Fernando y Vega Gallegos, Giancarlo Roberto (2019) en su Tesis “Evaluación de la capacidad de detección y respuesta a riesgo de ciberseguridad, caso de la empresa SISC”. Indica que: Los ciberataques son cada vez más constantes, por lo cual requiere de una respuesta rápida frente a estos ataques, debido a que es su principal objetivo son la información y sistemas de los negocios de las instituciones vulnerables. Por lo cual su objetivo es el diagnosticar el nivel de capacidad en la gestión de la ciberseguridad de la empresa, identificar las brechas para diseñar y proponer los controles claves para fortalecer la ciberseguridad. El diseño de la investigación es no experimental debido a que se centra en evaluar un contexto en un punto del tiempo. Con un diseño transversal. Se obtuvo como resultado a través de una evaluación de capacidad que la institución no cuenta con herramientas de seguridad suficiente para detectar y responder a posibles problemas de ciberseguridad. Por lo cual concluyó, de que a través de su trabajo pudo desarrollar un método que permita mejorar la capacidad de cualquier organización para detectar y responder a incidentes de ciberataques.

Para el autor Apahuasco Saccaco, Eber Jesús (2019) En su tesis “Evaluación del sistema de seguridad de la información en la organización DISAV SAC aplicando lineamiento ISO 27001”. Detalla que: El activo primordial y sensible dentro de

cualquier institución pública o privada es la información que gestiona y la cual debe encontrarse segura. Tiene como finalidad el evaluar la gestión de seguridad de la información basada en el estándar ISO 27001 en la organización Disav SAC. Se analizó de la seguridad de la información en los terminales tecnológicos y personal que labora por medio preguntas para su posteriormente capacitación al personal y terminales. El diseño de la investigación es no experimental, aplicada para evaluar a un grupo definición para realizar el pre prueba y post prueba. Obtuvo como resultado que la organización no cuenta con ningún lineamiento para salvaguardar su información por lo cual concluyo que por medio de la implementación de los controles de seguridad obtuvo como resultado se minimizó en un 63,33 % la vulnerabilidad de manera significativa.

Según el autor Villena Aguilar (2006) En su informe “Sistema de Gestión de Seguridad de Información para una Institución Financiera”. Indica que: La información es el principal activo de cualquier organización, apareciendo de diferentes formas como: impresa, almacenamiento digital, en películas o también en diálogos entre personas. Las amenazas se han incrementado de tal forma que estos ataques no solo vienen de una dirección sino de distintas como son los ataques internos, externos, accidentales o maliciosas para con la organización. Para toda organización es necesario un programa de gestión de seguridad el cual asegure la confidencialidad, integridad, disponibilidad y auditabilidad de la información, con el avance de la tecnología el poder brindar una seguridad en cuanto a la información se convierte en un grave problema. A todo esto, se debe considerar el presupuesto que se debe destinar a la administración de los riesgos.

Según los autores Flores Solís y Guerra Farfán (2017) en su Tesis de Maestría “Relación de la NTP ISO/IEC 27001:2008 EDI y la seguridad de la información en los Ministerios del Estado Peruano al 2015”. Indica que: La Resolución Ministerial N° 004-2016-PCM la cual aprueba al uso de manera obligatoria a todas las organizaciones del Estado la ISO NTP/IEC 27001:2014 para proteger la seguridad de los datos. Así mismo se debe comprobar si la norma implementada permitió una mejora en las entidades del estado peruano en la seguridad de la información. El trabajo que se realizado fue cuantitativa correlacional y de tipo no experimental y transversal, permitiendo establecer un nivel de implantación de la norma ISO, así como el grado de incidentes que existen en la población determinada, con respecto a la Seguridad de la Información (SI) en el cual

los participantes del estudio fueron el presidente del Consejo de ministros y los 18 ministerios.

El autor Vela Ríos, Erick (2021) nos indica en su tesis para su titulación "Seguridad en información basada en la Norma ISO/IEC 27001:2013 y nivel de seguridad en el Centro de Capacitaciones SENCICO - Ucayali 2018" se debe conocer la relación existente del nivel de seguridad informática y la seguridad de información en la institución. Esta investigación tuvo como objetivo establecer correlación de la seguridad informática, fundamentada en la “Norma ISO/IEC 27001:2013” y el Nivel de seguridad informática. La investigación es del tipo aplicada, ya que se está aplicando la Norma ISO el cual está enfocado a los sistemas informáticos según el nivel de seguridad, cuanta con un diseño de investigación No Experimental, dado que el autor observa y no interviene de ninguna manera con las variables, con una población de 30 trabajadores del Centro de capacitación SENCICO, usando como instrumento el cuestionario. Entre sus resultados más destácales se obtuvo la presencia de una relación porque el nivel de significancia fue de 0000 valor por debajo del nivel de significancia sugerido (α = 001). Así mismo el coeficiente Rho de Spearman muestra que el nivel de relación entre las dos varíales es de 0819 lo que significa que el nivel de relación directa es de moderado a muy bueno. Y finalmente la conclusión más relevante es la presencia de una correlación de la seguridad informática según la norma ISO y el nivel de seguridad en los sistemas informáticos, cada vez que aumenta un puntaje de seguridad de la información aumenta positivamente o directamente de promedio a muy bueno que siempre es un puntaje de nivel de seguridad en los sistemas informáticos porque así se generan los datos. En otras palabras, el coeficiente Rho de Spearman es de 0,819 lo que significa que el grado de relación positiva o directa es de moderado a muy bueno.

El autor Camapaza Quispe, Abdon (2019) nos indica en su trabajo de tesis “Diseño del plan de seguridad informática basado en la NTP ISO/IEC 27001:2014 para la municipalidad del centro poblado de Salcedo - Puno”, se encontró con la problemática de que las entidades públicas no se interesan en la seguridad de los datos, ya sea por la falta de conocimiento en la alta gerencia, la falta de personal experto en el tema de seguridad informática y la falta de presupuesto para llevarlo a cabo. La investigación es del tipo aplicada, ya que se está aplicando la NTP ISO 2700:2014 en el Nivel de seguridad de los sistemas informáticos, cuenta con un

diseño de investigación No Experimental, ya que no interviene de ninguna manera con las variables, cuenta con una muestra probabilística aleatoria simple donde la población puede ser usada como muestra, usando como instrumento el cuestionario. Entre los resultados más sobresalientes se evidenció que el diseño del plan de seguridad informática influyo de manera positiva para la seguridad de los datos, en sus 3 dimensiones. Y finalmente la conclusión más relevante fue la dé al identificar los riesgos se elabora una lista para los controles de seguridad, así mitigando los altos riesgos que se pudieron encontrar durante el diseño del plan de seguridad informática para la Municipalidad del Centro Poblado de Salcedo Puno.

Por tal motivo, es importante aplicar la norma técnica peruana NTP 27001:2014, el Instituto para la Defensa de la Competencia y la Propiedad Intelectual INDECOPI (2014) “determina que Sistema de Gestión de Seguridad de la Información (SGSI), permite proteger y minimizar los riesgos que pueden aquejar a los activos de las empresas. Los sistemas de gestión de seguridad de la información permiten que proteja el activo más importante de una institución que vendría a ser su información que posee, a través de los tres pilares de la seguridad de la información, para brindar confiabilidad a organizaciones, empleados, clientes; permite una respuesta rápida a incidencias que pueden afectar a las operaciones de actuación empresarial”. Es fundamental que las autoridades corporativas identifiquen de manera oportuna las vulnerabilidades y/o amenazas que puedan surgir que afecten a los activos de la organización, acciones que afecten la integridad, disponibilidad y seguridad de los activos de información. La organización puede convertirse en blanco de ataques por usuarios que no se encuentren con las credenciales necesarias para el uso de la información, con la sola intención de alterar la información de alguna manera, de tal manera que pueda afectar a la organización.

2.2. Bases Teóricas

2.2.1. Bases teóricas de la primera variable “Norma Técnica Peruana 20017:2014 ISO-IEC”

Establecer un marco de referencia común para los procesos del ciclo de vida del software. Contiene los procesos, actividades y tareas que se aplicarán al comprar un sistema que contenga software, incluye también el proceso por el cual puede utilizarse para poder definir, así como controlar y por último mejorar las diferentes fases por las cuales pasa el software, tal como se puede apreciar en la Tabla 1.

Tabla 1

Tabla de Categorías de Tecnologías de la Información

Ítem	Código	Título de la norma	Referenciado en
1	NTP-ISO/IEC 27001:2014	Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información.	R.M N° 004-2016-PCM
1	NTP-ISO/IEC 12207:2016	Ingeniería de software y sistemas. Procesos del ciclo de vida del software	R.M. N° 004-2016-PCM
3	NTP 392.030-1:1997	Microformas. Requisitos para las organizaciones que operan sistemas de producción de microformas.	D.S. 2-98-ITINCI (1998-02-21)
4	NTP 392.030-2:2015	Microformas. Requisitos para las organizaciones que administran sistemas de producción y almacenamiento.	RESOLUCION JEFATURA N° 000022-2016-J-ONPE

ISO-IEC 27001

Este es el estándar internacional para el Sistema de Gestión de Seguridad de la Información (SGSI). Proporciona un marco sólido para protección de la información que se puede ajustar a varias organizaciones y de diferentes tamaños.

Las organizaciones que corren mayor riesgo por la seguridad de la información eligen cada vez más implementar un SGSI que esté alineado con la norma ISO 27001.

Beneficios de la implementación

- **Comercial:** Contar con el respaldo de un SGSI granizado por un tercero le proporciona a una empresa o institución una gran ventaja competitiva, permitiéndose estar al día con sus competidores.

- **Tranquilidad:** Contar con información operativa crítica es importante para mantener su ventaja competitiva o integral para el valor financiero, la norma ISO 27001 es un estándar reconocido a nivel mundial para las mejores prácticas SGSI y su ejecución puede ser comprobado de forma independiente para generar confianza en el cliente y mejorar la imagen de la organización.

- **Operacional:** Fomenta el desarrollo de una cultura interna que comprenda los riesgos de seguridad de la información y tenga un enfoque coherente para abordarlos. Este enfoque consistente conduce a controles más fuertes en respuesta a las amenazas.

La norma Técnica Peruana 27001 (2017), se divide en dimensiones que facilitan su estudio y composición a nivel teórico como se presenta a continuación:

a) **Dimensión Confidencialidad**

Para los autores Romero et al. (2018), la confidencialidad es sumamente importante la cual se debe estar protegida y evitar filtrado de información sin previo conocimiento de la persona o institución. Debido a que todo esto es respaldado por un conjunto de reglas que son establecidas por la instrucción que limita el acceso a la información.

Un aspecto importante según el autor señalado, refiere que la confidencialidad es la Propiedad que determina que la información solo esté disponible y sea revelada a individuos, entidades o procesos autorizados.

Además, la clasificación Se refiere a la información no se encuentre disponible ni sea revelada a individuos, entidades o procesos no autorizados, esta se debe definir de acuerdo con las características de los activos que se manejan en cada entidad. A continuación, se puede observar las categorías de confidencialidad de la información en la Tabla 2.

Tabla 2

Tabla de Categorías Confidencialidad de la Información

Información pública reservada	Información disponible solo para un proceso de la entidad y que en caso de ser conocida por tercero sin autorización puede conllevar un impacto negativo de índole legal, operativa de perdida de imagen o económica.
Información pública clasificada	Información disponible para todos los procesos de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo para los procesos de la misma. Esta información es propia de la entidad o de terceros y puede ser utilizada para todos los funcionarios de la entidad para realizar labores propias de los procesos, pero no puede ser conocida por terceros sin autorización del propietario.
Información publica	Información que puede ser entregada o publicada sin restricciones a cualquier persona dentro y fuera de la entidad, sin que esto implique daños a terceros ni a las actividades y procesos de la entidad
No clasificada	Activos de información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de Información Publica Reservada

b) **Dimensión Integridad**

Para los autores Romero et al. (2018), la integridad de la información debe ser inalterable ante cualquier intento que afecte de alguna manera dicha información. Su modificación solo es posible a través de autorizaciones.

Un aspecto importante según el autor señalado, refiere que la integridad es la propiedad de salvaguardar la exactitud y estado completo de los activos.

Además, la clasificación Se refiere a la exactitud y completitud de la información (ISO 27000) esta propiedad es la que permite que la información sea precisa, coherente y completa desde su creación hasta su destrucción.

A continuación, se muestra en la Tabla 3, las diferentes categorías de integridad de la información.

Tabla 3

Tabla de Categorías de Integridad de la Información

A (ALTA)	Información cuya perdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar perdidas de imagen severas de la entidad.
M (MEDIA)	Información cuya perdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar perdida de imagen moderado a funcionarios de la entidad.
B (BAJA)	Información cuya perdida de exactitud y completitud conllevar un impacto no significativo para la entidad o entes externos.
NO CLASIFICADA	Activos de información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratado como activos de información de integridad ALTA.

c) **Dimensión Disponibilidad**

Garantiza que la información se encuentre disponible en todo momento cuando sea requerido por las personas o entidades previamente autorizadas para su manejo y conocimiento. Por lo cual las medidas de soporte y seguridad permiten acceder de manera controlada a la información y evitar que se produzcan interrupciones en los servicios. Para los autores Romero et al. (2018),

Disponibilidad: Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada, cuando así lo requiera.

Clasificación: Es la propiedad de la información que se refiere a que esta debe ser accesible y utilizables por solicitud de una persona entidad o proceso autorizada cuando así lo requiera esta, en el momento y en la forma que se requiere ahora y en el futuro, al igual que los recursos necesarios para su uso.

A continuación, se muestra las diferentes categorías de disponibilidad de información en la Tabla 4.

Tabla 4

Tabla de Categorías de Disponibilidad de la Información

1 (ALTA)	La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar perdidas de imagen severas a entes externos.
2 (MEDIA)	La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar perdida de imagen moderado de la entidad
3 (BAJA)	La no disponibilidad de la información puede afectar la operación normal de la entidad o entes externos, pero no conlleva implicaciones legales, económicas o de perdida de imagen.
NO CLASIFICADA	Activos de información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de información de disponibilidad ALTA

d) **Sistemas de información**

Para el autor Andreu, Ricart y Valor (1998) es la agrupación de procesos que se ejecutan a ciertos datos y/o información que se encuentra estructurada por la institución, para luego recoger, elaborar y enviar de manera selectiva esta información que previamente fue requerida para su uso dentro de la institución.

e) **Componentes de los sistemas de información**

engloban equipos y programas informáticos, telecomunicaciones, base de datos, recursos humanos y procedimientos.

- **Equipos informáticos:** Todas las empresas utilizan ordenadores personales y las grandes empresas usan grandes ordenadores.
- **Programas informáticos:** dentro de ello existen programas del sistema los cuales administran los recursos del sistema. Las aplicaciones ayudan directamente al usuario final a hacer su trabajo.
- **Base de datos:** Es la colección de datos interrelacionados. Un claro ejemplo es la información que maneja el área de recursos humanos de cualquier institución pública o privada. Para toda institución esta información tiene un gran valor. Pero como toda base de datos está correctamente estructurada y ordenada para así tener acceso a sus atributos.
- **Telecomunicaciones:** Son el medio por el cual permite realizar la transmisión electrónica de información a largas distancias. Pero todo depende de las instituciones que quieran interconectarse, los cuales pueden ser un área pequeña o local conocido como LAN o un área más amplia conocida como WAN lo cual amerita diferentes tipos de conexión.
- **Recursos humanos:** Existen dos tipos primeramente personas especialistas en sistemas de información los cuales se consideran a los analistas, desarrolladores y operadores. Por otro lado, tenemos al otro tipo que son los usuarios finales, son los que utilizan los sistemas de información que son la mayoría de los trabajadores de una institución.
- **Procedimientos:** Son las políticas y métodos que deben estar establecidos y permitan hacer uso de ellas, para mantener un sistema de información durante su ejecución.

f) Fiabilidad

Es la permanencia de un servicio por un largo tiempo. Además, que desempeñe su labor correctamente durante ese tiempo sin tener ningún problema. Existen también dos tipos de fiabilidad como:

- **Fiabilidad del hardware:** cuanta y cuál es la probabilidad de que el hardware falle y cuánto tiempo y dinero cuesta repáralo.
- **Fiabilidad del software:** Que tan fácil es que un sistema a la hora de utilizarlo nos devuelva una salida incorrecta, ya sea por el mal manejo del software o por un error que este tenga.

2.2.2. Bases teóricas de la segunda variable "Seguridad en Sistemas de Información"

Para los autores Laudon, Kenneth C. y Laudon Jane P. (2012), es la agrupación de componentes los cuales se encuentran interrelacionados para así poder recabar datos, para realizar el procesamiento de los datos, seguidamente realizar el almacenamiento, y su posterior distribución de información permitiendo así realizar la toma de decisiones. Por lo cual intervienen tres actividades: entrada, proceso y salida.

De igual manera el autor Gómez Vieites, A (2014), define Seguridad de la información como un conjunto de controles que permitirán prevenir riesgos a las organizaciones, para así mantener resguardado y protegido la información, manteniendo la confidencialidad, disponibilidad e integridad.

La Seguridad en Sistemas de Información, las dimensiones se obtuvieron de la tesis del autor Suyo Cruz (2017)donde sus dimensiones presentan relación con la seguridad en sistemas de información como se presenta a continuación:

a) Dimensión Elementos tangibles

Para el autor Matsumoto Nishizawa, Reina (2014), es todo aquello infraestructura física que se puede tocar como los ordenadores, materiales, empleados, etc. De igual manera el autor Jo Bitner (2004) concuerda con la definición de elementos tangibles.

Por otro lado, la Universidad Peruana de Ciencia Aplicadas (2007) concuerda con la definición de los anteriores autores, pero además menciona que todos esos elementos dentro de la empresa permiten construir y proyectar lealtad.

b) Dimensión Fiabilidad

El autor Farfán Machaco, Yheni (2007) describe la fiabilidad de un sistema el cual no tenga fallos y así evitar al mínimo el riesgo, desde el inicio hasta el final de la creación del producto o proceso.

En la revista ABB (2009) define que la fiabilidad es la disminución de problemas en los sistemas. Es tener la capacidad de identificar problemas dentro del sistema y realizar la relación pertinente de ello para evitar problemas de funcionamiento.

c) Dimensión Capacidad de respuesta

Según el autor Fontalvo y Vergara (2010) para él es la forma que como se brinda la atención a los ciudadanos por parte de los trabajadores, así como las habilidades que muestras y la confianza que genera.

El autor Camisón, Cruz y Gonzales (2006) coincide en con la definición del autor anterior debido a que el dar un servicio de manera eficiente y rápida al usuario.

2.3. Definición de términos

2.3.1. Sistema

Para el autor Zornoza, Cruz y Gonzales (2007) es la suma de elementos los cuales se encuentran interrelacionados y por lo cual interactúan entre sí.

2.3.2. Seguridad

Se puede definir a la seguridad que posee múltiples usos. Según el autor Gardey (2017). Una cosa segura es algo firme por lo cual se considera como una certeza.

2.3.3. Información

Según Definición (2017). Es el conjunto de diferentes datos ordenados, que permiten la construcción de uno o varios mensajes. Los mensajes permiten realizar la toma de decisiones para resolver algún problema.

2.3.4. TIC

Para García Canal, Rialp Criado, y Rialp Criado (2007). Las Tecnologías de información y comunicaciones permiten la eliminación de las barreras temporales, permitiendo unir equipos geográficamente separados para que así puedan trabajan desde diversas localizaciones y diferentes zonas horarias.

2.3.5. Normas ISO

Según una publicación en su sitio web (2015) menciona que es una organización que crea estándares que permiten que la calidad de la información se mantenga, la seguridad no se vea alterada y la eficacia se mantenga en los productos y servicios.

2.3.6. ISO 27001

En su artículo detalla que la Norma Internacional (2017). Se enfoca en el aseguramiento, la confidencialidad e integridad de los datos y de la información. Es una herramienta que permite mejorar la seguridad a través de su implementación y así permitan salvaguardar la información debido que es el activo de mayor importancia de una organización.

2.3.7. Sistema de información

Para el autor Whitten, J. et al (1996) es el conjunto de datos, redes, empleados y tecnologías las cuales se interrelacionan con el fin de mejorar los

procesos que se encuentran dentro de la organización. Debido a que todas funciones se unen en una sola, haciendo posible capturar de datos, almacenarlos, procesarlos y su posterior salida en forma de información.

2.3.8. Seguridad de la Información

Según Gómez, A (2011) define como las medias que permitan bloquear la ejecución de operaciones que no sean previamente autorizadas sobre algunos sistemas o red informática, que su manipulación pueda alterar o dañar la información o bloquear el acceso de usuarios.

CAPÍTULO III: MARCO METODOLÓGICO

3.1. Tipo y Nivel de la Investigación

3.1.1. Tipo de Investigación

Tipo Básica

Para el autor Muntané Relat (2010) Es una investigación el cual permite el incremento de conocimiento, pero sin el contraste con algún aspecto práctico. De igual manera el autor Nicomedes Teodoro (2014) considera que es una investigación la cual busca conocimiento, además de servir para la investigación aplicada.

Nivel Correlacional

Es el enfoque que permite determinar la existencia del grado de relación entre dos o más variables en una misma muestra, para lo cual se hace uso de técnicas o pruebas estadísticas relacionadas con el análisis de correlación según Sánchez et al (2018).

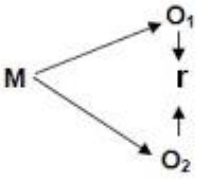
Para Hurtado de Barrera (2010) lo aprehensivo, implica la búsqueda de aspectos no tan evidentes en el evento de estudio, de aquello que parece oculto y subyace a la organización interna del evento, por ejemplo: analizar o comparar.

Esta tesis considera usar la Norma Técnica Peruana 27001:2014 ISO/IEC para establecer, implementar, utilizar, monitorear, revisar, mantener y mejorar la seguridad en sistemas de información de la Municipalidad Gregorio Albarracín, 2022. La correlación busca establecer la relación entre la variable V1 y la variable V2.

El nivel de investigación es aprehensivo ya que con esta investigación compararemos las 2 variables.

3.1.2. Diseño de Investigación

Para Hernández et-al (2014), define a la investigación no experimental, la cual se realiza sin ningún tipo de manipulación a las variables. Por lo cual solo se realiza la observación de los fenómenos como se desarrollan en su ambiente, para su posterior análisis.



Donde:

M = Muestra

O_1 = Observación de la V.1.

O_2 = Observación de la V.2.

r = Correlación entre dichas variables.

Así mismo según Hernández et-al (2014), un diseño no experimental de corte transversal y correlacional, es un diseño el cual obtiene los datos de un grupo, pero en un solo momento, es decir en un tiempo determinado. Para así describir las variables y realizar el análisis de su incidencia.

Esta tesis considera usar la Norma Técnica Peruana 27001:2014 ISO/IEC para establecer, implementar, utilizar, monitorear, revisar, mantener y mejorar la seguridad en sistemas de información de la Municipalidad Gregorio Albarracín, 2022. La Correlación busca establecer la relación entre la variable V1 y la variable V2. El diseño es No experimental de corte transversal correlacional.

3.2. Población y/o muestra de estudio

3.2.1. Población

La población viene hacer el conjunto de personas que según él aturo Hernández et al. (2014) Poseen características similares. De igual manera el Instituto Nacional de Estadística e Informática (2006), también define que es un conjunto de elementos que se encuentran en un lugar y tiempo específico y que pueden ser finitas e infinitas.

Para la presente investigación se tomó en cuenta a los empleados de las Gerencias y Sub Gerencias que existen dentro de la Municipalidad Gregorio Albarracín como:

Gerencia de Contabilidad de Administración, Gerencia Municipal, secretaria general, Administración Tributaria, Gerencia de Desarrollo Urbano y la Sub Gerencia de Gestión de Recursos Humanos, Tecnologías de la información y comunicación, Tesorería, Logística, Catastro y Margesí de bienes. En la tabla 5. Se puede observar las diferentes Gerencias y Sub Gerencias, así como la cantidad de empleados.

Tabla 5

Tabla de la Población del Personal de la Municipalidad

Gerencia / Sub Gerencia	Cantidad de empleados
Gerencia Municipal	7
Gerencia de Administración	6
Gerencia de Desarrollo Urbano	10
Gerencia de Administración Tributaria	10
Gerencia de secretaria general	6
Sub Gerencia de Contabilidad	10
Sub Gerencia de Tesorería	10
Sub Gerencia de Logística	10
Sub Gerencia TIC	10
Sub Gerencia de Catastro y Margesí	11
Sub Gerencia de Gestión de Recursos Humanos	10
Total	**100**

Fuente. Obtenida del Área de Recursos Humanos de la Municipalidad.

3.2.2. Muestra

Es la porción de algo según Tomás Sábado, J. (2009) , por tal motivo una muestra se puede decir que es parte de la población, a la cual se observa para estudiar y de la cual se obtendrán conclusiones.

De la misma manera el autor Tamayo y Tamayo (2000) lo define como una selección de un conjunto de elementos que se desea averiguar algo sobre la población, por tal motivo para conocer las características de las variables del estudio en la Municipalidad Gregorio Albarracín se calculó la muestra utilizando la fórmula para poblaciones finitas.

Por tanto, se aplicó el muestreo de población finita, el cual, según Malhotra, N. (2004) es aquel donde cada uno de los elementos de la población posee exactamente las mismas probabilidades de selección. Cada uno de los elementos de la muestra se selecciona de manera independiente de los otros elementos, se compara con el sistema de lotería.

$$\boldsymbol{n} = \frac{N * Z^2 * p * q}{e^2 * (N-1) + Z^2 * p * q} \quad (1)$$

Donde:

N = Total de la población

Z= 1,96 al cuadrado (si la seguridad es del 95 %)

p = proporción esperada (en este caso 5 % = 0,05)

q = 1 – p (en este caso 1-0,05 = 0,95)

e = precisión (en esta investigación un 5 %).

El resultado de la aplicación de la fórmula es de 79,51 por la cual se redondea a 80 trabajadores, los cuales tienen acceso e interactúan con los sistemas informáticos de la institución.

3.3. Operacionalización de las variables

Variable Norma Técnica Peruana 27001:2014 ISO-IEC

Def. Conceptual:

Conjunto de buenas prácticas para garantizar el resguardo y la protección de los datos, asegurando que los peligros asociados sean conocidos, asumidos, gestionados y minimizados.

Def. Operacional:

La NTP-ISO/IEC 27001:2014 se refiere a la confidencialidad, la integridad y la disponibilidad de la información y los datos importantes para la organización, cuenta con 3 dimensiones y se medirá mediante una encuesta de 12 ítems.

A continuación, se muestra la tabla 6, donde se detalla las dimensiones de la variable Norma Técnica Peruana 27001:2014 y de mas aspectos correspondientes a la tabla de operacionalización de variable.

Tabla 6

Tabla de Operacionalización de la Variable Norma Técnica Peruana 27001:2014 ISO-IEC

Variables	Dimensiones	Indicadores	Ítems	Instrumento	Escala de Medición	Niveles y Rango
Variable: Norma Técnica Peruana 27001:2014 ISO-IEC	Confidencialidad	• Control de Acceso • Autorización	01-04	Cuestionario	LIKERT 1. Totalmente en desacuerdo 2. En desacuerdo 3. Indeciso 4. De acuerdo 5. Totalmente de acuerdo	1) Bajo (4-9) 2) Medio (10-15) 3) Alto (16-20)
	Integridad	• Seguridad para las comunicaciones • Seguridad para los procedimientos	05-08			1) Bajo (4-9) 2) Medio (10-15) 3) Alto (16-20)
	Disponibilidad	• Acceso en el momento solicitado • Acceso a los datos	09-12			1) Bajo (4-9) 2) Medio (10-15) 3) Alto (16-20)

Variable Seguridad en Sistemas de Información

Def. Conceptual:

Es el conjunto de medidas, así como de herramientas las cuales permitan prevenir, proteger y poder reaccionar frente a un ataque que atente contra la información.

Def. Operacional:

La Seguridad en Sistemas de Información se refiere a las herramientas de seguridad y métodos para aumentar las medidas de protección de la información, cuenta con 3 dimensiones y se medirá mediante una encuesta de 14 ítems.

A continuación, se muestra la tabla 7, donde se detalla las dimensiones de la variable Seguridad en Sistemas de Información y de más aspectos correspondientes a la tabla de operacionalización de variable.

Tabla 7

Tabla de Operacionalización de la Variable Seguridad en Sistemas de Información

Variables	Dimensiones	Indicadores	Ítems	Instrumento	Escala de Medición	Niveles y Rango
Variable: Seguridad en Sistemas de Información	Elementos tangibles	• Equipos • Almacenamiento • Condiciones generales	01-06	Cuestionario	LIKERT 1. Totalmente en desacuerdo 2. En desacuerdo 3. Indeciso 4. De acuerdo 5. Totalmente de acuerdo	1) Bajo (6-14) 2) Medio (15-21) 3) Alto (22-30)
	Fiabilidad	• Compromiso • Servicio prometido	07-10			1) Bajo (4-9) 2) Medio (10-15) 3) Alto (16-20)
	Capacidad de Respuesta.	• Tiempo de respuesta • Mejora continua	11-14			1) Bajo (4-9) 2) Medio (10-15) 3) Alto (16-20)

3.4. Técnicas e instrumentos para la recolección de datos

Se ha utilizado la encuesta como técnica de recolección de datos y el cuestionario como instrumento, el cual fue ejecutado a los empleados de la entidad pública que en este caso corresponde a una municipalidad de acuerdo al diseño de la investigación, para obtener la información necesaria del presente trabajo de investigación.

Se diseñó un conjunto de preguntas de selección múltiple utilizando la escala Likert, los cuales han sido organizadas en un orden ordinal que permita comprender a los encuestados.

Técnica:

La técnica que se empleó en esta investigación fue la encuesta, según Carrasco Diaz (2019), es la técnica utilizada para estudios económicos o sociales, la cual permite recoger la información a partir de fuentes directas, lo cual le otorga un grado de fiabilidad para poder contrastar y analizar los resultados.

Instrumento:

El instrumento utilizado fue el cuestionario. De acuerdo con Carrasco Diaz (2019), el cuestionario es considerado como un canal de comunicación, entre la persona encuestada y quien aplica la encuesta. Esto permite que los propósitos y las variables del estudio se correlacionen, mediante un conjunto de interrogantes individuales.

El cuestionario incluye preguntas las cuales fueron formuladas de acuerdo a las variables de estudio, dimensiones e indicadores según la tabla de operacionalización de variables la cual se encuentra en el Anexo 02 y 03.

Validez de los instrumentos:

El Instrumento a utilizar, fue validado mediante el juicio de expertos. Según Dorantes et al. (2016), indican que, a partir de la selección de expertos se emitirá una invitación personalizada explicando los objetivos de la prueba, el propósito de la herramienta y los parámetros u otras técnicas para contextualizar a los examinadores; así como un link o enlace de acceso a la plataforma de encuestas. Se puede encontrar en el Anexo 09.

A continuación, en la tabla 8 se muestra los nombres de los tres expertos.

Tabla 8

Expertos validadores

	Nombre de los expertos	
Experto 1	Mg. Víctor Jimenez Flores	Especialista
Experto 2	Mg. Ricardo Carlos Inquilla Quispe	Especialista
Experto 3	Mg. Patrick José Cuadros Quiroga	Especialista

Confiabilidad del instrumento:

La confiabilidad del instrumento se determinó con base en lo que afirman Hernández et al. (2014), para asegurar que este pueda tener suficientes repeticiones sobre un mismo elemento o sujeto y que se produzcan los mismos resultados.

Se aplicó el coeficiente de Alfa de Cronbach, cuyo método es de consistencia que ha permitido apreciar el nivel de confianza del instrumento.

Tabla 9

Tabla de confiabilidad de la variable NTP-ISO/IEC 27001:2014

Estadística de fiabilidad	
Alfa de Cronbach	N de elementos
0,872	12

En la tabla 9, se puede apreciar el valor del coeficiente Alfa de Cronbach es 0,872 o 88 % obtenido de 12 ítems de la variable Norma Técnica Peruana 27001:2014. Dicho valor nos indica que la confiabilidad es alta para la variable Norma Técnica Peruana 27001:2014, entendiéndose que el instrumento aplicado es confiable y puede ser empleado para recolectar datos de la muestra elegida.

Tabla 10

Tabla de confiabilidad de la variable Seguridad en Sistemas de Información

Estadística de fiabilidad	
Alfa de Cronbach	N de elementos
0,843	14

En la tabla 10, se puede apreciar el valor del coeficiente Alfa de Cronbach es 0,843 o 86 % obtenido de 14 ítems de la variable seguridad en sistemas de información. Dicho valor nos indica que la confiabilidad es alta para la seguridad en sistemas de información, entendiéndose que el instrumento aplicado es confiable y puede ser empleado para recolectar datos de la muestra elegida.

Análisis Factorial:

Por otro lado, Malhotra, N. (2004) manifiesta que se usa con carácter exploratorio para identificar factores, sin restricciones o hipótesis previas.

En el análisis factorial, los factores son seleccionados para explicar las relaciones entre las variables. Se puede encontrar en el Anexo 06.

3.5. Procesamiento y análisis de datos

¿Cómo se preparan los datos o respuestas para analizarlos?

Como dice Encinas, (1993) los datos en sí mismos tienen limitada importancia, es necesario “hacerlos hablar”, en ello consiste, en esencia, el análisis e interpretación de los datos. El proceso del análisis de los datos se esquematiza según Moscariello, (2017) en:

- Describir el tratamiento estadístico de los datos a través de gráficos, tablas, cuadros, dibujos diagramas, generado por el análisis de los datos.

- Describir datos, valores, puntuación y distribución de frecuencia.

A continuación, se muestra la tabla 11, en la cual se observa el instrumento utilizado, así como el procesamiento de información.

Tabla 11

Tabla de Instrumento y procesamiento de información

Instrumento	Procesamiento de información
Cuestionario de preguntas para los empleados de la Municipalidad Gregorio Albarracín que hacen uso del sistema. Sobre la correlación entre la Norma Técnica Peruana 27001:2014 y la Seguridad en sistemas de información	La información cuantitativa recolectada a través de este instrumento se plasmó en tablas y gráficos estadísticos con su posterior análisis porcentual y analítico. La herramienta que fue usada para la creación de todas nuestras tabulaciones fue el Software SPSS versión 25.
Análisis de contenido	Se utilizó Rho de Spearman para medir la correlación entre las variables. Todos los datos e información recolectada para realizar las tablas de frecuencia de cada pregunta de la encuesta por medio del Software SPSS versión 25.

Técnica de procesamiento

Se realizará una encuesta al personal que hace uso del sistema de la Municipalidad Gregorio Albarracín, sobre la correlación entre la Norma Técnica Peruana 27001:2014 y la Seguridad en sistemas de la información.

Técnica de análisis de datos

Se utilizó Rho de Spearman para medir la correlación entre las variables y las tablas de frecuencia para analizar los datos recolectados de cada pregunta de la encuesta por medio del Software SPSS versión 25.

CAPÍTULO IV: RESULTADOS

4.1. Prueba de Normalidad

Tabla 12

Tabla de Prueba de Kolmogorov-Smirnov

		Norma Técnica Peruana 27001:2014 ISO-IEC	Seguridad en Sistemas de Información
N		80	80
Parámetros normales[a,b]	Media	51,1250	57,1875
	Desv. Desviación	5,48963	5,99387
Máximas diferencias extremas	Absoluto	0,119	0,141
	Positivo	0,119	0,141
	Negativo	-0,075	-0,085
Estadístico de prueba		0,119	0,141
Sig. asintótica(bilateral)		0,007[c]	0,000[c]

a. La distribución de prueba es normal.

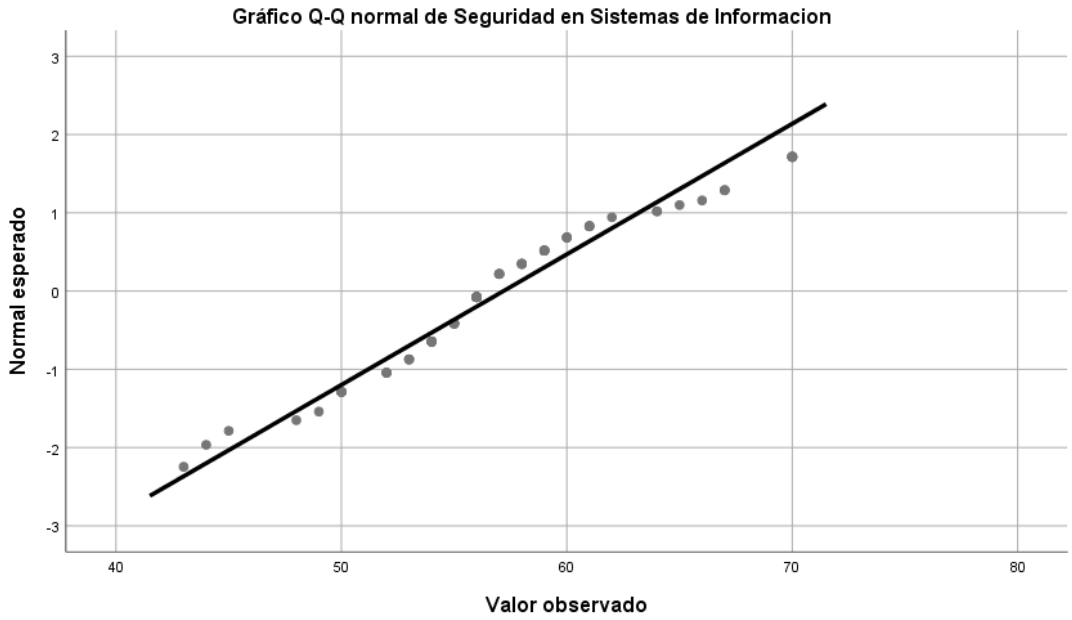
b. Se calcula a partir de datos.

c. Corrección de significación de Lilliefors.

Interpretación: en la tabla 12 titulada Prueba de Kolmogorov-Smirnov vemos que el valor de la variable de Seguridad en Sistemas de Información fue 57,18 con una desviación estándar de 5,99.

Figura 1

Gráfica de Normalidad de Seguridad en Sistemas de Información



Así mismo en la figura 1 se puede observar que la muestra el valor del estadígrafo que es Z de Kolmogorov-Smirnov es de 0,141. Ahora vemos el valor de p (Sig. asintót (bilateral)) fue de 0,00.

Como el valor de p fue menor que 0,05 se rechaza la hipótesis nula y se concluye que no hay evidencias suficientes para pensar que la muestra proviene de la distribución especificada, con un nivel de significancia del 5 %.

4.2. Resultados estadísticos descriptivos

Tablas cruzadas de las V1 y V2: Norma Técnica Peruana 27001:2014 ISO-IEC y Seguridad en Sistemas de Información

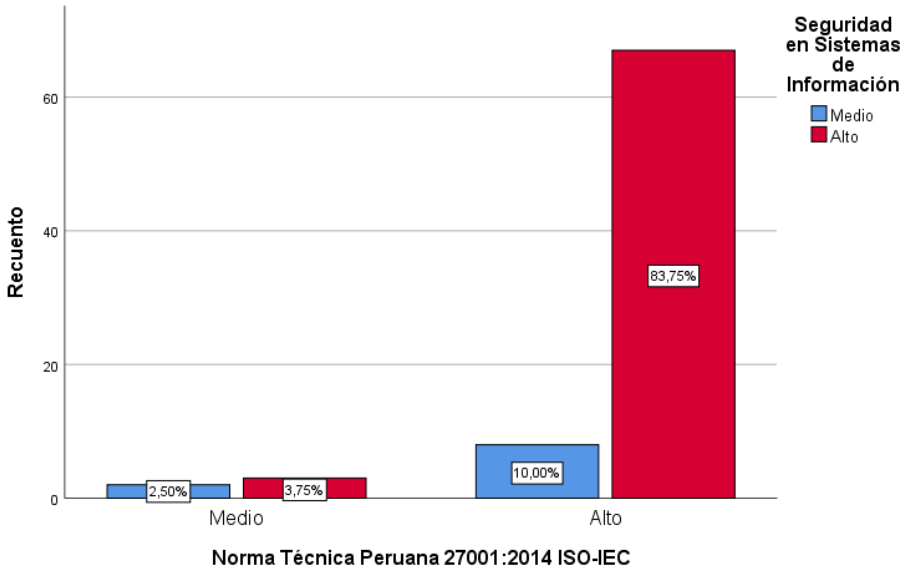
Tabla 13

Tabla cruzada de Norma Técnica Peruana 27001:2014 ISO-IEC y Seguridad en Sistemas de Información

			Seguridad en Sistemas de Información		Total
			Medio	Alto	
Norma Técnica Peruana 27001:2014 ISO-IEC	Medio	Recuento	2	3	5
		% del total	2,5 %	3,8 %	6,3 %
	Alto	Recuento	8	67	75
		% del total	10,0 %	83,8 %	93,8 %
Total		Recuento	10	70	80
		% del total	12,5 %	87,5 %	100,0 %

Figura 2

Gráfica de Norma Técnica Peruana 27001:2014 ISO-IEC y Seguridad en Sistemas de Información



Interpretación: Como se puede apreciar en la tabla 13 y en la figura 2, se muestra los porcentajes de la variable 1 Norma Técnica Peruana 27001:2014 ISO-IEC y la variable 2 Seguridad en Sistemas de Información, se puede interpretar que 6,3 % (5) consideran un nivel medio alto y el 93,8 % (75) consideran un nivel alto, según la percepción del personal de la Municipalidad que han participado.

Análisis: Como se puede apreciar con los valores obtenidos los encuestados están de acuerdos que la Norma Técnica Peruana 27001:2014 ISO-IEC, el cual abarca los puntos de confidencialidad, integridad y disponibilidad en las encuestas realizadas. Están relacionados con la Seguridad en Sistemas de Información, en específico con sus dimensiones que son elementos tangibles, fiabilidad y capacidad de respuesta.

4.2.1. Resultado del primer objetivo específico: Fiabilidad

Esta dimensión se encuentra asociada a dos indicadores con sus respectivas preguntas que fueron parte de la encuesta. Por lo cual a través del cuestionario realizado se obtuvo los presentes resultados que se observan en la siguiente tabla.

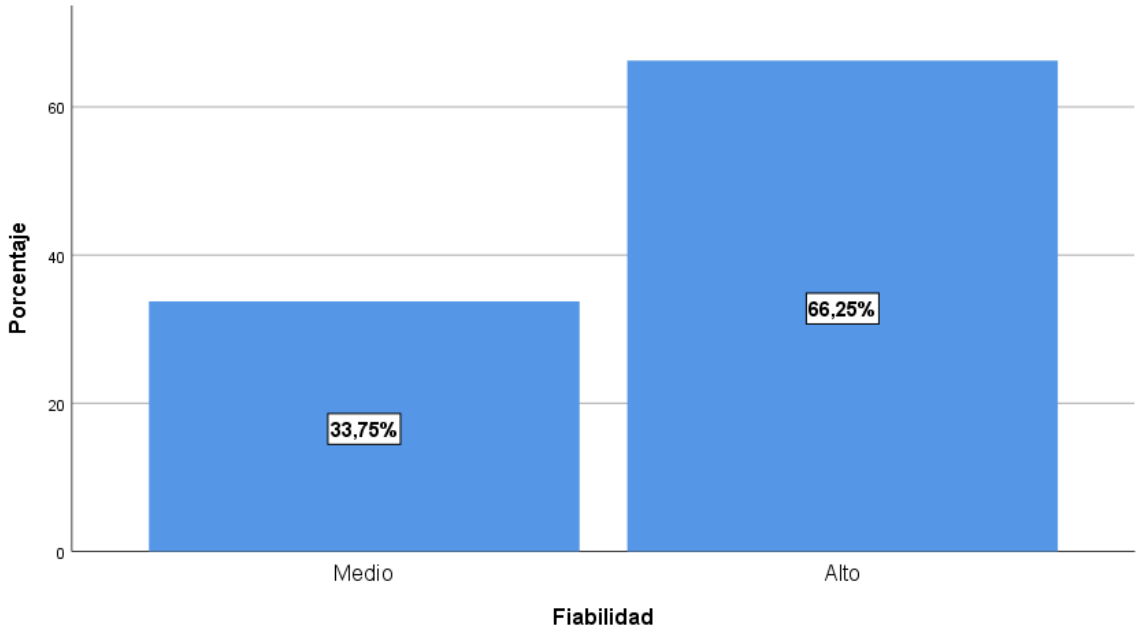
Tabla 14

Tabla de Frecuencias de la Dimensión Fiabilidad

		Frecuencia	Porcentaje	Porcentaje acumulado
Válido	Bajo	0	0	0
	Medio	27	33.8	33.8
	Alto	53	66,3	100,0
	Total	80	100,0	

Figura 3

Gráfica de la dimensión fiabilidad



Interpretación: Como se puede observar en la tabla 14 y en la figura 3, los porcentajes de la dimensión 1 Fiabilidad de la variable 2 Seguridad en Sistemas de Información, donde se puede entender que un 66,25 % (53) consideran Alto y un 33,75 % (27) consideran Medio.

Análisis: Como se puede apreciar con los valores obtenidos los encuestados están de acuerdos que la fiabilidad es de suma importancia debido a que abarca aspectos relacionados con el compromiso de los trabajadores para con el área, así como con el servicio prometido que concierne al acceso a la información.

4.2.2. Resultado del segundo objetivo específico: Capacidad de Respuesta

Esta dimensión se encuentra asociada a dos indicadores con sus respectivas preguntas que fueron parte de la encuesta. Por lo cual a través del cuestionario realizado se obtuvo los presentes resultados que se observan en la siguiente tabla.

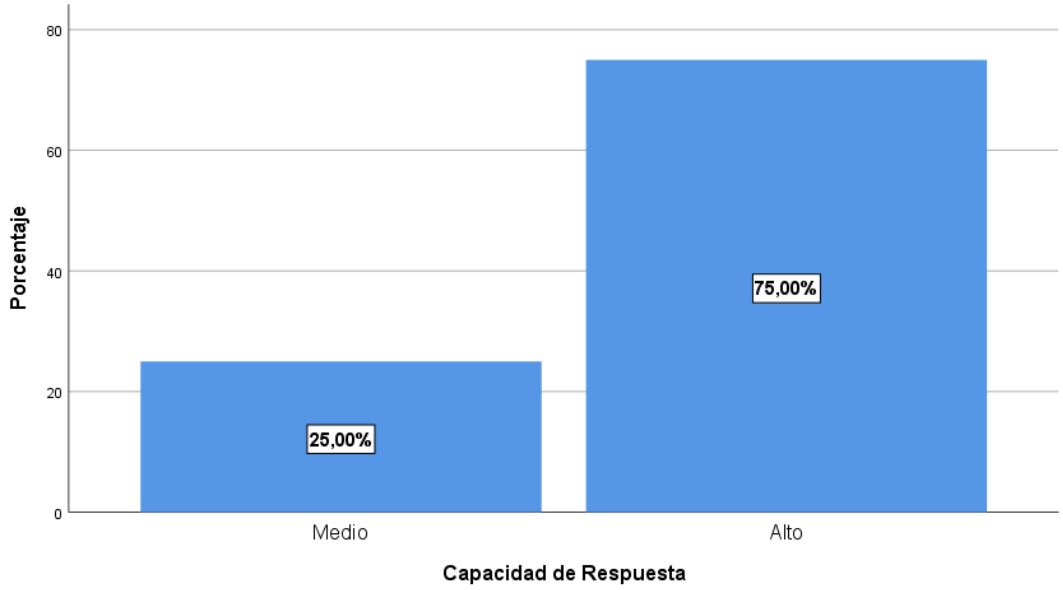
Tabla 15

Tabla de Frecuencias de la Dimensión Capacidad de Respuesta.

		Frecuencia	Porcentaje	Porcentaje acumulado
Válido	Bajo	0	0	0
	Medio	20	25,0	25,0
	Alto	60	75,0	100,0
	Total	80	100,0	

Figura 4

Gráfica de la dimensión capacidad de respuesta



Interpretación: Como se puede observar en la tabla 15 y en la figura 4, los porcentajes de la dimensión 2 Capacidad de Respuesta de la variable 2 Seguridad en Sistemas de Información, donde se puede entender que un 75,00 % (60) consideran Alto y un 25,0 % (20) consideran Medio.

Análisis: Como se puede apreciar con los valores obtenidos, los encuestados en su mayoría (60 trabajadores) están de acuerdo que la capacidad de respuesta, influye en la seguridad de los sistemas de información; así como la mejora continua también permite fortalecer la seguridad manteniendo la información a salvo.

4.2.3. Resultado del tercer objetivo específico: Elementos Tangibles

Esta dimensión se encuentra asociada a dos indicadores con sus respectivas preguntas que fueron parte de la encuesta. Por lo cual a través del cuestionario realizado se obtuvo los presentes resultados que se observan en la siguiente tabla.

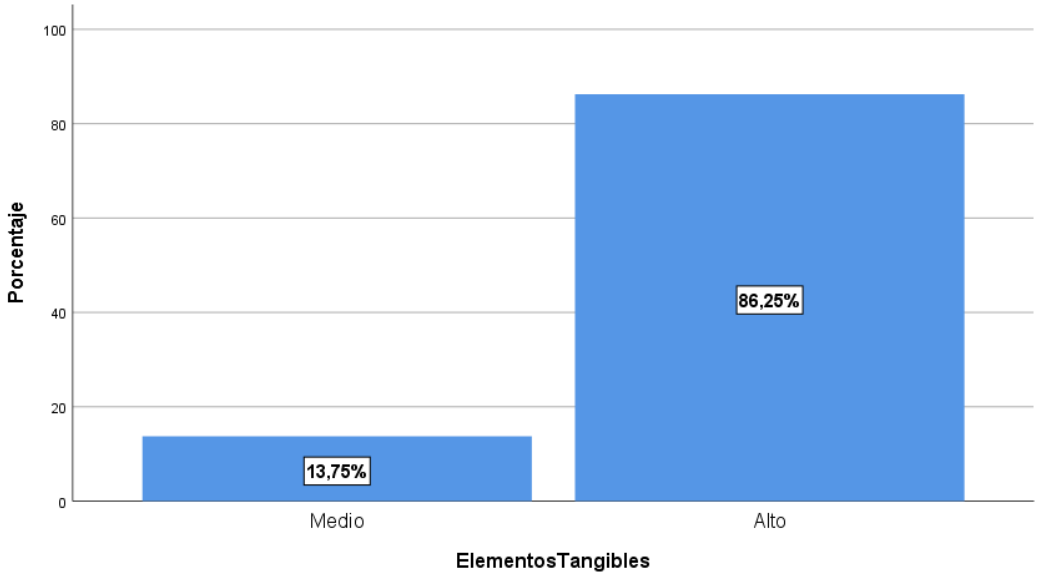
Tabla 16

Tabla de Frecuencias de la Dimensión Elementos Tangibles

		Frecuencia	Porcentaje	Porcentaje acumulado
Válido	Bajo	0	0	0
	Medio	11	13,8	13,8
	Alto	69	86,3	100.0
	Total	80	100.0	

Figura 5

Gráfica de la dimensión elementos tangibles



Interpretación: Como se puede observar en la tabla 16 y en la figura 5, los porcentajes de la dimensión 3 Elementos tangibles de la variable 2 Seguridad en Sistemas de Información, donde se puede entender que un 86,25 % (69) consideran Alto y un 13,75 % (11) consideran Medio.

Análisis: Como se puede apreciar con los valores obtenidos, 69 trabajadores encuestados están de acuerdo que los elementos tangibles, es considerado como uno de los puntos importantes debido que sin los equipos informáticos no es posible mantener una seguridad en los sistemas, así como un correcto plan de almacenamiento como los requisitos mínimos (condiciones generales) para que se pueda mantener la seguridad de los sistemas de información que existen.

4.2.4. Resultado de la Dimensión 1 Variable 2 y la Variable 1.

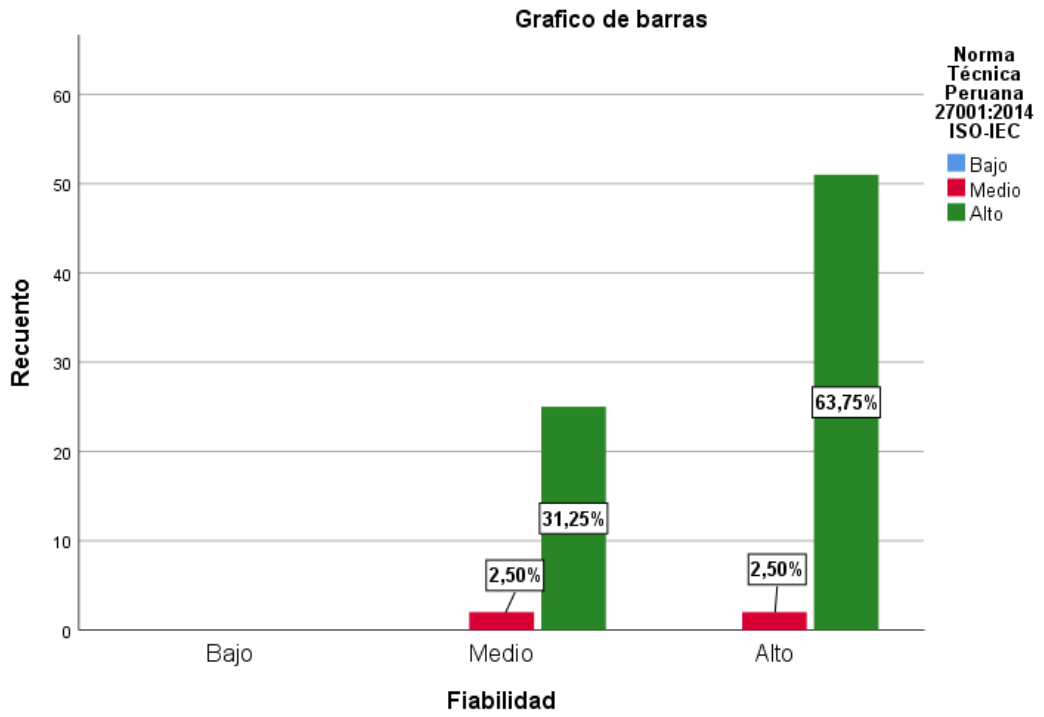
Tabla 17

Tabla cruzada de Fiabilidad y la Norma Técnica Peruana 27001:2014 ISO-IEC

			Norma Técnica Peruana 27001:2014 ISO-IEC		Total
			Medio	Alto	
Fiabilidad	Medio	Recuento	2	25	27
		% del total	2,5 %	31,3 %	33,8 %
	Alto	Recuento	2	51	53
		% del total	2,5 %	63,7 %	66,3 %
Total		Recuento	4	76	80
		% del total	5,0 %	95,0 %	100,0 %

Figura 6

Gráfica Tabla cruzada de Fiabilidad y la Norma Técnica Peruana 27001:2014 ISO-IEC



Interpretación: Como se puede apreciar en la tabla 17 y en la figura 6, se muestra los porcentajes de la dimensión 1 Fiabilidad de la variable 2 Seguridad en Sistemas de Información y la variable 1 Norma Técnica Peruana 27001:2014 ISO-IEC, se puede interpretar que 33,80 % (27) considera un nivel medio y el 66,03 % (53) considera un nivel alto.

Análisis: Se puede analizar que 76 encuestados están de acuerdo que la fiabilidad es de suma importancia debido que acabar puntos importantes que se encuentran relacionados con la Norma Técnica Peruana 27001:2014.

Se puede analizar que el 63,75 % de los encuestados percibe en base de los Reactivos que el compromiso de los trabajadores y brindar el servicio prometido son importantes para la fiabilidad en la Norma Técnica Peruana 27001:2014 ISO-IEC, a fin de cumplir con los estándares del usuario final.

4.2.5. Resultado de la Dimensión 2 Variable 2 y la Variable 1.

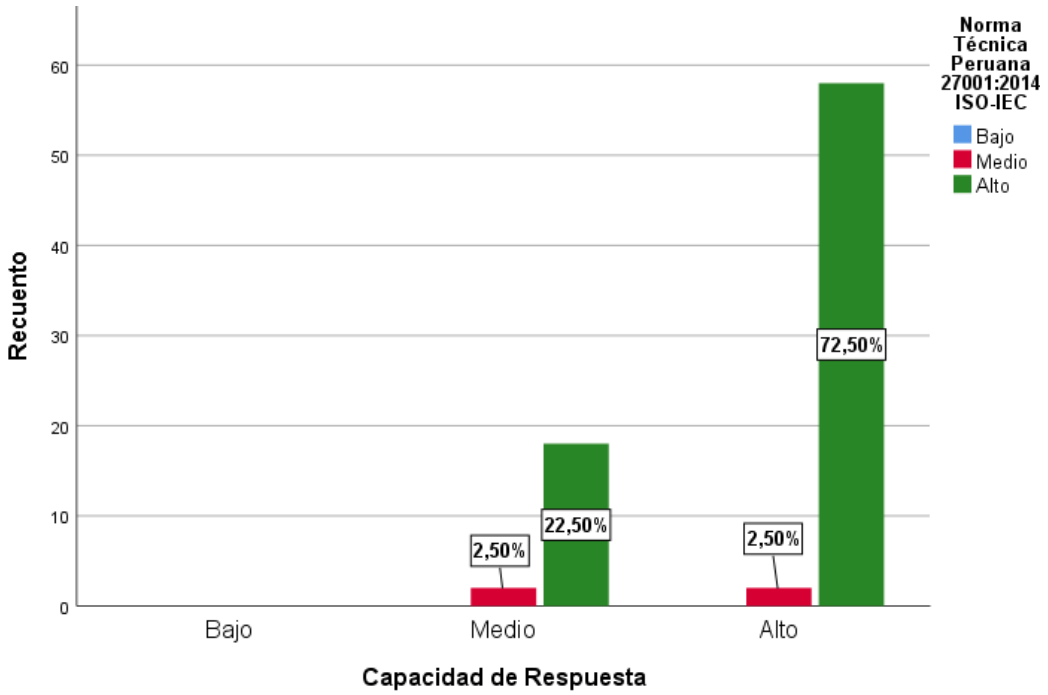
Tabla 18

Tabla cruzada de Capacidad de Respuesta y la Norma Técnica Peruana 27001:2014 ISO-IEC.

			Norma Técnica Peruana 27001:2014 ISO-IEC		Total
			Medio	Alto	
Capacidad de Respuesta	Medio	Recuento	2	18	20
		% del total	2,5 %	22,5 %	25,0 %
	Alto	Recuento	2	58	60
		% del total	2,5 %	72,5 %	75,0 %
Total		Recuento	4	76	80
		% del total	5,0 %	95,0 %	100,0 %

Figura 7

Gráfica Tabla cruzada de Capacidad de Respuesta y Seguridad en Sistemas de Información.



Interpretación: Como se puede apreciar en la tabla 18 y en la figura 7, se muestra los porcentajes de la dimensión 2 Capacidad de Respuesta de la variable 2 Seguridad en Sistemas de Información y la variable 1 Norma Técnica Peruana 27001:2014 ISO-IEC, se puede interpretar que 25,0 % (20) considera un nivel medio y el 75,0 % (60) considera un nivel alto.

Análisis: Se puede analizar que 76 encuestados están de acuerdo que la capacidad de respuesta es de suma importancia debido que acabar puntos importantes que se encuentran relacionados con la Norma Técnica Peruana 27001:2014.

Se puede analizar que el 72,50 % de los encuestados percibe en base a los Reactivos que hablan del tiempo de respuesta y la mejora continua de los procesos son esenciales para la capacidad de respuesta en la seguridad del sistema de información; entiendo que estos elementos son importantes para lograr efectivizar la capacidad de respuesta.

4.2.6. Resultado de la Dimensión 3 Variable 2 y la Variable 1.

Tabla 19

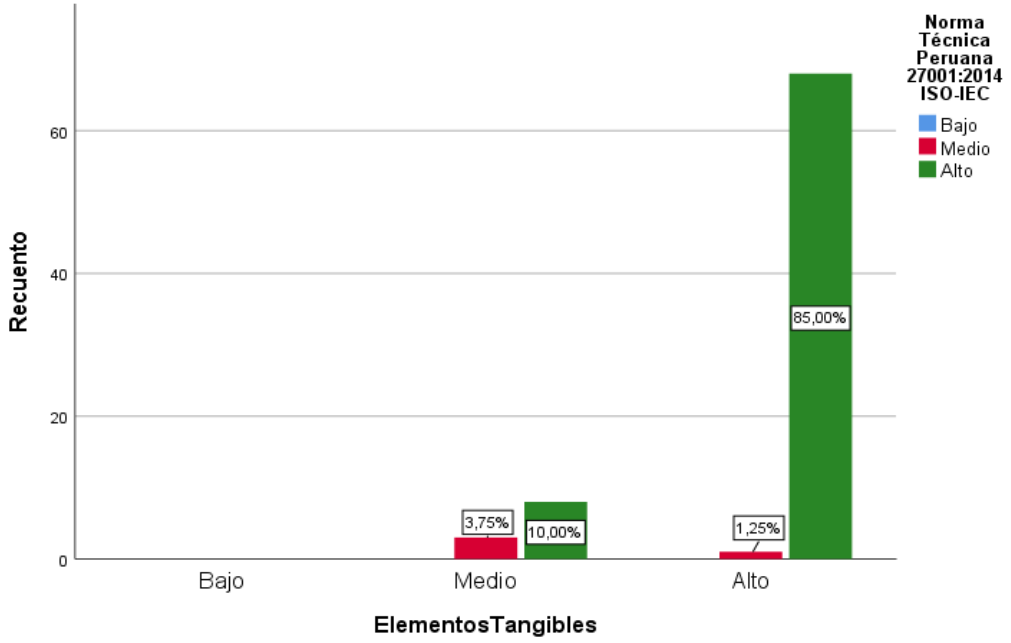
Tabla cruzada de Elementos Tangibles y la Norma Técnica Peruana 27001:2014 ISO-IEC

Tabla cruzada Elementos Tangibles y Norma Técnica Peruana 27001:2004 ISO-IEC

			Norma Técnica Peruana 27001:2014 ISO-IEC		Total
			Medio	Alto	
Elementos Tangibles	Medio	Recuento	3	8	11
		% del total	3,8 %	10,0 %	13,8 %
	Alto	Recuento	1	68	69
		% del total	1,3 %	85,0 %	86,3 %
Total		Recuento	4	76	80
		% del total	5,0 %	95,0 %	100,0 %

Figura 8

Gráfica Tabla cruzada de Elementos Tangibles y la Norma Técnica Peruana 27001:2014 ISO-IEC



Interpretación: Como se puede apreciar en la tabla 19 y en la figura 8, se muestra los porcentajes de la dimensión 3 Elementos Tangibles de la variable 2 Seguridad en Sistemas de Información y la variable 1 Norma Técnica Peruana

27001:2014 ISO-IEC, se puede interpretar que 13,80 % (11) considera un nivel medio y el 86,3 % (69) considera un nivel alto.

Análisis: Se puede analizar que 76 encuestados están de acuerdo que la fiabilidad es de suma importancia debido que acabar puntos importantes que se encuentran relacionados con la Norma Técnica Peruana 27001:2014.

Se puede analizar que el 85,00 % de los encuestados percibe en base a los Reactivos que hablan de los equipos informáticos y equipo de almacenamiento son importantes para los Elementos Tangibles en la Norma Técnica Peruana 27001:2014 ISO-IEC; entiendo que estos elementos son importantes para lograr efectivizar la capacidad de respuesta.

4.3. Resultados estadísticos inferenciales

Finalmente, para probar las hipótesis, se utilizó la estadística descriptiva no paramétrica coeficiente de correlación de Spearman, debido a que las hipótesis buscan demostrar la relación entre sus variables y dimensiones.

4.3.1. Contrastación de la hipótesis general

H_0: La Norma Técnica Peruana 27001:2014 ISO-IEC no se correlaciona positivamente con la seguridad en sistema de información de la Municipalidad Gregorio Albarracín, Tacna 2022.
H_1: La Norma Técnica Peruana 27001:2014 ISO-IEC se correlaciona positivamente con la seguridad en sistema de información de la Municipalidad Gregorio Albarracín, Tacna 2022.

Nivel de significación $\alpha = 0,05 = 5\ \%$
Regla de decisión: Si $p \geq \alpha$, se acepta H_1; Si $p < a$, se rechaza H_0
Prueba de estadística: Rho de Spearman, debido a que las variables tienen escala ordinal.

Tabla 20

Grado de correlación entre la Norma Técnica Peruana 27001:2014 ISO-IEC y la Seguridad en Sistemas de Información

Rho de Spearman	Seguridad en sistemas de información	
Norma Técnica Peruana 27001:2014 ISO-IEC	Coeficiente de correlación	0,576**
	Sig. (bilateral)	0,000

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

Como se puede observar en la tabla 20, el grado de correlación es de 0,576 entre las variables de estudio: Norma Técnica Peruana 27001:2014 ISO-IEC y seguridad en sistemas de información. Esta correlación recae en la categoría moderada, lo que significa que se encontró una relación de manera positiva moderada y que, a medida que el valor de una de las variables de estudio aumente, también lo hará el valor de la otra variable.

Por tanto, no se acepta la hipótesis nula y de esta manera si se acepta la hipótesis alterna dado que el “p-valor” es inferior a 0,05 como se observa en la significancia bilateral.

4.3.2. Contrastación de la primera hipótesis especifica

H_0: La Norma Técnica Peruana 27001-2014 ISO-IEC no se correlaciona significativamente con los elementos tangibles de la Municipalidad Gregorio Albarracín, Tacna 2022.

H_1: La Norma Técnica Peruana 27001-2014 ISO-IEC se correlaciona positivamente con los elementos tangibles de la Municipalidad Gregorio Albarracín, Tacna 2022.

Nivel de significación α= 0,05 = 5 %

Regla de decisión: Si p ≥ α, se acepta H_1; Si p < a, se rechaza H_0

Prueba de estadística: Rho de Spearman, debido a que las variables tienen escala ordinal.

Tabla 21

Grado de Correlación entre Norma Técnica Peruana 27001:2014 ISO-IEC y Elementos Tangibles

Rho de Spearman	Elementos tangibles	
Norma Técnica Peruana 27001:2014 ISO-IEC	Coeficiente de correlación	0,514**
	Sig. (bilateral)	0,000

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

Como se puede observar en la tabla 21, el grado de correlación es de 0,514 entre las variables de estudio: Seguridad en sistemas en información y Elementos tangibles. Esta correlación recae en la categoría moderada, según la tabla de interpretación de Bisquerra (2004) permite demostrar el grado de correlación que existe entre las dimensiones con su respectiva variable, lo cual permitió identificar de manera positiva moderada la relación, pero que según el valor de las variables de estudio aumente, también lo hará el valor de la otra variable.

Por tanto, se niega la hipótesis nula y por lo tanto se utilizará la hipótesis alterna dado que “p-valor” es menor que 0,05 tal como se muestra en el grado de compatibilidad.

4.3.3. Contrastación de la segunda hipótesis especifica

H_0: La Norma Técnica Peruana 27001-2014 ISO-IEC no se correlaciona positivamente con la fiabilidad de la Municipalidad Gregorio Albarracín, Tacna 2022.

H_1: La Norma Técnica Peruana 27001-2014 ISO-IEC se correlaciona positivamente con la fiabilidad de la Municipalidad Gregorio Albarracín, Tacna 2022.

Nivel de significación $\alpha = 0,05 = 5\ \%$

Regla de decisión: Si $p \geq \alpha$, se acepta H_1; Si $p < a$, se rechaza H_0

Prueba de estadística: Rho de Spearman, debido a que las variables tienen escala ordinal.

Tabla 22

Grado de Correlación entre Norma Técnica Peruana 27001:2014 ISO-IEC y Fiabilidad

Rho de Spearman		Fiabilidad
Norma Técnica Peruana 27001:2014 ISO-IEC	Coeficiente de correlación	0,406**
	Sig. (bilateral)	0,000

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

Como se puede observar en la tabla 22, el grado de correlación es de 0,406 entre las variables de estudio: Seguridad en sistemas en información y Fiabilidad. Esta correlación recae en la categoría baja, según la tabla de interpretación de Bisquerra (2004) permite demostrar el grado de correlación que existe entre las dimensiones con su respectiva variable, lo cual permitió identificar de manera positiva moderada la relación pero que según el valor de las variables de estudio aumente, también lo hará el valor de la otra variable.

Por tanto, se niega la hipótesis nula y por lo tanto se utilizará la hipótesis alterna dado que “p-valor” es menor que 0,05 tal como se muestra en el grado de compatibilidad.

4.3.4. Contrastación de la tercera hipótesis especifica

H_0: La Norma Técnica Peruana 27001-2014 ISO-IEC no se correlaciona positivamente con la capacidad de respuesta de la Municipalidad Gregorio Albarracín, Tacna 2022.

H_1: La Norma Técnica Peruana 27001-2014 ISO-IEC se correlaciona positivamente con la capacidad de respuesta de la Municipalidad Gregorio Albarracín, Tacna 2022.

Nivel de significación α= 0,05 = 5 %

Regla de decisión: Si p ≥ α, se acepta H_1; Si p < a, se rechaza H_0

Prueba de estadística: Rho de Spearman, debido a que las variables tienen escala ordinal.

Tabla 23

Grado de correlación entre Norma Técnica Peruana 27001:2014 ISO-IEC y Capacidad de Respuesta

Rho de Spearman	Capacidad de Respuesta	
Norma Técnica Peruana 27001:2014 ISO-IEC	Coeficiente de correlación	0,402**
	Sig. (bilateral)	0,000

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

Como se puede observar en la tabla 23, el grado de correlación es de 0,402 entre las variables de estudio: Seguridad en sistemas en información y Fiabilidad. Esta correlación recae en la categoría baja, según la tabla de interpretación de Bisquerra (2004) permite demostrar el grado de correlación que existe entre las dimensiones con su respectiva variable, lo cual permitió identificar de manera positiva moderada la relación pero que según el valor de las variables de estudio aumente, también lo hará el valor de la otra variable.

Por tanto, se niega la hipótesis nula y por lo tanto se utilizará la hipótesis alterna dado que “p-valor” es menor que 0,05 tal como se muestra en el grado de compatibilidad.

CAPÍTULO V: DISCUSIÓN

Según el objetivo general, determinar la relación entre la Norma Técnica Peruana 27001:2014 ISO-IEC y la Seguridad en sistemas de información en la Municipalidad Gregorio Albarracín, Tacna 2022. Siendo los resultados obtenidos, el nivel de correlación la cual es positiva considerable, con un valor de r = 0,576 entre la Norma Técnica Peruana 27001:2014 ISO-IEC y la Seguridad en sistemas de información, reflejaron que la Norma Técnica Peruana 27001:2014 ISO-IEC tienen una relación directa con la seguridad en sistemas de información de la Municipalidad Gregorio Albarracín de Tacna, datos que al ser comparados con lo encontrado por Flores, Solís y Guerra, Farfán (2017) indico en su tesis *"Relación de la NTP ISO/IEC 27001:2008 EDI y la Seguridad de la Información en los Ministerios del Estado Peruano al 2015",* el cual concluyó que la Oficina Nacional de Gobierno Electrónico ha intentado realizar la implementación de la Norma Técnica Peruana por medio de resoluciones ministeriales, para así exigir su implementación en los distintos Ministerios del Estado Peruana. En la normativa además define el "Que hacer", para mejorar la seguridad de la información. Con estos resultados se afirma que la Norma Técnica Peruana 27001:2014 ISO-IEC si contribuye de una manera favorable a la Seguridad en sistemas de información.

Según el primer objetivo específico, determinar la relación entre la Norma Técnica Peruana 27001:2014 ISO-IEC y los elementos tangibles de la Municipalidad Gregorio Albarracín, Tacna 2022. Siendo los resultados obtenidos, un nivel de correlación la cual es positiva considerable, con un valor de r = 0,315, entre la Norma Técnica Peruana 27001:2014 ISO-IEC y los elementos tangibles, reflejando que los procedimientos de la Norma Técnica Peruana tienen una relación directa con los elementos tangibles de la Municipalidad Gregorio Albarracín de Tacna en términos de seguridad de la información, datos que al ser comparados con lo encontrado por Burgos Salazar et al. (2008) En su tesis titulada "Modelo para Seguridad de la Información en TIC", el cual concluyó que a través de las normas y estándares establecidas por el estado, permiten disminuir las fallas en los patrimonios de información (hardware, software y datos) generando una base hacia el diseño del Modelo de Seguridad de la Información. Con estos resultados se afirma que la Norma Técnica Peruana 27001:2014 ISO-IEC si contribuye de una manera favorable a los elementos tangibles.

Según el segundo objetivo específico, determinar la relación entre la Norma Técnica Peruana 27001:2014 ISO-IEC y la fiabilidad de la Municipalidad Gregorio Albarracín, Tacna 2022. Siendo los resultados obtenidos los cuales evidenciaron el nivel de correlación la cual es positiva considerable, con un valor de r = 0,410, entre la Norma Técnica Peruana 27001:2014 ISO-IEC y la fiabilidad, reflejando que los procedimientos de la Norma Técnica Peruana tiene una relación directa con la fiabilidad de los trabajadores que laboran en la Municipalidad Gregorio Albarracín de Tacna, datos que al ser comparados con lo encontrado por Apahuasco Saccaco, Eber Jesús (2019) En su tesis titulada *"Evaluación del Sistema de Seguridad de la Información en la Organización DISAV SAC Aplicando Lineamientos ISO 27001"*, en el cual concluyo que la información debe encontrarse protegida debido a que se dedica al rubro de ventas lo cual implica protección de los datos de sus clientes, productos, ventas, etc. Por medio de la evaluación de los procesos y controles se obtuvo un resultado del 63,33 % en cuanto a la reducción de las vulnerabilidades, con estos resultados se afirma que la Norma Técnica Peruana 27001:2014 ISO-IEC si contribuyen de una manera favorable con la fiabilidad.

Según el tercer objetivo específico, determinar la relación entre la Norma Técnica Peruana 27001:2014 ISO-IEC y la capacidad de respuesta de la Municipalidad Gregorio Albarracín, Tacna 2022. Siendo los resultados obtenidos permitió evidenciar el nivel de correlación la cual es positiva considerable, con un valor de r= 0,571, entre la Norma Técnica Peruana 27001:2014 ISO-IEC y la capacidad de respuesta, reflejando que los procedimientos de la Norma Técnica Peruana tiene una relación directa con la capacidad de respuesta en la Municipalidad Gregorio Albarracín de Tacna, datos que al ser comparados con lo encontrado por Mendoza Silva, Luis Fernando y Vega Gallegos, Giancarlo Roberto (2019) En su tesis titulada *"Evaluación de la capacidad de detección y respuesta a riesgos de ciberseguridad, caso de la Empresa SISC"* se concluyó que los ciberataques cada vez está tomando protagonismo por lo cual la capacidad de respuesta debe ser de manera inmediata y por medio de una evaluación se detectó que sus herramientas de seguridad no son suficientes, la implementación y la mejora continua de los controles permitirá responder de manera inedia y reducir las vulnerabilidades, con estos resultados se afirma que la Norma Técnica Peruana 27001:2014 ISO-IEC si contribuyen de una manera favorable con la capacidad de respuesta.

CONCLUSIONES

Como primera conclusión se evaluó la Norma Técnica Peruana 27001:2014 ISO-IEC y su correlación con la seguridad en sistemas de información de la Municipalidad Gregorio Albarracín, Tacna 2022. Siendo positiva con un valor 0,576, al cruzar las variables V1 y V2 se interpretó que el 83,75 % del personal consideran un nivel alto, significando que la evaluación de la Norma Técnica Peruana 27001:2014 ISO-IEC es necesaria para la seguridad en sistema de información del tipo informático.

Como segunda conclusión se determinó que la Norma Técnica Peruana 27001:2014 ISO-IEC y su correlación con los elementos tangibles de la Municipalidad Gregorio Albarracín, Tacna 2022. Siendo positiva con un valor de 0,514, al cruzar la Dimensión 1 de la Variable 2 y la Variable 1 se interpretó que el 63,75 % del personal consideran un nivel alto, demostrando que los elementos tangibles son parte importante para la NTP 27001:2014 ISO-IEC. Debido a que por medio de las infraestructuras que cuente la municipalidad (ordenadores, laptops, servidores, impresoras, etc.) permitiera asegurar la información sensible que se maneja dentro de los diferentes sistemas que se encuentran en los servidores.

Como tercera conclusión se determinó que la Norma Técnica Peruana 27001:2014 ISO-IEC y su correlación con la fiabilidad de la Municipalidad Gregorio Albarracín, Tacna 2022. Siendo positiva con un valor de 0,406, al cruzar la Dimensión 2 de la Variable 2 y la Variable 1 se interpretó que el 63,75 % del personal consideran un nivel alto, demostrando que la fiabilidad es importante para la NTP 27001:2014 ISO-IEC. Debido a que por medio de las infraestructuras que cuente la municipalidad (ordenadores, laptops, servidores, impresoras, etc.) permitiera asegurar la información sensible que se maneja dentro de los diferentes sistemas que se encuentran en los servidores.

Como cuarta conclusión se determinó la Norma Técnica Peruana 27001:2014 ISO-IEC y su correlación con la capacidad de respuesta de la Municipalidad Gregorio Albarracín, Tacna 2022. Siendo positiva con un valor de 0,402, al cruzar la Dimensión 3 de la Variable 2 y la Variable 1 se interpretó que el 72,50 % del personal

consideran un nivel alto, demostrando que la capacidad de respuesta es importante para la NTP 27001:2014 ISO-IEC. El tiempo en dar una respuesta frente a algún problema, es el punto más importante para mantener la seguridad en los sistemas de información, porque la municipalidad brinda un servicio para con sus pobladores el cual debe ser eficiente.

Como quinta conclusión se determinó que el uso de la Norma Técnica Peruana 27001:2014 ISO-IEC permite mejorar significativamente la seguridad en los sistemas que cuenta la municipalidad, para así salvaguardar la información por medio de los tres términos que constituyen la norma que son la confidencialidad, integridad y disponibilidad.

RECOMENDACIONES

Como primera recomendación, la sub gerencia de TI debe realizar evaluaciones trimestrales aplicando la NTP y de preferencia sea realizado por una empresa externa a la municipalidad para poder identificar las nuevas posibles vulnerabilidades o riesgos que impliquen la adopción de nuevas tecnologías informáticas de manera imparcial debido a que surgen diferentes inconvenientes con el pasar de los años con respecto a los sistemas de información de la Municipalidad Gregorio Albarracín.

Como segunda recomendación, la Sub Gerencia de TIC debe realizar una actualización o cambio de equipos informáticos (ordenadores, equipos de red, contratos de internet) cada dos años debido al avance de la tecnología, así mejorar la infraestructura de la Municipalidad Gregorio Albarracín.

Como tercera recomendación, la Sub Gerencia de RRHH en coordinación con la Sub Gerencia de TIC, se debe realizar actividades que permitan reforzar el compromiso de los trabajadores al ser ellos quienes tienen contacto directo con la información que maneja la Municipalidad Gregorio Albarracín.

Como cuarta recomendación, la Sub Gerencia de TIC debe tener una estrategia o plan de contingencia para situaciones de ataques o posterior al ataque, para así minimizar el daño que pueda causar brindando una respuesta rápida. Además de realizar una evaluación de los sistemas informáticos una o dos veces al año para ver las mejoras que puedan realizarse.

Como quinta recomendación se propone continuar con el prototipo de SGSI para desarrollar un proyecto formal que cubra con todas las necesidades referente a la seguridad de sistemas de información del software usado en la Municipalidad Gregorio Albarracín de la cuidad de Tacna.

REFERENCIAS BIBLIOGRÁFICAS

ABB. (2009). Making reliability sustainable Barry Kleine ("El cambio del paradigma de fiabilidad"). *ABB*, Nueva Zelanda.

Andreu, R., Ricarte, J., & Valor, j. (1998). *Estrategia y sistemas de información.* Madrid.

Apahuasco Saccaco, E. J. (2019). *Evaluación del sistema de seguridad de la informacion en la organización DISAV SAC aplicando lineamientos ISO 27001.* Apurimac.

Ayudaleyprotecciondatos. (14 de 07 de 2020). *Ayudaleyprotecciondatos.es*. Obtenido de https://ayudaleyprotecciondatos.es/2020/07/14/seguridad-de-la-informacion/

Bisquerra, R. (2004). *Metodología de la investigación educativa.* Madrid: La Muralla S.A.

Bitner, M. J. (2004). *Marketing de servicios.* Mexico: Internacional.

Bunge, M. (1971). *La investigacion cientifica.* Barcelona.

Camisón Zornoza, C., Cruz, S., & Gonzáles, T. (2007). *Gestion de la calidad: Conceptos, enfoques, modelos y sistemas.*

Campaza Quispe, A. A. (2019). *Diseño del plan de seguridad informática basado en la NTP ISO/IEC 27001:2014 para la municipalidad del centro poblado de Salcedo - Puno.* Cusco.

Carrasco Diaz, S. (2019). *Metodologá de la Investigación Científica* (19 ed.). Lima: San Martcos EIRLTDA. Obtenido de https://www.academia.edu/26909781/Metodologia_de_La_Investigacion_Cientifica_Carrasco_Diaz_1_

CIBERTEC. (2007). *Servicio al cliente.* Lima: Reservados.

Crespo Chávez, N. J. (2018). *La aplicacion de las normas ISO 27001 y 2702 y su incidencia en la seguridad de las bases de datos de las Instituciones de Educacion Superior.* Ambato.

Cruz, C., & Gonzales. (2006). *Gestion de la calidad: conceptos, enfoques, modelos y sistemas.* Pearson Educacion S.A.

Davila Villanueva, M. A. (2018). *Evaluacion de un sistema de gestion de Seguridad de la Informacion Basado en la norma ISO 27001:2013, en la Municipalidad Distrital de Jose Crespo y Castillo-Aucayacu; 2018 .* Chimbote.

Definicion. (11 de 09 de 2017). *definicion.de*. Obtenido de definicion.de: https://definicion.de/informacion/

Dorantes Nova, J. A. (2016). Juicio de expertos para la validacion de un instrumento de medición del síndorme de burnout en la docencia. *Ra Ximhai*, 21.

Encinas, I. (1993). *proyectoseducativoscr*. Obtenido de proyectoseducativoscr: https://proyectoseducativoscr.wordpress.com/elaboracion-del-ante-proyecto/capitulo-iii-marco-metodologico-de-la-investigacion/3-6-tecnica-de-procesamiento-y-analisis-de-datos/

Farfán Machaco, Y. (2007). *La fiabilidad.* Cusco: Moderna.

Flores Solís, F. R., & Guerra Farfán, J. A. (2017). *Relación de la NTP ISO/IEC 27001:2008 EDI y La seguridad de la información en los ministerios del estado peruano al 2015.* Callao.

Fontalvo y Vergara. (2010). *La Gestion de la Calidad en los Servicios ISO 9001:2008.* Colombia: Vertice S.L.

García Canal, E., Rialp Criado, A., & Rialp Criado, J. (2007). *Inversiones en TIC y estrategias de crecimiento empresarial.*

Gardey, J. P. (04 de 09 de 2017). *definicion.de*. Obtenido de definicion.de: https://definicion.de/seguridad/

Gobierno de Mexico. (25 de 04 de 2013). *incmnsz.mx*. Obtenido de https://www.incmnsz.mx/opencms/contenido/investigacion/comiteEtica/confidencialidadInformacion.html

Gómez Vieites, A. (28 de 03 de 2014). *Wikipedia*. Obtenido de http://es.wikipedia.org/wiki/Seguridad_de_la_informaci %C3%B3n

Gómez, A. (2011). *Enciclopedia de la Seguridad Informatica.* México.

Gomez, N. (2006). *Introducción a la metodologia de la investigación cientifica.* Cordoba: Editorial Brujas.

Hernández Sampieri, R. (1998). *Metodologia de La Investigacion.* Mexico.

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, P. (2014). *Metodologia de la Investigacion.* Mexico: McGraw-Hill.

Hurtado de Barrera, J. (2010). *Metodología de la investigación : guía para la comprensión holística de la ciencia.*

ICONTEC. (2016). *Sistema de gestión de la seguridad de la información (SGSI).* Colombia.

INEI. (2006). *Glosario básico de términos estadísticos.* Lima.

Instituto para la Defensa de la Competencia y la Propiedad Intelectual. (2014). *Instituto para la Defensa de la Competencia y la Propiedad Intelectual.* Lima.

Kaspersky. (31 de Agosto de 2021). *latam.kaspersky.com*. Obtenido de latam.kaspersky.com: https://latam.kaspersky.com/blog/ciberataques-en-america-latina-crecen-un-24-durante-los-primeros-ocho-meses-de-2021/22718/

Keith Denton, D. (1991). *Calidad en el servicio a los clientes.* Houston.

Laudon, K. C., & P., L. J. (2012). *Sistemas de Información Gernecial.* Mexico.

Malhotra, N. (2004). *Investigación de mercados. Un enfoque práctico.* México.

Matsumoto Nishizawa, R. (2014). *Desarrollo del Modelo Servqual para la medicion de la calidad del servicio en la empresa del publicidad ayuda experto.* Cochabamba: Internacional.

Mendoza Silva, L. F., & Vega Gallegos, G. R. (2019). *Evaluación de la capacidad de detencción y respuesta a riesgos de ciberseguridad, caso de la empresa SISC.* Lima.

Moscariello, M. G. (2017). *proyectoseducativoscr.wordpress.com*. Obtenido de proyectoseducativoscr.wordpress.com: https://proyectoseducativoscr.wordpress.com/elaboracion-del-ante-proyecto/capitulo-iii-marco-metodologico-de-la-investigacion/3-6-tecnica-de-procesamiento-y-analisis-de-datos/

Muntané Relat, J. (2010). *Introduccón a la Investigación Básica.* Madrid.

Nicomedes Teodoro, E. N. (2014). *Tipos de Investigación.* Santo Domingo.

Norma Internacional ISO 27001. (15 de 07 de 2017). *pmg-ssi.com*. Obtenido de https://www.pmg-ssi.com/2017/07/iso-27001-contextoalcance-y-politica/

Organización Internacional para la Normalizacion (ISO). (04 de Febrero de 2015). *iso.org*. Obtenido de https://www.iso.org/files/live/sites/isoorg/files/archive/pdf/en/fast_forwardes.pdf

pirani. (2018). *Manual para implementar la seguridad de la información según la ISO 27001.* Medellin. Obtenido de https://www.piranirisk.com: https://www.piranirisk.com/es/academia/especiales/iso-27001-que-es-y-como-implementarla#:~:text=La%20norma%20ISO%2027001%20establece,tus%20clientes%2C%20proveedores%20y%20empleados

PMG. (05 de 02 de 2018). *pmg-ssi.com*. Obtenido de https://www.pmg-ssi.com/2018/02/confidencialidad-integridad-y-disponibilidad/

Renteri Echeverry, F. A. (2016). *Inicio y evolución de la seguridad informática en el mundo.* Colombia.

Romero Castro, M. I., Figueroa Morán, G. L., Vera Navarrete, D. S., Álava Cruzatty, J. E., Parrales Anzúles, G. R., Álava Mero, C. J., . . . Castillo Merino, M. A. (2018). *Introducción a la Seguridad Informática y el Análisis de Vulnerabilidades.* Manabi: Área de Innovación y Desarrollo, S.L.

Salazar Burgos, J., & Campos G., P. (2008). *Modelo para Seguridad de la Informacion en TIC.* Concepción: Universidad del Bío-Bío.

Sánchez Carlessi, H., & Reyes Romero, C. M. (2018). *Manual de Término en investigación científica, tecnológica y humanística.* Lima.

Suyo Cruz, L. A. (2017). *Calidad de servicio y satisfacción del asegurado en la oficina de normalización previsional, centro de atención Lima Centro.* Lima.

Tamayo y Tamayo, M. (2000). *Aprende a Investigar.* Santa fe de Bogota: Internacional.

Tomás Sábado, J. (2009). *Fundamentos de bioestadística y análisis de datos para enfermeria.* Barcelona.

Torres Chango, C. D. (2020). *Plan de Seguridad Informática basado en la Norma ISO 27001, para proteger la informacón y activos de la empresa privada Megaprofer S.A.* Ambato.

Vela Rios, E. M. (2021). *Seguridad de información basada en la norma ISO/IEC 27001:2013 y nivel de seguridad en el centro de capacitaciones SENCICO – Ucayali 2018.* Ucayali.

Villena Aguilar, M. A. (2006). *Sistema de Gestion de Seguirdad de Informacion para una Institucion Financiera.* Lima: Pontificia Univerisdad Catolica del Peru.

Whitter, J., Bentley, L., & Barlow, V. (1996). *Análisis y Diseño de Sistemas de Informacion.* España.

Zapata Chasiguasin, K. B. (2020). *Sistema de gestion de seguridad de la informacion basado en las normas ISO/IEC 27001, en el departamento de Tecnologias de la informacion del Gobierno Autonomo descentralizado de la Municipalidad de Ambato.* Ambato.

Anexo 01 Matriz de consistencia.

PROBLEMA	OBJETIVOS	HIPÓTESIS	VARIABLES E INDICADORES	METODOLOGÍA
Problema principal ¿Cómo se correlaciona la Norma Técnica Peruana 27001:2014 ISO-IEC y la seguridad en sistemas de información de la Municipalidad Gregorio Albarracín, Tacna 2022? **Problemas Específicos:** • ¿Cómo se correlaciona la Norma Técnica Peruana 27001:2014 ISO-IEC y los elementos tangibles de la Municipalidad Gregorio Albarracín, Tacna 2022? • ¿Cómo se correlaciona la Norma Técnica Peruana 27001:2014 ISO-IEC y la fiabilidad de la Municipalidad Gregorio Albarracín, Tacna 2022? • ¿Cómo se correlaciona la Norma Técnica Peruana 27001:2014 ISO-IEC y la capacidad de respuesta de la Municipalidad Gregorio Albarracín, Tacna 2022?	**Objetivo principal** Evaluar la correlación entre Norma Técnica Peruana 27001:2014 ISO-IEC y la seguridad en sistemas de información de la Municipalidad Gregorio Albarracín, Tacna 2022 **Objetivos específicos:** • Medir la correlación entre la Norma Técnica Peruana 27001:2014 ISO-IEC y los elementos tangibles de la Municipalidad Gregorio Albarracín, Tacna 2022. • Medir la correlación entre la Norma Técnica Peruana 27001:2014 ISO-IEC y la fiabilidad de la Municipalidad Gregorio Albarracín, Tacna 2022. • Medir la correlación entre la Norma Técnica Peruana 27001:2014 ISO-IEC y la capacidad de respuesta de la Municipalidad Gregorio Albarracín, Tacna 2022	**Hipótesis Principal** Existe correlación significativa entre la Norma Técnica Peruana 27001:2014 ISO-IEC y la seguridad en sistemas de información de la Municipalidad Gregorio Albarracín, Tacna 2022 **Hipótesis especificas:** • Existe correlación significativa entre la Norma Técnica Peruana 27001:2014 ISO-IEC y los elementos tangibles de la Municipalidad Gregorio Albarracín, Tacna 2022. • Existe correlación significativa entre la Norma Técnica Peruana 27001:2014 ISO-IEC y la fiabilidad de la Municipalidad Gregorio Albarracín, Tacna 2022. • Existe correlación significativa entre la Norma Técnica Peruana 27001:2014 ISO-IEC y la capacidad de respuesta de la Municipalidad Gregorio Albarracín, Tacna 2022.	**Variable:** Norma Técnica Peruana 27001:2014 ISO-IEC Dimensiones - Confidencialidad - Integridad - Disponibilidad ---------- **Variable:** Seguridad en sistemas de información Dimensiones - Elementos tangibles - Fiabilidad - Capacidad de Respuesta	**1. Tipo de investigación** Básica **2. Diseño de investigación** No experimental de corte transversal correlacional **3. Nivel de investigación** Correlacional **4. Población** 100 (cuantos conforman la población) **5.Muestra** 80 encuestados **6.Técnicas:** Encuesta **7. Instrumentos:** Cuestionario

Anexo 02 Cuestionario de la Variable Norma Técnica Peruana 27001:2014 ISO-IEC.

Es grato dirigirme a usted, para hacerle llegar el presente cuestionario, que tiene por finalidad obtener información sobre la Norma Técnica Peruana 27001:2014 ISO-IEC en la Municipalidad Gregorio Albarracín. Hago de su conocimiento que este cuestionario es anónimo.

A continuación, se le presenta un cuestionario léalo detenidamente y según su opinión rellene con una X el casillero que crea conveniente.

Palabras clave:

Confidencialidad	El objetivo de la confidencialidad es, prevenir la divulgación no autorizada de la información sobre nuestra organización.
Integridad	El objetivo de la integridad es prevenir modificaciones no autorizadas de la información.
Disponibilidad	El objetivo es necesario prevenir interrupciones no autorizadas de los recursos informáticos.

1	2	3	4	5
Totalmente en desacuerdo	En desacuerdo	Indeciso	De acuerdo	Totalmente de acuerdo

VARIABLE: Norma Técnica Peruana 27001:2014 ISO-IEC								
DIMENSIONES		INDICADORES	1	2	3	4	5
Confidencialidad	1	**Control de Acceso**					
	1	¿Cree usted que para garantizar la seguridad de los datos es requerida la confidencialidad en el control de accesos?					
	2	¿Usted cree que la confidencialidad debe ser tomada en cuenta como uno de los pilares en la seguridad de los datos?					
	2	**Autorización**					
	3	¿Usted considera que la autorización debe ser de carácter confidencial?					
	4	¿Considera que la autorización es una exigencia necesaria para poder acceder a los datos?					
Integridad	3	**Seguridad para las comunicaciones**					
	5	¿Usted considera que la integridad es una parte esencial para la seguridad de las comunicaciones?					
	6	¿Considera que para la seguridad de las comunicaciones la integridad es de carácter relevante en la seguridad de los datos?					

	4	**Seguridad para los procedimientos**
	7	¿Cree usted que la integridad precisa en la seguridad de los procedimientos, los cuales serían de consideración significativa para la seguridad de los datos?
	8	¿Es correcto que los procesos deban tener un adecuado manejo para así certificar la integridad en la seguridad en los datos?
Disponibilidad	5	**Acceso en el momento solicitado**
	9	¿Cree usted que contar con la información en el momento solicitado sea a consecuencia de la disponibilidad de los datos seguros?
	10	¿Cree usted que contar con la información en el momento solicitado se debe considerar como elemento primordial a la disponibilidad?
	6	**Acceso a los datos**
	11	¿Considera que para garantizar la fidelidad de los datos la disponibilidad debe tomar en consideración el acceso a los datos?
	12	¿Se debe considerar como elemento primordial a la disponibilidad para así garantizar el acceso de los datos?

Anexo 03 Cuestionario de la Variable Seguridad en Sistemas de Información.

Es grato dirigirme a usted, para hacerle llegar el presente cuestionario, que tiene por finalidad obtener información sobre la Seguridad en sistemas de información en la Municipalidad Gregorio Albarracín. Hago de su conocimiento que este cuestionario es anónimo.

A continuación, se le presenta un cuestionario léalo detenidamente y según su opinión rellene con una X el casillero que crea conveniente.

1	2	3	4	5
Totalmente en desacuerdo	En desacuerdo	Indeciso	De acuerdo	Totalmente de acuerdo

VARIABLE: Seguridad en Sistemas de Información								
DIMENSIONES		INDICADORES	1	2	3	4	5
Elementos tangibles	1	**Equipos**					
	1	¿Considera que los equipos informáticos (computadoras, laptops y otros periféricos) son herramientas necesarias para brindar una mejor seguridad en sistemas de información?					
	2	¿Considera que los equipos informáticos (computadoras, laptops y otros periféricos) utilizados actualmente son adecuadamente para la infraestructura de la seguridad en sistemas de información?					
	2	**Almacenamiento**					
	3	¿Considera que los equipos de almacenamiento de información (backup) son un factor relevante para mantener la seguridad en sistemas de información?					
	4	¿Considera que debe existir un plan de copias de seguridad semanal y mensual de los datos para tener una adecuada seguridad en sistemas de información?					
	3	**Condiciones generales**					
	5	¿Considera que la infraestructura (ordenadores, internet, equipos de red) son los adecuados o cumplen los requisitos mínimos (condiciones generales) para permitir mantener la seguridad en sistemas de información?					
	6	¿Considera que la infraestructura (ordenadores, internet, equipos de red) deben ser renovados cada dos años y cumplan con los requisitos recomendados o mínimos (condiciones generales) al comprar de nuevos ordenadores, equipos de red y actualización del plan de internet para mejorar la seguridad en sistemas de información?					

Fiabilidad	4	**Compromiso**
	7	¿Considera usted que el compromiso por parte de los trabajadores de la Sub Gerencia de TIC debe ser considerado un factor fundamental para el logro de la seguridad en sistemas de información?
	8	¿Considera usted que los trabajadores deben que manejan información importante por medio de los sistemas deben firmar un documento de compromiso de no divulgación de información confidencial para una eficiente seguridad en sistemas de información?
	5	**Servicio prometido**
	9	¿Considera que la seguridad en sistemas de información debe cumplir con el servicio prometido (acceso a la información y acceso a los sistemas)?
	10	¿El servicio prometido (acceso a los sistemas y acceso a internet) influye de tal manera que permita alcanzar la seguridad en sistemas de información?
Capacidad de respuesta	6	**Tiempo de respuesta**
	11	¿Considera que el tiempo de repuesta al solicitar algún tipo de información depende de la seguridad en sistemas de información?
	12	¿Considera que cuan menor sea el tiempo de respuesta influye positivamente la seguridad en sistemas de información?
	7	**Mejora continua**
	13	¿Consideraría que la seguridad en sistemas de información requiere de actualizaciones según la necesidad que requieran los trabajadores así poder permitir tener una mejora continua?
	14	¿Considera que por medio de la mejora continua de la seguridad en sistemas de información favorece en gran medida capacidad de respuesta que se le brinda al usuario (poblador) cuando requiera información?

Anexo 04 Tabulación de datos de la variable Norma Técnica Peruana 27001:2014.

	xP1	xP2	xP3	xP4	xDim1	xP5	xP6	xP7	xP8	xDim2	xP9	xP10	xP11	xP12	xDim3	xVar
E1	5	4	4	5	18	5	4	4	5	18	4	5	4	5	18	54
E2	5	5	4	4	18	4	4	4	4	16	4	4	4	4	16	50
E3	5	5	5	4	19	5	5	5	5	20	4	4	3	3	14	53
E4	4	4	3	5	16	4	4	4	4	16	4	4	4	4	16	48
E5	5	5	5	5	20	5	5	5	5	20	5	5	5	4	19	59
E6	4	5	5	4	18	5	5	4	5	19	5	5	4	5	19	56
E7	4	4	5	5	18	4	4	4	3	15	3	4	2	3	12	45
E8	5	5	5	5	20	4	4	4	4	16	4	4	4	4	16	52
E9	4	4	4	5	17	4	4	4	4	16	4	4	4	3	15	48
E10	5	5	3	5	18	4	2	3	2	11	3	3	3	3	12	41
E11	4	4	3	4	15	4	4	3	5	16	4	4	4	4	16	47
E12	5	5	4	4	18	4	5	4	4	17	3	4	4	4	15	50
E13	4	4	5	4	17	5	5	5	4	19	3	4	3	4	14	50
E14	5	5	5	5	20	5	5	5	5	20	5	5	5	5	20	60
E15	5	5	4	4	18	4	4	4	4	16	3	4	4	4	15	49

E16	5	5	5	4	19	4	4	5	5	18	5	4	4	4	17	54
E17	5	5	3	4	17	5	5	4	5	19	5	4	4	3	16	52
E18	4	5	5	5	19	5	5	4	5	19	5	4	4	5	18	56
E19	5	5	3	5	18	5	5	5	5	20	5	3	5	5	18	56
E20	4	4	4	4	16	4	4	4	5	17	5	5	4	5	19	52
E21	4	5	4	4	17	4	4	4	5	17	5	4	5	4	18	52
E22	4	4	5	5	18	5	4	5	4	18	3	4	3	4	14	50
E23	5	5	5	5	20	5	5	4	5	19	4	5	5	5	19	58
E24	4	4	4	4	16	4	4	4	4	16	4	4	4	4	16	48
E25	4	3	4	4	15	4	4	3	4	15	4	4	4	5	17	47
E26	4	4	4	4	16	4	4	4	5	17	4	4	3	2	13	46
E27	3	4	3	2	12	3	3	3	3	12	5	3	3	2	13	37
E28	4	4	4	4	16	5	4	3	4	16	3	5	5	5	18	50
E29	4	4	4	4	16	4	4	4	5	17	3	4	4	4	15	48
E30	5	5	5	5	20	5	4	4	4	17	4	4	4	4	16	53

E31	5	5	5	5	20	4	4	4	4	16	5	4	4	5	18	54
E32	4	4	4	4	16	4	4	4	4	16	4	4	4	4	16	48
E33	5	5	5	5	20	5	5	4	5	19	5	5	5	4	19	58
E34	5	4	4	4	17	4	4	4	5	17	4	4	4	4	16	50
E35	5	5	4	5	19	5	5	5	5	20	5	5	5	5	20	59
E36	5	5	4	5	19	5	5	5	5	20	4	5	5	5	19	58
E37	4	4	4	4	16	4	4	4	3	15	4	4	4	3	15	46
E38	3	5	4	4	16	4	3	4	3	14	3	4	3	4	14	44
E39	4	4	3	4	15	4	4	4	4	16	4	5	4	4	17	48
E40	5	4	5	4	18	4	5	5	5	19	4	5	5	4	18	55
E41	4	5	5	3	17	4	3	3	4	14	3	4	4	4	15	46
E42	4	5	4	4	17	4	3	4	3	14	4	4	4	3	15	46
E43	5	4	4	3	16	4	5	3	4	16	4	4	3	3	14	46
E44	5	4	4	5	18	4	5	5	4	18	5	4	5	5	19	55
E45	5	5	5	4	19	5	5	5	5	20	4	4	4	4	16	55

E46	5	5	3	5	18	5	5	5	4	19	5	5	4	4	18	55
E47	5	5	5	5	20	5	5	4	4	18	4	5	4	4	17	55
E48	5	5	5	5	20	4	5	5	5	19	5	4	3	4	16	55
E49	4	4	4	4	16	4	4	4	4	16	4	3	4	4	15	47
E50	5	5	2	5	17	5	5	5	5	20	5	5	5	5	20	57
E51	5	5	5	5	20	5	5	5	4	19	3	4	3	4	14	53
E52	4	4	4	2	14	5	5	4	4	18	4	4	4	4	16	48
E53	5	5	2	5	17	5	5	5	5	20	5	5	5	5	20	57
E54	5	5	5	5	20	5	5	5	5	20	5	5	5	5	20	60
E55	5	5	5	5	20	5	5	5	5	20	5	5	5	5	20	60
E56	5	5	3	5	18	5	5	5	5	20	4	5	5	4	18	56
E57	5	5	5	5	20	5	5	5	5	20	5	5	5	5	20	60
E58	5	4	4	3	16	5	5	4	4	18	4	4	4	4	16	50
E59	4	4	4	4	16	4	4	4	4	16	4	4	4	4	16	48
E60	2	2	2	2	8	4	4	4	4	16	4	4	2	4	14	38

E61	5	5	5	5	20	5	5	5	5	20	5	5	5	5	20	60
E62	5	5	5	5	20	4	3	4	4	15	2	2	4	3	11	46
E63	4	4	4	4	16	4	4	4	4	16	4	4	4	4	16	48
E64	5	5	5	4	19	4	3	4	4	15	4	4	4	4	16	50
E65	5	5	4	4	18	4	4	4	4	16	3	4	4	4	15	49
E66	4	4	4	4	16	4	4	3	4	15	4	4	4	5	17	48
E67	5	5	5	4	19	4	4	4	4	16	5	5	4	4	18	53
E68	5	5	4	4	18	4	2	4	4	14	4	4	4	4	16	48
E69	4	4	2	2	12	5	5	4	4	18	3	4	4	4	15	45
E70	3	3	4	4	14	4	4	4	4	16	4	3	4	4	15	45
E71	3	4	4	3	14	3	3	3	3	12	3	3	3	3	12	38
E72	5	5	5	5	20	5	5	5	5	20	5	5	5	5	20	60
E73	4	5	4	4	17	5	4	4	5	18	4	5	4	4	17	52
E74	3	4	5	4	16	4	4	2	4	14	4	4	4	4	16	46
E75	4	5	4	5	18	4	3	4	4	15	4	5	3	4	16	49

E76	5	5	5	5	20	5	5	5	5	20	5	5	5	4	19	59
E77	5	5	5	4	19	5	4	4	4	17	4	4	2	4	14	50
E78	5	5	2	4	16	5	4	4	4	17	5	4	4	4	17	50
E79	3	4	4	4	15	4	4	3	5	16	3	5	4	3	15	46
E80	5	5	5	5	20	5	5	5	5	20	5	5	5	5	20	60

Anexo 05 Tabulación de datos de la variable Seguridad en Sistemas de Información.

	yP1	yP2	yP3	yP4	yDim1	yP5	yP6	yP7	yP8	yDim2	yP9	yP10	yP11	yP12	yP13	yP14	yDim3	yVar
E1	4	4	4	4	26	5	5	5	4	17	4	4	5	4	4	5	18	61
E2	4	4	4	4	24	4	4	4	4	16	4	4	4	4	4	4	16	56
E3	5	3	4	4	26	5	5	4	5	17	4	4	4	2	3	5	14	57
E4	5	5	4	5	28	5	4	4	4	16	4	4	4	4	4	4	16	60
E5	5	5	5	5	30	5	5	5	5	20	5	5	5	5	5	5	20	70
E6	5	4	4	4	26	4	5	5	5	20	5	5	4	5	5	5	19	65
E7	4	4	4	2	21	3	4	3	4	14	3	4	4	3	4	4	15	50
E8	4	4	4	4	24	4	4	5	5	18	4	4	4	4	4	3	15	57
E9	4	3	2	4	19	3	3	3	4	15	4	4	3	3	4	4	14	48
E10	3	4	5	5	25	5	3	4	3	13	2	4	3	4	4	4	15	53
E11	4	5	5	3	24	4	3	4	3	15	4	4	5	4	4	4	17	56
E12	4	4	4	4	24	4	4	4	4	17	5	4	2	4	4	4	14	55
E13	5	5	3	5	24	4	2	5	5	18	4	4	4	3	4	4	15	57
E14	5	5	5	5	30	5	5	5	5	20	5	5	5	5	5	5	20	70
E15	4	4	5	5	27	4	5	5	4	17	4	4	3	4	5	5	17	61
E16	3	4	5	4	24	4	4	4	4	17	4	5	5	4	5	4	18	59
E17	5	2	4	4	23	3	5	5	5	17	3	4	2	4	4	4	14	54

E18	3	3	4	5	25	5	5	4	5	18	5	4	2	3	5	5	15	58
E19	5	5	3	5	27	4	5	4	4	16	4	4	4	4	4	4	16	59
E20	4	4	5	4	26	5	4	4	5	17	4	4	4	5	4	4	17	60
E21	5	2	4	4	23	4	4	4	4	16	4	4	4	4	3	4	15	54
E22	4	3	4	4	24	4	5	4	3	15	4	4	3	3	5	5	16	55
E23	4	4	4	4	24	4	4	4	4	16	4	4	4	4	4	4	16	56
E24	4	4	2	4	23	4	5	4	4	16	4	4	3	3	4	4	14	53
E25	5	4	4	4	24	4	3	4	3	15	4	4	3	4	4	3	14	53
E26	4	4	5	4	24	4	3	5	4	17	4	4	4	3	5	5	17	58
E27	3	3	4	2	18	3	3	3	3	13	4	3	5	3	3	3	14	45
E28	5	3	3	5	26	5	5	3	3	13	3	4	5	3	3	4	15	54
E29	4	4	4	4	25	5	4	4	5	18	4	5	4	4	5	5	18	61
E30	4	4	4	4	24	4	4	4	4	16	4	4	4	4	4	4	16	56
E31	5	5	5	5	29	4	5	5	5	19	5	4	5	3	5	3	16	64
E32	4	4	4	4	24	4	4	5	5	19	5	4	4	4	4	4	16	59
E33	5	5	4	4	27	5	4	4	4	16	4	4	4	4	4	4	16	59
E34	4	4	3	4	23	4	4	4	5	17	4	4	4	4	4	4	16	56

E35	5	5	5	5	30	5	5	5	5	20	5	5	5	4	4	4	17	67
E36	5	5	5	5	30	5	5	5	5	20	5	5	5	5	5	5	20	70
E37	3	4	4	3	22	4	4	3	4	15	4	4	4	4	3	4	15	52
E38	4	3	4	4	23	4	4	4	3	12	2	3	4	3	4	4	15	50
E39	4	4	4	4	24	4	4	4	4	16	4	4	4	4	4	4	16	56
E40	5	5	5	4	29	5	5	4	5	19	5	5	4	5	4	5	18	66
E41	4	3	3	4	20	3	3	3	4	14	4	3	4	3	4	4	15	49
E42	3	3	3	3	18	3	3	4	3	13	3	3	3	3	3	3	12	43
E43	4	4	4	3	22	3	4	4	4	15	4	3	3	3	3	4	13	50
E44	2	4	4	5	22	2	5	5	5	20	5	5	4	5	5	5	19	61
E45	3	3	4	5	23	4	4	5	5	18	4	4	3	4	4	4	15	56
E46	5	5	5	5	29	5	4	4	5	18	5	4	5	5	5	5	20	67
E47	3	3	4	4	22	4	4	4	5	18	4	5	4	4	3	5	16	56
E48	5	3	4	3	23	4	4	4	2	13	3	4	4	5	3	4	16	52
E49	4	4	4	4	24	4	4	4	4	16	4	4	4	4	4	4	16	56
E50	4	4	5	5	27	4	5	5	5	17	5	2	5	5	5	5	20	64
E51	5	3	4	4	24	4	4	4	3	13	3	3	4	4	4	5	17	54

E52	4	3	5	4	23	3	4	4	4	16	4	4	2	2	3	4	11	50
E53	5	4	4	4	26	5	4	5	5	19	5	4	4	5	4	4	17	62
E54	5	5	5	5	30	5	5	4	3	17	5	5	3	2	4	4	13	60
E55	5	5	5	5	26	3	3	3	3	13	4	3	3	2	2	4	11	50
E56	4	3	5	4	24	3	5	5	5	18	5	3	4	2	5	3	14	56
E57	5	5	5	5	28	3	5	5	5	20	5	5	5	4	5	5	19	67
E58	4	4	4	4	24	4	4	4	4	16	4	4	4	4	4	4	16	56
E59	4	4	4	4	24	4	4	4	4	16	4	4	4	4	4	4	16	56
E60	4	4	4	4	26	5	5	5	4	17	4	4	2	2	4	4	12	55
E61	5	5	5	5	30	5	5	5	5	20	5	5	5	5	5	5	20	70
E62	5	5	5	4	28	4	5	3	4	13	4	2	4	5	4	3	16	57
E63	4	4	4	4	24	4	4	4	4	16	4	4	4	4	4	4	16	56
E64	4	4	4	4	24	4	4	4	4	16	4	4	4	4	4	4	16	56
E65	2	4	4	4	22	4	4	4	4	16	4	4	4	4	4	5	17	55
E66	2	4	4	4	20	2	4	4	4	14	4	2	2	2	4	2	10	44
E67	4	4	4	4	24	4	4	5	4	18	5	4	5	4	4	4	17	59
E68	5	3	2	4	22	3	5	5	3	16	4	4	3	4	4	4	15	53

E69	4	2	4	4	24	5	5	4	5	17	4	4	3	4	4	3	14	55
E70	4	4	3	4	23	4	4	4	4	16	4	4	4	4	4	4	16	55
E71	3	4	4	4	25	5	5	5	5	19	5	4	4	4	3	3	14	58
E72	5	5	5	5	30	5	5	5	5	20	5	5	5	5	5	5	20	70
E73	5	5	4	4	27	4	5	4	3	15	4	4	4	4	5	4	17	59
E74	4	4	4	4	25	5	4	4	4	17	4	5	2	4	2	4	12	54
E75	4	3	5	5	25	4	4	4	3	16	4	5	5	3	3	4	15	56
E76	4	3	4	4	21	2	4	4	5	17	4	4	4	4	4	4	16	54
E77	4	4	5	4	24	3	4	4	4	17	5	4	4	4	4	5	17	58
E78	3	2	4	4	19	2	4	4	5	16	3	4	4	4	4	5	17	52
E79	5	5	3	2	23	4	4	4	4	15	4	3	4	4	4	4	16	54
E80	5	5	5	5	30	5	5	5	5	20	5	5	5	5	5	5	20	70

Anexo 06 Análisis factorial de la Variable de Norma Técnica Peruana 27001;2014 ISO-IEC y Seguridad en Sistemas de Información.

Tabla de Prueba de KMO y Bartlett de la Variable de Norma Técnica Peruana 27001;2014 ISO-IEC

Prueba de KMO y Bartlett		
Medida Kaiser-Meyer-Olkin de adecuación de muestreo		,839
Prueba de esfericidad de Bartlett	Aprox. Chi-cuadrado	424,801
	gl	66
	Sig.	,000

Interpretación:

Según la tabla anteriormente mostrada, la medida de Káiser Meyer Olkin (KMO) de adecuación de muestreo tiene un valor de 0.839, cantidad que se encuentra por encima del 0.50, es decir que existe correlación entre sus ítems; asimismo, de acuerdo al resultado de la esfericidad de Bartlett, su p-valor es 0.00 menor que 0,05, el cual comprueba que existe relación entre sus variables y por lo tanto es posible realizar el análisis factorial.

Tabla de Varianza total explicada la Variable de Norma Técnica Peruana 27001;2014 ISO-IEC

Varianza total explicada

Componente	Autovalores iniciales			Sumas de cargas al cuadrado de la extracción			Sumas de cargas al cuadrado de la rotación		
	Total	% de varianza	% acumulado	Total	% de varianza	% acumulado	Total	% de varianza	% acumulado
1	5,302	44,184	44,184	5,302	44,184	44,184	2,662	22,186	22,186
2	1,556	12,967	57,150	1,556	12,967	57,150	2,611	21,756	43,942
3	,911	7,588	64,738	,911	7,588	64,738	2,496	20,796	64,738
4	,875	7,295	72,033						
5	,688	5,735	77,768						
6	,582	4,852	82,620						
7	,537	4,473	87,093						
8	,443	3,691	90,784						
9	,329	2,742	93,525						
10	,319	2,660	96,186						
11	,283	2,357	98,542						
12	,175	1,458	100,000						

Método de extracción: análisis de componentes principales.

Interpretación:

Según la tabla anteriormente vista, son 2 los componentes que superan la unidad, en ese sentido el instrumento de Norma Técnica Peruana 27001:2014 ISO-IEC podría contar con 2 dimensiones, con el componente 1 explica la mayor parte de la varianza con el 44.18 % de la varianza total explicada y hasta el componente 2 se logra cubrir el 57.15 %. Sin embargo, al ser materia de estudio del investigador rechaza la propuesta dada.

Tabla de Prueba de KMO y Bartlett de la Variable de Seguridad en Sistemas de Información

Prueba de KMO y Bartlett		
Medida Kaiser-Meyer-Olkin de adecuación de muestreo		,821
Prueba de esfericidad de Bartlett	Aprox. Chi-cuadrado	318,005
	gl	91
	Sig.	,000

Interpretación:

Según la tabla anteriormente mostrada, la medida de Káiser Meyer Olkin de adecuación de muestreo tiene un valor de 0.821 cantidad que se encuentra por encima del 0.50, es decir que existe correlación entre sus ítems; asimismo, de acuerdo al resultado de la esfericidad de Bartlett, su p-valor es 0.00, menor que 0,05, el cual comprueba que existe relación entre sus variables y por lo tanto es posible realizar el análisis factorial.

Tabla de Varianza total explicada la Variable de Seguridad en Sistemas de Información

Varianza total explicada

Componente	Autovalores iniciales			Sumas de cargas al cuadrado de la extracción			Sumas de cargas al cuadrado de la rotación		
	Total	% de varianza	% acumulado	Total	% de varianza	% acumulado	Total	% de varianza	% acumulado
1	4,749	33,920	33,920	4,749	33,920	33,920	3,250	23,217	23,217
2	1,485	10,604	44,524	1,485	10,604	44,524	2,194	15,670	38,887
3	1,129	8,065	52,589	1,129	8,065	52,589	1,918	13,702	52,589
4	1,107	7,906	60,495						
5	,889	6,348	66,844						
6	,784	5,597	72,441						
7	,672	4,799	77,240						
8	,604	4,314	81,554						
9	,567	4,053	85,607						
10	,501	3,579	89,186						
11	,481	3,438	92,624						
12	,424	3,028	95,653						
13	,338	2,416	98,069						
14	,270	1,931	100,000						

Método de extracción: análisis de componentes principales.

Interpretación:

Según la tabla anteriormente vista, son 2 los componentes que superan la unidad, en ese sentido el instrumento de Seguridad en Sistemas de Información podría contar con 4 dimensiones, con el componente 1 explica la mayor parte de la varianza con el 33.92 % de la varianza total explicada y hasta el componente 4 se logra cubrir el 60.49 %. Sin embargo, al ser materia de estudio del investigador rechaza la propuesta dada.

Anexo 07 Desarrollo de la Propuesta.

Título: Prototipo de Tablero de control para una Municipalidad

Responsables: Área de Sub Gerencia de TIC, Alta Gerencia de la Municipalidad y Área de RRHH.

Lugar de aplicación: Municipalidad Gregorio Albarracín, TACNA

Metodología:

La metodología a utilizar es la Norma ISO 27001 según la revista de Pirani (2018), desarrolla 8 puntos que permitieron primeramente el determinar los objetivos que se pretende alcanzar para dar pie a las políticas de seguridad que brinda seguridad a los sistemas de información, todo previamente haber realizado una identificación, análisis y evaluación de los riesgos que se encuentren dentro de la municipalidad.

Para así hacer el registro en la tabla de control, de esta manera poder hacer el tratamiento de los riesgos, por medio de los controles. Por último, el monitoreo de los controles a través de los gráficos de cada control previamente registrado para ver el estado de cada uno.

Alcance:

El alcance de la propuesta es el diseño de un prototipo de tablero control del SGSI basado en la Norma Técnica Peruana 27001:2014 ISO-IEC exclusivamente en el nivel informático de la seguridad en sistemas de información de la municipalidad Gregorio Albarracín, Región Tacna.

Desarrollo de la propuesta

1. Definir la política de seguridad: En este primer punto es donde se determina los objetivos, requerimientos legales, seguidamente los criterios con los cuales serán evaluados los riesgos, pero todo esto debe estar aprobada por la alta dirección.

2. Definir el alcance del SGSI: En este punto se tiene claro lo que se conseguirá cuando el plan de acción se implemente en la organización, tomando en cuenta los activos y las tecnologías que cuente la organización.

3. Identificar los riesgos: En este punto como menciona se identifica las amenazas que puedan afectar a la organización, y el impacto que causaría en caso de que la confidencialidad, integridad y disponibilidad de la información se encuentren vulnerados.

4. Analizar y evaluar los riesgos: En el cuarto punto se realiza la evaluación en caso de que algunos de los riesgos identificados legaran a materializarse; para poder conocer cómo afectaría a las medidas de control que se encuentran implementados y evaluar si el riesgo se puede aceptar o se debe mitigar.

5. Hacer un tratamiento de riesgos: Es decir, aplicar los controles pertinentes, clasificar los niveles de riesgo, evitarlos o transferirlos a terceros si es posible.

6. Declarar la aplicabilidad: Debes establecer los objetivos de control y seleccionar los controles que se van a implementar.

7. Realizar la gestión: El punto 7 abarcar la gestión de cómo tratar los riesgos y el tratamiento de los controles. Además de generar conciencia dentro de la organización y fomentar una cultura que permita que todos los empleados conozcan el SGSI.

8. Monitorear: Por último, realizar una revisión del SGSI para verificar el cumplimiento de la norma ISO 27001, con los objetivos establecidos, así mismo, reportar las mejoras que sean necesarias y las acciones a ejecutar para lograr esto.

Stack de tecnologías utilizadas:

Lenguaje de programación PHP:

En esta tesis se desarrolló el prototipo de la NTP con el lenguaje de programación PHP, el cual se puede utilizar con cualquier tipo de servidor y cualquier sistema operativo virtual. Por otro lado, soporta una gran cantidad de bases de datos diferentes. Finalmente, brinda soporte completo para que el servidor se comunique con otros protocolos. PHP es muy fácil de usar para principiantes, pero también ofrece una amplia gama de funciones avanzadas para programadores profesionales.

Bootstrap:

Se hizo uso de Bootstrap es un marco diseñado para acelerar y reducir el tiempo que lleva crear páginas web, Bootstrap tiene códigos CSS y JavaScript que se pueden reutilizar para desarrollar cualquier sitio web de una manera más sencilla, está diseñado también para desarrollar sitios con un diseño receptivo, que se adapta a cualquier tipo de pantalla, y principalmente para teléfonos inteligentes. Proporciona herramientas con estilos ya establecidos para tipografía, botones, interfaces de navegación y más.

Javascript:

Es una especie de lenguaje de programación ligera, interpretado por la mayoría de los navegadores y que les proporciona a las páginas web, efectos y funciones complementarias a las consideradas como estándar HTML Este tipo de lenguaje de programación, con frecuencia son empleados en los sitios web, para realizar acciones en el lado del cliente, estando centrado en el código fuente de la página web.

Base de Datos en MySQL:

MySQL es un sistema de gestión de bases de datos relacionales de código abierto respaldado por Oracle y basado en el lenguaje de consulta estructurado (SQL). MySQL funciona prácticamente en todas las plataformas, incluyendo Linux, UNIX y Windows. Aunque puede utilizarse en una amplia gama de aplicaciones, MySQL se asocia más a menudo con las aplicaciones web y la publicación en línea.

Pantalla de Inicio de sesión

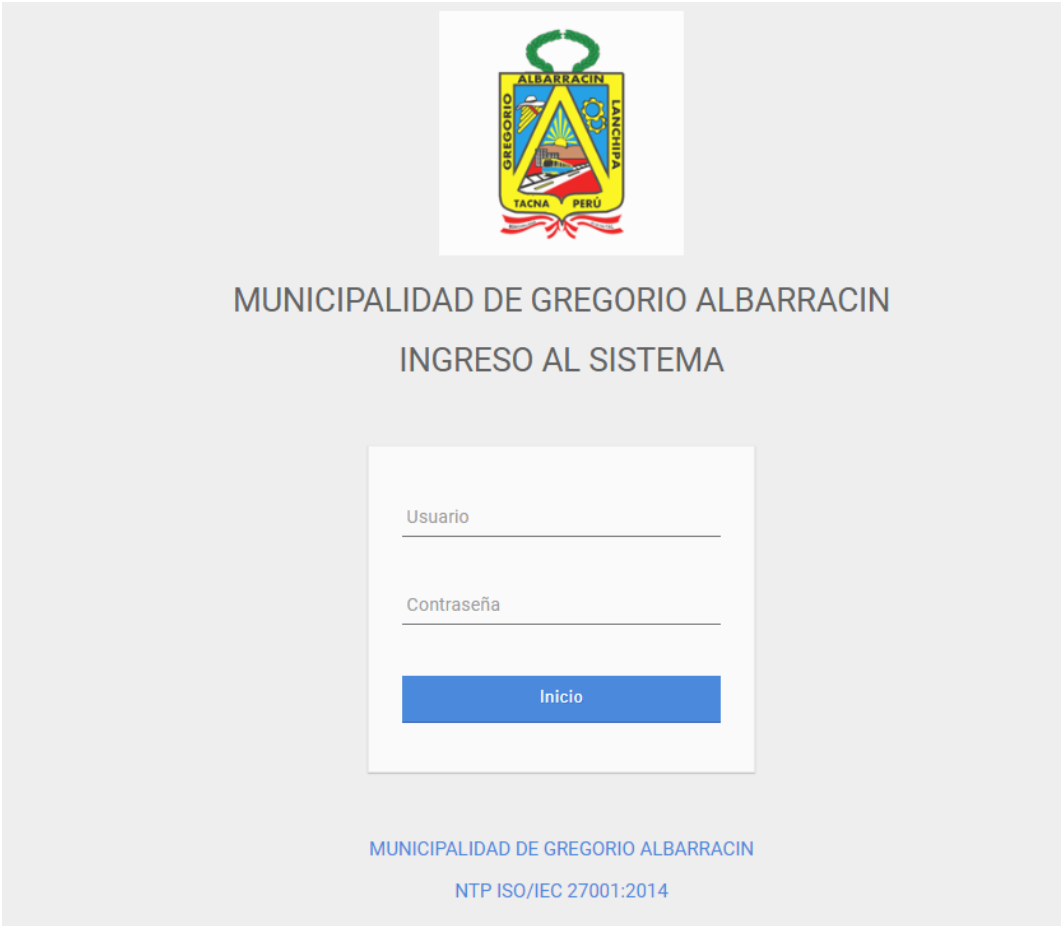
Login:

Descripción técnica:

La presente imagen fue construida con bootstrap, donde los campos de usuario y contraseña se encuentran validados, en la base de datos MySQL que están registrados previamente. Además de mostrar una alerta en caso de que el usuario o contraseña sean equivocados, con un límite de 3 intentos, de superar los intentos se bloqueara la cuenta de usuario por un día.

Descripción funcional:

Ingresamos con el usuario y contraseña de administrador, para ver el panorama general. En este apartado abordamos los indicadores de *confidencialidad* para el usuario y las claves de acceso y *fiabilidad* de los datos obtenidos por el Administrador.

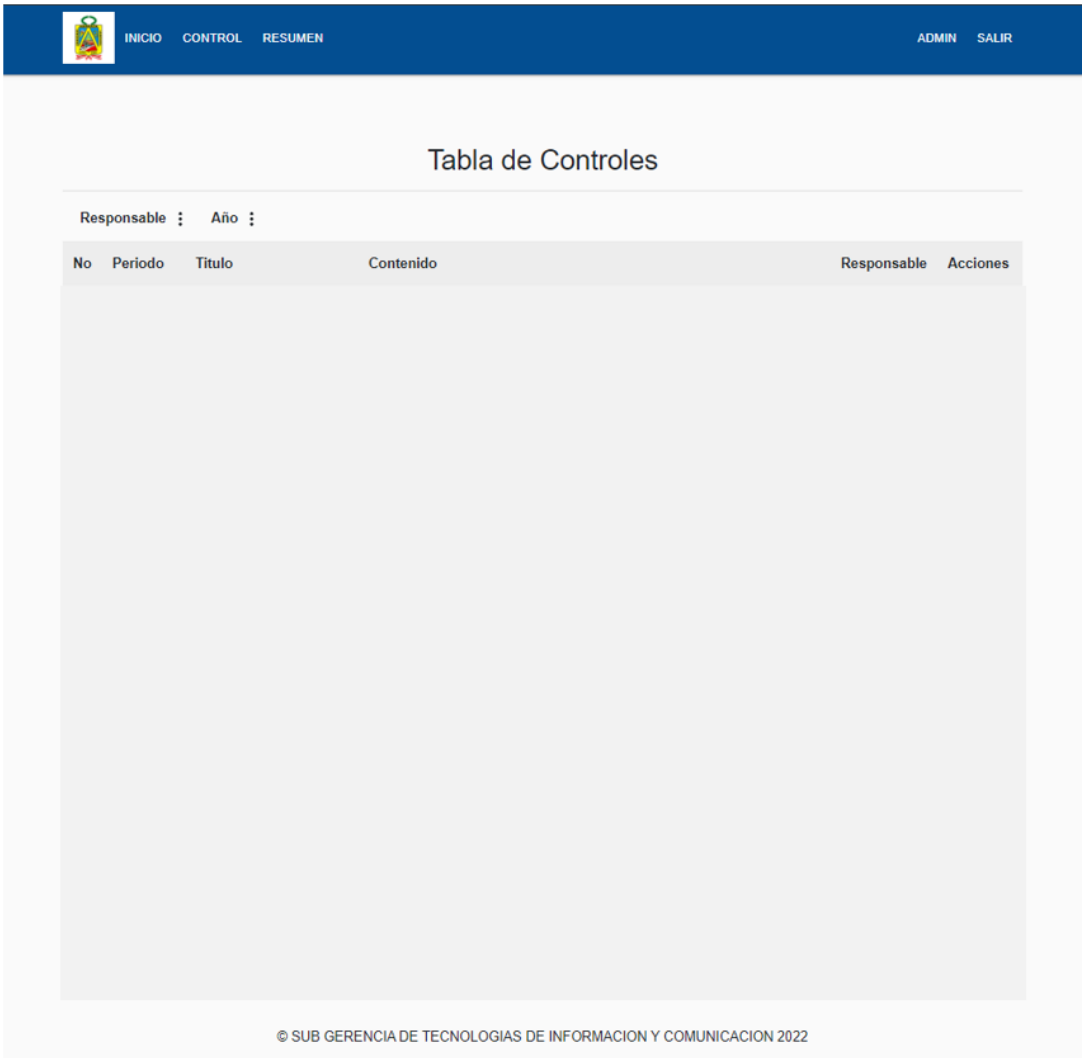


Definición funcional:

Al acceder se mostrará el menú principal del administrador el cual está vacío, ya que usaremos de ejemplo para la creación de los controles orientado a la *Norma Técnica Peruana 27001:2014 ISO-IEC* y a sus dimensiones de *Confidencialidad, Integridad y Disponibilidad.*

Descripción técnica:

En la siguiente captura se muestra la tabla de controles, la cual consta de 6 columnas que se encuentran validados donde solo se pueda ingresar texto con excepción de la columna N° la cual se autogenera según cada control sea registrado. Además, cada control registrado se almacenará en la base de datos MySQL y se mostrará en esta Tabla de Controles.



Definición funcional:

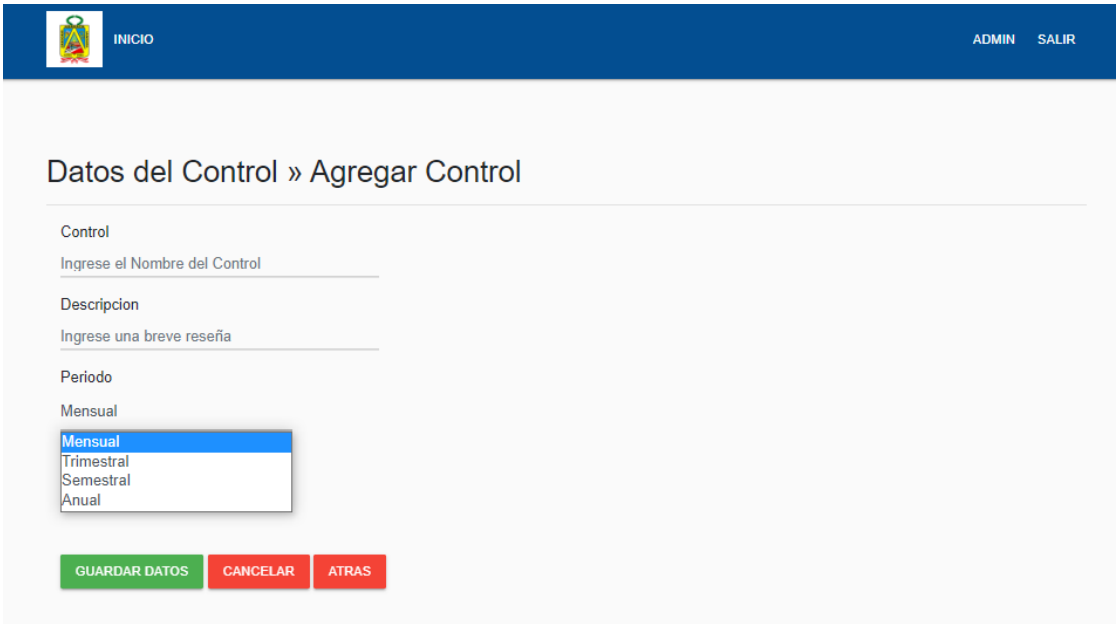
Para agregar un nuevo control nos ubicamos en la parte superior del encabezado.

Descripción técnica:

En la siguiente captura se muestra la barra de menú, que también fue diseñado con Bootstrap, en la cual podemos observar las opciones de Inicio, Control y Resumen. Las cuales están enlazadas a diferentes formularios.

Descripción funcional:

Se ingresa el nombre del control y una breve descripción (concepto del mismo). En la creación de los controles se cuenta con periodos para así poder monitorear de manera mensual, trimestral, semestral o anual los controles alojados en el sistema para así evaluar la *capacidad de respuesta* de los controles.

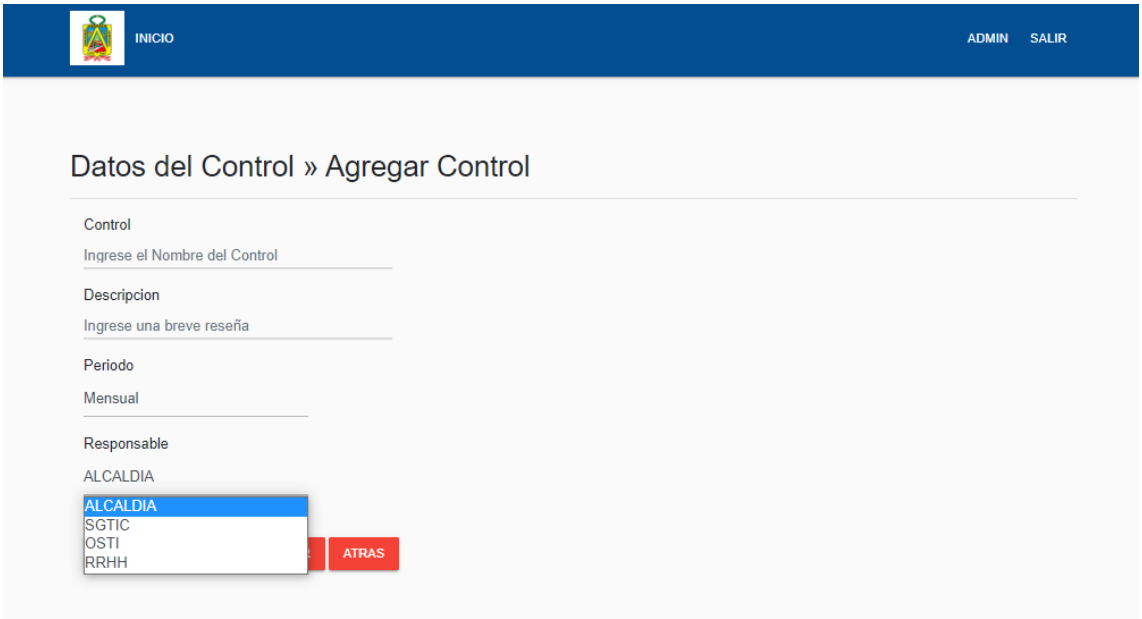


Descripción funcional:

Se cuenta además con el apartado de responsable donde podremos designar entre (Alcaldía, SGTIC, OSTI y RRHH) para la óptima gestión de los controles y así asegurar la *integridad* de la información

Descripción Técnica:

En el formulario de *Agregar Control***,** los campos se encuentran validados, además que los campos Periodo y Responsable son de múltiples opciones las cuales solo se puede seleccionar uno, Tiene la validación que todos los campos son requeridos antes de Guardar los datos, caso contrario los datos están correctamente completados se almacenaran en la base de datos.

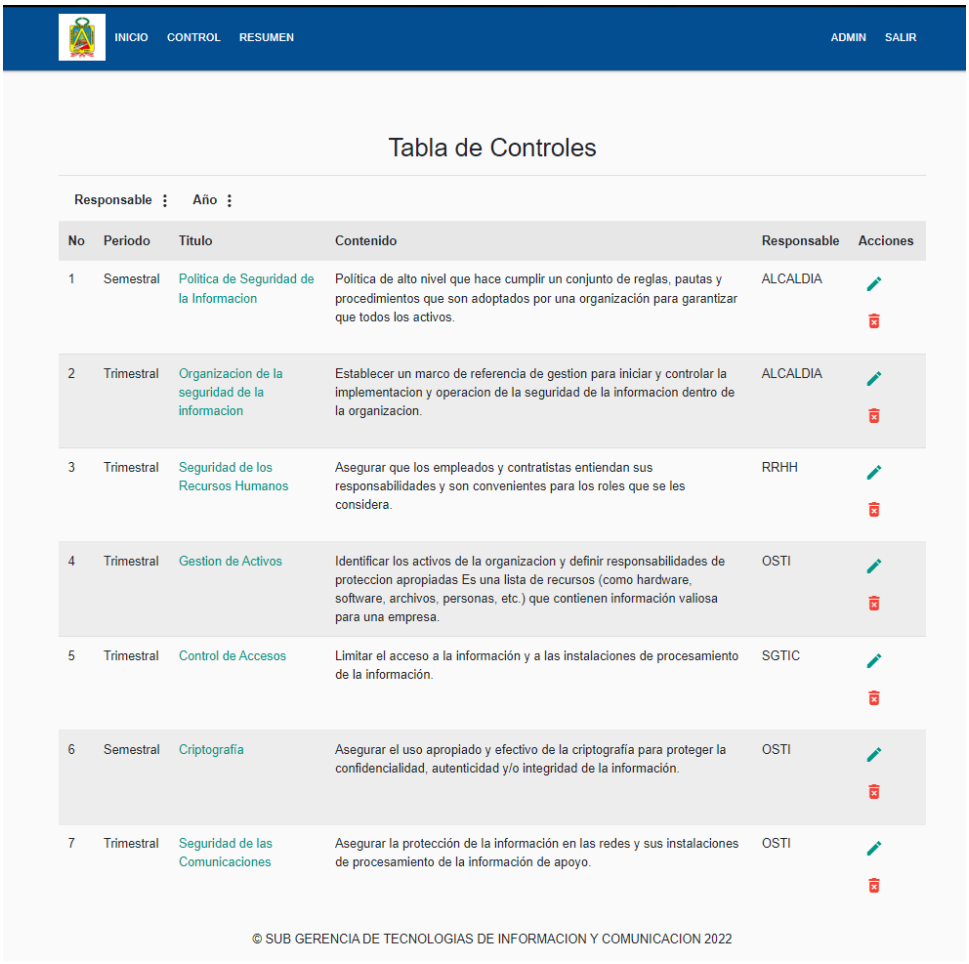


Definición funcional:

Una vez ingresado todos los controles a utilizar basado en la *Norma Técnica Peruana 27001:2014 ISO-IEC*, podremos visualizar el orden de la lista, el periodo en el cual se tiene como duración de dicho control, el título del control, el contenido (resumen teórico del control), el responsable a cargo del control y el apartado de acciones podremos agregar ubicándonos en el lápiz de color verde.

Descripción técnica:

En la siguiente captura, muestra todos los controles que están registrados en la base de datos. Además, cada información se muestra según el título de cada columna correspondiente.



Definición funcional:

Una vez dentro de la acción veremos según el periodo previamente elegido nos muestra los meses en el cual se tiene que cumplir la meta del control aclarando la *disponibilidad* de los datos, según el estado de Pendiente o Controlado.

Definición técnica:

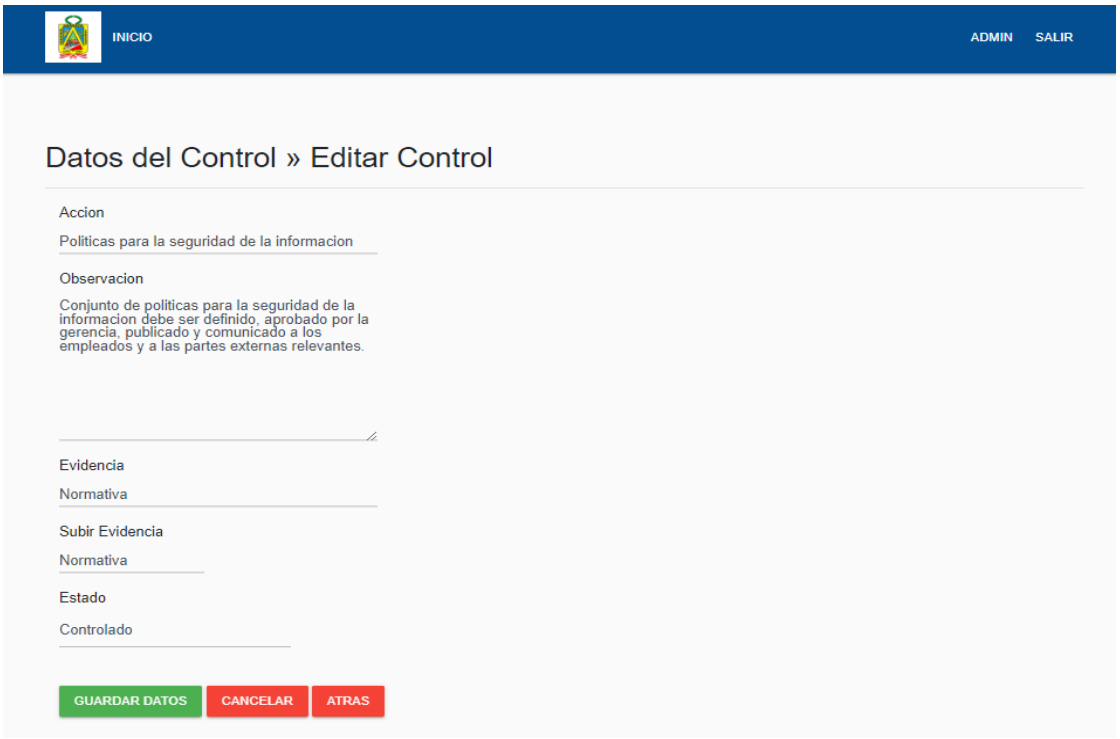
En la siguiente captura observamos las Acciones de Editar, el cual se utilizado un icono de un Lápiz para ser más amigable la interfaz; además de un icono de un tacho que significa la Acción de Eliminar.

Definición funcional:

Ingresamos a editar en acciones para especificar la acción a tomar, donde podremos aprecia el nombre del control, el resumen de la misma, podremos también agregar la evidencia en este caso sería una normativa (previamente aprobada por la institución) y también podremos.

Definición Técnica:

La opción de *Editar Control***,** envía al formulario del control donde cada campo se completa con la información previamente registrada en la base de datos. Donde cualquier campo es posible modificar y para su almacenamiento se grabe en la base de datos por medio del botón *Guardar Datos***,** que permite actualizar la información.



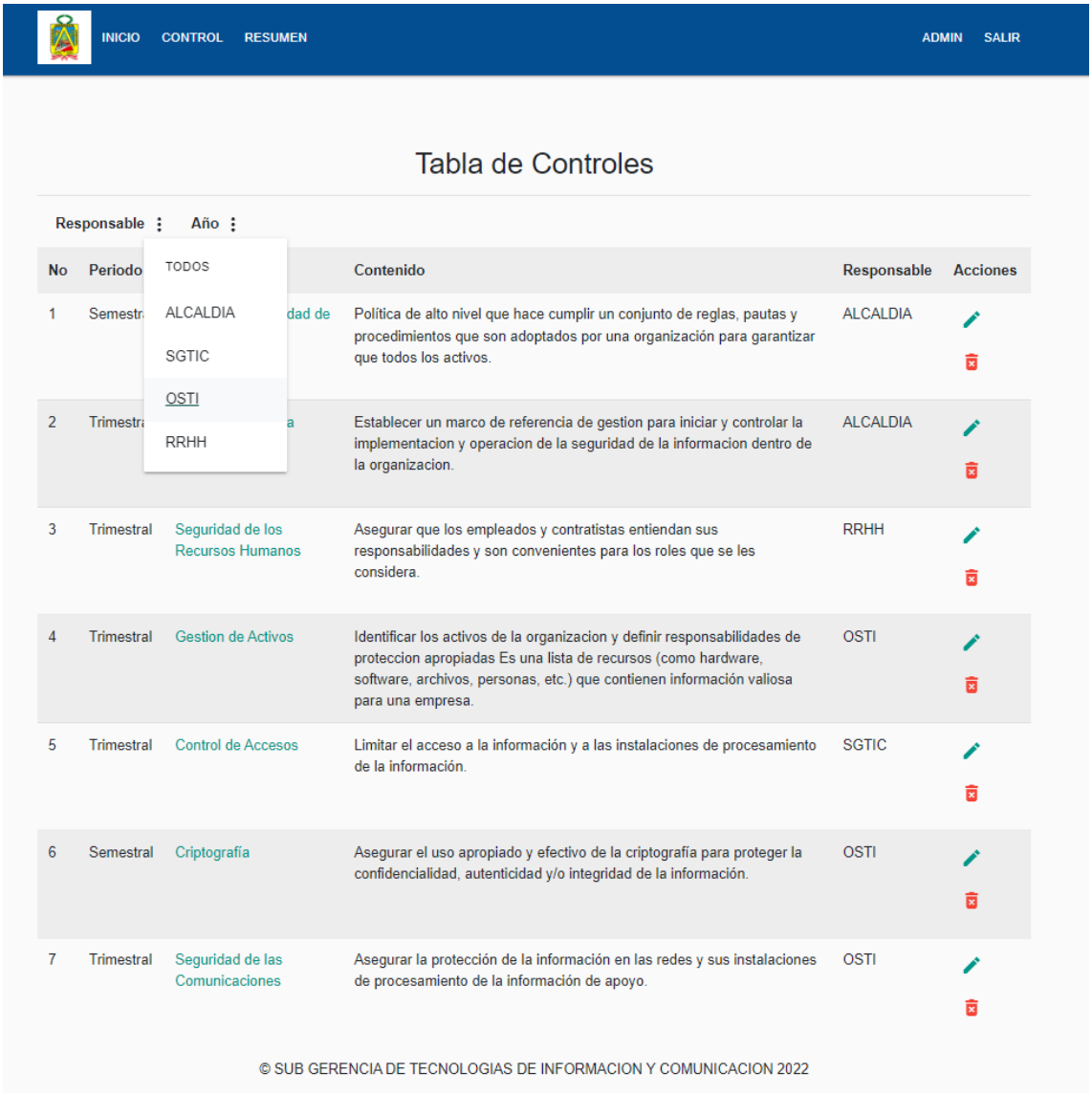
En el caso que sea controlado o esté pendiente, se vera de la siguiente manera.

Definición funcional:

También podemos filtrar por responsable, para tener una vista más limpia de los controles que maneja cada responsable en la Municipalidad.

Definición técnica:

En esta captura se muestra las opciones de filtro las cuales son Responsable, lo cual hace una búsqueda dentro de la base de datos según el filtro seleccionado. Los resultados se mostrarán en la vista.



Definición funcional:

En el caso que se requiera hacer consultas por un año específico también se podría filtrar, en el caso de contar con años pasados para ver qué tan efectivo fue la implementación de la misma.

Definición técnica:

En esta captura se muestra las opciones de filtro las cuales son Responsabilidad y Año, Lo cual hace una búsqueda dentro de la base de datos según el filtro seleccionado. Los resultados se mostrarán en la vista.

Vista del Oficial de Seguridad de Tecnologías de Información.

Definición funcional:

En el caso se puede apreciar el control que el usuario de Oficial de Seguridad de Tecnologías de Información (OSTI) tiene para su control.

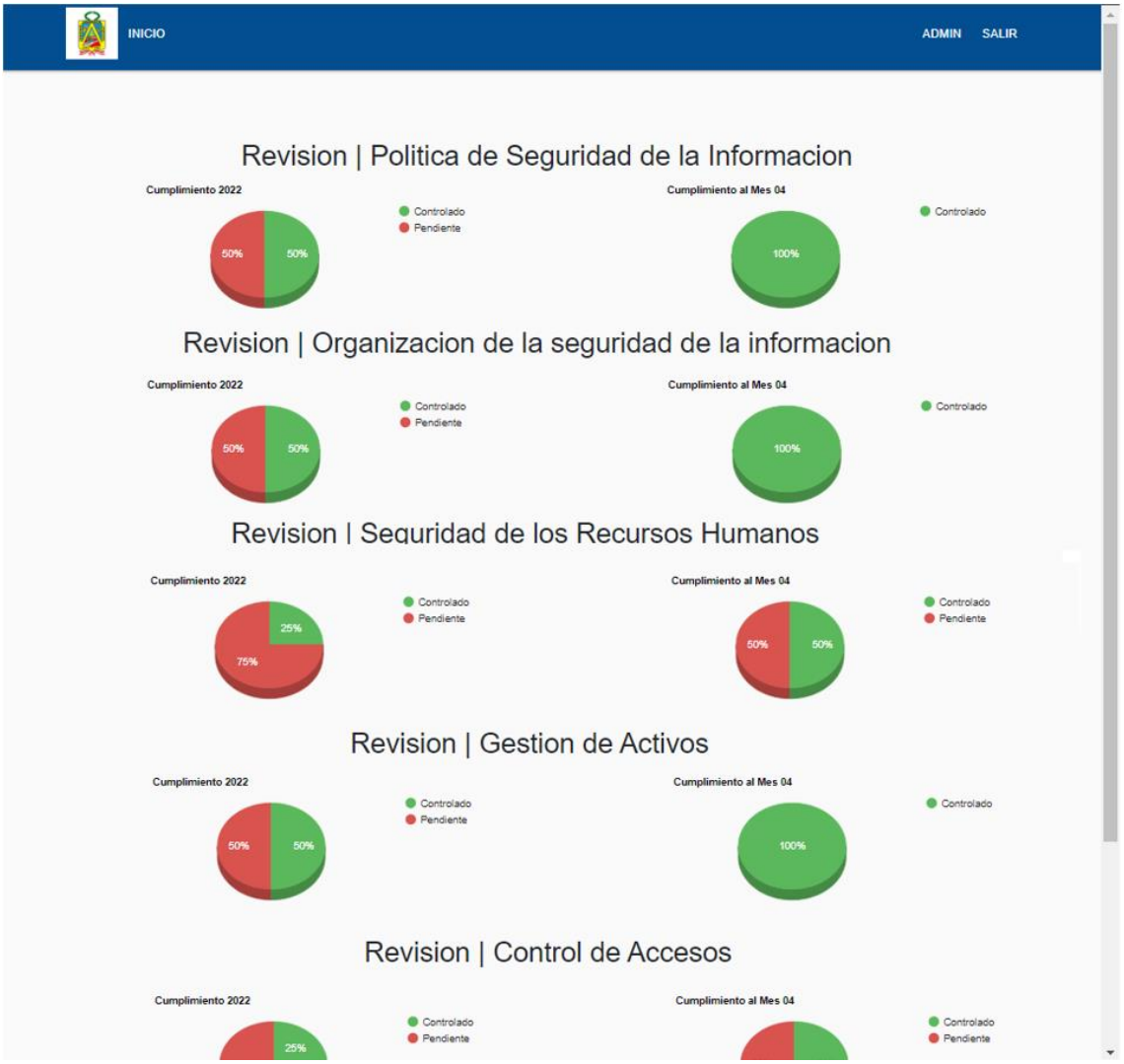
En el caso que se quiera acceder a resumen

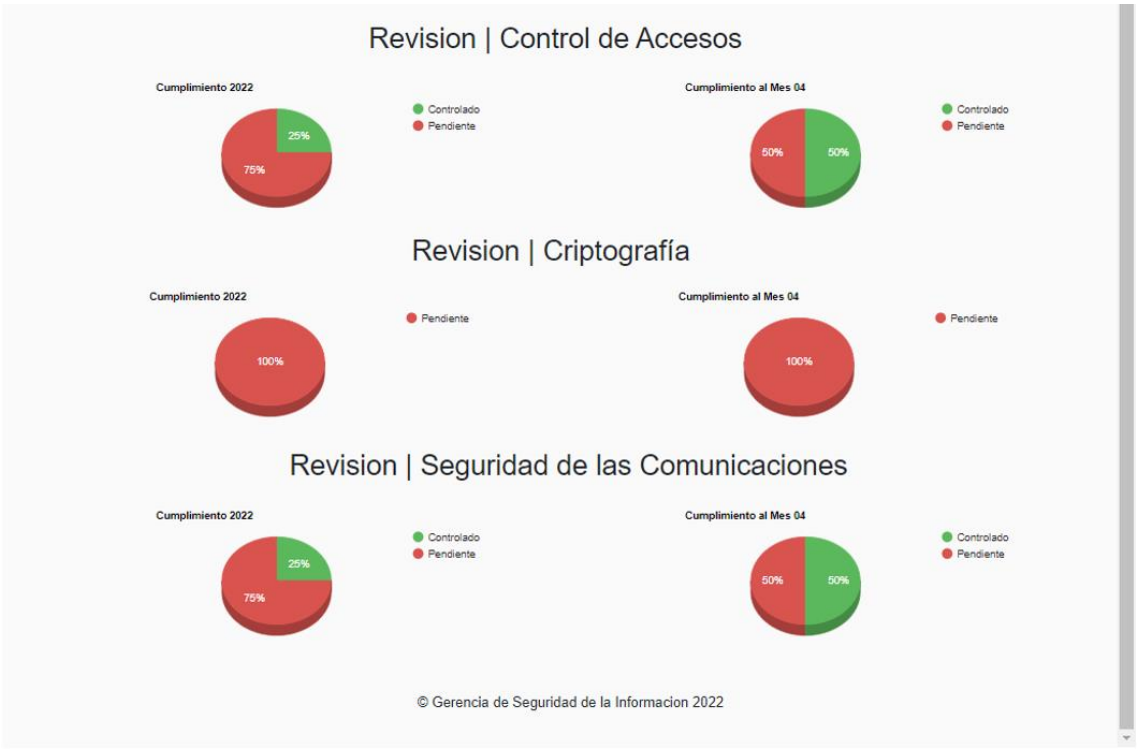
Definición funcional:

Tendremos esta vista la cual es un resumen de todos los controles para poder así tener un mayor control y monitoreo de la misma, para conocer el estado y poder tomar medidas correctivas en el caso se requiera.

Definición técnica:

En esta captura al presionar la opción de resumen**,** el sistema mostrara un reporte de todos los controles previamente registrados. Mostrará el reporte de manera gráfica por lo cual se utilizó JavaScript para realizar el diseño según el estado del control.


INICIO
ADMIN
SALIR
Revision | Politica de Seguridad de la Informacion
Cumplimiento 2022
Controlado
Pendiente
50%
50%
Cumplimiento al Mes 04
Controlado
100%
Revision | Organizacion de la seguridad de la informacion
Cumplimiento 2022
Controlado
Pendiente
50%
50%
Cumplimiento al Mes 04
Controlado
100%
Revision | Seguridad de los Recursos Humanos
Cumplimiento 2022
Controlado
Pendiente
25%
75%
Cumplimiento al Mes 04
Controlado
Pendiente
50%
50%
Revision | Gestion de Activos
Cumplimiento 2022
Controlado
Pendiente
50%
50%
Cumplimiento al Mes 04
Controlado
100%
Revision | Control de Accesos
Cumplimiento 2022
Controlado
Pendiente
25%
Cumplimiento al Mes 04
Controlado
Pendiente

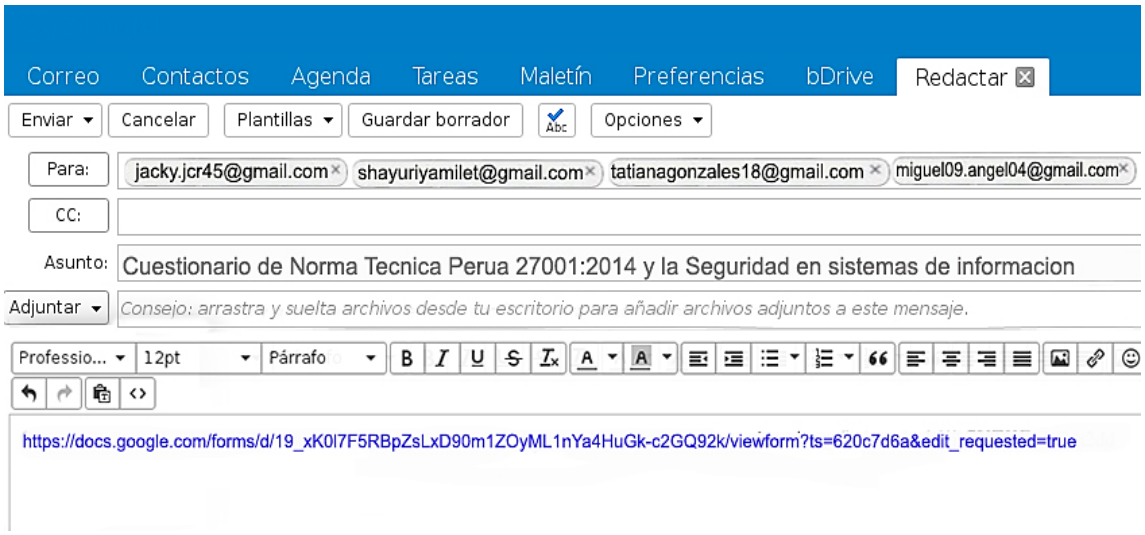

Revision | Control de Accesos
Cumplimiento 2022
25%
75%
Controlado
Pendiente
Cumplimiento al Mes 04
50%
50%
Controlado
Pendiente
Revision | Criptografía
Cumplimiento 2022
100%
Pendiente
Cumplimiento al Mes 04
100%
Pendiente
Revision | Seguridad de las Comunicaciones
Cumplimiento 2022
25%
75%
Controlado
Pendiente
Cumplimiento al Mes 04
50%
50%
Controlado
Pendiente
© Gerencia de Seguridad de la Informacion 2022

Anexo 08 Evidencia de recolección de datos

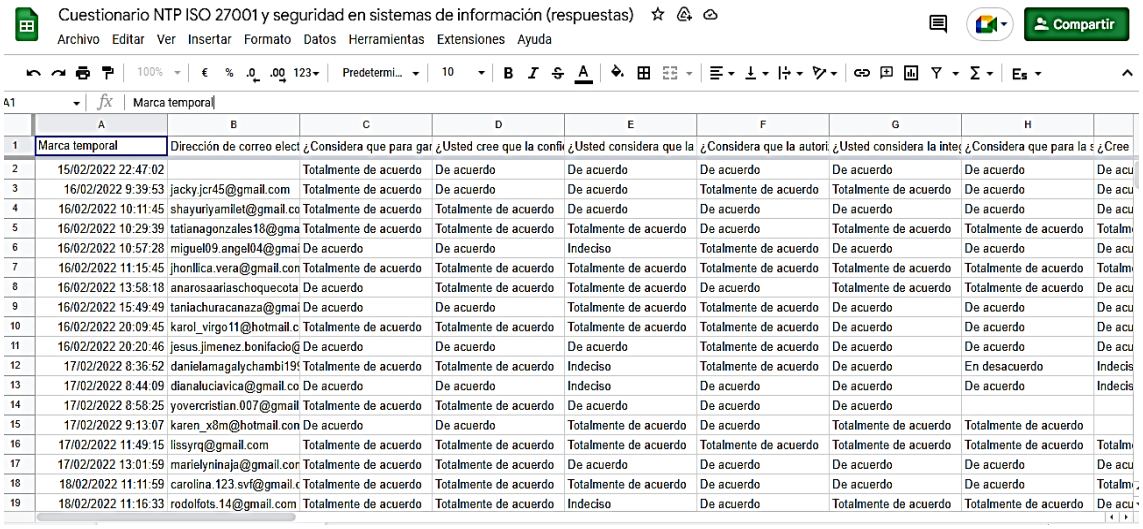
Se realizó una encuesta virtual de 26 preguntas relacionadas a las dos variables de estudio, se enviaron a 80 empleados por medio de correo electrónico los cuales previamente fueron seleccionados de una población de 100 empleados.

Las preguntas se realizaron por medio de Google Forms, por lo cual se generó un link el cual fue enviado a los correos a continuación, se muestra el link del cuestionario.

https://docs.google.com/forms/d/19_xK0l7F5RBpZsLxD90m1ZOyML1nYa4HuGk-c2GQ92k/viewform?ts=620c7d6a&edit_requested=true



Captura del reporte en Excel con los correos, fecha, hora y las respuestas seleccionadas de los trabajadores encuestados.



Cuestionario NTP ISO 27001 y seguridad en sistemas de información (respuestas)

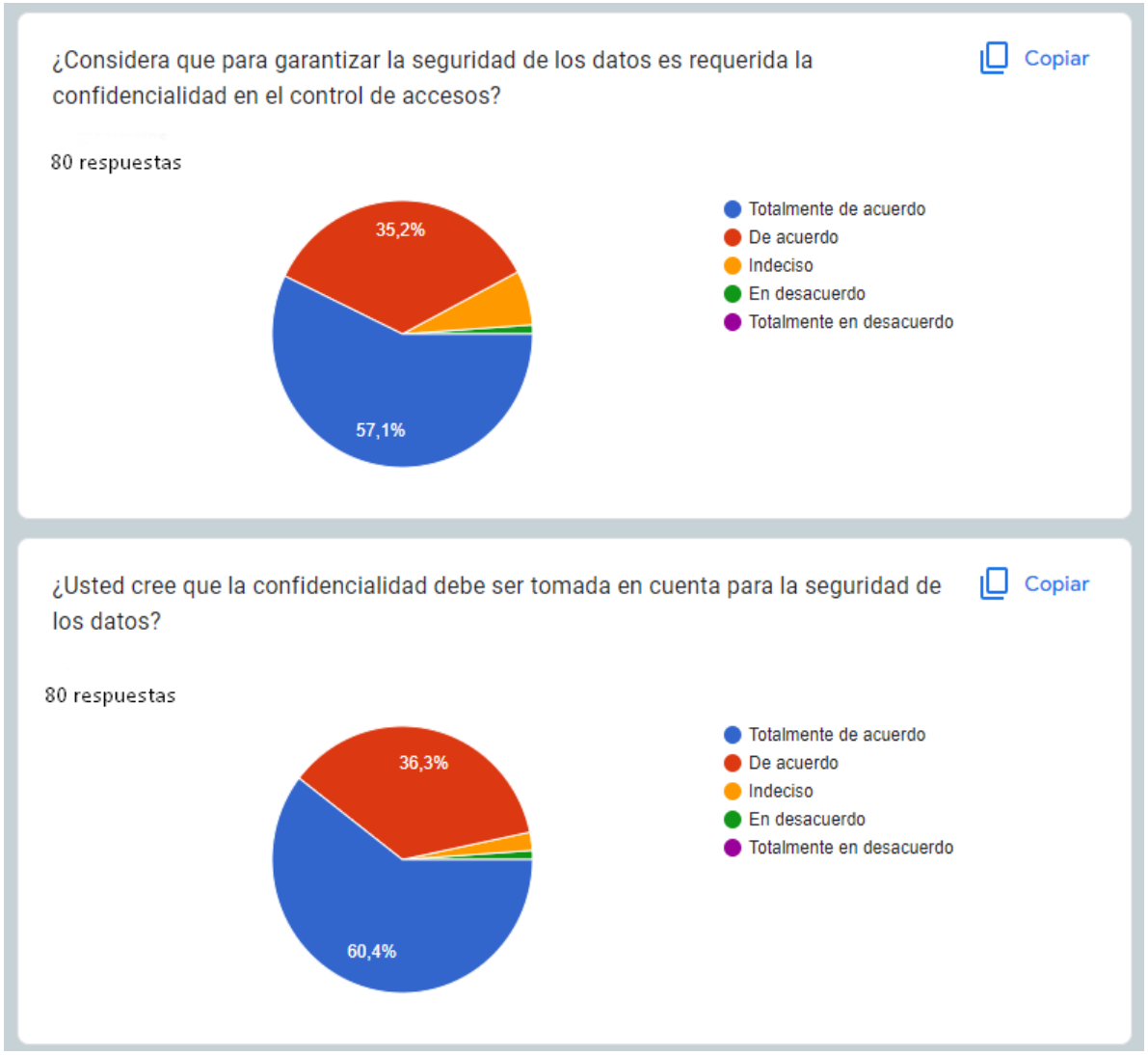
Archivo Editar Ver Insertar Formato Datos Herramientas Extensiones Ayuda

Compartir

A1 Marca temporal

	A	B	C	D	E	F	G	H	
1	Marca temporal	Dirección de correo elect	¿Considera que para gar	¿Usted cree que la confi	¿Usted considera que la	¿Considera que la autori	¿Usted considera la inte	¿Considera que para la s	¿Cree
2	15/02/2022 22:47:02		Totalmente de acuerdo	De acuerdo	De acuerdo	De acuerdo	De acuerdo	De acuerdo	De acu
3	16/02/2022 9:39:53	jacky.jcr45@gmail.com	Totalmente de acuerdo	De acuerdo	De acuerdo	Totalmente de acuerdo	Totalmente de acuerdo	De acuerdo	De acu
4	16/02/2022 10:11:45	shayuriyamilet@gmail.co	Totalmente de acuerdo	Totalmente de acuerdo	De acuerdo	De acuerdo	De acuerdo	De acuerdo	De acu
5	16/02/2022 10:29:39	tatianagonzales18@gma	Totalmente de acuerdo	Totalmente de acuerdo	Totalmente de acuerdo	De acuerdo	Totalmente de acuerdo	Totalmente de acuerdo	Totalm
6	16/02/2022 10:57:28	miguel09.angel04@gmai	De acuerdo	De acuerdo	Indeciso	Totalmente de acuerdo	De acuerdo	De acuerdo	De acu
7	16/02/2022 11:15:45	jhonllica.vera@gmail.con	Totalmente de acuerdo	Totalmente de acuerdo	Totalmente de acuerdo	Totalmente de acuerdo	Totalmente de acuerdo	Totalmente de acuerdo	Totalm
8	16/02/2022 13:58:18	anarosaariaschoquecota	De acuerdo	Totalmente de acuerdo	Totalmente de acuerdo	De acuerdo	Totalmente de acuerdo	Totalmente de acuerdo	De acu
9	16/02/2022 15:49:49	taniachuracanaza@gmai	De acuerdo	De acuerdo	Totalmente de acuerdo	Totalmente de acuerdo	De acuerdo	De acuerdo	De acu
10	16/02/2022 20:09:45	karol_virgo11@hotmail.c	Totalmente de acuerdo	Totalmente de acuerdo	Totalmente de acuerdo	Totalmente de acuerdo	De acuerdo	De acuerdo	De acu
11	16/02/2022 20:20:46	jesus.jimenez.bonifacio@	De acuerdo	De acuerdo	De acuerdo	Totalmente de acuerdo	De acuerdo	De acuerdo	De acu
12	17/02/2022 8:36:52	danielamagalychambi19	Totalmente de acuerdo	Totalmente de acuerdo	Indeciso	Totalmente de acuerdo	De acuerdo	En desacuerdo	Indecis
13	17/02/2022 8:44:09	dianaluciavica@gmail.co	De acuerdo	De acuerdo	Indeciso	De acuerdo	De acuerdo	De acuerdo	Indecis
14	17/02/2022 8:58:25	yovercristian.007@gmail	Totalmente de acuerdo	Totalmente de acuerdo	De acuerdo	De acuerdo	De acuerdo		
15	17/02/2022 9:13:07	karen_x8m@hotmail.con	De acuerdo	De acuerdo	Totalmente de acuerdo	De acuerdo	Totalmente de acuerdo	Totalmente de acuerdo	
16	17/02/2022 11:49:15	lissyrq@gmail.com	Totalmente de acuerdo	Totalmente de acuerdo	Totalmente de acuerdo	Totalmente de acuerdo	Totalmente de acuerdo	Totalmente de acuerdo	Totalm
17	17/02/2022 13:01:59	marielyninaja@gmail.cor	Totalmente de acuerdo	Totalmente de acuerdo	De acuerdo	De acuerdo	De acuerdo	De acuerdo	De acu
18	18/02/2022 11:11:59	carolina.123.svf@gmail.c	Totalmente de acuerdo	Totalmente de acuerdo	Totalmente de acuerdo	De acuerdo	De acuerdo	De acuerdo	Totalm
19	18/02/2022 11:16:33	rodolfots.14@gmail.com	Totalmente de acuerdo	Totalmente de acuerdo	Indeciso	De acuerdo	Totalmente de acuerdo	Totalmente de acuerdo	De acu

Captura del resumen de algunas preguntas realizadas.



Anexo 09 Juicio de Expertos

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO QUE MIDE LA VARIABLE NORMA TÉCNICA PERUANA 27001:2014 ISO-IEC

N.º	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	DIMENSIÓN 1 CONFIDENCIALIDAD	Si	No	Si	No	Si	No	
1	¿Cree usted que para garantizar la seguridad de los datos es requerida la confidencialidad en el control de accesos?	✓		✓		✓		
2	¿Usted cree que la confidencialidad debe ser tomada en cuenta como uno de los pilares en la seguridad de los datos?	✓		✓		✓		
3	¿Usted considera que la autorización debe ser de carácter confidencial?	✓		✓		✓		
4	¿Considera que la autorización es una exigencia necesaria para poder acceder a los datos?	✓		✓		✓		
	DIMENSIÓN 2 INTEGRIDAD	Si	No	Si	No	Si	No	
5	¿Usted considera que la integridad es una parte esencial para la seguridad de las comunicaciones?	✓		✓		✓		
6	¿Considera que para la seguridad de las comunicaciones la integridad es de carácter relevante en la seguridad de los datos?	✓		✓		✓		
7	¿Cree usted que la integridad precisa de la seguridad de los procedimientos, los cuales serían de consideración significativa para la seguridad de los datos?	✓		✓		✓		
8	¿Es correcto que los procesos deban tener un adecuado manejo para así garantizar la integridad en la seguridad de los datos?	✓		✓		✓		
	DIMENSIÓN 3 DISPONIBILIDAD	Si	No	Si	No	Si	No	
9	¿Cree usted que contar con el acceso a la información en el momento solicitado es a consecuencia de la disponibilidad de los datos seguros?	✓		✓		✓		
10	¿Cree usted que contar con el acceso a la información en el momento solicitado se debe considerar como elemento primordial a la disponibilidad?	✓		✓		✓		
11	¿Considera que para garantizar la fidelidad de los datos la disponibilidad debe tomar en consideración el acceso a los datos?	✓		✓		✓		
12	¿Se debe considerar como elemento primordial a la disponibilidad para así garantizar el acceso a los datos?	✓		✓		✓		

Observaciones (precisar si hay suficiencia): Existe suficiencia en la aplicación del instrumento.

Opinión de aplicabilidad: **Aplicable [✓]** **Aplicable después de corregir [_]** **No aplicable [ ]**

Apellidos y nombres del juez validador. Dr/ Mg: Mg. Ricardo Carlos Inquilla Quispe **DNI:** 00515158

Especialidad del validador: Especialidad Magister e ingeniero de Sistemas

[1]**Pertinencia**: El ítem corresponde al concepto teórico formulado.
[2]**Relevancia**: El ítem es apropiado para representar al componente o dimensión específica del constructo
[3]**Claridad**: Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

05 de mayo del 2022

Firma del Experto Informante.

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE LA VARIABLE SEGURIDAD EN SISTEMAS DE INFORMACIÓN

N°	DIMENSIONES / Ítems	Pertinencia		Relevancia		Claridad		Sugerencias
	DIMENSION 1 ELEMENTOS TANGIBLES	Si	No	Si	No	Si	No	
1	¿Considera que los equipos informáticos (computadoras, laptops y otros periféricos) utilizados actualmente son adecuadamente para la infraestructura de la seguridad en sistemas de información?	✓		✓		✓		
2	¿Considera que los equipos informáticos (computadoras, laptops y otros periféricos) utilizados actualmente son adecuadamente para la infraestructura de la seguridad en sistemas de información?	✓		✓		✓		
3	¿Considera que los equipos de almacenamiento de información (backup) son un factor relevante para mantener la seguridad en sistemas de información?	✓		✓		✓		
4	¿Considera que debe existir un plan de copias de seguridad semanal y mensual de los datos para tener una adecuada seguridad en sistemas de información?	✓		✓		✓		
5	¿Considera que la infraestructura (ordenadores, internet, equipos de red) son los adecuados o cumplen los requisitos mínimos (condiciones generales) para permitir mantener la seguridad en sistemas de información?	✓		✓		✓		
6	¿Considera que la infraestructura (ordenadores, internet, equipos de red) deben ser renovados cada dos años y cumplan con los requisitos recomendados o mínimos (condiciones generales) al comprar de nuevos ordenadores, equipos de red y actualización del plan de internet para mejorar la seguridad en sistemas de información?	✓		✓		✓		
	DIMENSION 2 FIABILIDAD							
7	¿Considera usted que el compromiso por parte de los trabajadores de la Sub Gerencia de TIC debe ser considerado un factor fundamental para el logro de la seguridad en sistemas de información?	✓		✓		✓		
8	¿Considera usted que los trabajadores deben que manejan información importante por medio de los sistemas deben firmar un documento de compromiso de no divulgación de información confidencial para una eficiente seguridad en sistemas de información?	✓		✓		✓		
9	¿Considera que la seguridad en sistemas de información debe cumplir con el servicio prometido (acceso a la información y acceso a los sistemas)?	✓		✓		✓		
10	¿El servicio prometido (acceso a los sistemas y acceso a internet) influye de tal manera que permita alcanzar la seguridad en sistemas de información?	✓		✓		✓		
	DIMENSION 3 CAPACIDAD DE RESPUESTA							
11	¿Considera que el tiempo de repuesta al solicitar algún tipo de información depende de la seguridad en sistemas de información?	✓		✓		✓		
12	¿Considera que cuan menor sea el tiempo de respuesta influye positivamente la seguridad en sistemas de información?	✓		✓		✓		
13	¿Consideraría que la seguridad en sistemas de información requiere de actualizaciones según la necesidad que requieran los trabajadores así poder permitir tener una mejora continua?	✓		✓		✓		
14	¿Considera que por medio de la mejora continua de la seguridad en sistemas de información favorece en gran medida capacidad de respuesta que se le brinda al usuario (poblador) cuando requiera información?	✓		✓		✓		

Observaciones (precisar si hay suficiencia): Existe suficiencia en la aplicación del instrumento.

Opinión de aplicabilidad: **Aplicable [✓]** **Aplicable después de corregir [_]** **No aplicable [ ]**

Apellidos y nombres del juez validador. Dr/ Mg: Mg. Ricardo Carlos Inquilla Quispe **DNI:** 00515158

Especialidad del validador: Especialidad Magister e ingeniero de Sistemas

05 de mayo del 2022

Pertinencia: El ítem corresponde al concepto teórico formulado.
Relevancia: El ítem es apropiado para representar al componente o dimensión específica del constructor.
Claridad: Se entiende sin dificultad alguna el enunciado del ítem es conciso, exacto y directo.

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados medir la dimensión.

Firma del Experto Informante.

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO QUE MIDE LA VARIABLE NORMA TÉCNICA PERUANA 27001:2014 ISO-IEC

N.°	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	DIMENSIÓN 1 CONFIDENCIALIDAD	**Si**	**No**	**Si**	**No**	**Si**	**No**	
1	¿Cree usted que para garantizar la seguridad de los datos es requerida la confidencialidad en el control de accesos?	✓		✓		✓		
2	¿Usted cree que la confidencialidad debe ser tomada en cuenta como uno de los pilares en la seguridad de los datos?	✓		✓		✓		
3	¿Usted considera que la autorización debe ser de carácter confidencial?	✓		✓		✓		
4	¿Considera que la autorización es una exigencia necesaria para poder acceder a los datos?	✓		✓		✓		
	DIMENSIÓN 2 INTEGRIDAD	**Si**	**No**	**Si**	**No**	**Si**	**No**	
5	¿Usted considera que la integridad es una parte esencial para la seguridad de las comunicaciones?	✓		✓		✓		
6	¿Considera que para la seguridad de las comunicaciones la integridad es de carácter relevante en la seguridad de los datos?	✓		✓		✓		
7	¿Cree usted que la integridad precisa de la seguridad de los procedimientos, los cuales serían de consideración significativa para la seguridad de los datos?	✓		✓		✓		
8	¿Es correcto que los procesos deban tener un adecuado manejo para así garantizar la integridad en la seguridad de los datos?	✓		✓		✓		
	DIMENSIÓN 3 DISPONIBILIDAD	**Si**	**No**	**Si**	**No**	**Si**	**No**	
9	¿Cree usted que contar con el acceso a la información en el momento solicitado es a consecuencia de la disponibilidad de los datos seguros?	✓		✓		✓		
10	¿Cree usted que contar con el acceso a la información en el momento solicitado se debe considerar como elemento primordial a la disponibilidad?	✓		✓		✓		
11	¿Considera que para garantizar la fidelidad de los datos la disponibilidad debe tomar en consideración el acceso a los datos?	✓		✓		✓		
12	¿Se debe considerar como elemento primordial a la disponibilidad para así garantizar el acceso a los datos?	✓		✓		✓		

Observaciones (precisar si hay suficiencia): Existe suficiencia en el instrumento

Opinión de aplicabilidad: **Aplicable [✓]** **Aplicable después de corregir [_]** **No aplicable [ ]**

Apellidos y nombres del juez validador. Dr/ Mg: Mg. Víctor Jimenez Flores **DNI:** 71203062

Especialidad del validador: Mag. En administración y dirección de empresas e Ing. De sistemas

[1]**Pertinencia**: El ítem corresponde al concepto teórico formulado.
[2]**Relevancia**: El ítem es apropiado para representar al componente o dimensión específica del constructo
[3]**Claridad**: Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

05 de mayo del 2022

Firma del Experto Informante.

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE LA VARIABLE SEGURIDAD EN SISTEMAS DE INFORMACIÓN

N°	DIMENSIONES / Ítems	Pertinencia		Relevancia		Claridad		Sugerencias
	DIMENSION 1 ELEMENTOS TANGIBLES	**Si**	**No**	**Si**	**No**	**Si**	**No**	
1	¿Considera que los equipos informáticos (computadoras, laptops y otros periféricos) utilizados actualmente son adecuadamente para la infraestructura de la seguridad en sistemas de información?	✓		✓		✓		
2	¿Considera que los equipos informáticos (computadoras, laptops y otros periféricos) utilizados actualmente son adecuadamente para la infraestructura de la seguridad en sistemas de información?	✓		✓		✓		
3	¿Considera que los equipos de almacenamiento de información (backup) son un factor relevante para mantener la seguridad en sistemas de información?	✓		✓		✓		
4	¿Considera que debe existir un plan de copias de seguridad semanal y mensual de los datos para tener una adecuada seguridad en sistemas de información?	✓		✓		✓		
5	¿Considera que la infraestructura (ordenadores, internet, equipos de red) son los adecuados o cumplen los requisitos mínimos (condiciones generales) para permitir mantener la seguridad en sistemas de información?	✓		✓		✓		
6	¿Considera que la infraestructura (ordenadores, internet, equipos de red) deben ser renovados cada dos años y cumplan con los requisitos recomendados o mínimos (condiciones generales) al comprar de nuevos ordenadores, equipos de red y actualización del plan de internet para mejorar la seguridad en sistemas de información?	✓		✓		✓		
	DIMENSION 2 FIABILIDAD							
7	¿Considera usted que el compromiso por parte de los trabajadores de la Sub Gerencia de TIC debe ser considerado un factor fundamental para el logro de la seguridad en sistemas de información?	✓		✓		✓		
8	¿Considera usted que los trabajadores deben que manejan información importante por medio de los sistemas deben firmar un documento de compromiso de no divulgación de información confidencial para una eficiente seguridad en sistemas de información?	✓		✓		✓		
9	¿Considera que la seguridad en sistemas de información debe cumplir con el servicio prometido (acceso a la información y acceso a los sistemas)?	✓		✓		✓		
10	¿El servicio prometido (acceso a los sistemas y acceso a internet) influye de tal manera que permita alcanzar la seguridad en sistemas de información?	✓		✓		✓		
	DIMENSION 3 CAPACIDAD DE RESPUESTA							
11	¿Considera que el tiempo de repuesta al solicitar algún tipo de información depende de la seguridad en sistemas de información?	✓		✓		✓		
12	¿Considera que cuan menor sea el tiempo de respuesta influye positivamente la seguridad en sistemas de información?	✓		✓		✓		
13	¿Consideraría que la seguridad en sistemas de información requiere de actualizaciones según la necesidad que requieran los trabajadores así poder permitir tener una mejora continua?	✓		✓		✓		

14	¿Considera que por medio de la mejora continua de la seguridad en sistemas de información favorece en gran medida capacidad de respuesta que se le brinda al usuario (poblador) cuando requiera información?	✓		✓		✓		

Observaciones (precisar si hay suficiencia): Existe suficiencia en la aplicación del instrumento
Opinión de aplicabilidad: Aplicabilidad [✓] Aplicabilidad después de corregir [ ] No aplicable [ ]

Apellidos y nombres del juez validador. Dr/ Mg: Mg. Víctor Jimenez Flores **DNI:** 71203062

Especialidad del validador: Mag. En administración y dirección de empresas e Ing. De sistemas

05 de mayo del 2022

[1]**Pertinencia**: El ítem corresponde al concepto teórico formulado.
[2]**Relevancia**: El ítem es apropiado para representar al componente o dimensión específica del constructo
[3]**Claridad**: Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

Firma del Experto Informante.

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO QUE MIDE LA VARIABLE NORMA TÉCNICA PERUANA 27001:2014 ISO-IEC

N.º	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	DIMENSIÓN 1 CONFIDENCIALIDAD	Si	No	Si	No	Si	No	
1	¿Cree usted que para garantizar la seguridad de los datos es requerida la confidencialidad en el control de accesos?	✓		✓		✓		
2	¿Usted cree que la confidencialidad debe ser tomada en cuenta como uno de los pilares en la seguridad de los datos?	✓		✓		✓		
3	¿Usted considera que la autorización debe ser de carácter confidencial?	✓		✓		✓		
4	¿Considera que la autorización es una exigencia necesaria para poder acceder a los datos?	✓		✓		✓		
	DIMENSIÓN 2 INTEGRIDAD	Si	No	Si	No	Si	No	
5	¿Usted considera que la integridad es una parte esencial para la seguridad de las comunicaciones?	✓		✓		✓		
6	¿Considera que para la seguridad de las comunicaciones la integridad es de carácter relevante en la seguridad de los datos?	✓		✓		✓		
7	¿Cree usted que la integridad precisa de la seguridad de los procedimientos, los cuales serían de consideración significativa para la seguridad de los datos?	✓		✓		✓		
8	¿Es correcto que los procesos deban tener un adecuado manejo para así garantizar la integridad en la seguridad de los datos?	✓		✓		✓		
	DIMENSIÓN 3 DISPONIBILIDAD	Si	No	Si	No	Si	No	
9	¿Cree usted que contar con el acceso a la información en el momento solicitado es a consecuencia de la disponibilidad de los datos seguros?	✓		✓		✓		
10	¿Cree usted que contar con el acceso a la información en el momento solicitado se debe considerar como elemento primordial a la disponibilidad?	✓		✓		✓		
11	¿Considera que para garantizar la fidelidad de los datos la disponibilidad debe tomar en consideración el acceso a los datos?	✓		✓		✓		
12	¿Se debe considerar como elemento primordial a la disponibilidad para así garantizar el acceso a los datos?	✓		✓		✓		

Observaciones (precisar si hay suficiencia): La suficiencia es pertinente para aplicar a la población.

Opinión de aplicabilidad: **Aplicable [✓]** **Aplicable después de corregir [ ]** **No aplicable [ ]**

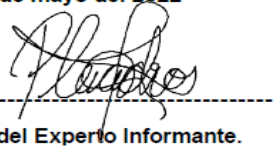
Apellidos y nombres del juez validador. Dr/ Mg: Mg. Patrick José Cuadros Quiroga **DNI: 41827083**

Especialidad del validador: Magister en Administración de Empresas (MBA)

[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.
[2]**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo
[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

05 de mayo del 2022



Firma del Experto Informante.

CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE LA VARIABLE SEGURIDAD EN SISTEMAS DE INFORMACIÓN

N°	DIMENSIONES / Ítems	Pertinencia		Relevancia		Claridad		Sugerencias
	DIMENSION 1 ELEMENTOS TANGIBLES	Si	No	Si	No	Si	No	
1	¿Considera que los equipos informáticos (computadoras, laptops y otros periféricos) utilizados actualmente son adecuadamente para la infraestructura de la seguridad en sistemas de información?	✓		✓		✓		
2	¿Considera que los equipos informáticos (computadoras, laptops y otros periféricos) utilizados actualmente son adecuadamente para la infraestructura de la seguridad en sistemas de información?	✓		✓		✓		
3	¿Considera que los equipos de almacenamiento de información (backup) son un factor relevante para mantener la seguridad en sistemas de información?	✓		✓		✓		
4	¿Considera que debe existir un plan de copias de seguridad semanal y mensual de los datos para tener una adecuada seguridad en sistemas de información?	✓		✓		✓		
5	¿Considera que la infraestructura (ordenadores, internet, equipos de red) son los adecuados o cumplen los requisitos mínimos (condiciones generales) para permitir mantener la seguridad en sistemas de información?	✓		✓		✓		
6	¿Considera que la infraestructura (ordenadores, internet, equipos de red) deben ser renovados cada dos años y cumplan con los requisitos recomendados o mínimos (condiciones generales) al comprar de nuevos ordenadores, equipos de red y actualización del plan de internet para mejorar la seguridad en sistemas de información?	✓		✓		✓		
	DIMENSION 2 FIABILIDAD							
7	¿Considera usted que el compromiso por parte de los trabajadores de la Sub Gerencia de TIC debe ser considerado un factor fundamental para el logro de la seguridad en sistemas de información?	✓		✓		✓		
8	¿Considera usted que los trabajadores deben que manejan información importante por medio de los sistemas deben firmar un documento de compromiso de no divulgación de información confidencial para una eficiente seguridad en sistemas de información?	✓		✓		✓		
9	¿Considera que la seguridad en sistemas de información debe cumplir con el servicio prometido (acceso a la información y acceso a los sistemas)?	✓		✓		✓		
10	¿El servicio prometido (acceso a los sistemas y acceso a internet) influye de tal manera que permita alcanzar la seguridad en sistemas de información?	✓		✓		✓		
	DIMENSION 3 CAPACIDAD DE RESPUESTA							
11	¿Considera que el tiempo de repuesta al solicitar algún tipo de información depende de la seguridad en sistemas de información?	✓		✓		✓		
12	¿Considera que cuan menor sea el tiempo de respuesta influye positivamente la seguridad en sistemas de información?	✓		✓		✓		
13	¿Consideraría que la seguridad en sistemas de información requiere de actualizaciones según la necesidad que requieran los trabajadores así poder permitir tener una mejora continua?	✓		✓		✓		
14	¿Considera que por medio de la mejora continua de la seguridad en sistemas de información favorece en gran medida capacidad de respuesta que se le brinda al usuario (poblador) cuando requiera información?	✓		✓		✓		

Observaciones (precisar si hay suficiencia): Es pertinente y suficiente para aplicar a la población.

Opinión de aplicabilidad: **Aplicable [✓]** **Aplicable después de corregir [ ]** **No aplicable [ ]**

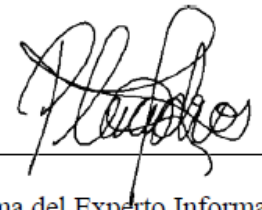
Apellidos y nombres del juez validador. Dr/ Mg: Mg. Patrick José Cuadros Quiroga **DNI: 41827083**

Especialidad del validador: Magister en Administración de Empresas (MBA)

05 de mayo del 2022

Pertinencia: El ítem corresponde al concepto teórico formulado.
Relevancia: El ítem es apropiado para representar al componente o dimensión específica del constructor.
Claridad: Se entiende sin dificultad alguna el enunciado del ítem es conciso, exacto y directo.

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión.



Firma del Experto Informante.