UNIVERSIDAD NACIONAL DEL ALTIPLANO

FACULTAD DE INGENIERÍA MECÁNICA ELÉCTRICA, ELECTRÓNICA Y SISTEMAS

ESCUELA PROFESIONAL DE INGENIERIA DE SISTEMAS

NORMA ISO 27001 Y EL CONTROL DE LA SEGURIDAD DE INFORMACIÓN EN BOTICAS DE LA CIUDAD DE JULIACA AÑO 2023.

TESIS

PRESENTADA POR:

CESAR ADRIAN ALAYZA TAPIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO DE SISTEMAS

PUNO – PERÚ

2024

Reporte de similitud

NOMBRE DEL TRABAJO	AUTOR
NORAMA ISO 27001 Y EL CONTROL DE L A SEGURIDAD DE INFORMACION EN BO TICAS DE LA CIUDDAD DE JULIACA AÑO	CESAR ADRIAN ALAYZA TAPIA

RECUENTO DE PALABRAS	RECUENTO DE CARACTERES
11840 Words	64717 Characters
RECUENTO DE PÁGINAS	**TAMAÑO DEL ARCHIVO**
74 Pages	2.1MB
FECHA DE ENTREGA	**FECHA DEL INFORME**
Jan 25, 2024 10:10 AM GMT-5	Jan 25, 2024 10:11 AM GMT-5

20% de similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para cada base c

- 17% Base de datos de Internet
- 1% Base de datos de publicaciones
- Base de datos de Crossref
- Base de datos de contenido publicado de Crossr
- 12% Base de datos de trabajos entregados

Excluir del Reporte de Similitud

- Material bibliográfico
- Material citado
- Material citado
- Coincidencia baja (menos de 12 palabras)
- Bloques de texto excluidos manualmente

Fabiola Nuturo Romero Flores
CPD 2061028

Dr. Ing. Henry Ivan Corkori Alejo
CIP: 56664

Resumen

DEDICATORIA

Este trabajo va dedicado primeramente a DIOS con mucho cariño, a mis padres, mi pareja, mi hija y familiares los cuales me brindaron un apoyo moral, y por sobre todas las cosas cariño para continuar con el transcurso de mi carrera profesional, por los consejos que siempre me dan, gracias a ello sigo adelante a pesar de que haya muchos obstáculos, Seguidamente, a mis docentes, Quienes me ha inculcado conocimiento y sus buenas experiencias y me han sabido guiar en el transcurso de la ejecución de mi proyecto, tanto como en la vida.

Cesar Adrian Alayza Tapia

ÍNDICE GENERAL

Pág.

CAPÍTULO IV35

RESULTADOS Y DISCUSIÓN

Línea: Desarrollo, gestión, seguridad y auditoría de sistemas de información.

Tema: Seguridad de información.

Puno, 26 de enero de 2024

ÍNDICE DE FIGURAS

Pág.

ÍNDICE DE TABLAS

Pág.

ACRONIMOS

SI:	Seguridad de la información.
ISO:	International Organization for standardization.
CSI:	Control de seguridad de la información.

RESUMEN

Su objetivo fue determinar la relación significativa entre la Norma ISO 27001 y control de la seguridad de información en boticas de la ciudad de Juliaca año 2023. La metodología fue de enfoque cuantitativo, tipo básica, nivel descriptivo correlacional diseño no experimental, la muestra estuvo conformada por 15 boticas de la ciudad de Juliaca, se utilizó como técnica la observación e instrumento el cuestionario. Muestra como resultados según el coeficiente es de 0.789, lo que indica una correlación positiva alta además en un valor de p es de 0.001 es menor a 0.05, en cuanto a las dimensiones ejecución y adaptabilidad tiene un coeficiente de 0.957, lo que indica una correlación positiva muy alta además el valor de p es de 0.000 es menor a 0.05, y las dimensiones de verificación y accesibilidad muestran un coeficiente de 0.839, lo que indica una correlación positiva alta tiene un valor de p de 0.000 es menor a 0.05, las dimensiones de mejoramiento y resguardo su coeficiente es de 0.884, lo que indica una relación positiva alta, el valor de p es de 0.000 es menor a 0.05. Se **concluye** que si existe relación positiva moderada entre las variables de Norma ISO 27001 y control de la seguridad de información porque se observa un coeficiente de correlación de 0.460, presenta una correlación positiva moderada, porque valor de p es 0.004 menor a 0.05, se deduce que si mejora la variable ISO también se mejora la seguridad de información.

Palabras clave: Boticas, Control, ISO 270001, Normas, Seguridad de información.

ABSTRACT

Its objective was to determine the significant relationship between the ISO 27001 Standard and control of information security in pharmacies in the city of Juliaca in 2023. The methodology was a quantitative approach, basic type, correlational descriptive level, non-experimental design, the sample was made up for 15 pharmacies in the city of Juliaca, observation was used as a technique and the questionnaire was used as an instrument. It shows as results according to the coefficient is 0.789, which indicates a high positive compensation. Furthermore, the p value is 0.001 and is less than 0.05. Regarding the dimensions execution and adaptability, it has a coefficient of 0.957, which indicates a positive compensation. very high, in addition, the p value is 0.000 is less than 0.05, and the dimensions of verification and accessibility show a coefficient of 0.839, which indicates a high positive correlation. It has a p value of 0.000 is less than 0.05, the dimensions of improvement and protection its coefficient is 0.884, which indicates a high positive relationship, the p value is 0.000 and less than 0.05. It is concluded that if there is a moderate positive relationship between the variables of ISO 27001 Standard and information security control because a correlation coefficient of 0.460 is observed, it presents a moderate positive correlation, because p value is 0.004 less than 0.05, it is It deduces that if the ISO variable improves, information security is also improved.

Keywords: Pharmacies, Control, ISO 27001, Standards, Information security.

CAPÍTULO I

INTRODUCCIÓN

Mencionan algunos autores como Kalambkar (2021) la seguridad de la información se ha convertido en un elemento crítico en el entorno empresarial y tecnológico actual. Con la creciente dependencia de las organizaciones en la tecnología y la gestión de datos, garantizar la confidencialidad, integridad y disponibilidad de la información se ha vuelto esencial. En este contexto, la norma ISO 27001 y el control de seguridad emergen como herramientas fundamentales para establecer un marco sólido de gestión de la seguridad de la información.

Por otro lado, también menciona alemán (2023) la norma ISO 27001 es un estándar internacionalmente reconocido que proporciona un enfoque integral para la gestión de la seguridad de la información en organizaciones de todos los tamaños y sectores. Esta norma establece los requisitos necesarios para establecer, implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI) efectivo.

De igual manera Steve (2019) el control de seguridad abarca una amplia variedad de medidas y prácticas diseñadas para proteger los activos de información de una organización contra amenazas internas y externas. Estos controles pueden incluir políticas, procedimientos, tecnologías y prácticas de gestión que buscan garantizar que la información se mantenga segura y confidencial.

También, menciona Camposano (2020) su importancia, alcance y beneficios para las organizaciones que buscan proteger su información y cumplir con las regulaciones y estándares internacionales. A medida que avanzamos, descubriremos

cómo estas herramientas contribuyen a la construcción de un entorno empresarial más seguro y confiable en la era digital.

Dice Pinto (2021) también es una gran preocupación para las empresas. Es esencial reconocer el valor de la seguridad de la información y proponer medidas seguras, los procedimientos y los controles adecuados para que una institución sobreviva y prospere. Es fundamental preocuparse por la información en la seguridad ya que una parte importante de la cadena de valor y procesos que producen información operativas y funcionales de una institución está enfocada específicamente. Es fundamental contar con procedimientos adecuados de respaldo de información y planes de recuperación ante desastres. Esto garantizará que, en caso de un incidente o pérdida de datos, sea posible restaurar la información crítica de manera oportuna.

Ticona (2021) la seguridad de la Información es la disciplina que busca evitar amenazas a la privacidad. Por medio de la implementación de políticas, procedimientos y controles se busca garantizar la confidencialidad y disponibilidad en el manejo de la información. los documentos físicos que tiene la empresa, o los riesgos a los cuales se podría enfrentar uno de los activos más importantes, sus empleados, también llamados el recurso humano.

1.1. DESCRIPCIÓN DEL PROBLEMA

Se plantea una serie de problemas y riesgos significativos para estas instituciones. A continuación, se describen algunos de los problemas clave asociados con la falta de control de seguridad en boticas en relación con la norma ISO 27001 así como varios factores, uno de ellos es vulnerabilidad de datos de pacientes, las boticas manejan información confidencial de los pacientes, como historiales médicos, recetas y datos personales. La falta de control de seguridad puede resultar en la exposición no

autorizada de estos datos, lo que podría tener graves implicaciones para la privacidad de los pacientes. La integridad de la Información, es esencial en el sector de la salud podría permitir la manipulación no autorizada de registros médicos o la dispensación incorrecta de medicamentos, lo que pone en peligro la salud de los pacientes y sobre todo esto aqueja al. Cumplimiento Normativo, la industria farmacéutica está sujeta a regulaciones estrictas, y las boticas deben cumplir con normativas de privacidad y seguridad de datos. La falta de controles de seguridad puede resultar en incumplimientos normativos y posibles sanciones legales. Y por ende se vendría la pérdida de confianza del cliente en una botica, la divulgación de incidentes de seguridad o la mala gestión de datos pueden hacer que los pacientes busquen servicios en otro lugar es por ello que motiva a la investigación.

1.1.1. Problema general

¿Cuál será la relación significativa entre la Norma ISO 27001 y control de la seguridad de información en boticas de la ciudad de Juliaca año 2023?

1.1.2. Problemas específicos

¿Cuál será la relación significativa entre las dimensiones de Planificación y disponibilidad en boticas de la ciudad de Juliaca año 2023?

¿Cuál será la relación significativa entre las dimensiones de Ejecución y adaptabilidad en boticas de la ciudad de Juliaca año 2023?

¿Cuál será la relación significativa entre las dimensiones de Verificación y accesibilidad en boticas de la ciudad de Juliaca año 2023?

¿Cuál será la relación significativa entre las dimensiones de Mejoramiento y resguardo en boticas de la ciudad de Juliaca año 2023?

1.2. HIPÓTESIS DE LA INVESTIGACIÓN

Ha= Existe relación positiva significativa entre las variables de la Norma ISO 27001 y control de la seguridad de información en boticas de la ciudad de Juliaca año 2023.

Ho= No existe relación positiva significativa entre las variables de la Norma ISO 27001 y control de la seguridad de información en boticas de la ciudad de Juliaca año 2023.

1.3. OBJETIVOS DE LA INVESTIGACIÓN

1.3.1. Objetivo general.

Determinar la relación significativa entre la Norma ISO 27001 y control de la seguridad de información en boticas de la ciudad de Juliaca año 2023.

1.3.2. Objetivos específicos.

Determinar la relación significativa entre las dimensiones de Planificación y disponibilidad en boticas de la ciudad de Juliaca año 2023.

Determinar la relación significativa entre las dimensiones de Ejecución y adaptabilidad en boticas de la ciudad de Juliaca año 2023.

Determinar la relación significativa entre las dimensiones de Verificación y accesibilidad en boticas de la ciudad de Juliaca año 2023.

Determinar la relación significativa entre las dimensiones de Mejoramiento y resguardo en boticas de la ciudad de Juliaca año 2023.

CAPÍTULO II

REVISION DE LA LITERATURA

2.1. ANTECEDENTES DE LA INVESTIGACIÓN

2.1.1. Internacional

Rodríguez (2020) el objetivo de la investigación fue evaluar cómo la implementación de la norma ISO 27001 afectó la seguridad de los datos de una empresa privada de Lima, Perú. Como metodología se utilizó un estudio pre - experimental para determinar el impacto de la aplicación de la ISO 27001. Esto se realizó luego de aplicar una metodología cuantitativa. Muestra los resultados que entre otras cosas hay la necesidad de gestionar información crucial que puede ser fundamental para los intereses estratégicos de las empresas. La conclusión cuantitativa indica que el uso de la ISO tiene un impacto en la seguridad de la información, incluyendo la confidencialidad y la disponibilidad.

Pinto (2021) el objetivo del proyecto es desarrollar un sistema de gestión de seguridad de la información que cumpla con los estándares ISO/IEC 27001:2013. La metodología de riesgos, el inventario de actividades, la identificación y vulnerabilidades, la evaluación de riesgos, el establecimiento de controles está establecidos en el diseño del sistema. Los resultados muestran asegurar la confidencialidad, integridad y accesibilidad de la información y alienta a las organizaciones, asegurando la continuidad del negocio de las buenas prácticas descritas en la norma ISO 27001 complementan la gestión de la seguridad de la información. Se concluye que el sistema de gestión diseñado se transforma en una herramienta para elevar el nivel de madurez ayudando a la

organización a reducir los riesgos que está expuesta y sirviendo como piedra angular para establecer una cultura de seguridad de la información.

Camposano (2020) el objetivo fue establecer y mantener un ambiente cómodo, animado y organizado que permita a las personas preservar sus actividades relacionadas con la información. Metodología Cuantitativa de la Investigación. Investigación exploratoria. técnicas para la investigación. Instrumento. 1.1 Población y exhibición Se decidió reunir a todo el personal porque la organización es muy pequeña. Muestran como resultado que es fundamental el uso de la ISO 27001, las personas activas y pasivas utilizando herramientas comerciales y de comunicación que incluyen sublíneas, redes y tecnologías de software y hardware inteligente. potenciales después de los servidores, lugares de trabajo, dispositivos móviles, etc. Se concluye que la relevancia de la auditoría de la información Los sistemas de información son particularmente vulnerables a los ataques de usuarios malintencionados.

Mera (2022) la investigación se hizo una evaluación de la seguridad de la información de la empresa utilizando la norma ISO/IEC 27001 como guía. La metodología para ello, se clasificaron las actividades disponibles de la empresa y se agruparon en cuatro categorías: actividades relacionadas con la información, talento humano, hardware y sistemas relacionados con la información. Como resultado se calculó el riesgo y priorizar las actividades requeridas para el remedio, se examinaron las amenazas y vulnerabilidades que estas actividades podrían encontrar. Se concluye que se eligieron ciertos controles enumerados y se examinó su cumplimiento para establecer recomendaciones sobre cómo mejorar la seguridad dentro de la empresa más adelante.

2.1.2. Nacional

Alemán (2023) el objetivo del presente estudio, que buscó determinar cuánto afectó la implementación de la norma ISO 27001:2013 al control de la seguridad de la información en una determinada organización. La metodología fue enfoque cuantitativo diseño experimental luego, utilizando como guía mediciones con las dimensiones definidas de la variable dependiente, se realizó un análisis de resultados. Esto fue aprobado por el juicio de tres expertos. Teniendo en cuenta una prueba de distribución no normal no paramétrica, los resultados de la prueba posterior fueron menos significativos que los resultados de la prueba previa en un nivel de significación de 0,5, se concluye la norma ISO 27001:2013 mejorará la seguridad de la información en las empresas de consultoría privadas.

Villamar (2021) el objetivo fue determinar la seguridad de la información un gran interés en el campo de las tecnologías de la información. La metodología fue el enfoque de este estudio se amplió para incluir, que dice: "Comunicación y negocios y emprendimientos tecnológicos, de la misma manera, muchos temas relacionados con la seguridad de la información y la ISO 27001 necesitaban ser fortalecidos en este estudio. aun cuando el uso de las computadoras ha sido cada día más fácil. Muestran los resultados que la gestión de la información, y cómo se relacionan con la minimización de impactos en la norma ISO 27001 porque siempre es importante tratarlos para evitar y evitar tener que lamentarse. la pérdida total de datos. Se concluye que todos ellos eran ingenieros de sistemas en la ciudad de Babahoyo. Su experiencia fue invaluable para lograr el análisis adecuado necesario para este proyecto final.

Gonzales (2019) tiene como objetivo determinar cómo la implementación de la NTP/ISO 27001. La investigación tuvo como metodología de tipo aplicada porque busca abordar el tema planteado; su nivel es explicativo porque busca establecer la relación entre causa y efecto de la solución del problema, y su diseño es preexperimental. La población utilizada para el estudio estuvo formada por todos los miembros del departamento de telemática, y el método de demostración utilizado fue el muestreo aleatorio probabilístico básico se utilizó la Norma Técnica Peruana ISO 27001:2014. como resultados fue implementar las normas después del principal hallazgo de la investigación mejoro el procedimiento de seguridad de la información. Se concluye que la implementación de NTP/ISO 27001 mejoró significativamente el proceso de seguridad de la información en la división de telemática de la oficina económica nacional.

Benites (2019) el proyecto tiene como objetivo crear un SGSI para una organización privada. La metodología utilizada para la investigación, incluyendo las estrategias de hipótesis y la recolección y análisis estadístico para la propuesta del SGSI, muestra los resultados que, desde el análisis final del panorama político, discutirá los tiempos, presupuestos y personas responsables de llevar a cabo el desarrollo de este proyecto, se incluirán todas las conclusiones, referencias bibliográficas y anexos utilizados en el desarrollo de este proyecto.

Ticona (2021) el objetivo del presente estudio es conocer en qué medida el uso de la ISO 27001 afecta la seguridad de la información de la empresa ICO en 2021. La metodología que se utilizó un enfoque cuantitativo. El objetivo del presente estudio se logró mediante un diseño experimental del tipo

preexperimental, se utilizaron 18 personas. Se aplicó un pretest y un postest a las unidades de estudio de la muestra escogida, utilizándose un enquistar como herramienta y un cuestionario como técnica de recolección de datos. Los resultados al evaluar cada una de sus diversas dimensiones, los administradores de sistemas de planificación proporcionaron información sobre la variable dependiente ISO 27001. Sin embargo, la presente investigación. Se concluye que el uso de la ISO 27001 no afecta significativamente la mejoro la seguridad de la información en los sistemas ERP.

Chávez (2021) el objetivo declarado del proyecto de investigación fue determinar cómo el proceso de auditoría ISO 27001 mejoraría los controles de seguridad de la información en el Distrito Municipal de San Juan Bautista en 2018. La metodología no fue experimental porque no hubo manipulación de variables. En el 2018, 39 empleados de la OIT del Distrito Municipal San Juan Bautista conformaron la población, demostrando un 100% de conformidad. La selección de la muestra para cada enfoque se realizó de manera intencional y no aleatoria. La encuesta fue el método utilizado para recolectar los datos, junto con el análisis de documentos y el acto de evaluación como instrumentos. Los resultados fueron: el nivel de significancia de p =.001 indica que p es menor a 0,05, indicando que la relación es significativa. Se concluye que existe una relación significativa entre el proceso de auditoría y los controles mejorados de seguridad de la información.

Chávarry (2021) La investigación tuvo como objetivo conocer el impacto de la implementación de las normas modificadas para la seguridad de la información en la Dirección de la Policía Peruana. La metodología debido a que se realizarán estudios con dos grupos, el primer grupo en pre y post test, el tipo

de investigación que se utilizará será algo experimental. Los resultados el tema central de la investigación fue cómo la implementación por parte del Secretariado Ejecutivo de la PNP de las normas ISO 27001 y 27002 adaptadas a la seguridad de la información afecta la seguridad de la información en la Unidad Policial.

2.2. MARCO TEÓRICO

2.2.1. Definición de la ISO 27001

Según **Steve (2019)** la norma ISO 27001 es un estándar internacional que establece los requisitos para un sistema de gestión de seguridad de la información (SGSI). Fue desarrollada por la Organización Internacional de Normalización (ISO) y se utiliza en todo el mundo como referencia para establecer, implementar, mantener y mejorar la seguridad de la información en una organización.

Por otro lado, menciona **Kalambkar (2021)** se enfoca en la gestión de la seguridad de la información, lo que implica la protección de la confidencialidad, la integridad y la disponibilidad de la información dentro de una organización. El estándar proporciona un marco de trabajo que ayuda a las organizaciones a identificar y gestionar los riesgos de seguridad de la información, y a establecer controles y medidas para mitigar esos riesgos. Además, promueve un enfoque basado en procesos para la seguridad de la información, lo que significa que las organizaciones deben planificar, implementar, controlar y mejorar continuamente sus prácticas de seguridad de manera sistemática.

La ISO 27001 es aplicable a organizaciones de cualquier tamaño y en diversos sectores, y su adopción ayuda a las empresas a demostrar su

compromiso con la seguridad de la información ante clientes, socios comerciales y reguladores. Además, puede ser utilizada como base para la certificación por parte de organismos de certificación independientes, lo que confirma que una organización cumple con los requisitos de seguridad de la información establecidos en la norma.

2.2.2. Importancia de la ISO 27001

Menciona Adidas (2019) dice que la protección de la información: La ISO 27001 proporciona un marco sólido para proteger la información sensible y crítica de una organización. Esto incluye datos de clientes, propiedad intelectual, información financiera y cualquier otro tipo de información que sea valiosa y confidencial.

También menciona **Aleman (2023)** cumplimiento legal y regulatorio: Cumplir con la ISO 27001 ayuda a las organizaciones a cumplir con las leyes y regulaciones relacionadas con la seguridad de la información, como el Reglamento General de Protección de Datos (GDPR) de la Unión Europea, la Ley de Privacidad del Consumidor de California (CCPA) y muchas otras normativas locales e internacionales.

Gestión de riesgos: La ISO 27001 se centra en la identificación y gestión de riesgos de seguridad de la información. Ayuda a las organizaciones a evaluar las amenazas y vulnerabilidades y a implementar controles adecuados para mitigar los riesgos **Aleman (2023)**

Estándar internacional: La ISO 27001 es un estándar globalmente reconocido y aceptado. Esto facilita la colaboración y el comercio internacional

al establecer un lenguaje común para la seguridad de la información **Aleman (2023)**

2.2.3. Dimensiones de las ISO 27001

Según Cazurro (2022) es un estándar internacional para la gestión de la seguridad de la información. Define un conjunto de requisitos y mejores prácticas para establecer, implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI) en una organización. La norma no especifica dimensiones físicas, como tamaño o longitud, sino que se centra en aspectos relacionados con la gestión de la seguridad de la información.

2.2.3.1. Planificación

La planificación es una parte fundamental de la norma ISO 27001. Esto implica identificar los riesgos de seguridad de la información, establecer objetivos de seguridad, desarrollar políticas y procedimientos, asignar roles y responsabilidades, y definir un alcance para el SGSI. La planificación es esencial para determinar cómo la organización abordará la seguridad de la información.

2.2.3.2. Ejecución

Una vez que se ha realizado la planificación, se procede a la ejecución de las medidas y controles de seguridad definidos en el SGSI. Esto incluye la implementación de políticas, procedimientos y controles de seguridad, así como la capacitación del personal y la asignación de recursos necesarios.

2.3.3.3. Verificación

La verificación implica evaluar si las medidas de seguridad implementadas están funcionando de manera efectiva. Esto implica la realización de auditorías internas y revisiones periódicas para asegurarse de que el SGSI esté cumpliendo con los requisitos de la norma y que se estén gestionando los riesgos de seguridad de la información de manera adecuada.

2.2.3.4. Mejoramiento

La mejora continua es un principio clave de la norma ISO 27001. Esto implica tomar medidas correctivas y preventivas para abordar cualquier no conformidad o incidente de seguridad de la información que se identifique durante la verificación. También se busca mejorar constantemente el SGSI y las prácticas de seguridad en la organización.

2.2.4. Definición de control de seguridad de información

Dice Villalón (2020) se refiere a un conjunto de prácticas, políticas, procedimientos y medidas diseñadas para proteger la confidencialidad, integridad y disponibilidad de la información en una organización. Su objetivo principal es garantizar que la información crítica y sensible esté resguardada de amenazas y riesgos, tanto internos como externos, que puedan comprometerla de alguna manera.

implica la implementación de medidas técnicas, administrativas y físicas para mitigar riesgos y amenazas, y asegurar que la información esté protegida de

acuerdo con los estándares y regulaciones pertinentes. Algunos de los aspectos clave que aborda el Control de Seguridad de la Información incluyen:

Confidencialidad: Garantizar que la información solo esté disponible para personas autorizadas y que no se divulgue a individuos no autorizados.

Integridad: Asegurar que la información no se altere de manera no autorizada y que se mantenga precisa y completa.

Disponibilidad: Asegurar que la información esté disponible cuando sea necesaria y que no esté sujeta a interrupciones o ataques que la hagan inaccesible.

Autenticación: Verificar la identidad de los usuarios y dispositivos que acceden a la información, asegurando que solo las personas autorizadas puedan hacerlo.

Autorización: Definir y controlar los niveles de acceso de los usuarios a la información, garantizando que solo tengan acceso a los datos necesarios para llevar a cabo sus funciones.

Auditoría y monitoreo: Establecer mecanismos para registrar y supervisar las actividades relacionadas con la información, con el fin de detectar y responder a posibles incidentes de seguridad.

Gestión de riesgos: Evaluar y gestionar de manera continua los riesgos relacionados con la seguridad de la información y tomar medidas para mitigarlos.

2.2.5. Clases de control de seguridad de información

Para Villalón (2020) para lograr esto, se utilizan diversas clases de controles de seguridad de información. Estos controles se agrupan comúnmente en tres categorías principales: controles técnicos, controles administrativos y controles físicos. Aquí hay una descripción general de cada clase de control de seguridad de información:

Controles Técnicos:

Control de Acceso: Se refiere a la gestión de quién tiene acceso a los sistemas y los datos. Esto incluye autenticación, autorización, controles de contraseñas, sistemas de registro y seguimiento de actividad.

Cifrado: La información sensible se cifra para que sea ilegible para personas no autorizadas. Esto se aplica tanto a datos en reposo como en tránsito.

Firewalls y Seguridad de Red: Se utilizan para proteger la red y los sistemas de amenazas externas. Esto incluye cortafuegos, detección de intrusiones, filtrado de contenido y prevención de malware.

Seguridad de Aplicaciones: Se refiere a la seguridad de las aplicaciones y sistemas de software, incluyendo pruebas de penetración, parches de seguridad y desarrollo seguro de software.

Detección y Respuesta a Incidentes: Implementación de sistemas y procedimientos para detectar y responder a incidentes de seguridad.

Controles Administrativos:

Políticas y Procedimientos: Establecimiento de políticas y procedimientos de seguridad, así como la educación y concienciación de los empleados sobre las mejores prácticas de seguridad.

Gestión de Riesgos: Identificación y evaluación de riesgos, seguido de la implementación de medidas para mitigar esos riesgos.

Gestión de Identidad y Acceso: Administración centralizada de cuentas de usuario y derechos de acceso.

Capacitación y Concienciación: Entrenar a los empleados para que sean conscientes de las amenazas de seguridad y sepan cómo responder ante ellas.

Gestión de Incidentes: Procedimientos para gestionar y responder a incidentes de seguridad cuando ocurren.

Controles Físicos:

Seguridad Física: Protección de las instalaciones físicas que albergan sistemas de información, incluyendo cámaras de seguridad, sistemas de control de acceso y seguridad en la infraestructura de TI.

Protección de Datos Físicos: Almacenamiento seguro de medios de respaldo y dispositivos de almacenamiento físico, como discos duros y cintas.

Gestión de Hardware y Software: Control de acceso y mantenimiento de equipos de TI y software.

2.2.6. Dimensiones del control de seguridad de información

Ladrón (2020) las dimensiones que mencionaste son importantes aspectos a considerar en este contexto, pero es importante aclarar que estas

dimensiones suelen estar asociadas más específicamente a la gestión de la seguridad de la información. Aquí tienes una breve descripción de cada una de las dimensiones:

2.2.6.1. Disponibilidad:

La disponibilidad se refiere a garantizar que los sistemas y recursos de información estén disponibles y funcionando cuando los usuarios los necesiten. Esto implica prevenir y mitigar interrupciones no planificadas, como fallas de hardware, ataques cibernéticos o desastres naturales, para asegurar que los servicios críticos estén disponibles de manera continua.

2.2.6.2. Adaptabilidad (o Resiliencia):

La adaptabilidad o resiliencia se relaciona con la capacidad de los sistemas de información para adaptarse a situaciones cambiantes o enfrentar amenazas y recuperarse rápidamente de eventos disruptivos. Esto incluye la capacidad de planificar y responder eficazmente a incidentes de seguridad y garantizar la continuidad del negocio.

2.2.6.3. Accesibilidad:

La accesibilidad se refiere a garantizar que los usuarios autorizados puedan acceder a los recursos de información de manera segura y eficiente. Esto implica implementar controles de acceso adecuados, autenticación sólida y políticas de acceso que eviten accesos no autorizados o maliciosos.

2.2.6.4. Resguardo (o Salvaguardia)

El resguardo se relaciona con la protección de la información contra amenazas y riesgos, como el acceso no autorizado, la divulgación accidental o malintencionada, y el robo de datos. Esto incluye la implementación de medidas de seguridad tecnológicas y políticas de seguridad para proteger la información confidencial.

CAPÍTULO III

MATERIALES Y MÉTODOS

3.1. ENFOQUE

Fue Cuantitativo es un método de investigación utilizado en diversas disciplinas, como la ciencia, la psicología, la sociología, la economía y muchas otras áreas. Se caracteriza por su énfasis en la recopilación y análisis de datos numéricos y estadísticos para comprender patrones, relaciones y regularidades en fenómenos estudiados Barriento (2021)

3.2. TIPO

Fue básica, porque se determina por el hecho de que surge y permanece dentro de un marco teórico. Su intención es adicionar el conocimiento científico, pero no lo niega desde un punto de vista práctico Hernández (2014).

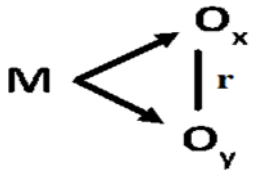
3.3. NIVEL

Fue descriptivo según Quispe (2023) son las mismas que, además de no manipular variables, intentan identificar propiedades y rasgos importantes de cada fenómeno analizado, y en su trabajo de investigación, diseñado nos permitió analizar un instrumento denominado batería de habilidades motoras básicas.

3.4. DISEÑO DE LA INVESTIGACIÓN

La presente investigación fue de diseño no experimental, Correlacional – transversal. La definición de investigación no experimental es "estudios que se llevan a cabo sin la manipulación de variables y en los que los fenómenos se observan los entornos naturales Hernández et al. (2014) p. 152

El siguiente diagrama corresponde a este tipo de diseño:



Dónde:

M: Trabajadores la empresa

OX: Norma ISO 27001

OY: V control de la seguridad de información

r: Relación existentes entre variables.

Transversal porque recolectas datos en un momento único su incidencia e interrelación Hernández (2014)

3.5. TÉCNICAS E INSTRUMENTOS

3.5.1. Técnicas

Según Carrasco (2013) la técnica se refiere al conjunto de principios que orientan las acciones que se van a realizar en la investigación científica". Se utilizará la técnica de la encuesta para recopilar los datos de las variables. Según Carrasco (2013), "la encuesta es un método destacado para la investigación social" (p. 314).

3.5.2. Instrumentos

El instrumento de medida, según Hernández (2014) es la herramienta que utilizara la información o datos sobre las variables que tiene en mente medir" (p. 199). El instrumento que se utilizará será el cuestionario para cada variable con su respectiva dimensión

Se utilizará el instrumento validado mediante juicio de expertos para cada variable y sus respectivas dimensiones ver (Anexo 01)

3.6. POBLACIÓN Y MUESTRA

3.6.1. Población.

Para Hernández (2014) menciona cómo un conjunto de sujetos o individuos que no son inusuales y presentan residencias coincidentes, luego se delimita el contexto a estudiar las consecuencias. (p. 174) la población estará conformado las boticas del distrito de ciudad de Juliaca.

3.6.2. Muestra.

Para Hernández (2014) la muestra de estudio estará conformada por 15 boticas formales que emiten boletas y facturas y están habidos y activos en la SUNAT, todos ellos pertenecerán al distrito de Juliaca, se utilizó el muestreo no probabilístico, donde todas las boticas formales tienen la misma probabilidad de ser testeados al azar ya que todos reúnen las condiciones.

3.7. PROCEDIMIENTO

Se describirán en gráficos y tablas, además se presentaron tablas de contingencia que relacionan las dos variables con sus respectivos gráficos de barras tridimensionales.

Dado que las variables en estudio son de naturaleza ordinal, se utilizó la prueba de correlación de Spearman para contrastar las hipótesis (análisis inferencial). Los resultados finales de las variables y sus dimensiones se describirán en tablas para el análisis descriptivo, además se presentarán tablas de contingencia que relacionarán las dos variables con sus respectivos gráficos de barras tridimensionales. Dado que las variables en estudio son de naturaleza ordinal, se utilizará la prueba de correlación de Spearman para contrastar las hipótesis (análisis inferencial)

3.8. ANÁLISIS DE LOS RESULTADOS

Los resultados se analizaron con el coeficiente de correlación de Spearman. Los datos teóricos se utilizaron para la investigación, se procesaron estadísticamente de manera cuantitativa utilizando tablas y gráficos estadísticos, se tabularon y se usaron a lo largo del estudio para el análisis estadístico según el siguiente cuadro.

Cuadro de coeficiente de correlación

Valor de rho	Significado
- 1	Correlación negativa grande y perfecta
-0.9 a -0.99	Correlación negativa muy alta
-0.7 a -0.89	Correlación negativa alta
-0.4 a -0.69	Correlación negativa moderada
-0.2 a -0.39	correlación negativa baja
-0.01 a -0.19	Correlación muy baja
0.	Correlación nula
+0.01 a +0.19	Correlación positiva muy baja
+0.2 a +0.39	Correlación positiva baja
+0.4 a +0.69	Correlación positiva moderada
+0.7 a +0.89	Correlación positiva alta
+0.9 a +0.99	Correlación positiva alta
1	Correlación positiva grande y perfecta

Fuente. *Hernández (2014) y Batista (2018)*

CAPÍTULO IV

RESULTADOS Y DISCUSIÓN

4.1. RESULTADO

Tabla 1

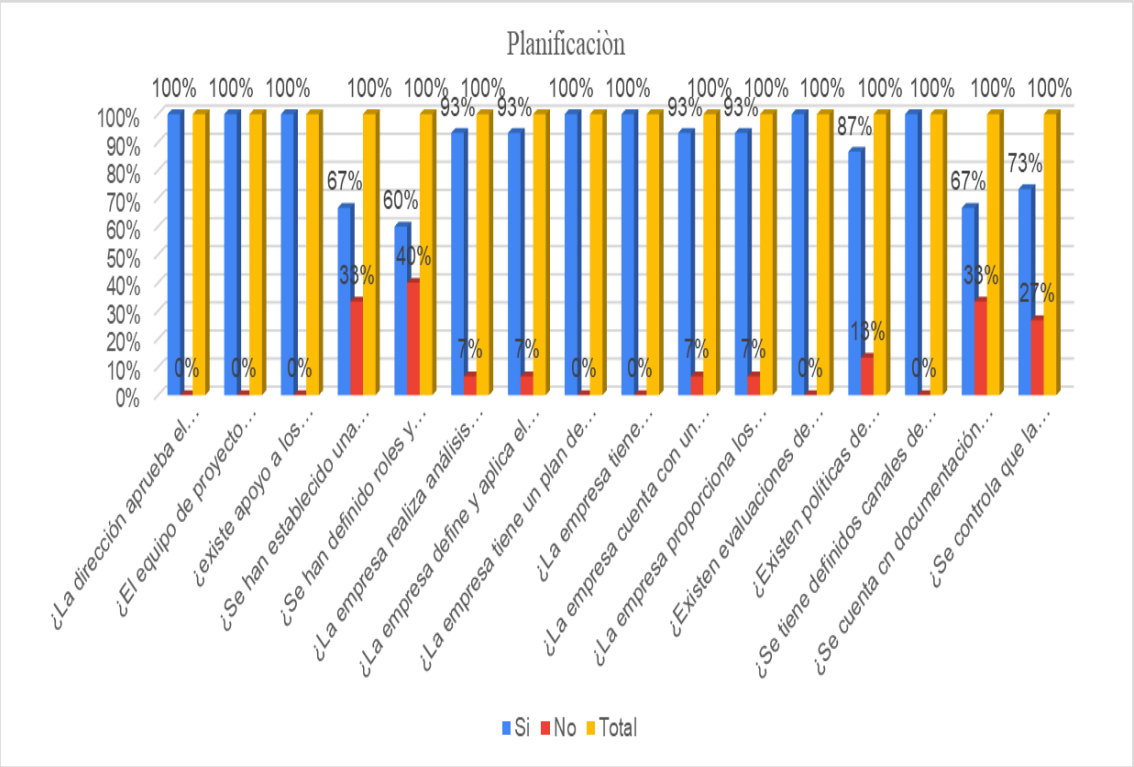
Planificación

Planificación	Si		No		Total	
	fi	%	fi	%	fi	%
¿La dirección aprueba el cumplimiento de los objetivos de la seguridad de la información para la implantación de la ISO 27001?	15	100%	0	0%	15	100%
¿El equipo de proyecto asegura la integración de los requisitos para implementar la ISO 27001 en los procesos de la empresa?	15	100%	0	0%	15	100%
¿existe apoyo a los trabajadores para su contribución efectiva de la ISO 27001?	15	100%	0	0%	15	100%
¿Se han establecido una política de seguridad de información?	10	67%	5	33%	15	100%
¿Se han definido roles y responsabilidades para la seguridad de información?	9	60%	6	40%	15	100%
¿La empresa realiza análisis de riesgo de la seguridad de información?	14	93%	1	7%	15	100%
¿La empresa define y aplica el proceso de valoración?	14	93%	1	7%	15	100%
¿La empresa tiene un plan de tratamiento de riesgos de la seguridad de la información?	15	100%	0	0%	15	100%
¿La empresa tiene documentado los objetivos de la seguridad de la información?	15	100%	0	0%	15	100%
¿La empresa cuenta con un plan de mejora basado en el cumplimiento de objetivos?	14	93%	1	7%	15	100%
¿La empresa proporciona los recursos necesarios para la gestión de la seguridad de información?	14	93%	1	7%	15	100%
¿Existen evaluaciones de desempeño a cerca de la seguridad de información?	15	100%	0	0%	15	100%
¿Existen políticas de Seguridad de Información?	13	87%	2	13%	15	100%
¿Se tiene definidos canales de atención para la seguridad de información?	15	100%	0	0%	15	100%
¿Se cuenta con documentación de la seguridad de información para asegurar la efectividad?	10	67%	5	33%	15	100%
¿Se controla que la información requerida para la gestión de la seguridad está disponible y protegida?	11	73%	4	27%	15	100%

Fuente: *realizado según datos de la encuesta*

Figura 1

Planificación



Interpretación

En la tabla 1 y en la figura 1 de la dimensión Planificación en sus indicadores, el 100% de las personas encuestadas marcaron el Sí en la pregunta ¿La dirección aprueba el cumplimiento de los objetivos de la seguridad de la información para la implantación de la ISO 27001? en boticas de la ciudad de Juliaca año 2023, por otro lado, de las personas encuestadas un 67% de las personas marcaron Sí en la pregunta ¿Se han establecido una política de seguridad de información? Es decir, solo un 67% optaron por el SÍ y el 33% marcaron No; así mismo, solo un 60% de las personas encuestadas marcaron el Sí en la pregunta ¿Se han definido roles y responsabilidades para la seguridad de información? Y un 40% marcaron No en dicha pregunta.

Tabla 2

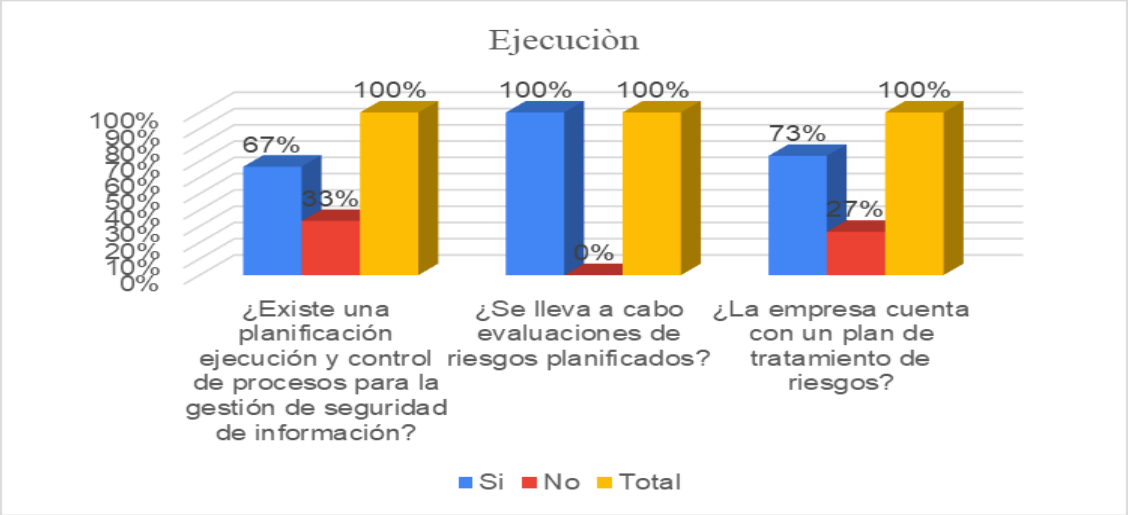
Ejecución

Ejecución	Si		No		Total	
	fi	%	fi	%	fi	%
¿Existe una planificación ejecución y control de procesos para la gestión de seguridad de información?	10	67%	5	33%	15	100%
¿Se lleva a cabo evaluaciones de riesgos planificados?	15	100%	0	0%	15	100%
¿La empresa cuenta con un plan de tratamiento de riesgos?	11	73%	4	27%	15	100%

Fuente: *realizado según datos de la encuesta*

Figura 2

Ejecución



Interpretación

En la tabla 2 y en la figura 2 de la dimensión ejecución en sus indicadores, de un 100% de encuestados solo el 67% de las personas marcaron el Sí en la pregunta ¿Existe una planificación ejecución y control de procesos para la gestión de seguridad de información? en boticas de la ciudad de Juliaca año 2023 y un 33% de las personas encuestadas marcaron No; por otro lado, el 100% de las personas marcaron Sí en la pregunta ¿Se lleva a cabo evaluaciones de riesgos planificados?; así mismo, solo el 73%

marcaron Sí en la pregunta ¿La empresa cuenta con un plan de tratamiento de riesgos?

Y un 27% marcaron por el No.

Tabla 3

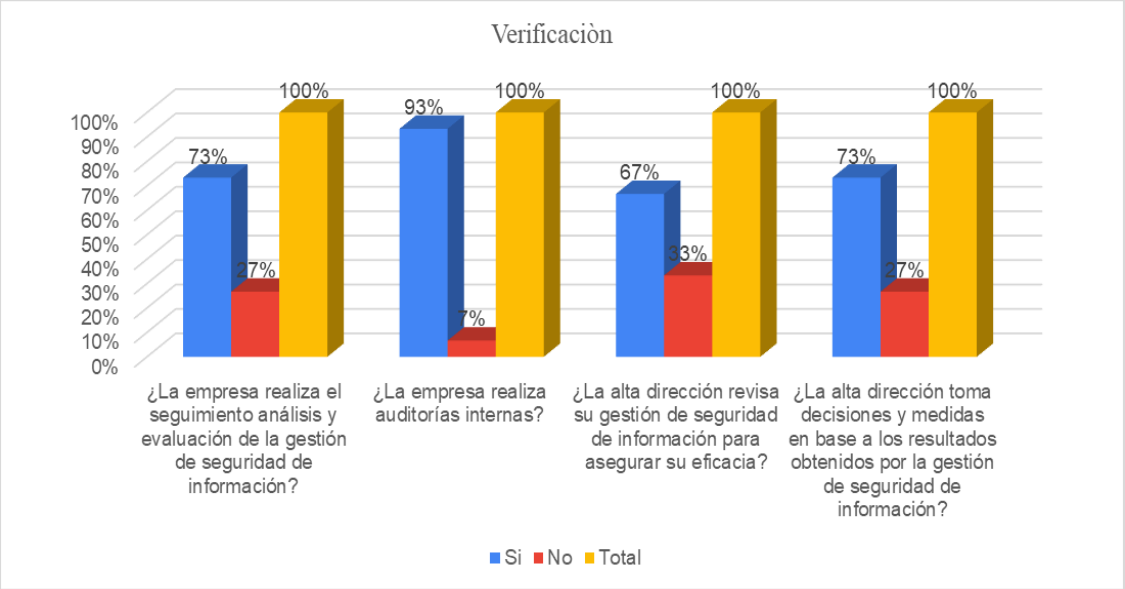
Verificación

Verificación	Si		No		Total	
	fi	%	fi	%	fi	%
¿La empresa realiza el seguimiento análisis y evaluación de la gestión de seguridad de información?	11	73%	4	27%	15	100%
¿La empresa realiza auditorías internas?	14	93%	1	7%	15	100%
¿La alta dirección revisa su gestión de seguridad de información para asegurar su eficacia?	10	67%	5	33%	15	100%
¿La alta dirección toma decisiones y medidas en base a los resultados obtenidos por la gestión de seguridad de información?	11	73%	4	27%	15	100%

Fuente: *realizado según datos de la encuesta*

Figura 3

Verificación



Interpretación

En la tabla 3 y en la figura 3 de la dimensión verificación en sus indicadores, de un 100% solo el 73% de las personas marcaron el Sí en la pregunta ¿La empresa realiza el seguimiento análisis y evaluación de la gestión de seguridad de información? en boticas de la ciudad de Juliaca año 2023 y un 27% de las personas encuestadas marcaron No; por otro lado, 93% de las personas encuestadas marcaron Sí en la pregunta ¿La empresa realiza auditorías internas? Y un 7% marcó No; así mismo, solo un 67% marcaron el Sí en la pregunta ¿La alta dirección revisa su gestión de seguridad de información para asegurar su eficacia? Y un 33% marcaron por el No de la dicha pregunta y por último un 73% de las personas marcaron por el Sí en la pregunta ¿La alta dirección toma decisiones y medidas en base a los resultados obtenidos por la gestión de seguridad de información? Y un 27% marcaron No.

Tabla 4

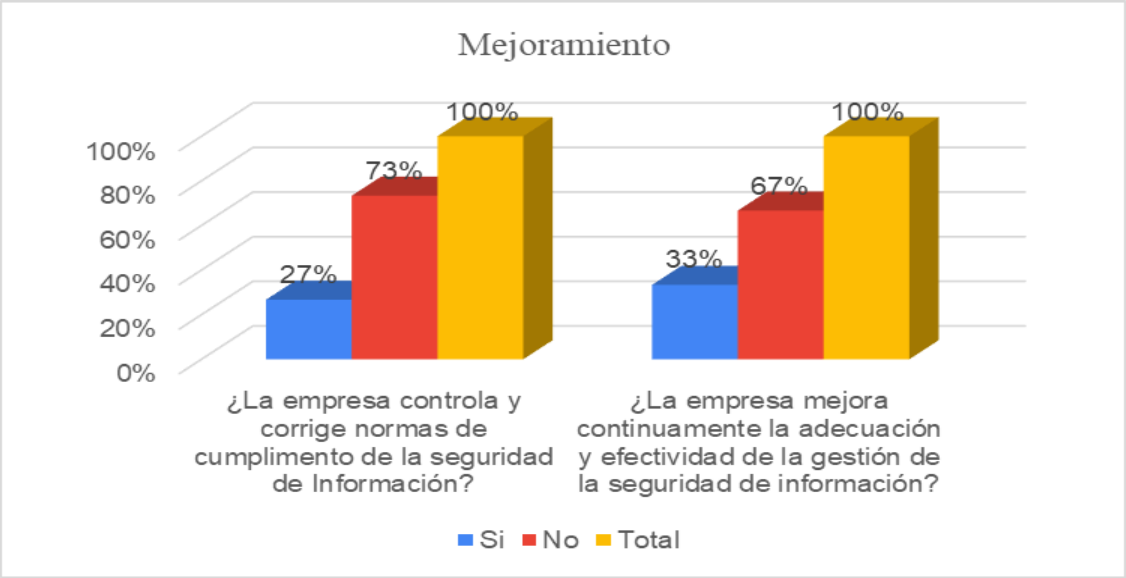
Mejoramiento

Mejoramiento	Si		No		Total	
	fi	%	fi	%	fi	%
¿La empresa controla y corrige normas de cumplimento de la seguridad de Información?	4	27%	11	73%	15	100%
¿La empresa mejora continuamente la adecuación y efectividad de la gestión de la seguridad de información?	5	33%	10	67%	15	100%

Fuente: *realizado según datos de la encuesta*

Figura 4

Mejoramiento



Interpretación

En la tabla 4 y en la figura 4 de la dimensión mejoramiento en sus indicadores, de un 100% de encuestados, 73% de las personas marcaron el No en la pregunta ¿La empresa controla y corrige normas de cumplimento de la seguridad de Información? en boticas de la ciudad de Juliaca año 2023 y un 27% de las personas encuestadas marcaron Sí; por otro lado, el 67% de las personas encuestadas marcaron No en la pregunta ¿La empresa mejora continuamente la adecuación y efectividad de la gestión de la seguridad de información? Y un 33% marcaron por Sí en la dicha pregunta.

Tabla 5

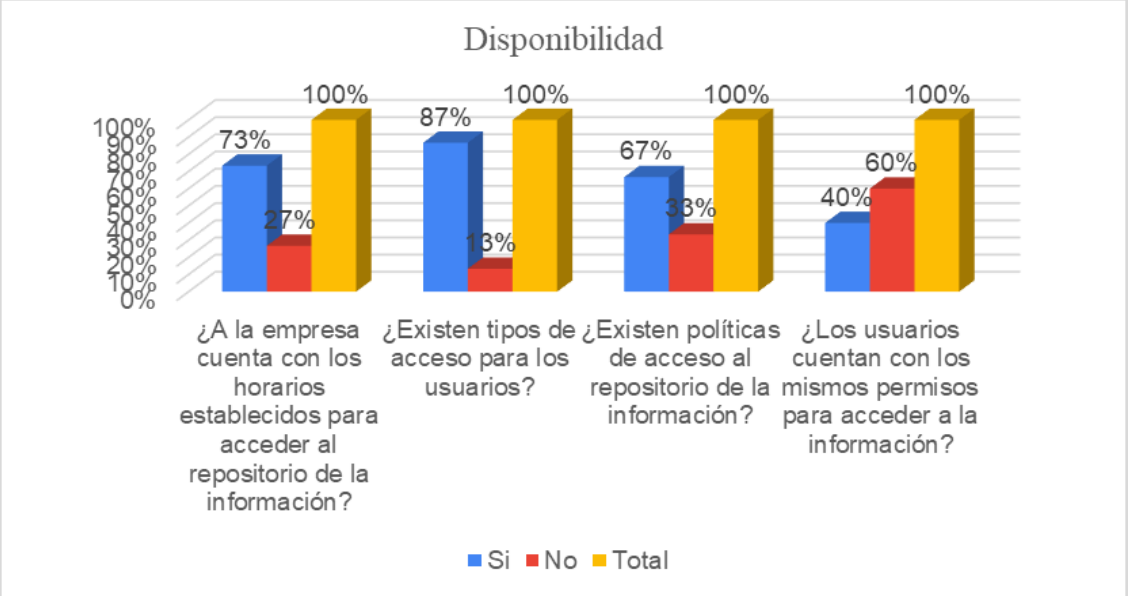
Disponibilidad

Disponibilidad	Si		No		Total	
	fi	%	fi	%	fi	%
¿A la empresa cuenta con los horarios establecidos para acceder al repositorio de la información?	11	73%	4	27%	15	100%
¿Existen tipos de acceso para los usuarios?	13	87%	2	13%	15	100%
¿Existen políticas de acceso al repositorio de la información?	10	67%	5	33%	15	100%
¿Los usuarios cuentan con los mismos permisos para acceder a la información?	6	40%	9	60%	15	100%

Fuente: *realizado según datos de la encuesta*

Figura 5

Disponibilidad



Interpretación

En la tabla 5 y en la figura 5 de la dimensión disponibilidad en sus indicadores, de un 100% de encuestados solo el 73% de las personas marcaron el Sí en la pregunta ¿A la empresa cuenta con los horarios establecidos para acceder al repositorio de la información? en boticas de la ciudad de Juliaca año 2023 y un 27% marcaron No; por otro lado, un 87% de las personas encuestadas marcaron Sí en la pregunta ¿Existen tipos

de acceso para los usuarios? Y un 13% marcaron No; así mismo, solo el 67% marcaron el Sí en la pregunta ¿Existen políticas de acceso al repositorio de la información? Y un 33% marcaron No, en dicha pregunta y por último un 40% de las personas marcaron Sí en la pregunta ¿Los usuarios cuentan con los mismos permisos para acceder a la información? Y un 60% marcaron No.

Tabla 6

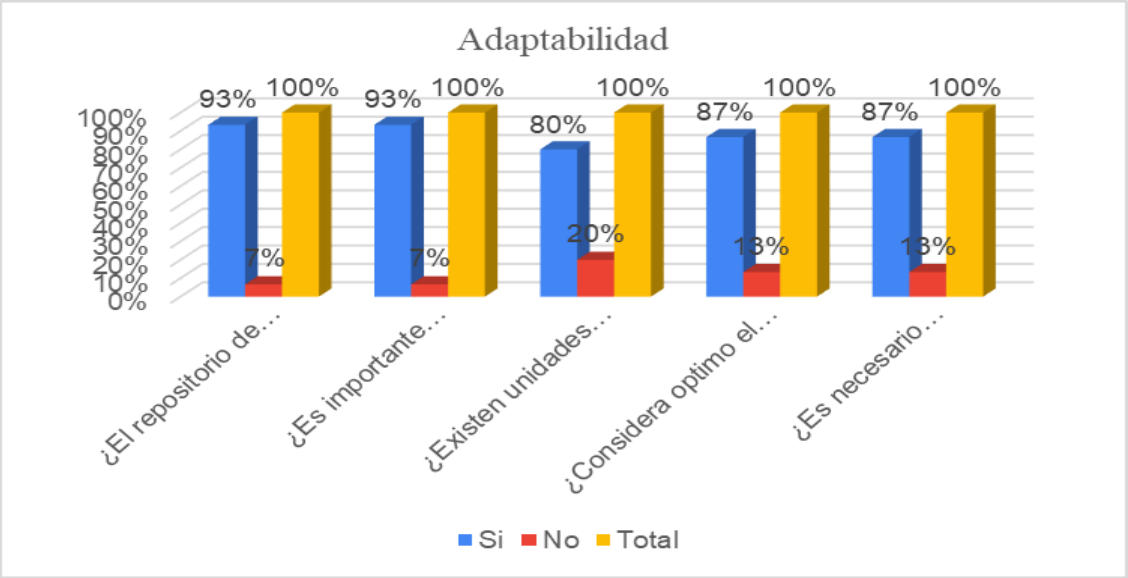
Adaptabilidad

Adaptabilidad	Si		No		Total	
	fi	%	fi	%	fi	%
¿El repositorio de información puede ser adaptables a nuevas tecnológicas?	14	93%	1	7%	15	100%
¿Es importante mejorar la adaptabilidad del repositorio de la información?	14	93%	1	7%	15	100%
¿Existen unidades de almacenamiento de respaldo?	12	80%	3	20%	15	100%
¿Considera optimo el espacio asignado a la PC/ Laptop asignado?	13	87%	2	13%	15	100%
¿Es necesario mejorar la capacidad física de la PC/ Laptop asignado?	13	87%	2	13%	15	100%

Fuente: *realizado según datos de la encuesta*

Figura 6

Adaptabilidad



Interpretación

En la tabla 6 y en la figura 6 de la dimensión adaptabilidad en sus indicadores, de un total 100% de encuestados el 97% de las personas marcaron Sí en la pregunta ¿El repositorio de información puede ser adaptables a nuevas tecnológicas? en boticas de la ciudad de Juliaca año 2023 y un 7% marcó No; por otro lado, un 93% de las personas encuestadas marcaron Sí en la pregunta ¿Es importante mejorar la adaptabilidad del repositorio de la información? Y un 7% marcó No; así mismo, solo el 80% marcaron el Sí en la pregunta ¿Existen unidades de almacenamiento de respaldo? Y un 20% marcaron No; por otro lado, el 87% marcaron Sí y un 13% marcaron No en la pregunta ¿Considera optimo el espacio asignado a la PC/ Laptop asignado? y por último un 87% de las personas marcaron Sí en la pregunta ¿Es necesario mejorar la capacidad física de la PC/ Laptop asignado Y un 13% marcaron No de dicha pregunta.

Tabla 7

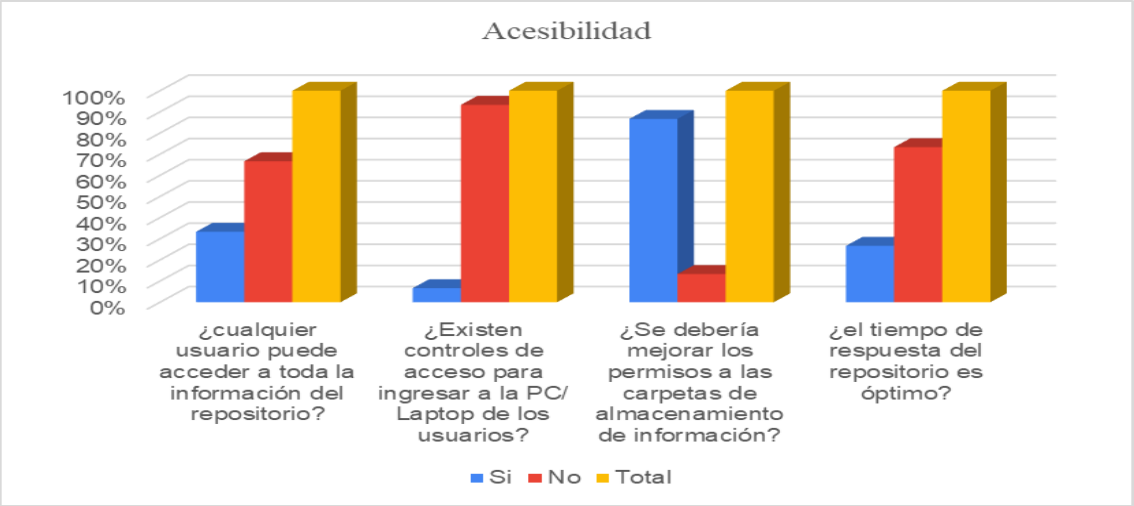
Accesibilidad

Accesibilidad	Si		No		Total	
	fi	%	fi	%	fi	%
¿cualquier usuario puede acceder a toda la información del repositorio?	5	33%	10	67%	15	100%
¿Existen controles de acceso para ingresar a la PC/ Laptop de los usuarios?	1	7%	14	93%	15	100%
¿Se debería mejorar los permisos a las carpetas de almacenamiento de información?	13	87%	2	13%	15	100%
¿el tiempo de respuesta del repositorio es óptimo?	4	27%	11	73%	15	100%

Fuente: *realizado según datos de la encuesta*

Figura 7

Accesibilidad



Interpretación

En la tabla 7 y en la figura 7 de la dimensión accesibilidad en sus indicadores, de un de encuestados del 100%, un 67% de las personas marcaron No en la pregunta ¿cualquier usuario puede acceder a toda la información del repositorio? en boticas de la ciudad de Juliaca año 2023 y un 33% marcó Sí; por otro lado, el 93% de las personas encuestadas marcaron No en la pregunta ¿Existen controles de acceso para ingresar a la

PC/ Laptop de los usuarios? Y un 7% marcó SÍ; así mismo, el 87%marcaro Sí en la pregunta ¿Se debería mejorar los permisos a las carpetas de almacenamiento de información? Y un 13% marcaron No; por otro lado, el 73% de los encuestaos marcaron No y un 27% marcaron Sí en la pregunta ¿el tiempo de respuesta del repositorio es óptimo?, es decir que la mayoría indica que no es óptimo.

Tabla 8

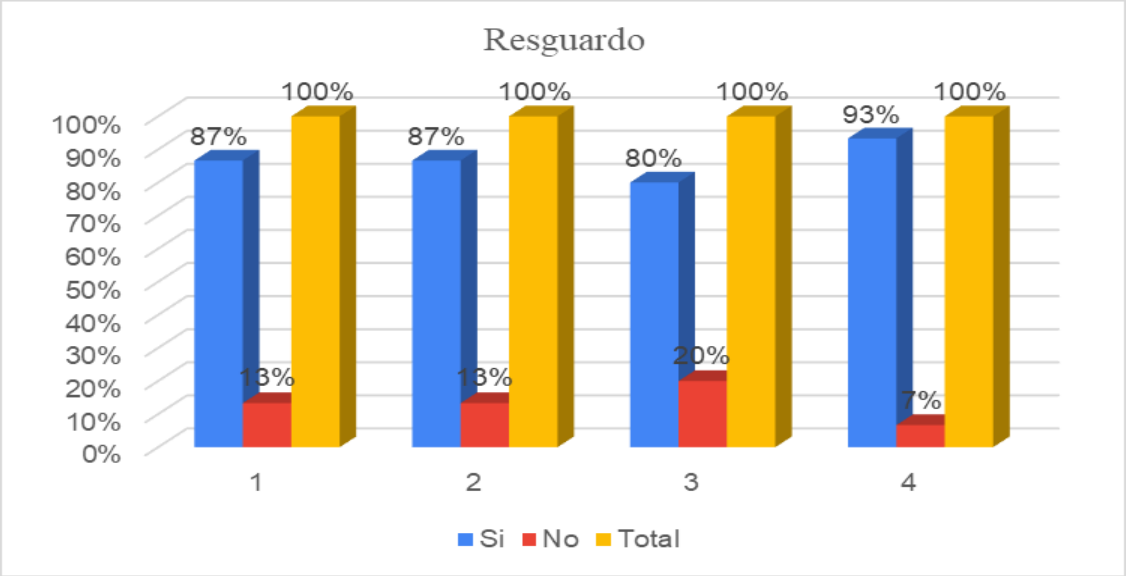
Resguardo

Resguardo	Si		No		Total	
	fi	%	fi	%	fi	%
¿Se considera primordial realizar copias de resguardo periódicamente?	13	87%	2	13%	15	100%
¿Se cuenta con una ubicación asignada para el almacenamiento de información de los usuarios en la PC / Laptop asignada?	13	87%	2	13%	15	100%
¿Se cuenta con protocolos para acceder a las copias de resguardo de información?	12	80%	3	20%	15	100%
¿Se cuenta con seguridad física al repositorio de información?	14	93%	1	7%	15	100%

Fuente: *realizado según datos de la encuesta*

Figura 8

Resguardo



Interpretación

En la tabla 8 y en la figura 8 de la dimensión accesibilidad en sus indicadores, de un 100% de encuestados, el 87% de las personas marcaron Sí en la pregunta ¿Se considera primordial realizar copias de resguardo periódicamente? en boticas de la ciudad de Juliaca año 2023 y un 13% marcó No; por otro lado, un 87% de las personas encuestadas marcaron Sí en la pregunta ¿Se cuenta con una ubicación asignada para el almacenamiento de información de los usuarios en la PC / Laptop asignada? Y un 13% marcó No; así mismo, solo el 80% marcaron Sí en la pregunta ¿Se cuenta con protocolos para acceder a las copias de resguardo de información? Y un 20% marcaron No; por último, el 93% marcaron Sí y un 7% marcó No en la pregunta ¿Se cuenta con seguridad física al repositorio de información?

4.1.1. Objetivo específico 01

Determinar la relación significativa entre las dimensiones de Planificación y disponibilidad en boticas de la ciudad de Juliaca año 2023.

Tabla 9

Correlaciones Planificación Disponibilidad

Correlaciones				
			Planificación	Disponibilidad
Rho de Spearman	Planificación	Coeficiente de correlación	1.000	0,789**
		Sig. (bilateral)		0.001
		N	14	14
	Disponibilidad	Coeficiente de correlación	0,789**	1.000
		Sig. (bilateral)	0.001	
		N	14	14

Elaboración propia

Interpretación:

En la tabla 9 se evidencia que el valor de p es 0.001 menor a 0.05, por lo tanto, se rechaza la hipótesis nula a partir de ello se evidencia que, si existe relación entre dimensión planificación y disponibilidad, así mismo un coeficiente de correlación de spearman es 0.789 presenta una correlación positiva alta, eso indica que con la planificación presenta una mejora en la dimensión de disponibilidad.

4.1.2. Objetivo específico 02

Determinar la relación significativa entre las dimensiones de Ejecución y adaptabilidad en boticas de la ciudad de Juliaca año 2023.

Tabla 10

Correlaciones Ejecución Adaptabilidad

Correlaciones				
			Ejecución	Adaptabilidad
Rho de Spearman	Ejecución	Coeficiente de correlación	1.000	0,957**
		Sig. (bilateral)		0.000
		N	14	14
	Adaptabilidad	Coeficiente de correlación	0,957**	1.000
		Sig. (bilateral)	0.000	
		N	14	14

Elaboración propia

Interpretación

En la tabla 10 se evidencia que el valor de p es 0.000 menor a 0.05, debido a esto se rechaza la hipótesis nula a partir de ello se evidencia que, si existe relación entre dimensión ejecución y adaptabilidad, así mismo se observa

un coeficiente de correlación de spearman es 0.957 presenta una correlación positiva muy alta, se concluye que a mayor ejecución se presenta una mejora en la adaptabilidad.

4.1.3. Objetivo específico 03

Determinar la relación significativa entre las dimensiones de Verificación y accesibilidad en boticas de la ciudad de Juliaca año 2023.

Tabla 11

Correlaciones Verificación Accesibilidad

Correlaciones				
			Verificación	Accesibilidad
Rho de Spearman	Verificación	Coeficiente de correlación	1.000	0,839**
		Sig. (bilateral)		0.000
		N	14	14
	Accesibilidad	Coeficiente de correlación	0,839**	1.000
		Sig. (bilateral)	0.000	
		N	14	14

Elaboración propia

Interpretación

En la tabla 11 se evidencia que el valor de p es 0.000 menor a 0.05, por tal motivo se rechaza la hipótesis nula a partir de ello se evidencia que, si existe relación entre dimensión verificación y accesibilidad, así mismo se observa un coeficiente de correlación de spearman es 0.839 presenta una correlación positiva alta, se concluye que si mejora la ejecución se mejora también la adaptabilidad.

4.1.4. Objetivo específico 04

Determinar la relación significativa entre las dimensiones de Mejoramiento y resguardo en boticas de la ciudad de Juliaca año 2023.

Tabla 12

Correlaciones Mejoramiento Resguardo

Correlaciones				
			Mejoramiento	Resguardo
Rho de Spearman	Mejoramiento	Coeficiente de correlación	1.000	,884**
		Sig. (bilateral)		0.000
		N	14	14
	Resguardo	Coeficiente de correlación	,884**	1.000
		Sig. (bilateral)	0.000	
		N	14	14

Elaboración propia

Interpretación:

En la tabla 12 se evidencia que el valor de p es 0.000 menor a 0.05, es así que se rechaza la hipótesis nula a partir de ello se evidencia que, si existe relación entre dimensión mejoramiento y resguardo, así mismo se observa un coeficiente de correlación de spearman es 0.884, presenta una correlación positiva alta, se concluye que si se mejora el mejoramiento también se mejorara el resguardo.

Objetivo General

Determinar la relación significativa entre la Norma ISO 27001 y control de la seguridad de información en boticas de la ciudad de Juliaca año 2023.

Tabla 13

Estadísticos descriptivos ISO 27001 y Control de Seguridad de la Información

Estadísticos descriptivos			
	Media	Desv. Desviación	N
Variable ISO 27001	29.67	1.589	15
Variable Control de Seguridad de la Información	23.20	1.897	15

Elaboración propia

Tabla 14

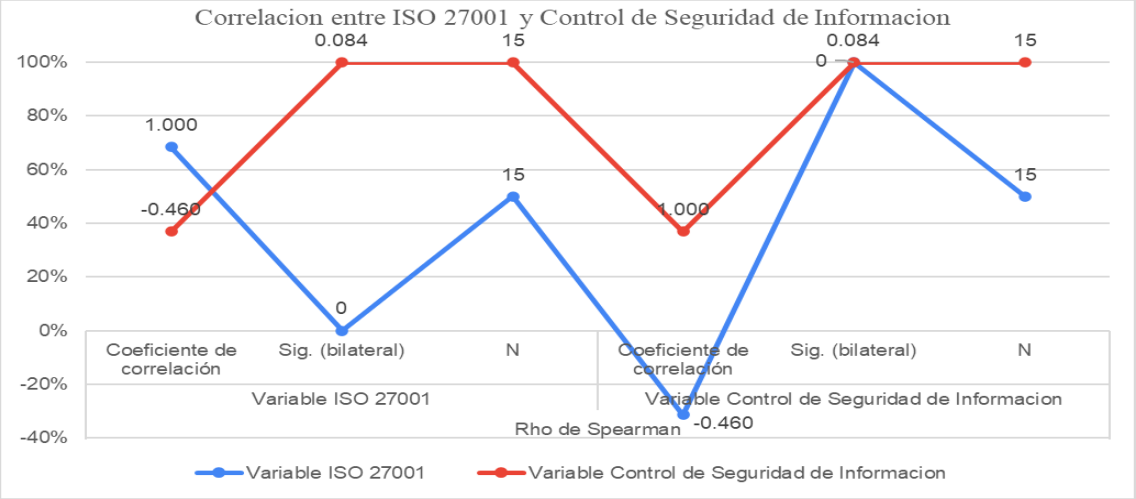
Correlaciones ISO 27001 y Control de Seguridad de Información

Correlaciones				
			Variable ISO 27001	Variable Control de Seguridad de Información
Rho de Spearman	Variable ISO 27001	Coeficiente de correlación	1.000	0.460
		Sig. (bilateral)		0.084
		N	15	15
	Variable Control de Seguridad de Información	Coeficiente de correlación	0.460	1.000
		Sig. (bilateral)	0.004	
		N	15	15

Elaboración propia

Figura 9

Correlaciones ISO 27001 y Control de Seguridad de Información



Interpretación:

En la tabla 14 se evidencia que el valor de p es 0.004 menor a 0.05, por ello se rechaza la hipótesis nula y se acepta la hipótesis alterna a partir de ello se evidencia que si existe relación entre las variables de ISO 27001 y la Variable Control de Seguridad de Información, así mismo se observa un coeficiente de correlación de 0.460 porque según presenta una correlación positiva moderada, se concluye que si mejora la variable ISO también se mejora la seguridad de información.

4.2. DISCUSIÓN

Los resultados de la investigación se corroboraron con los antecedentes citados en el trabajo:

según Rodríguez (2020) en su investigación muestra los resultados que entre otras cosas hay la necesidad de gestionar información crucial que puede ser fundamental para los intereses estratégicos de las empresas. La conclusión cuantitativa indica que el uso de la ISO tiene un impacto en la seguridad de la información, incluyendo la confidencialidad y la disponibilidad. Por otro lado, Pinto (2021) utilizo la metodología de riesgos, el inventario de actividades, la identificación y vulnerabilidades, la evaluación de riesgos, el establecimiento de controles está establecidos en el diseño del sistema. Los resultados muestran asegurar la confidencialidad, integridad y accesibilidad de la información y alienta a las organizaciones, asegurando la continuidad del negocio de las buenas prácticas descritas en la norma ISO 27001 complementan la gestión de la seguridad de la información. Se concluye que el sistema de gestión diseñado se transforma en una herramienta para elevar el nivel de madurez ayudando a la organización a reducir los riesgos que está expuesta y sirviendo como piedra angular para establecer una cultura de seguridad de la

información. Menciona también Camposano (2020) en su resultado que es fundamental el uso de la ISO 27001, las personas activas y pasivas utilizando herramientas comerciales y de comunicación que incluyen sublíneas, redes y tecnologías de software y hardware inteligente. potenciales después de los servidores, lugares de trabajo, dispositivos móviles, etc. Se concluye que la relevancia de la auditoría de la información Los sistemas de información son particularmente vulnerables a los ataques de usuarios malintencionados. Para Mera (2022) mostro como resultado se calculó el riesgo y priorizar las actividades requeridas para el remedio, se examinaron las amenazas y vulnerabilidades que estas actividades podrían encontrar. Se concluye que se eligieron ciertos controles enumerados y se examinó su cumplimiento para establecer recomendaciones sobre cómo mejorar la seguridad dentro de la empresa más adelante. En al ámbito nacional existen autores en el ámbito Nacional menciona Alemán (2023) el objetivo del presente estudio, que buscó determinar cuánto afectó la implementación de la norma ISO 27001:2013 al control de la seguridad de la información en una determinada organización. La metodología fue enfoque cuantitativo diseño experimental luego, utilizando como guía mediciones con las dimensiones definidas de la variable dependiente, se realizó un análisis de resultados. Esto fue aprobado por el juicio de tres expertos. Teniendo en cuenta una prueba de distribución no normal no paramétrica, los resultados de la prueba posterior fueron menos significativos que los resultados de la prueba previa en un nivel de significación de 0,5, se concluye la norma ISO 27001:2013 mejorará la seguridad de la información en las empresas de consultoría privadas. Menciona Villamar (2021). Muestran los resultados que la gestión de la información, y cómo se relacionan con la minimización de impactos en la norma ISO 27001 porque siempre es importante tratarlos para evitar y evitar tener que lamentarse. la pérdida total de datos. Se concluye que todos ellos eran ingenieros de sistemas en la

ciudad de Babahoyo. Su experiencia fue invaluable para lograr el análisis adecuado necesario para este proyecto final. Por otro lado, Gonzales (2019). como resultados fue implementar las normas después del principal hallazgo de la investigación mejoro el procedimiento de seguridad de la información. Se concluye que la implementación de NTP/ISO 27001 mejoró significativamente el proceso de seguridad de la información en la división de telemática de la oficina económica nacional. Para Benites (2019) muestra los resultados que, desde el análisis final del panorama político, discutirá los tiempos, presupuestos y personas responsables de llevar a cabo el desarrollo de este proyecto, se incluirán todas las conclusiones, referencias bibliográficas y anexos utilizados en el desarrollo de este proyecto. Ticona (2021) los resultados al evaluar cada una de sus diversas dimensiones, los administradores de sistemas de planificación proporcionaron información sobre la variable dependiente ISO 27001. Sin embargo, la presente investigación. Se concluye que el uso de la ISO 27001 no afecta significativamente la mejoro la seguridad de la información en los sistemas ERP. Según Chávez (2021) los resultados fueron: el nivel de significancia de p =.001 indica que p es menor a 0,05, indicando que la relación es significativa. Se concluye que existe una relación significativa entre el proceso de auditoría y los controles mejorados de seguridad de la información. Por otro lado, Chávarry (2021) Los resultados el tema central de la investigación fue cómo la implementación por parte del Secretariado Ejecutivo de la PNP de las normas ISO 27001 y 27002 adaptadas a la seguridad de la información afecta la seguridad de la información en la Unidad Policial.

V. CONCLUSIONES

PRIMERO. En boticas de la ciudad de Juliaca, de acuerdo con el primer objetivo específico se determinó que existe una **correlación positiva alta** con un coeficiente de 0.789 entre las dimensiones de planificación y disponibilidad. Concluyendo de que aumenta la disponibilidad de recursos necesarios para llevar a cabo la planificación.

SEGUNDA. En boticas de la ciudad de Juliaca, en el segundo objetivo específico se determinó que existe una **correlación positiva muy alta** con un coeficiente de 0.957 entre las dimensiones de ejecución y adaptabilidad. Lo que significa que, cuando una persona, sistema es capaz de llevar a cabo las acciones o planes de manera efectiva, existe capacidad de adaptarse de manera adecuada a los cambios, imprevistos que se presenta a su entorno.

TERCERA. En las boticas de la ciudad de Juliaca, en el tercer objetivo específico se determinó que existe una **correlación positiva alta** con un coeficiente de 0.839 entre las dimensiones de verificación y accesibilidad. Lo que quiere decir es que, cuanto más accesible sea la información relevante, más efectiva será la capacidad de verificar su veracidad.

CUARTA. En las boticas de la ciudad de Juliaca, en el cuarto objetivo específico se determinó que existe una **correlación positiva alta** con un coeficiente de 0.884 entre las dimensiones de mejoramiento y resguardo. Concluyendo que el mejoramiento constante de la información, como su relevancia y accesibilidad, impulsa a la buena toma de decisiones. A la vez, llevar una

adecuada protección y resguardo de la información es esencial para prevenir pérdida de datos.

QUINTA. En cuanto al objetivo general se determinó que existe una **correlación positiva moderada** entre la norma ISO 27001 y control de la seguridad de información en boticas de la ciudad de Juliaca. Es decir, ambos aspectos son esenciales para garantizar la seguridad de la información en las boticas o en cualquier empresa.

VI. RECOMENDACIONES

PRIMERA: Establecer objetivos claros y medibles define metas y objetivos específicos para tu proyecto o proceso. La planificación debe estar alineada con estos objetivos y la disponibilidad de recursos debe ser evaluada en función de su contribución a la consecución de esos objetivos. Crear un plan detallado desarrolla un plan de proyecto detallado que incluya tareas, plazos, responsabilidades y recursos necesarios. Esto permitirá una asignación precisa de los recursos disponibles y una planificación adecuada de su uso.

SEGUNDA: Análisis detallado es importante realizar un análisis detallado para comprender la naturaleza de la relación entre las dimensiones de ejecución y adaptabilidad. Esto puede ayudar a identificar las razones detrás de esta correlación y si existe alguna relación causal subyacente. Desarrollo de estrategias si estás trabajando en un entorno donde la ejecución y la adaptabilidad son críticas (por ejemplo, en una empresa), esta alta correlación podría sugerir que invertir en estrategias que mejoren tanto la ejecución como la adaptabilidad podría ser beneficioso. Monitoreo constante, dado que estas dos dimensiones están altamente correlacionadas, es importante monitorear regularmente ambas para detectar cualquier cambio en la relación a lo largo del tiempo. Si esta correlación cambia significativamente, podría ser una señal para revisar y ajustar tus estrategias.

TERCERA: Seguimiento a lo largo del tiempo si tienes datos en series temporales, sigue la evolución de la correlación con el tiempo. Puede ser útil para

identificar tendencias y cambios. Implementación de mejoras si estas dimensiones son importantes para tu proyecto o negocio, trabaja en la mejora de ambas dimensiones. Por ejemplo, si la accesibilidad de un sitio web influye en la verificación de usuarios, podría ser necesario optimizar la accesibilidad para mejorar la verificación.

CUARTA: Utilizar la información en la toma de decisiones, si ambas dimensiones son importantes para tu objetivo o área de estudio, esta fuerte correlación puede indicar que mejorar una también puede mejorar la otra. Por ejemplo, si estás trabajando en un proyecto de desarrollo empresarial, el aumento en las inversiones (mejoramiento) podría estar correlacionado con un aumento en la seguridad financiera (resguardo). Esto podría sugerir que invertir más en mejoramiento podría mejorar la seguridad financiera de la empresa. Monitorear y ajustar estrategias, si estás tomando medidas para mejorar una dimensión específica, como el rendimiento en una empresa, asegúrate de monitorear cómo afecta a la otra dimensión. Si notas que el aumento en el mejoramiento tiene un impacto negativo en el resguardo, es posible que debas ajustar tus estrategias para equilibrar ambos aspectos.

QUINTA. Realiza una Evaluación de Riesgos, comienza por realizar una evaluación de riesgos de seguridad de la información específica para tu botica en Juliaca. Identifica los activos críticos de información, las amenazas y vulnerabilidades, y evalúa el impacto potencial de los riesgos. Implementa un Sistema de Gestión de Seguridad de la Información (SGSI), la ISO 27001 establece los requisitos para un SGSI efectivo.

Desarrolla un sistema que incluya políticas, procedimientos y procesos para gestionar los riesgos de seguridad de la información. puede ser beneficiosa para garantizar la confidencialidad, integridad y disponibilidad de los datos y la protección de la información sensible de los clientes.

VII. REFERENCIAS BIBLIOGRÁFICAS

Adidas, W. (2019). *Lo esencial del hackeo La guía para principiantes sobre hackeo ético y pruebas de penetración.* (A. Wilson, Ed.) Recuperado el 12 de Agosto de 2023, de https://www.google.com.pe/books/edition/Lo_esencial_del_hackeo/mBuyDwAAQBAJ?hl=es-419&gbpv=0

Aleman, B. F. (2023). *Norma ISO 27001 para el control de la seguridad de información en una consultoría privada, Lima 2023.* Recuperado el 7 de Mayo de 2022, de https://hdl.handle.net/20.500.12692/106824

Arias, G. J. (2020). *Técnicas e instrumentos de investigación científica.* doi:file:///C:/Users/USUARIO/Downloads/AriasGonzales_TecnicasEInstrumentosDeInvestigacion_libro.pdf

Barriento, N. (2021). *Metologia de la Imvestigacion.* doi:https://es.scribd.com/document/504549046/Metodologia-de-la-Investigacion-Nelly-Barrientos-C-I29933584

Benites, D. C. (2019). *Implementación de un sistema de gestión de seguridad de la información - Norma ISO 27001 para la fábrica Radiadores Fortaleza.* Recuperado el 07 de Mayo de 2023, de https://hdl.handle.net/20.500.12867/1933

Camposano, M. G. (2020). *Propuesta para el control y seguridad de la información de la empresa de ventas en Línea Buy Now aplicando Norma ISO 27001.* Recuperado el 12 de Mayo de 2023, de http://dspace.utb.edu.ec/handle/49000/8614

Carrasco, D. S. (2005). *Metodologia de la Investigacion Cientifica.* Lima: San Marcos . doi:file:///C:/Users/Usuario/Downloads/Metodologia_de_La_Investigacion_Cientifi.pdf

Cazurro, B. V. (2022). *Seguridad del tratamiento: Aspectos técnicos (Parte I).* (J. B. Editor, Ed.) Recuperado el 12 de Agosto de 2023, de https://www.google.com.pe/books/edition/Seguridad_del_tratamiento_Aspectos_t%C3%A9cn/8Uu3EAAAQBAJ?hl=es-419&gbpv=0

Chávarry, B. S. (2021). *Implementación de ISO 27001 y 27002 adaptadas para gestión de seguridad de información en Secretaría Ejecutiva de Policía Nacional del Perú.* Recuperado el 06 de Mayo de 2023, de https://hdl.handle.net/20.500.12692/79133

Chavez, C. L. (2021). *Proceso de auditoria ISO 27001 para la mejora de los controles de seguridad de la información en la municipalidad distrital de San Juan Bautista 2018.* Recuperado el 12 de Mayo de 2023, http://repositorio.ucp.edu.pe/handle/UCP/1292

DICCIONARIO. (8 de Setiembre de 2021). Obtenido de https://www.google.com/search?q=ejercicios+f%C3%ADsicos+recreativos&oq=ejercicios+f%C3%ADsicos+recreativos&aqs=chrome..69i57j0i19i22i30l2j0i10i19i22i30.3567j0j7&sourceid=chrome&ie=UTF-8

Gonzales Aybar, R. G. (2019). *Implementación de la NTP/ISO 27001 para mejorar el proceso de seguridad de información en el Departamento Telemática de la Oficina de Economía del Ejército del Perú.* Recuperado el 14 de Mayo de 2023, de https://hdl.handle.net/20.500.13067/1039

Hernández, S. R. (2014). *Metodologia de la Investigacion* (Sexta edición ed.). (S. D. McGRAW-HILL / INTERAMERICANA EDITORES, Ed.) México, Mexico . Recuperado el 15 de Diciembre de 2022, de https://www.esup.edu.pe/wp-content/uploads/2020/12/2.%20Hernandez,%20Fernandez%20y%20Baptista-Metodolog%C3%ADa%20Investigacion%20Cientifica%206ta%20ed.pdf

Kalambkar, D. D. (2021). *Implementing ISO 27001 Simplified Full Fledged Information on Implementing End-to-End Information Security with Real Time Statistical Data and Analysis.* (N. Press, Ed.) Recuperado el 13 de Agosto de 2023, de https://www.google.com.pe/books/edition/Implementing_ISO_27001_Simplified/QrEcEAAAQBAJ?hl=es-419&gbpv=0

Ladrón, d. G. (2020). *Transmisión de información por medios convencionales e informáticos. UF0512.* (E. T. Formación, Ed.) Recuperado el 13 de Agosto de 2023, de https://www.google.com.pe/books/edition/Transmisi%C3%B3n_de_informaci%C3%B3n_por_medios/cAIAEAAAQBAJ?hl=es-419&gbpv=0

Mera, A. I. (2022). *Propuesta de gestión de la seguridad de la información basado en la norma ISO 27001. Caso de estudio: empresa ALTAC.* Recuperado el 12 de Mayo de 2023, de http://repositorio.puce.edu.ec:80/handle/22000/21108

Pinto, A. D. (2021). *Análisis y diseño de un sistema de gestión de la seguridad de la información basado en la norma ISO 27001, orientado a la disminución de riesgos en la unidad de informática del GAD municipal del cantón Pujilí.* Recuperado el 07 de Mayo de 2023, de http://repositorio.espe.edu.ec/bitstream/21000/26482/1/T-ESPE-050862.pdf

Quispe, Q. Y. (2022). INTRODUCCION A LA INVESTIGACIÓN. Juliaca, San Roman, Peru : Ediciones Andinas de Yasmín Lucero Mendoza Juárez. doi: https://www.researchgate.net/publication/373976021_INTRODUCCION_A_LA_INVESTIGACION

Quispe, Q. Y. (2023). Diseños y Secuencia Didáctica para la Investigación en un Nuevo Paradigma. (C. -C. Desarrollo, Ed.) Paraguay. doi: https://doi.org/10.37811/cli_w957

Rodriguez, B. L. (2020). *Aplicación de ISO 27001 y su influencia en la seguridad de la información de una empresa privada peruana.* Recuperado el 13 de Mayo de 2023, de http://www.scielo.org.pe/pdf/pyr/v8n3/2310-4635-pyr-8-03-e786.pdf

Steve, W. A. (2019). *Information Security Risk Management for ISO 27001/ISO 27002, third edition.* (I. G. Ltd, Ed.) Recuperado el 13 de Agosto de 2023, de https://www.google.com.pe/books/edition/Information_Security_Risk_Management_for/GEGuDwAAQBAJ?hl=es-419&gbpv=0

Tamayo, T. M. (2004). *Diccionario de la investigación científica.* Mexico: Limusa, México y cop. 2004.

Ticona, L. H. (2021). *Uso de la norma ISO 27001 y su influencia en la seguridad de información de la empresa Ico el año 2021.* Recuperado el 13 de Mayo de 2023, de https://hdl.handle.net/11537/28162

Villalón, H. A. (2020). *Seguridad en Unix y redes. Versión 2.1'.* (N. Llibres, Ed.) Recuperado el 13 de Agosto de 2023, de https://www.google.com.pe/books/edition/Seguridad_en_Unix_y_redes_Versi%

C3%B3n_2_1/i-LTDwAAQBAJ?hl=es-419&gbpv=0

Villamar, S. C. (2021). *Análisis de seguridad de la información basado en la norma ISO 27001 en el Área Técnica de Reparación e Instalación de la Corporación Nacional de Telecomunicaciones "CNT EP" de la ciudad de Babahoyo.* Recuperado el 07 de Mayo de 2023, de http://dspace.utb.edu.ec/handle/49000/10549

Wikipedia. (22 de Agosto de 2021). Obtenido de La enciclopedia libre: https://www.google.com/search?q=wikipedia+espa%C3%B1ol&oq=wikipedia&aqs=chrome.1.69i57j0i512l9.9367j0j7&sourceid=chrome&ie=UTF-8

ANEXOS

Anexo 01. Validez de instrumento

Validez del instrumento para la dimensión de la variable dependiente norma ISO 27001

Experto	Controles para el instrumento de medición				Condición
	No existe	Inicio	Desarrollo	Completado	
Dr. Marlon Frank Acuña Benites	-	-	X	X	Aplicable
Mg. Giancarlo Sánchez Atuncar	-	-	X	X	Aplicable
Mg. Juan Orlando Pérez Alvarado	-	-	X	X	Aplicable

En la tabla se visualiza la evaluación de expertos que se realizó para el presente estudio, se puede observar que los tres expertos han considerado la condición como aplicable en lo que respecta la medición de instrumentos, así como también se muestra la concordancia que han tenido los expertos ya que han considerado que para la aprobación de las dimensiones estos deben oscilar entre " casi siempre" y " siempre", debido a que de esta manera existirá un control adecuado en lo que respecta a la variable ISO 27001.

Validez del instrumento para la dimensión de la variable independiente control de seguridad de información.

Experto	Controles para el instrumento de medición				Condición
	No existe	Inicio	Desarrollo	Completado	
Dr. Marlon Frank Acuña Benites	-	-	X	X	Aplicable
Mg. Giancarlo Sánchez Atuncar	-	-	X	X	Aplicable
Mg. Juan Orlando Pérez Alvarado	-	-	X	X	Aplicable

En la tabla se visualiza la evaluación de expertos que se realizó para el presente estudio, se puede observar que los tres expertos han considerado la condición como aplicable en lo que respecta la medición de instrumentos, así como también se muestra la concordancia que han tenido los expertos ya que han considerado que para la aprobación de las dimensiones estos deben oscilar entre " casi siempre" y " siempre", debido a que de esta manera existirá un control adecuado en lo que respecta a la variable seguridad de información.

Escala de confiablidad

Según, Arias (2021) en referencia a la confiabilidad del instrumento, es el nivel en que el mismo objeto medido genera el mismo resultado.

Escala	Nivel de confiabilidad
< a 0.9	Muy aceptable
Entre 0.8 a 0.89	Aceptable
Entre 0.7 a 0.79	Baja
> a 0.69	Inaceptable

Fuente: Arias (2021)

Experto 01

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO QUE MIDE MIDE LOS INSTRUMENTOS DE RECOLECCIÓN DE DATOS.
VARIABLE : Norma iso 27001

Nº	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	DIMENSION 1 : Planificación	Si	No	Si	No	Si	No	
1	5.1. ¿La dirección aprueba el cumplimiento de los objetivos de seguridad de la información para la implementación de la ISO 27001?							
2	5.1. ¿El equipo de proyecto asegura la integración de los requisitos para implementar la ISO 27001 en los procesos de la empresa?							
3	5.2. ¿Existe apoyo a los trabajadores para su contribución efectiva de la ISO 27001?							
4	5.3. ¿Se ha establecido una política de seguridad de la información?							
5	5.3. ¿Se han definido roles y responsabilidades para la seguridad de información?							
6	6.1.1. ¿La empresa realiza análisis de riesgos de la seguridad de información?							
7	6.1.2. ¿La empresa define y aplica el proceso de valoración de riesgos de la seguridad de información?							
8	6.1.3. ¿La empresa tiene un plan de tratamiento de riesgos de la seguridad de la información?							
9	6.2. ¿La empresa tiene documentado los objetivos de la seguridad de información?							
10	6.2. ¿La empresa cuenta con un plan de mejora basado en el cumplimiento de objetivos?							
11	7.1. ¿La empresa proporciona los recursos necesarios para la gestión de la seguridad informática?							
12	7.2. ¿Existen evaluaciones de desempeño acerca de la seguridad de información?							
13	7.3 ¿Existen políticas de seguridad de información?							
14	7.4. ¿Se tienen definidos canales de atención para la seguridad de información?							
15	7.5.1. ¿Se cuenta con documentación de la seguridad de información para asegurar la efectividad?							
16	7.5.3. ¿Se controla que la información requerida para la gestión de la seguridad esté disponible y protegida?							
	DIMENSION 2 : Ejecución	Si	No	Si	No	Si	No	
17	8.1. ¿Existe una planificación, ejecución y control de procesos para la gestión de seguridad de información?							
18	8.2. ¿Se llevan a cabo evaluaciones de riesgo planificados?							
19	8.3. ¿La empresa cuenta con un plan de tratamiento de riesgos?							
	DIMENSION 3 : Verificacion	Si	No	Si	No	Si	No	
20	9.1. ¿La empresa realiza el seguimiento, análisis y evaluación de la gestión de seguridad de información?							
21	9.2. ¿La empresa realiza auditorías internas?							
22	9.3. ¿La alta dirección revisa su gestión de seguridad de información para asegurar su eficacia?							
23	9.4. ¿La alta dirección toma decisiones y medidas en base a los resultados obtenidos por la gestión de seguridad de información?							
	DIMENSION 4 : Mejoramiento	Si	No	Si	No	Si	No	
24	10.1. ¿La empresa controla y corrige las normas de cumplimiento de la seguridad de información?							
25	10.2. ¿La empresa mejora continuamente la adecuación y efectividad de la gestión de la seguridad de información?							

Observaciones (precisar si hay suficiencia):_____

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

Apellidos y nombres del juez validador. Dr/ Mg: **MARLON FRANK ACUÑA BENITES** **DNI: 42097456**

Especialidad del validador:.....

24 de octubre del 2022

[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.
[2]**Relevancia:** El ítem es apropiado para representar el 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 LOS INSTRUMENTOS DE RECOLECCIÓN DE DATOS

VARIABLE : Control de seguridad de la información

N°	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	DIMENSION 1 : Disponibilidad	Si	No	Si	No	Si	No	
1	¿La empresa cuenta con horarios establecidos para acceder al repositorio de información?							
2	¿Existen tipos de acceso para los usuarios?							
3	¿Existente políticas de acceso al repositorio de la información?							
4	¿Los usuarios cuentan con los mismos permisos para acceder a la información?							
	DIMENSION 2 : Adaptabilidad	Si	No	Si	No	Si	No	
5	¿El repositorio de información pueden ser adaptables a nuevas tecnologías?							
6	¿Es importante mejorar la adaptabilidad del repositorio de información?							
7	¿Existen unidades de almacenamiento de respaldo?							
8	¿Considera optimo el espacio asignado a la PC/Laptop asignado?							
9	¿Es necesario mejorar la capacidad física de la PC/Laptop asignado?							
	DIMENSION 3 : Accesibilidad	Si	No	Si	No	Si	No	
10	¿Cualquier usuario puede acceder a toda la información del repositorio?							
11	¿Existen controles de acceso para ingresar a la PC/Laptop de los usuarios?							
12	¿Se debería mejorar los permisos a las carpetas de almacenamiento de información?							
13	¿El tiempo de respuesta del repositorio de información es optimo?							
	DIMENSION 4 : Resguardo	Si	No	Si	No	Si	No	
14	¿Se realizan copias de resguardo del repositorio de información?							

N°	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
15	¿Se considera primordial realizar copias de resguardo periódicamente?							
16	¿Se cuenta con una ubicación asignada para el almacenamiento de información de los usuarios en la PC/Laptop asignada?							
17	¿Se cuenta con protocolos para acceder a las copias de resguardo de información?							
18	¿Se cuenta con seguridad física al repositorio de información?							

Observaciones (precisar si hay suficiencia): .....

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

Apellidos y nombres del juez validador. Dr/ Mg: **MARLON FRANK ACUÑA BENITES** **DNI: 42097456**

Especialidad del validador: .....

[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

24 de octubre del 2022

Firma del Experto Informante.

Experto 02

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO QUE MIDE MIDE LOS INSTRUMENTOS DE RECOLECCIÓN DE DATOS.
VARIABLE : Implementacion de norma iso 27001

Nº	DIMENSIONES / Ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	DIMENSION 1 : Planificación	Si	No	Si	No	Si	No	
1	5.1. ¿La dirección aprueba el cumplimiento de los objetivos de seguridad de la información para la implementación de la ISO 27001?	x		x		x		
2	5.1. ¿El equipo de proyecto asegura la integración de los requisitos para implementar la ISO 27001 en los procesos de la empresa?	x		x		x		
3	5.2. ¿Existe apoyo a los trabajadores para su contribución efectiva de la ISO 27001?	x		x		x		
4	5.3. ¿Se ha establecido una política de seguridad de la información?	x		x		x		
5	5.3. ¿Se han definido roles y responsabilidades para la seguridad de información?	x		x		x		
6	6.1.1. ¿La empresa realiza análisis de riesgos de la seguridad de información?	x		x		x		
7	6.1.2. ¿La empresa define y aplica el proceso de valoración de riesgos de la seguridad de información?	x		x		x		
8	6.1.3. ¿La empresa tiene un plan de tratamiento de riesgos de la seguridad de la información?	x		x		x		
9	6.2. ¿La empresa tiene documentado los objetivos de la seguridad de información?	x		x		x		
10	6.2. ¿La empresa cuenta con un plan de mejora basado en el cumplimiento de objetivos?	x		x		x		
11	7.1. ¿La empresa proporciona los recursos necesarios para la gestión de la seguridad informática?	x		x		x		
12	7.2. ¿Existen evaluaciones de desempeño acerca de la seguridad de información?	x		x		x		
13	7.3 ¿Existen políticas de seguridad de información?	x		x		x		
14	7.4. ¿Se tienen definidos canales de atención para la seguridad de información?	x		x		x		
15	7.5.1. ¿Se cuenta con documentación de la seguridad de información para asegurar la efectividad?	x		x		x		
16	7.5.3. ¿Se controla que la información requerida para la gestión de la seguridad esté disponible y protegida?	x		x		x		
	DIMENSION 2 : Ejecución	Si	No	Si	No	Si	No	
17	8.1. ¿Existe una planificación, ejecución y control de procesos para la gestión de seguridad de información?	x		x		x		
18	8.2. ¿Se llevan a cabo evaluaciones de riesgo planificados?							
19	8.3. ¿La empresa cuenta con un plan de tratamiento de riesgos?							
	DIMENSION 3 : Verificación	Si	No	Si	No	Si	No	
20	9.1. ¿La empresa realiza el seguimiento, análisis y evaluación de la gestión de seguridad de información?	x		x		x		
21	9.2. ¿La empresa realiza auditorías internas?							
22	9.3. ¿La alta dirección revisa su gestión de seguridad de información para asegurar su eficacia?							
23	9.4. ¿La alta dirección toma decisiones y medidas en base a los resultados obtenidos por la gestión de seguridad de información?							
	DIMENSION 4 : Mejoramiento	Si	No	Si	No	Si	No	
24	10.1. ¿La empresa controla y corrige las normas de cumplimiento de la seguridad de información?	x		x		x		
25	10.2. ¿La empresa mejora continuamente la adecuación y efectividad de la gestión de la seguridad de información?							

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

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

Apellidos y nombres del juez validador **Mg. Giancarlo Sánchez Atuncar** **DNI: 41488834**

Especialidad del validador: 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

25 de octubre del 2022

Firma del Experto Informante.

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO QUE MIDE LOS INSTRUMENTOS DE RECOLECCIÓN DE DATOS

VARIABLE : Control de seguridad de la información

Nº	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	DIMENSION 1 : Disponibilidad	Si	No	Si	No	Si	No	
1	¿La empresa cuenta con horarios establecidos para acceder al repositorio de información?	x		x		x		
2	¿Existen tipos de acceso para los usuarios?	x		x		x		
3	¿Existente políticas de acceso al repositorio de la información?	x		x		x		
4	¿Los usuarios cuentan con los mismos permisos para acceder a la información?							
	DIMENSION 2 : Adaptabilidad	Si	No	Si	No	Si	No	
5	¿El repositorio de información pueden ser adaptables a nuevas tecnologías?	x		x		x		
6	¿Es importante mejorar la adaptabilidad del repositorio de información?	x		x		x		
7	¿Existen unidades de almacenamiento de respaldo?	x		x		x		
8	¿Considera optimo el espacio asignado a la PC/Laptop asignado?	x		x		x		
9	¿Es necesario mejorar la capacidad física de la PC/Laptop asignado?							
	DIMENSION 3 : Accesibilidad	Si	No	Si	No	Si	No	
10	¿Cualquier usuario puede acceder a toda la información del repositorio?	x		x		x		
11	¿Existen controles de acceso para ingresar a la PC/Laptop de los usuarios?	x		x		x		
12	¿Se debería mejorar los permisos a las carpetas de almacenamiento de información?	x		x		x		
13	¿El tiempo de respuesta del repositorio de información es óptimo?	x		x		x		
	DIMENSION 4 : Resguardo	Si	No	Si	No	Si	No	
14	¿Se realizan copias de resguardo del repositorio de información?	x		x		x		

Nº	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
15	¿Se considera primordial realizar copias de resguardo periódicamente?	x		x		x		
16	¿Se cuenta con una ubicación asignada para el almacenamiento de información de los usuarios en la PC/Laptop asignada?	x		x		x		
17	¿Se cuenta con protocolos para acceder a las copias de resguardo de información?	x		x		x		
18	¿Se cuenta con seguridad física al repositorio de información?	x		x		x		

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

Opinión de aplicabilidad: Aplicable [X] Aplicable después de corregir [ ] No aplicable [ ]

Apellidos y nombres del juez validador. Mg. Giancarlo Sánchez Atuncar DNI: 41488834

Especialidad del validador: 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

25 de octubre del 2022

Firma del Experto Informante.

Experto 03

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO QUE MIDE MIDE LOS INSTRUMENTOS DE RECOLECCIÓN DE DATOS.
VARIABLE : Norma iso 27001

Nº	DIMENSIONES / Ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	DIMENSION 1 : Planificación	Si	No	Si	No	Si	No	
1	5.1. ¿La dirección aprueba el cumplimiento de los objetivos de seguridad de la información para la implementación de la ISO 27001?	X		X		X		
2	5.1. ¿El equipo de proyecto asegura la integración de los requisitos para implementar la ISO 27001 en los procesos de la empresa?	X		X		X		
3	5.2. ¿Existe apoyo a los trabajadores para su contribución efectiva de la ISO 27001?	X		X		X		
4	5.3. ¿Se ha establecido una política de seguridad de la información?	X		X		X		
5	5.3. ¿Se han definido roles y responsabilidades para la seguridad de información?	X		X		X		
6	6.1.1. ¿La empresa realiza análisis de riesgos de la seguridad de información?	X		X		X		
7	6.1.2. ¿La empresa define y aplica el proceso de valoración de riesgos de la seguridad de información?	X		X		X		
8	6.1.3. ¿La empresa tiene un plan de tratamiento de riesgos de la seguridad de la información?	X		X		X		
9	6.2. ¿La empresa tiene documentado los objetivos de la seguridad de información?	X		X		X		
10	6.2. ¿La empresa cuenta con un plan de mejora basado en el cumplimiento de objetivos?	X		X		X		
11	7.1. ¿La empresa proporciona los recursos necesarios para la gestión de la seguridad informática?	X		X		X		
12	7.2. ¿Existen evaluaciones de desempeño acerca de la seguridad de información?	X		X		X		
13	7.3 ¿Existen políticas de seguridad de información?	X		X		X		
14	7.4. ¿Se tienen definidos canales de atención para la seguridad de información?	X		X		X		
15	7.5.1. ¿Se cuenta con documentación de la seguridad de información para asegurar la efectividad?	X		X		X		
16	7.5.3. ¿Se controla que la información requerida para la gestión de la seguridad esté disponible y protegida?	X		X		X		
	DIMENSION 2: Ejecución	Si	No	Si	No	Si	No	
17	8.1. ¿Existe una planificación, ejecución y control de procesos para la gestión de seguridad de información?	X		X		X		

Nº	DIMENSIONES / Ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
18	8.2. ¿Se llevan a cabo evaluaciones de riesgo planificados?	X		X		X		
19	8.3. ¿La empresa cuenta con un plan de tratamiento de riesgos?	X		X		X		
	DIMENSION 3 : Verificación	Si	No	Si	No	Si	No	
20	9.1. ¿La empresa realiza el seguimiento, análisis y evaluación de la gestión de seguridad de información?	X		X		X		
21	9.2. ¿La empresa realiza auditorías internas?	X		X		X		
22	9.3. ¿La alta dirección revisa su gestión de seguridad de información para asegurar su eficacia?	X		X		X		
23	9.4. ¿La alta dirección toma decisiones y medidas en base a los resultados obtenidos por la gestión de seguridad de información?	X		X		X		
	DIMENSION 4 : Mejoramiento	Si	No	Si	No	Si	No	
24	10.1. ¿La empresa controla y corrige las normas de cumplimiento de la seguridad de información?	X		X		X		
25	10.2. ¿La empresa mejora continuamente la adecuación y efectividad de la gestión de la seguridad de información?	X		X		X		

Observaciones (precisar si hay suficiencia): SI HAY SUFICIENCIA EN EL INSTRUMENTO

Opinión de aplicabilidad: Aplicable [X] Aplicable después de corregir [ ] No aplicable [ ]

Apellidos y nombres del juez validador : Mg. Juan Orlando Perez Alvaro **DNI:** 40545360

Especialidad del validador: Ingeniero de Sistemas

24 de octubre 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 DIGITAL
Firmado digitalmente por: PEREZ ALVARO Juan Orlando FAU 20131370998 soft
Motivo: Soy el autor del documento
Fecha: 25/10/2022 09:50:27-0500

Firma del Experto Informante.

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO QUE MIDE LOS INSTRUMENTOS DE RECOLECCIÓN DE DATOS

VARIABLE : Control de seguridad de la información

Nº	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	DIMENSION 1 : Disponibilidad	Si	No	Si	No	Si	No	
1	¿La empresa cuenta con horarios establecidos para acceder al repositorio de información?	X		X		X		
2	¿Existen tipos de acceso para los usuarios?	X		X		X		
3	¿Existente políticas de acceso al repositorio de la información?	X		X		X		
4	¿Los usuarios cuentan con los mismos permisos para acceder a la información?	X		X		X		
	DIMENSION 2 : Adaptabilidad	Si	No	Si	No	Si	No	
5	¿El repositorio de información pueden ser adaptables a nuevas tecnologías?	X		X		X		
6	¿Es importante mejorar la adaptabilidad del repositorio de información?	X		X		X		
7	¿Existen unidades de almacenamiento de respaldo?	X		X		X		
8	¿Considera optimo el espacio asignado a la PC/Laptop asignado?	X		X		X		
9	¿Es necesario mejorar la capacidad física de la PC/Laptop asignado?	X		X		X		
	DIMENSION 3 : Accesibilidad	Si	No	Si	No	Si	No	
10	¿Cualquier usuario puede acceder a toda la información del repositorio?	X		X		X		
11	¿Existen controles de acceso para ingresar a la PC/Laptop de los usuarios?	X		X		X		
12	¿Se debería mejorar los permisos a las carpetas de almacenamiento de información?	X		X		X		
13	¿El tiempo de respuesta del repositorio de información es óptimo?	X		X		X		
	DIMENSION 4 : Resguardo	Si	No	Si	No	Si	No	
14	¿Se realizan copias de resguardo del repositorio de información?	X		X		X		

Nº	DIMENSIONES / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
15	¿Se considera primordial realizar copias de resguardo periódicamente?	X		X		X		
16	¿Se cuenta con una ubicación asignada para el almacenamiento de información de los usuarios en la PC/Laptop asignada?	X		X		X		
17	¿Se cuenta con protocolos para acceder a las copias de resguardo de información?	X		X		X		
18	¿Se cuenta con seguridad física al repositorio de información?	X		X		X		

Observaciones (precisar si hay suficiencia): SI HAY SUFICIENCIA EN EL INSTRUMENTO

Opinión de aplicabilidad: Aplicable [X] Aplicable después de corregir [ ] No aplicable [ ]

Apellidos y nombres del juez validador: Mg. Juan Orlando Perez Alvaro DNI: 40545360

Especialidad del validador: Ingeniero de Sistemas

24 de octubre 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 DIGITAL
Firmado digitalmente por: PEREZ ALVARO Juan Orlando FAU 20131370998 soft
Motivo: Soy el autor del documento
Fecha: 25/10/2022 09:50:56-0500

Firma del Experto Informante.

Anexo 02. Base de datos

ISO 27001																								Control de la Seguridad de Información																					
Planificación																Ejecución			Verificación				**Mejoramiento**		Disponibilidad				**Adaptabilidad**					**Accesibilidad**					Resguardo					
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	1	2	1	1	2	2	1	1	1	2	2	1	2	1	2	1	1	1	1	1
1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	2	2	1	1	2	1	1	1	2	2	1	1	2	2	1	1	2	1	1	2	1	1	1	1	1	2	2	1
1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	2	2	1	1	1	1	1	1	2	2	2	1	1	1	1	1	1	1	1	2	2	1	2	2	1	1	1	1
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	1	1	1	1	1	1	1	2	2	1	1	1	2	1	1	1	1	1	2	2	2	2	2	1	2	1	1
1	1	1	1	2	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1	1	1	1	2	1	1	1	2	1	2	1	1	1	1	1	2	1	2	1	1	1	2	2
1	1	1	2	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	1	2	2	1	1	1	1	1	2	1	1	2	1	2	1	2	2	1	1	1	1
1	1	1	2	1	1	1	1	1	1	1	1	1	1	2	1	2	1	2	2	1	1	1	1	1	2	1	1	1	1	1	1	1	1	1	2	1	2	1	1	1	1	1
1	1	1	1	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	1	2	2	2	1	2	2	1	1	1	1	1	2	2	2	2	2	1	2	1	1
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	1	2	1	2	1	1	1	1	2	1	1	1	1	1	1	1	1	2	2	1	2	1	1	1	1	1
1	1	1	1	2	2	1	1	1	1	1	2	1	1	2	1	1	2	2	1	1	2	1	2	1	1	2	1	1	1	1	1	1	1	2	2	1	2	1	1	1	1	1
1	1	1	2	1	1	1	1	1	1	1	2	1	1	1	1	1	1	1	1	1	2	1	1	2	1	2	2	2	1	1	2	1	1	1	2	1	1	1	1	1	1	1
1	1	1	2	2	1	1	1	1	1	1	1	1	1	2	1	1	1	1	1	1	1	1	2	2	1	1	1	2	1	1	1	1	1	2	2	1	2	1	1	1	1	1
1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	1	1	1	2	1	1	2	1	2	2	2	1	1	2	1	1	1	2	1	2	2	1	2	1	2	1	1	1
1	1	1	2	2	1	1	1	1	1	1	1	1	1	1	1	2	1	1	1	1	1	2	1	1	1	1	1	2	1	1	1	1	1	2	2	1	1	1	1	1	1	1
1	1	1	1	1	1	2	1	1	1	2	1	1	1	1	1	1	1	1	2	1	2	2	2	2	1	1	1	1	1	1	1	1	1	2	2	1	2	1	1	1	1	1

Anexo 03. Total de cada dimensión

16	3	5	3	6	6	6	5	7	6
17	3	5	3	7	5	5	5	7	6
16	5	5	2	5	6	6	5	7	6
17	5	5	2	5	6	6	5	7	6
17	4	5	3	5	6	6	5	7	6
18	3	4	4	5	7	7	5	7	6
18	3	5	4	4	6	6	6	8	6
18	3	4	3	5	6	6	7	7	6
18	3	7	2	4	7	7	5	8	6
20	4	4	4	5	7	7	6	8	6
18	4	5	4	6	5	5	7	8	6
20	4	6	3	5	7	7	5	8	6
17	4	5	4	6	7	7	6	8	7
19	3	4	4	5	8	8	7	8	7
17	3	5	4	7	8	8	8	7	8

Anexo 04. Declaración jurada de autenticidad de tesis

Universidad Nacional del Altiplano Puno | Vicerrectorado de Investigación | Repositorio Institucional

DECLARACIÓN JURADA DE AUTENTICIDAD DE TESIS

Por el presente documento, Yo **CESAR ADRIÁN ALAYZA TAPIA** ,identificado con DNI **70229265** en mi condición de egresado de:

☒ **Escuela Profesional,** ☐ **Programa de Segunda Especialidad,** ☐ **Programa de Maestría o Doctorado**
INGENIERÍA DE SISTEMAS

informo que he elaborado el/la ☒ **Tesis** o ☐ **Trabajo de Investigación** denominada:
" NORMA ISO 270001 Y EL CONTROL DE LA SEGURIDAD DE LA INFORMACIÓN EN BOTICAS DE LA CIUDAD DE JULIACA AÑO 2023"

Es un tema original.

Declaro que el presente trabajo de tesis es elaborado por mi persona y **no existe plagio/copia** de ninguna naturaleza, en especial de otro documento de investigación (tesis, revista, texto, congreso, o similar) presentado por persona natural o jurídica alguna ante instituciones académicas, profesionales, de investigación o similares, en el país o en el extranjero.

Dejo constancia que las citas de otros autores han sido debidamente identificadas en el trabajo de investigación, por lo que no asumiré como suyas las opiniones vertidas por terceros, ya sea de fuentes encontradas en medios escritos, digitales o Internet.

Asimismo, ratifico que soy plenamente consciente de todo el contenido de la tesis y asumo la responsabilidad de cualquier error u omisión en el documento, así como de las connotaciones éticas y legales involucradas.

En caso de incumplimiento de esta declaración, me someto a las disposiciones legales vigentes y a las sanciones correspondientes de igual forma me someto a las sanciones establecidas en las Directivas y otras normas internas, así como las que me alcancen del Código Civil y Normas Legales conexas por el incumplimiento del presente compromiso

Puno 18 de enero del 2023

FIRMA (obligatoria)

Huella

Anexo 05. Autorización para el depósito de tesis en el repositorio institucional.

Universidad Nacional del Altiplano Puno | Vicerrectorado de Investigación | Repositorio Institucional

AUTORIZACIÓN PARA EL DEPÓSITO DE TESIS O TRABAJO DE INVESTIGACIÓN EN EL REPOSITORIO INSTITUCIONAL

Por el presente documento, Yo **CESAR ADRIÁN ALAYZA TAPIA**, identificado con DNI **70229265** en mi condición de egresado de:

☒ **Escuela Profesional,** ☐ **Programa de Segunda Especialidad,** ☐ **Programa de Maestría o Doctorado**

INGENIERÍA DE SISTEMAS

informo que he elaborado el/la ☒ **Tesis** o ☐ **Trabajo de Investigación** denominada:

"NORMA ISO 27001 Y EL CONTRO DE SEGURIDAD DE LA INFORMACIÓN EN BOTICAS DELA CIUDAD DE JULIACA AÑO 2023"

para la obtención de ☐**Grado,** ☒ **Título Profesional** o ☐ **Segunda Especialidad.**

Por medio del presente documento, afirmo y garantizo ser el legítimo, único y exclusivo titular de todos los derechos de propiedad intelectual sobre los documentos arriba mencionados, las obras, los contenidos, los productos y/o las creaciones en general (en adelante, los "Contenidos") que serán incluidos en el repositorio institucional de la Universidad Nacional del Altiplano de Puno.

También, doy seguridad de que los contenidos entregados se encuentran libres de toda contraseña, restricción o medida tecnológica de protección, con la finalidad de permitir que se puedan leer, descargar, reproducir, distribuir, imprimir, buscar y enlazar los textos completos, sin limitación alguna.

Autorizo a la Universidad Nacional del Altiplano de Puno a publicar los Contenidos en el Repositorio Institucional y, en consecuencia, en el Repositorio Nacional Digital de Ciencia, Tecnología e Innovación de Acceso Abierto, sobre la base de lo establecido en la Ley N° 30035, sus normas reglamentarias, modificatorias, sustitutorias y conexas, y de acuerdo con las políticas de acceso abierto que la Universidad aplique en relación con sus Repositorios Institucionales. Autorizo expresamente toda consulta y uso de los Contenidos, por parte de cualquier persona, por el tiempo de duración de los derechos patrimoniales de autor y derechos conexos, a título gratuito y a nivel mundial.

En consecuencia, la Universidad tendrá la posibilidad de divulgar y difundir los Contenidos, de manera total o parcial, sin limitación alguna y sin derecho a pago de contraprestación, remuneración ni regalía alguna a favor mío; en los medios, canales y plataformas que la Universidad y/o el Estado de la República del Perú determinen, a nivel mundial, sin restricción geográfica alguna y de manera indefinida, pudiendo crear y/o extraer los metadatos sobre los Contenidos, e incluir los Contenidos en los índices y buscadores que estimen necesarios para promover su difusión.

Autorizo que los Contenidos sean puestos a disposición del público a través de la siguiente licencia:

Creative Commons Reconocimiento-NoComercial-CompartirIgual 4.0 Internacional. Para ver una copia de esta licencia, visita: https://creativecommons.org/licenses/by-nc-sa/4.0/

En señal de conformidad, suscribo el presente documento.

Puno 18 de enero del 2023

FIRMA (obligatoria)

Huella