UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

PROGRAMA ACADÉMICO DE MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN

ISO 27001 en la Gestión de Seguridad de la Información en el área TI en una institución pública, Lima 2023

TESIS PARA OBTENER EL GRADO ACADÉMICO :

Maestro en Ingeniería de Sistemas con mención en Tecnologías de la Información

AUTOR:

Trujillo Bailon, Flavio Cesar (orcid.org/0000-0001-8822-1120)

ASESORES:

Dr. Acuña Benites, Marlon Frank (orcid.org/0000-0001-5207-9353)

Mtro. Aliaga Cerna, Dante (orcid.org/0000-0002-5775-3885)

LÍNEA DE INVESTIGACIÓN:

Auditoria de Sistemas y Seguridad de la Información

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:

Desarrollo económico, empleo y emprendimiento

LIMA – PERÚ

2023

DEDICATORIA

El presente trabajo investigativo lo dedico a mis padres, por su amor, trabajo y sacrificio en todos estos años, por estar presente en los buenos y malos momentos. A mi pareja, durante este tiempo, has sido mi confidente, mi consejero y mi motivación. Y a todas las personas que me han acompañado, apoyado y han hecho que el trabajo se logre realizar con éxito, especialmente a aquellos que me han aportado en la formación tanto profesional y personal.

AGRADECIMIENTOS

Agradecer a Dios por guiar mi camino y brindar salud, fortaleza y capacidad. Agradecer a mis padres, por confiar y creer en mis expectativas, por los consejos, valores y principios que me han inculcado. Agradecer a mi pareja que me apoyo y brindo la fortaleza en este camino. Agradecer a nuestros docentes, por haber compartido sus conocimientos y experiencias a lo largo de la preparación de la profesión.

DECLARATORIA DE AUTENTICIDAD DEL ASESOR

UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN

Declaratoria de Autenticidad del Asesor

Yo, ACUÑA BENITES MARLON FRANK, docente de la ESCUELA DE POSGRADO MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA NORTE, asesor de Tesis titulada: "ISO 27001 en la Gestión de Seguridad de la Información en el área TI en una Institución Pública, Lima 2023", cuyo autor es TRUJILLO BAILON FLAVIO CESAR, constato que la investigación tiene un índice de similitud de 11.00%, verificable en el reporte de originalidad del programa Turnitin, el cual ha sido realizado sin filtros, ni exclusiones.

He revisado dicho reporte y concluyo que cada una de las coincidencias detectadas no constituyen plagio. A mi leal saber y entender la Tesis cumple con todas las normas para el uso de citas y referencias establecidas por la Universidad César Vallejo.

En tal sentido, asumo la responsabilidad que corresponda ante cualquier falsedad, ocultamiento u omisión tanto de los documentos como de información aportada, por lo cual me someto a lo dispuesto en las normas académicas vigentes de la Universidad César Vallejo.

LIMA, 31 de Julio del 2023

Apellidos y Nombres del Asesor:	**Firma**
ACUÑA BENITES MARLON FRANK **DNI:** 42097456 **ORCID:** 0000-0001-5207-9353	Firmado electrónicamente por: MACUNABE el 31-07-2023 22:59:54

Código documento Trilce: TRI - 0632289

INVESTIGA UCV

DECLARATORIA DE ORIGINALIDAD DEL AUTOR

UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN

Declaratoria de Originalidad del Autor

Yo, TRUJILLO BAILON FLAVIO CESAR estudiante de la ESCUELA DE POSGRADO MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA NORTE, declaro bajo juramento que todos los datos e información que acompañan la Tesis titulada: "ISO 27001 en la Gestión de Seguridad de la Información en el área TI en una Institución Pública, Lima 2023", es de mi autoría, por lo tanto, declaro que la Tesis:

1. No ha sido plagiada ni total, ni parcialmente.
2. He mencionado todas las fuentes empleadas, identificando correctamente toda cita textual o de paráfrasis proveniente de otras fuentes.
3. No ha sido publicada, ni presentada anteriormente para la obtención de otro grado académico o título profesional.
4. Los datos presentados en los resultados no han sido falseados, ni duplicados, ni copiados.

En tal sentido asumo la responsabilidad que corresponda ante cualquier falsedad, ocultamiento u omisión tanto de los documentos como de la información aportada, por lo cual me someto a lo dispuesto en las normas académicas vigentes de la Universidad César Vallejo.

Nombres y Apellidos	**Firma**
FLAVIO CESAR TRUJILLO BAILON **DNI:** 75401367 **ORCID:** 0000-0001-8822-1120	Firmado electrónicamente por: FTRUJILLOB13 el 31-07-2023 22:46:10

Código documento Trilce: TRI - 0632290

INVESTIGA UCV

Índice de Contenidos

Índice de tablas

Índice de figuras

Resumen

El objetivo de la presente investigación fue determinar la mejora con la ISO 27001 en la gestión de seguridad de la información en el área TI de la institución pública. El estudio fue de tipo básica, nivel descriptivo, tuvo un enfoque cuantitativo, de diseño no experimental, transversal y correlacional, su población y muestra fue de 50 trabajadores, se aplicó el instrumento de la encuesta como técnica y el cuestionario como instrumento de recopilación de datos. Se utilizó la herramienta de Google Forms para adquirir los resultados de la encuesta. Se realizó la prueba de confiabilidad de Alfa de Cronbach con un valor de 0.803, obteniendo un instrumento confiable. Además, se utilizó el juicio de expertos para validar ambos instrumentos y se analizó los resultados mediante tablas, gráficos, clasificación de la información, determinación de valores. En la presente investigación, se obtuvo un valor de p = 0.000 y un coeficiente de 0.882 en la prueba Rho Spearman, de donde se concluye que ISO 27001 impacta significativamente en un 88.82% Gestión de Seguridad de la Información en el área TI en una Institución Pública, Lima 2023.

Palabras Clave: Gestión de Seguridad de la Información, iso 27001, seguridad digital, ciberseguridad, protección de datos

Abstract

The objective of the present research was to determine the improvement with ISO 27001 in the management of information security in the IT area of the public institution. The study was of a basic type, descriptive level, with a quantitative approach, non-experimental, cross-sectional, and correlational design. The population and sample consisted of 50 workers. The survey instrument was applied as a technique, and the questionnaire was used as a data collection tool. Google Forms was used as the tool to acquire survey results. The reliability test of Cronbach's Alpha was conducted, yielding a value of 0.803, indicating a reliable instrument. Additionally, expert judgment was used to validate both instruments, and the results were analyzed using tables, graphs, information classification, and value determination. In the present research, a p-value of 0.000 and a coefficient of 0.882 were obtained in the Spearman's Rho test, leading to the conclusion that ISO 27001 significantly impacts 88.82% of Information Security Management in the IT area of a Public Institution, Lima 2023.

Keywords: Information Security Management, ISO 27001, Digital Security, Cybersecurity, Data Protection.

I.INTRODUCCIÓN

En la época actual, la seguridad informática es fundamental para los entes gubernamentales. Con el avance de los riesgos de seguridad en el ámbito de la ciberseguridad, el progreso de la tecnología y el aumento de volumen de información, la gestión de datos confidenciales se ha vuelto cada vez más complicada. Con el fin de asegurar el cuidado de los datos sensibles y privados de los entes y la durabilidad de los servicios públicos, es esencial aplicar un enfoque de control.

En los últimos años se ha venido desplegando la migración masiva de datos y aumento de la operación remota debido a la pandemia de Covid-19, por lo que garantizar la seguridad informática se ha tornado un panorama crítico para las organizaciones. Los especialistas en TIC se enfrentan al desafío constante de mantener a salvo los datos, dada la complejidad del proceso de gestión de información ha aumentado considerablemente. Para hacer frente a estos nuevos desafíos, las organizaciones necesitan cumplir con estándares internacionales la seguridad informática, que proporcionan técnicas, métodos y recursos para salvaguardar la integridad de los datos. (Alexei, 2021).

Asimismo, la situación de la ciberseguridad en latinoamericana el brote de COVID-19, el 49% de las organizaciones de Perú que fueron encuestadas reportaron un aumento en los ciberataques durante la pandemia. Además, el 21% de las empresas considera que el phishing o la manipulación psicológica es la táctica de ciberataque que más ha aumentado, mientras que el 20% cree que el malware ha sido el aspecto más destacado. Según estudios se registró más de 433 millones de casos de ataques cibernéticos registrados en el año 2020 y se espera el aumento del 15% en 2021. A pesar de que el 60% de las entidades peruanas encuestadas muestran intranquilidad por su volumen de respuesta ante estos ataques, solo el 20% ha aumentado su inversión en seguridad cibernética durante la pandemia, con un 51% enfocado en seguridad de conexión remota y un 44% en resguardo de datos en la nube. (Revista Economia,2021)

Asimismo, las entidades públicas se ven afectadas por amenazas de ciberseguridad. De acuerdo con el Informe Nacional de Ciberseguridad 2020 del Centro Nacional de Ciberseguridad (CNCS) del Perú, los incidentes de seguridad cibernética aumentaron en un 82% en 2019 en comparación con el año anterior. Se destaca que las organizaciones públicas son especialmente vulnerables debido a la carencia de políticas de seguridad adecuadas, el poco entendimiento de los usuarios y la carencia de recursos financieros para poner en práctica. (López et al, 2019).

Sin embargo, en Perú - Lima, la preservación de los datos de los organismos públicos, es una preocupación vital. No obstante, de contar con una normativa específico en el ámbito de la prevención de datos sensibles, como el Decreto Ministerial Nº 068-2016-JUS, muchas organizaciones públicas aún no han implementado acciones de ciberseguridad apropiadas para resguardar la información que manejan.

Seguido de explicar la situación problemática, se expone el planteamiento de la problemática en general: ¿Cómo mejorara el ISO 27001 en la gestión de seguridad de la información en las áreas de TI de la institución pública? Así cómo también se formulación tres problemas específicos siendo ellos: ¿Cómo mejorara el ISO 27001 la disponibilidad de información en la seguridad de la información en el área de TI de la institución pública?;¿Cómo mejorara el ISO 27001 la adaptabilidad de la información para la seguridad de la información en el área de TI de la institución pública?;¿Cómo el ISO 27001 en la accesibilidad de la información para la gestión de seguridad de la información en el área de TI de la institución pública?;¿Cómo el ISO 27001 en el resguardo de la información para la gestión de seguridad de la información en el área de TI de la institución pública?

El respaldo teórico de la presente investigación se toma en consideración que se busca aportar al conocimiento que existe sobre la adecuada Integridad de los datos mediante el apoyo del ISO 27001, el proceso incluirá una revisión bibliográfica exhaustiva para comprender los conceptos clave relacionados con las variables.

Asimismo, la metodología se justifica ya que la implementación exitosa en esta investigación se descubre el perfeccionamiento entre las dos variables, mediante una evaluación y los datos obtenidos.

Adicionalmente, se justifica prácticamente la investigación se sustenta de que el ISO 27001 permitirá incrementar la administración de protección de datos y la eficiencia de la organización, al mismo tiempo que se reducen los riesgos y se respalda la privacidad, fidelidad y accesibilidad de la información.

Con el motivo de afrontar la problemática previamente referida fue establecido como objetivo fundamental: Determinar el ISO 27001 mejora en la gestión de seguridad de la información en el área TI de la institución pública. De igual manera, se definen cuatro objetivos específicos, siendo ellos: Determinar cómo mejora el ISO 27001 la disponibilidad de información en la seguridad de la información en el área de TI de la institución pública; Determinar cómo mejora el ISO 27001 la adaptabilidad de la información para la seguridad de la información en el área de TI de la institución pública; Determinar cómo mejora el ISO 27001 en la accesibilidad de la información para la gestión de seguridad de la información en el área de TI de la institución pública; Determinar cómo mejora el ISO 27001 en el resguardo de la información para la gestión de seguridad de la información en el área de TI de la institución pública.

Finalmente, la hipótesis general de la investigación fue: El ISO 27001 mejora significativamente la gestión de seguridad de la información en el área TI de la institución pública. Las hipótesis especificas fueron: El ISO 27001 mejora significativamente la disponibilidad de la información para la gestión seguridad de la información en el área de TI de la institución pública; El ISO 27001 mejora significativamente la adaptabilidad de la información para la gestión seguridad de la información en el área de TI de la institución pública; El ISO 27001 mejora significativamente la accesibilidad de la información para la gestión seguridad de la información en el área de TI de la institución pública.

II. MARCO TEÓRICO

Investigaciones previas en el ámbito nacional, según Díaz (2021) indica que esta investigación examina la incorporación de la norma ISO 27001:2014 en instituciones gubernamentales en el Perú. La problemática es ataques informáticos cada vez más sofisticadas. La metodología utilizada fue el enfoque cuantitativo con una muestra de 76 servidores públicos, donde se encontró que alrededor del 50% percibe que la incorporación de la norma. Esta investigación destaca la importancia de ciberseguridad en las entidades, especialmente en un contexto de amenazas cada vez más sofisticadas.

También Vega et al. (2022) mencionan que el estándar ISO 27001:2013 prioriza la seguridad como un concepto integral, la problemática fue afectado por los ciberataques e incluso, mediante el estudio virtual, donde la información se podría perder si no se fija correctamente una gestión de seguridad. La metodología utilizada es prisma, la población fue un 59,1% lo realizó exitosamente. Se concluye que fue gran ayuda porque permitió identificar si la información es segura, pudiendo analizar qué controles cumple y cuáles no, y por último en qué grado se encuentra.

Según Bustamante et al. (2021), la implementación de lineamientos basadas en la normativa ISO mejora notablemente la administración de la seguridad digital al controlar los procesos de seguridad y la integridad. El estudio se enfocó en abordar los mecanismos deficientes. La herramienta es técnica de observación y entrevista. La población consistió en 90 trabajadores. Los resultados en porcentaje 90%. En conclusión, el estudio logró mejorar a dirección de la seguridad informática, destacando los elementos clave fundamentales de preservación, integridad y disponibilidad.

De acuerdo a las palabras de Lugo et al. (2020), nos dicen que los SGSI establecidos de la ISO 27001 el enfoque asegura la privacidad, veracidad y accesibilidad de la información, sin importar su forma de almacenamiento. La herramienta del estudio documental y descriptiva con un abordaje cuantitativo y cualitativo. La población del estudio 80 empresa. Se identificó un promedio al 39%.

Se concluye que las empresas participantes mostraron poco interés en aprovechar la información como fuente de ventaja competitiva y no se encuentran interesados.

En palabras de Atencio (2019), menciona que las instituciones enfrentan riesgos y amenazas para su información debido al aumento de hackers maliciosos y usuarios internos considerados de alto riesgo. Estos factores afectan Facilitar la transferencia directa de datos mediante la red informática. El enfoque metodológico fue descriptivo y transversal. Se utilizo la ficha de observación. La población 50 instituciones. Los resultados en porcentaje 90,0%. Se concluyó que la resolución de la inseguridad informática no se limita a identificar los servicios de seguridad a proteger.

Asimismo, García, et al (2018) expresan que la incorporación de sistemas de información está aumentando en las empresas. El costo del impacto del riesgo se ha vuelto más elevado debido a la carencia de una gestión apropiada de las vulnerabilidades. Con el fin de encontrar una solución práctica a un problema de administración de tecnología de la información (TI), es vital llevar a cabo un diseño formal y un proceso de evaluación que garantice la calidad de la solución. El estudio se respalda con el enfoque cualitativo y utiliza técnicas de evaluación y recopilación de información. El resultado de la implementación del modelo en una evaluación de caso en una pequeña y mediana compañía del sector de arcilla y cerámica indican una reducción del 53% en el nivel de riesgos. En conclusión, se demostró que el modelo es fácil de usar y permite identificar los controles necesarios para mitigar el riesgo, cuya implementación es crucial.

Por otro lado, Niño (2018), indica que los sistemas de información enfrentan riesgos y amenazas tanto internas como externas, lo cual plantea un problema. La información se considera un valioso activo para el buen funcionamiento de una organización. La investigación tiene un enfoque descriptivo y transversal, y se utiliza la encuesta como método para recopilar información a 60 usuarios. Se encontró que el 64% de porcentaje. Como conclusión, se observó un alto grado de acuerdo en establecer procedimientos para minimizar el impacto y garantizar la continuidad en relación a la seguridad de los activos críticos.

Tal como menciona Rincón (2019), el estudio de su principal ejecución y auditoría del ISO 27001 en una universidad. Se utilizaron diversas etapas metodológicas, como el Diagnóstico de la realidad actual, detectar amenazas, la instalación de los controles de protección, y la ejecución de revisiones externas e internas. Los resultados mostraron 28 riesgos, la implementación de 51 controles de resguardo, y revisiones internas y externas con altos índices de conformidad 95%. En conclusión, la implementación fue exitosa, logrando establecer un marco de seguridad informática y la mejora de administración de riesgos en la organización.

Por otro lado, los antecedentes intencionales, Mohammed & Jasim (2022) el texto aborda la problemática del gobierno de la información documentada de la empresa de exploración petrolera en Irak y cómo incrementar la ciberseguridad en la empresa. Su enfoque es cualitativo y mediante encuesta fue la recolección de datos. La exploración de datos fue de 321 empresa de exploración petrolera en Irak que se analizó en el estudio. Los resultados en porcentaje 64%. Como conclusión, se enfatiza la prioridad de potenciar el gobierno de la información documentada de la empresa dando valor de poner en práctica medidas de proteger la integridad de los datos corporativos.

Según Ferreira et al. (2018), el estudio aborda la necesidad de comprender y adoptar prácticas efectivas de la administración de seguridad. La problemática es detectar factores que impactan la comprensión de prácticas de administración de ciberseguridad entre los Agentes del Gobierno pertenecientes a la Junta de Tecnología de la Información de la Fuerza Aérea Brasileña. La metodología utilizada es cuantitativa, de naturaleza exploratoria y descriptiva. Se emplea un cuestionario para recopilar datos. La población 256 de profesionales. Los resultados 78,3%. Se concluyó el estudio es que la comprensión y adopción de prácticas de administración de seguridad, así como por las percepciones de la facilidad de uso y utilidad de los protocolos de seguridad de la información.

Tal como menciona Qusef & Alkilani (2022) señala estudio tenía como objetivo evaluar si las redes sociales y la inteligencia de código abierto (OSINT)

eran efectivas para ayudar a los investigadores digitales. La metodología del estudio cuantitativo. La herramienta utilizada en este estudio fue una encuesta. La población encuestas a los participantes y se examinaron los perfiles de los usuarios de LinkedIn. Resultados en porcentaje el 89% de los participantes estuvo de acuerdo en que el conocimiento obtenido de las redes sociales era útil para la investigación digital, mientras que solo el 56% estuvo de acuerdo en que la información adquirida a través de las redes de inteligencia de código abierto era valiosa.

En palabras de Hannigan et al (2019), la idea principal del estudio es insertar un sistema integrado de gestión en Qatar Biobank (QBB), combinando los estándares ISO 9001:2015 e ISO 27001:2013, con el fin de mejorar la dirección de la organización. El estudio es cuantitativo para la recolección de datos fueron encuesta. La población del estudio 145. Los resultados 95%. En conclusión, la integración del sistema de gestión en QBB, combinando los estándares ISO 9001:2015 e ISO 27001, ha perfeccionado la gestión de la organización, impactando positivamente en la experiencia de los usuarios y los hallazgos de las auditorías internas.

Tal como menciona Chen et al. (2022), se destaca la importancia del comportamiento de seguridad informática de los empleados de las organizaciones. En estudio utilizó un método cuasiexperimental de campo, donde se recopilaron datos de 217 empleados de tres empresas chinas. Se utilizaron cuestionarios de medición de estrés. Los resultados en porcentaje 58%. En conclusión, este estudio amplía el conocimiento sobre el estrés desafiante en el contexto de ciberdefensa y positivas en el cumplimiento los estándares de seguridad.

En su estudio Bai (2022), la seguridad informática es un desafío para la tecnología de la información, especialmente debido a las nuevas amenazas generadas por la tecnología de big data. La problemática es la necesidad de introducir un sistema de operación y verificación en tiempo instantáneo para asegurar la seguridad de datos en la red. El enfoque es cuantitativo la estrategia utilizada para recopilar datos es el cuestionario. La población de 80 personas. El

resultado en porcentaje 64%. En conclusión, se destaca lo importante de abordar la seguridad informática para TI, proponiendo soluciones como un uso de sistemas empotrados y el aumento de las leyes de seguridad informática.

Según Prislan et al. (2020), medir el rendimiento de la seguridad informática es un desafío para las empresas debido a su complejidad. Se utilizó el modelo ISP 10x10M. Su enfoque multidimensional socio-técnico para medir el rendimiento del SGSI. Los resultados en porcentaje es 69% Se concluye que las empresas medianas de Eslovenia tienen ciertas capacidades en seguridad de la información y reconocen su importancia, sus prácticas actuales dificultan mantenerse al día con las tendencias tecnológicas y de seguridad.

Para Zhao et al (2019), menciona los inconvenientes de la seguridad informática en los parques inteligentes incluyen el acceso confuso de las personas, la ausencia de gestión de seguridad, el flujo desordenado de datos y la insuficiente recopilación de pruebas de auditoría, entre otros. En su estudio cuantitativo, la metodología es observación. La población fue 125.Los resultados es 94%. Se concluye que aborda los inconvenientes de la seguridad informática en los parques inteligentes, permitiendo un control más preciso del movimiento de personal en diferentes áreas del parque.

En palabras de Chen et al (2021), a pesar de que la investigación sobre la estructura y el formato de los sistemas de información médica es cada vez más madura, la integración entre ellos sigue siendo insuficiente, lo que dificulta la movilidad de los registros médicos y la recopilación de información. La situación problema se plantea en el estudio un sistema centralizado de información médica con políticas de seguridad y protección de privacidad. El enfoque es cuantitativo la metodología fue encuesta. La población fue 365 personas. Los resultados en porcentaje 75%. Se concluye puede aumentar la prestación de servicios de salud al integrar registros electrónicos.

Asimismo, Tanović & Marjanovic (2019), el estudio compara los estándares internacionales ISO 20000-1:2011 e ISO 27001:2013 en un entorno real de un

servicio de IPTV/VoIP de un operador de telecomunicaciones en Bosnia y Herzegovina. Enfoque cuantitativo método de encuesta. La población de 354 obtuvo un resultado insatisfactorio del 65% en las mediciones, mientras que los procesos dentro de ISO 27001:2013 alcanzaron un éxito del 98.50%, lo cual es significativo y positivo. Se concluye que el estudio logró crear un nuevo modelo mejorado de ISO 20000-1:2011 basado en las recomendaciones y actividades clave de ISO 27001:2013.

De acuerdo con Monev (2020), existe una falta de metodología técnica para evaluar la madurez de la seguridad informática en organizaciones que utilizan una administración basada en estándar ISO 27001. El estudio propone una metodología práctica que utiliza un enfoque comparable. La metodología utiliza una herramienta de evaluación para analizar la madurez de las medidas de seguridad y las cláusulas. La población del estudio es 140 profesionales. Resultados en porcentaje de madurez del 56.6% en formato de escala de 0 a 5. Se concluye que la metodología propuesta ofrece a los profesionales de seguridad y cumplimiento una forma práctica de realizar evaluaciones de madurez de la seguridad informática en base en la norma ISO 27001.

Como menciona Velasco et al (2018), destacan que, en la industria manufacturera, la gran cantidad de información y la escasa seguridad en los procesos críticos representan un riesgo para el desempeño de la empresa. La investigación es metodologías de Deming (PDCA) y la gestión de riesgos (Magerit). La población es 105 empresa manufacturera Imptek-Chova en Ecuador, líder en el mercado de cubiertas ajardinadas en la región. Resultado en porcentaje en 98%. Se concluye que es necesario implementar un SGSI en la industria manufacturera y se sugiere utilizar enfoques como el ciclo PDCA y Magerit II para gestionar los riesgos.

Desde la perspectiva de Ari et al. (2018), comparan los marcos de ciberseguridad y debatieron las ventajas y desventajas. El estudio utiliza una metodología de revisión de literatura y comparación entre los dos marcos. Las herramientas aplicadas son cuantitativas con encuestas. La población 69. Los

resultados en porcentaje 58%. La conclusión menciona que recomienda por las mejores prácticas de SGSI.

En su estudio Maingak et al. (2018) indican que la problemática que perjudica los procesos empresariales de una organización. El enfoque es cuantitativo. Se utiliza una metodología es observación. La población 174. Los resultados porcentajes 43,86%. Se concluye que ISO/IEC 27001:2013 es un recurso útil para evaluar la madurez de la administración de seguridad informática.

También Agustino (2018), expresa que el estudio se enfoca en la brecha entre el nivel de resguardo de la información de una entidad gubernamental específica y las políticas estándares del ISO 27001.El estudio es cuantitativo. La población es 114 controles, la entidad gubernamental aplicó solo 64, lo que representa el 56,14% de los controles. El estudio concluye que la organización gubernamental evaluada no se ajusta a los estándares de la seguridad informática establecidos en la norma.

Asimismo, Thoyyibah (2018) indica que es fundamental la seguridad informática para la continuidad operativa de una organización, especialmente en la era digital en la que nos encontramos. La problemática de la seguridad de informática que adopten medidas efectivas para la ciberseguridad informática. En este estudio es correlacional. La recolección de datos es encuesta. La población del estudio fue de 10 personas. Los resultados en porcentaje 35%. El estudio concluyó que la necesidad de implementar mejoras en SGSI en la universidad.

Basándonos en las conclusiones de Lopes et al. (2019) expresa que la problemática es evaluar la ciberseguridad en un sistema de información académico en una universidad en Indonesia. Metodología del estudio la evaluación se realizó utilizando la herramienta Indeks KAMI. Para la obtención de datos se realizó mediante cuestionarios y entrevistas al personal. Población del estudio 577. Resultados en porcentaje 60%. Se concluye que los sistemas informáticos académico de la institución educativa evaluada satisface con los estándares de

seguridad establecidos en ISO 27001:2013 y que se necesita una documentación clara y pruebas y monitoreo continuos para estar estable en la seguridad.

Partiendo de la premisa de Prasetyowati et al. (2019) Indican que el estudio analiza si la integración del ISO 27001 puede ser una herramienta útil para que las organizaciones cumplan con la privacidad de datos personales. El estudio es de naturaleza exploratoria y utiliza un enfoque cuantitativo. La herramienta utilizada para analizar los sitios web de las organizaciones fue la observación directa. La población 15 organizaciones. Resultados en porcentaje analizadas, el 60% mencionó que ISO 27001 identifica los datos personales como un activo de seguridad informática. Se concluyo que la norma ISO 27001 puede ser una herramienta útil para que las organizaciones cumplan con los requisitos ciberseguridad.

En el marco de Husaeni et al. (2019) señala que la problemática es la medición del nivel de madurez en la administración de activos del Laboratorio de Computación de la Universidad Singaperbangsa Karawang. Es investigación descriptiva. Se utilizaron cuestionarios. La población del estudio se compone de los 65 usuarios del Laboratorio. Los resultados mostraron un 48%. El estudio concluyó que la universida no cumple con los estándares de gestión de activos establecidos en el marco ISO/IEC 27001.

Tomando como referencia a Handayani et al. (2019) señala que el estudio se enfocó en detectar los inconvenientes de ciberseguridad en el sistema informático de la Universidad. El estudio utilizó el procedimiento FMEA. La población 85, resultados en porcentaje el 68%. El estudio concluye que el sistema informático de la SIFT UNDIP es fundamental para minimizar los riesgos y avalar el progreso de las operaciones.

En palabras de Di et al. (2022) señala que la problemática abarcada en esta investigación es la planificación de seguridad en las empresas durante su proceso de transformación digital. La metodología es algoritmo genético. La herramienta aplicada en este estudio es el algoritmo genético, específicamente un algoritmo

genético mejorado que tiene como objetivo superar las limitaciones del algoritmo genético tradicional. Se concluyo que la organización la ciberseguridad en las empresas es de gran importancia en el contexto del desarrollo económico actual, y que el algoritmo genético es una herramienta útil para la optimización de esta estructura.

También Peikari et al. (2018) señala que el estudio se enfoca en la deficiencia de ciberdefensas en hospitales y cómo afecta la percepción de los pacientes. El estudio utilizó una metodología cuantitativa. Se utilizó para analizar los datos recopilados a través de encuestas. La población del estudio consistió en pacientes que habían visitado hospitales en Turquía durante el año 2017. El resultado en porcentaje 45,7%. El estudio concluye que la capacitación del personal, la protección técnica, la supervisión de los empleados, la ética del personal y la confianza de los pacientes en los hospitales son importantes.

Tal como menciona Kim y Kim (2021) mencionan que el estudio analiza los factores que afectan la intención y el fortalecimiento de la SGSI en las empresas. El estudio utilizó un modelo TOE (Tecnología, Organización y Entorno) y un formulario virtual para obtener respuestas de los trabajadores. La población fue 107 trabajadores. Resultados en porcentaje 58%. Se concluye el estudio que es importante el SGSI para fortalecimiento de la empresa.

Para Jelovčan et al. (2022) señala que la problemática abordada en este estudio fue la elección entre gestionar internamente o externalizar los servicios de seguridad informática en las organizaciones. La investigación utilizó el método de análisis jerárquico. También se empleó una encuesta en línea para la adquisición de información. La población del estudio fueron 37 profesionales. Los resultados en porcentaje 43%. Se concluyo que la herramienta de análisis jerárquico resultó ser efectiva en la decisión para la elección entre gestión interna o externalización de los servicios de seguridad informática en las organizaciones.

También Yang & Wang (2022) indican que la problemática es la ciberseguridad de los estudiantes y la necesidad de implementar tecnologías de

seguridad de datos confiables en los SGIS en estudiantes. El enfoque es cuantitativo. Herramienta aplicada recopilaron datos de encuesta. La población fue un modelo de datos académicos comunes para ambas pruebas de seguridad. Resultado en porcentaje del 87%. El estudio concluye que blockchain technology tiene un efecto positivo en la SGIS en estudiantes y puede ser un recurso valioso para mejorar la protección de datos en sistemas similares.

Asimismo, Sikman et al. (2022) mencionan que la problemática de evaluación de la ciberseguridad de las universidades en relación con el estándar ISO 27001.Metodología del estudio se utilizó un sistema experto. Herramienta aplicada se utilizó un sistema experto difuso implementado en MATLAB. La población fue varias universidades y se ha comprobado que el sistema evalúa correctamente, pero estas universidades no deben ser nombrado públicamente, el porcentaje fue de 70%. El estudio concluye que los SGSI de las universidades es una técnica útil y efectiva que puede ayudar a mejorar la seguridad.

En su estudio Chu y So (2020) mencionan que la problemática del estudio busca analizar y medir cuatro tipos de comportamiento no ético de la seguridad informática en el lugar de trabajo: mal comportamiento en redes/aplicativos, uso peligroso de la web, comportamiento de seguridad omiso y control de acceso deficiente. El enfoque es cuantitativo. El estudio utiliza un cuestionario en línea para la recopilación de datos. La población del estudio son 496 empleados de empresas en Taiwán. El resultado en porcentaje 41,9%. Se concluye los resultados ayudarán a los gerentes a entender las diferentes manifestaciones de este comportamiento y desarrollar mejores estrategias de seguridad.

Como menciona Tanadi et al. (2021) que es fundamental para salvaguardar los activos de información. Sin embargo, las entidades a menudo enfrentan desafíos en la implementación y mantenimiento de estos sistemas, lo que puede llevar a vulnerabilidades y riesgos de seguridad. El estudio utiliza una muestra de 578. Herramienta aplicada utiliza el análisis de regresión Logit y STATA 14 para analizar los datos. La población es 578. Resultados en porcentaje tienen una

influencia significativa al 5%. Se concluye que la ejecución de SGSI, como ISO 27001, es crítica para cuidar los activos de información de las entidades.

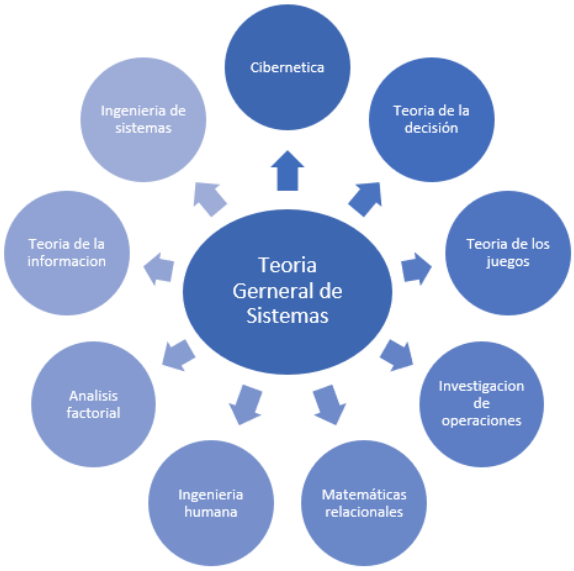
Asimismo, Ključnikov et al. (2019) mencionan la problemática es en identificar los factores de éxito en el control de ciberseguridad en organizaciones de escala pequeña y mediana. El método es evaluación de expertos estructurados para recopilar datos. Luego, aplicaron la técnica DEMATEL para analizar la importancia relativa y las interconexiones entre los factores. La población de estudio fue 88. Resultados en porcentaje 53 %. Se concluyó el estudio que la clave para el éxito de la ciberseguridad en organizaciones chica y intermedia en Eslovaquia son los controles de seguridad.

En su investigación Safonova & Kotelnikov (2020) indican que problemática es debido a los peligros inherentes a la confidencialidad de datos, sensibles y la urgencia de cumplir con regulaciones legales y corporativas, se presentan los procesos y procedimientos recomendados por la ISO 27001 para la implementación. Enfoque cuantitativo, la obtención de información mediante encuestas. La población específica del estudio está dirigido a organizaciones del sector médico que manejan datos sensibles y buscan mejorar su control en la seguridad informática que su porcentaje fue de un 56%. Se deduce que la introducción de un estándar de seguridad es un proceso complejo pero necesario para las organizaciones del sector médico que manejan datos sensibles.

Asimismo, en el enfoque de sistemas, según Bertalanffy (1976) indica que el enfoque principal es la teoría sistémica en su totalidad, es proporcionar la estructura conceptual para entender sistemas complejos en diversos campos. La teoría se centra en la idea de que los sistemas son entidades complejas compuestas por partes interconectadas e interdependientes que interactúan para lograr objetivos comunes. En lugar de analizar las partes de un sistema de manera aislada, la teoría se enfoca en el estudio de los esquemas y nuevos procesos tendencias que surgen de los vínculos entre las partes del sistema. Se aplica en campos como la biología, la sociología y la ingeniería y se ha transformado en un método crucial para el pensamiento sistémico y la gestión de sistemas complejos (Figura 1).

Figura 1

Campos de la teoría general de sistemas

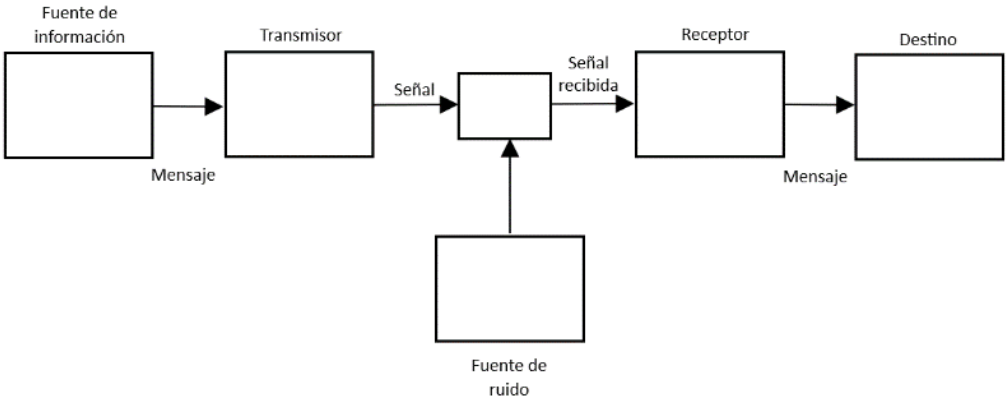


Fuente: *Bertalanffy (1976).*

Por otro lado, tenemos otro enfoque de la información, según Shannon & Weaver (1964) menciona que consistió en crear una teoría matemática rigurosa que pudiera ser aplicada a cualquier tipo de información. Para lograrlo desarrollar un modelo formal de comunicación utilizando conceptos matemáticos y cuantificando la información contenida en una señal y la capacidad de un canal de comunicación para transmitirla. Este enfoque estableció principios de la teoría de la información moderna y ha tenido una gran influencia en campos como la ingeniería de la comunicación, la informática y en la teoría de la complejidad. El sistema de comunicación considerado puede representarse simbólicamente (Figura 2).

Figura 2

Demostración simbólicamente de comunicación.

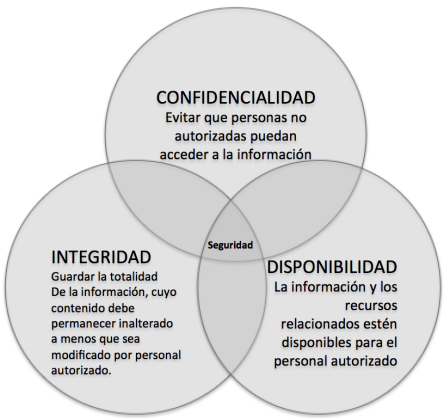


Fuente: *Shannon & Weaver (1964)*

Como teoría general para la presenta investigación se consideró: La seguridad informática, según Figueroa et al. (2018) mencionan que la integridad informática es una especialidad que se enfoca en garantizar y salvaguardar dicha información contra riesgos y amenazas. Su objetivo es preserva la privacidad, inviolabilidad y acceso a los datos. Esto se logra mediante la implementación de políticas, estándares y buenas prácticas que establecen medidas de protección adecuadas (Figura 3).

Figura 3

La seguridad informática se basa en tres pilares.



Fuente: *Figueroa et al. (2018)*

Como teoría específica para la presenta investigación se consideró: Gestión de Riesgos, Normas técnicas ISO, según Bailon (2019) menciona que la administración de riesgos con la finalidad de minimizar la probabilidad de que ocurran eventos adversos o negativos, a través de la detección, análisis, corrección, monitoreo y supervisión de los riesgos.

Asimismo, Vela et al. (2019) nos menciona que los lineamientos ISO, la infraestructura y los servicios de TI incluyen aspectos como el alcance, los límites, las partes interesadas, el tipo de TI, la comunicación y el tipo de organización. Por ello, es crucial su ejecución en entidades enfocadas en tecnología de la información.

Según Bailon (2019) indica que ISO 27001, se creó con la intención de validar la elección de salvaguardas la ciberseguridad adecuada para cuidar los bienes de información relacionados. Este estándar puede utilizarse en diversos tipos de instituciones, incluyendo negocios comerciales, entidades del gobierno y organizaciones no gubernamentales. La normativa expone las exigencias para la elaboración, aplicación, ejecución, vigilancia, inspección, preservación y refinamiento de la ciberseguridad.

Las dimensiones de este estudio se subdividen en Planificación, Implementación, Verificación y Mejora Continua. La fase de planificación implica la comprensión y tratamiento de los variados elementos asociados a la organización, como la delimitación de la relevancia del SGSI, asignación de roles y obligaciones para la seguridad informática, trazado del plan de control de riesgos, revisión de documentación y la estructuración organizativa para determinar una serie coherente de acciones y prevenir amenazas potenciales (Cardona y Restrepo, 2020). Por otra parte, la fase de implementación se centra en las tareas relacionadas con efectuar evaluaciones y gestión de vulnerabilidades. De igual manera, con la aplicación del estándar ISO 27001, se percibe un avance en la puesta en marcha del control de seguridad informática, basándose en los criterios establecidos (Vergara, 2019). En este sentido, la verificación supone la revisión y el estudio de los fines de la Institución. Además, señala la necesidad de evaluación

constante y validación de los componentes para asegurar el cumplimiento de ciberseguridad (Cardona y Restrepo, 2020). Finalmente, la mejora continua se refiere a las exigencias requeridas para efectuar ajustes que permitan un avance innovador. Es decir, es crucial corregir deficiencias y propender a su mejora constante para el adecuado desarrollo (Córdova, 2021).

Adicionalmente, la variable dependiente mencionada por Atención (2019), se enfatiza y menciona la administración de ciberseguridad. Apoya el establecimiento de políticas, procesos y controles en función de los propósitos empresariales de la Institución, con el objetivo de sostener la incertidumbre siempre inferior del nivel tolerable por el propio ente. En resumen, la institución adquiere conocimiento sobre los peligros a los cuales se expone la información y los maneja a través de un enfoque sistemático que está claramente definido, documentado y comprendido por todos, que se revisa y perfecciona de manera constante.

Las dimensiones de este análisis incluyen Disponibilidad, Flexibilidad, Acceso y Protección. La disponibilidad alude a la habilidad de los recursos para acceder a la información, para aquellos que estén autorizados y posean la competencia para gestionarla. Es esencial que el personal asignado tenga la formación necesaria para prevenir fallos en la entidad (Mejía, 2020). Por otro lado, la flexibilidad se asocia con la habilidad de la información para incorporar nuevas alternativas y disponer del espacio apropiado para almacenarla, asegurando su protección en caso de ser amenazada (Mejía, 2020). De igual manera, el acceso se fundamenta en el periodo de respuesta al que está sujeta los datos, el cual es instantáneo y estable incluso ante un aumento considerable de la cantidad de datos. (Mejía,2020). La protección abarca lo repetido, competencia, beneficio y ambiente en que se debe hacer un respaldo de datos. Igualmente, poseer con una protección completa datos sería un soporte vital, ya que evitaría la pérdida parcial o total de contenido restringido (Mejía, 2020).

III. METODOLOGÍA

3.1Tipo, enfoque y diseño de investigación

Tipo de investigación

En esta pesquisa, se ejecutó la investigación básica. Por ello, Patel et al. (2019) aclaran que este tipo de investigación tiene como propósito ampliar la sabiduría. Se lleva a cabo con el objetivo de descubrir eventos inexplicables, está centrada en las normas universales y en la formulación de nuevas teorías. Aunque posiblemente genere respuestas o resultados al inconveniente actual, contribuye a la investigación científica con nuevos conocimientos.

Enfoque

En la averiguación en desarrollo se caracteriza por ser cuantitativa, dado que las variables deben ser medibles y observable. Además, El proceso se desarrolla desde lo amplio hacia lo específico, lo cual posibilita desglosar las variables de acuerdo a las dimensiones analizadas (Arias, 2021).

Diseño

Este trabajo de investigación tiene carácter no experimental por motivo a la ausencia de manipulación en el presente estudio, además es tipo transversal debido a que se realizó en un solo momento. (Ordoñez et al. 2018).

3.2 Variables y operacionalización

Variable independiente

ISO 27001

Definición conceptual

Tomando en cuenta la postura como un manual de optimo procedimientos para la creación e insertar los procesos que determinarán la ciberseguridad frente a diversos riesgos. Por ello, su aplicación permitirá asegurar el equilibrio, pugnacidad y presencia oportuna en el ámbito de las corporaciones (Silva et al, 2019).

Definición operacional

Se trata de la aplicación de los conceptos vinculados de defensa cibernética en interacción con la institución, dado que a partir de esto se desarrollará una estrategia operativa destinado a la asesoría personalizada.

Indicadores

Asimismo, Silva et al. (2019) el esquema del estándar ISO 27001 comprende 10 cláusulas, dentro de las cláusulas del 5 al 10 tienen dimensiones asociadas.

Variable dependiente

Gestión de Seguridad de la Información

Definición conceptual

La finalidad es resguardar todos los bienes que incluyan datos empresariales, contemplando sistemas, aplicaciones de software, infraestructura física, datos y equipos. Para asegurar y reducir consumos frente a posibles pérdidas originados por algún riesgo, es necesario implementar políticas y estrategias de ciberseguridad (Silva et al., 2019).

Definición operacional:

Se refiere al resguardo de datos, a través de las mejores prácticas definidas por diversas metodologías o estándares ya establecidos en el ámbito de cuidar y salvaguardar datos.

Indicadores:

De acuerdo con Mejía (2020), fundamenta en la dimensión de disponibilidad, flexibilidad, accesibilidad y resguardo, las cuales poseen atributos que permiten su cuantificación.

3.3 Población, muestra y muestreo

Población

En palabras de Arias (2021), define mediante la agrupación, limitada o ilimitada, de sujetos con cualidades similares. La población consiste en un grupo de 50 empleados que desempeñan sus labores en la entidad pública.

Muestra

De acuerdo con Arias (2021), si una muestra (N) es pequeña o limitada, se puede abordar en su totalidad en el muestreo. De este modo, considerando que la población se compone de 50 empleados, se contempla la totalidad de estos individuos para la muestra.

Muestreo

Según Arias (2021), se entiende como una técnica que facilita el análisis de la muestra. Su distribución puede ser probabilística o no probabilística. Este estudio en particular emplea una técnica probabilístico aleatorio simple de muestreo utilizada en estadísticas y ciencias sociales para seleccionar una muestra representativa de una población más amplia

3.4 Técnicas e instrumentos

Técnicas

La recopilación de información se realizará por medio de la metodología conocida como encuesta, utilizando elementos de cada dimensión para generar preguntas, que serán parte de los cuestionarios diseñados para evaluar la variable.

Instrumento

La técnica de encuesta facilita la acumulación de datos al entrevistar a los participantes con el propósito de recabar datos necesarios para un estudio. Según Arias (2021), dicha técnica es a menudo aplicada en el contexto académico de las ciencias sociales, y con el paso del tiempo ha cobrado relevancia en el estudio científico. En consecuencia, es notable subrayar que para alcanzar resultados

basados en fenómenos visibles que el investigador prevé, obtenidos respaldándo en los indicadores especificados para cada dimensión de la variable en estudio.

Validez y confiabilidad

En el estudio Arias (2021), menciona que un instrumento se valida al ser capaz de cuantificar el valor de la variable, y la confiabilidad del instrumento puede evaluarse mediante el proceso de validación. En el marco de esta investigación, se ejecutó la comprobación de la validez del instrumento para cada variable, respaldada por los juicios de tres expertos.

En el presente estudio, se percibe como fiable la herramienta utilizada dado que los tres especialistas convergen en un resultado similar, además se reafirmará esta fiabilidad a través de la valoración en el programa de análisis estadístico SPSS.

3.5 Procedimientos

Se comienza el proceso recolectando los datos de los expertos de la entidad, incluyendo auditores, líderes y personal administrativo de la entidad pública, a quienes se les explican los objetivos que se buscan alcanzar con la investigación. Se detallan las dimensiones e indicadores utilizados con cada una de las variables identificada y cómo se vinculan con el tema principal de mejorar la seguridad informática. Una vez obtenida la aprobación de los líderes, se planifican las actividades a llevar a cabo, se seleccionan las herramientas para la captura de datos y se elige la herramienta de software para tratar los datos obtenidos. Posteriormente, se formulan las metas de la investigación y revisan las fuentes de investigación que respaldarán el estudio. Después aceptación de especialistas se realiza una encuesta en línea entre los especialistas, empleando técnicas para medir las variables, teniendo en cuenta todos los datos recabados ingresados en sistema estadístico SPSS 25 para su posterior tratamiento estadístico. En última instancia, se procede a interpretar los datos obtenidos y a partir de ellos se elaboran los cuadros para explicar y evaluar las hipótesis propuestas en el estudio.

3.6 Método de análisis de datos

Las herramientas empleadas durante la indagación se obtuvieron validadas mediante la evaluación de los expertos para corroborar su fiabilidad. Por ello, para confirmar si el instrumento es consistente y digno de confianza, se calculó el Alfa de Cronbach (Toro, 2022).

El coeficiente Alfa de Cronbach aceptable como mínimo es de 0,7; por debajo de este valor, la consistencia interna del instrumento utilizado es escasa (Toro, 2022). La investigación en curso adopta un enfoque cuantitativo, utilizando herramientas para recolectar datos y determinar la corroboración de la veracidad de las hipótesis concretas de cada indicador. (Wang et al., 2019).

De acuerdo a Arias (2021), la credibilidad se refiere a su estabilidad con la que un mismo objeto medido produce resultados idénticos. Villavicencio et al (2019) lo definen como la habilidad para replicar una medida en condiciones similares. En la investigación en curso, el instrumento usado es considerado fiable dado que los 03 expertos convergen en un resultado similar. La confirmación de esta confiabilidad se realizará con la ayuda del análisis del Alfa de Cronbach, empleando el software estadístico SPSS 25.

3.7 Aspectos éticos

Este estudio es de mi auditoria, dado que el procedimiento de obtención, análisis e interpretación de resultados fue llevado a cabo desde mi punto de vista y análisis. Las fuentes citadas empleadas en la investigación se citan conforme a los estándares de APA 7ma Edición. Adicionalmente, este estudio de tesis es evaluada con el software Turnitin, para la originalidad basado en la Resolución N° 008-2017-VI de la UCV. Finalmente, se emplearon encuestas para obtener datos mediante un cuestionario dirigido a expertos del área de la entidad pública con el código Nº 0200-2018 de la UCV.

IV. RESULTADOS

Análisis descriptivo

El análisis descriptivo se centra en el análisis de los acontecimientos importantes, presentes en las estadísticas disponibles y en la observación de situaciones que puedan generar nuevos hallazgos. Este enfoque se sustenta en una o varias interrogantes del estudio. Luego se organizan, se presentan en forma de tablas y se describen los resultados obtenidos.

Tabla 1

Frecuencia variable 1: ISO 27001

		Frecuencia	%	% válido	% acumulado
Válido	Nunca	2	4,0	4,0	4,0
	Casi Nunca	1	2,0	2,0	6,0
	A veces	10	20,0	20,0	26,0
	Casi Siempre	13	26,0	26,0	52,0
	Siempre	24	48,0	48,0	100,0
	Total	50	100,0	100,0	

Se analizaron los datos recopilados a través de una encuesta en línea y los resultados se presentaron de manera visual mediante la tabla 1 y figura 4, se manifiesta que 24 participantes del área TI simboliza el 48,00% tiene un nivel de siempre, a su vez, 13 colaboradores que representa el 26,00% tiene un nivel de casi siempre, asimismo 10 colaboradores que representa un 20,0% tiene un nivel de a veces, otro 1 un colaborador que representa el 2,00% tiene un nivel de casi nunca y 2 colaboradores que representa el 4,00% tiene un nivel de nunca.

Figura 4

Gráfico de columnas de variable 1: ISO 27001

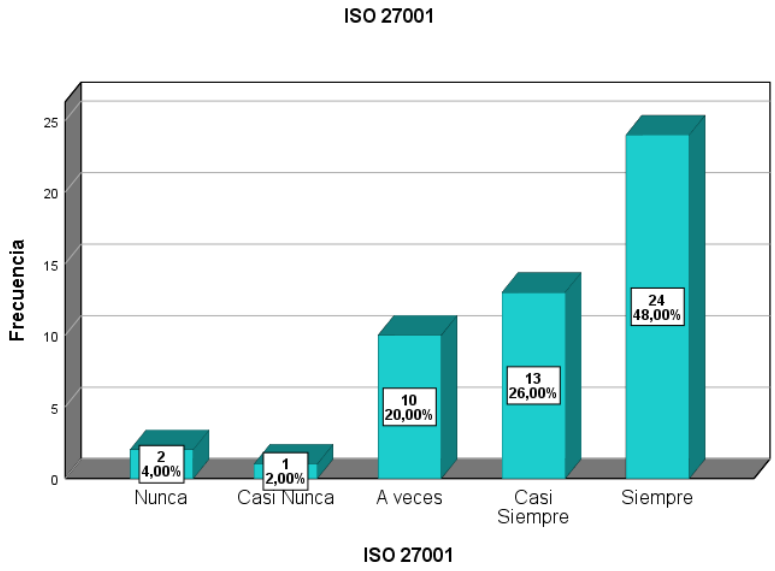


Tabla 2

Frecuencia variable 2

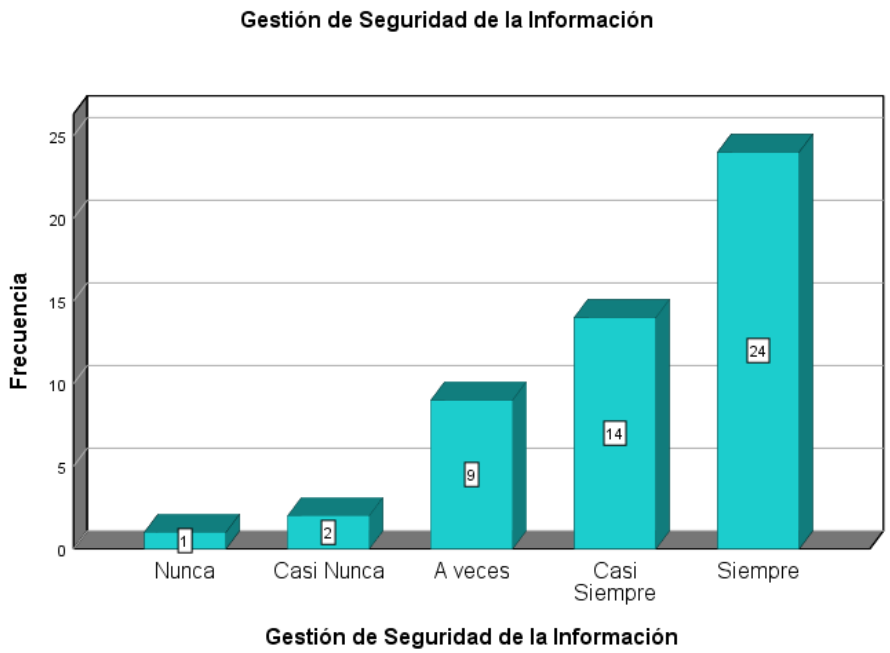
		Frecuencia	%	% válido	% acumulado
Válido	Nunca	1	2,0	2,0	2,0
	Casi Nunca	2	4,0	4,0	6,0
	A veces	9	18,0	18,0	24,0
	Casi Siempre	14	28,0	28,0	52,0
	Siempre	24	48,0	48,0	100,0
	Total	50	100,0	100,0	

Se analizaron los datos recopilados a través de una encuesta en línea y los resultados se presentaron de manera visual mediante la tabla 2 y figura 5, se manifiesta que 24 colaboradores del área TI representa el 48,00% tiene un nivel de siempre, a su vez, 14 colaboradores que representa el 28,00% tiene un nivel de casi siempre, asimismo 9 colaboradores que representa un 18,0% tiene un nivel de a veces, otro 2 un

colaborador que representa el 4,00% tiene un nivel de casi nunca y 1 colaborador que representa el 2,00% tiene un nivel de nunca.

Figura 5

Gráfico de columnas de variable 2: Gestión de Seguridad de la Información



Dimensión 1: Disponibilidad

Tabla 3

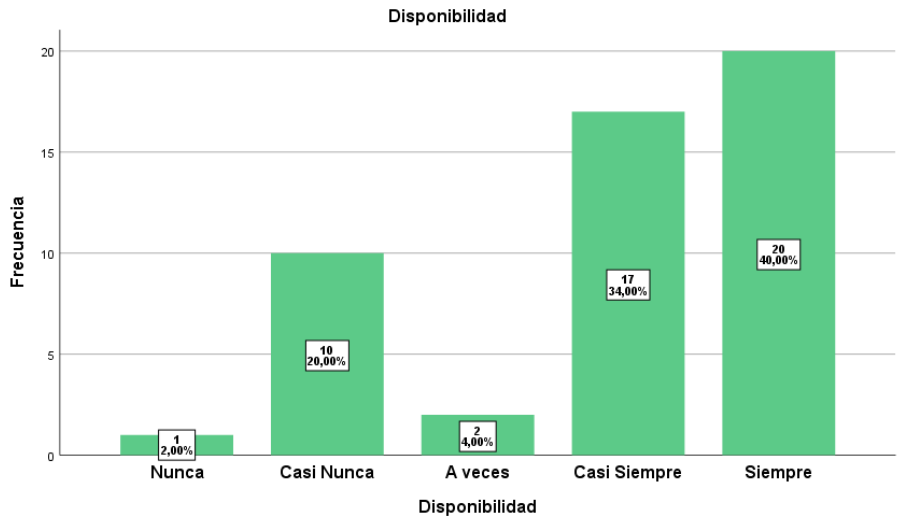
Frecuencia dimensión 1: Disponibilidad

		Frecuencia	%	% válido	% acumulado
Válido	Nunca	1	2,0	2,0	2,0
	Casi Nunca	10	20,0	20,0	22,0
	A veces	2	4,0	4,0	26,0
	Casi Siempre	17	34,0	34,0	60,0
	Siempre	20	40,0	40,0	100,0
	Total	50	100,0	100,0	

Se analizaron los datos recopilados a través de una encuesta en línea y los resultados se presentaron de manera visual mediante la tabla 3 y figura 6, se manifiesta que 20 colaboradores del área TI representa el 40,00% tiene un nivel de siempre, a su vez, 17 colaboradores que representa el 34,00% tiene un nivel de casi siempre, asimismo 2 colaboradores que representa un 4,0% tiene un nivel de a veces, otro 10 un colaborador que representa el 20,00% tiene un nivel de casi nunca y 1 colaborador que representa el 2,00% tiene un nivel de nunca.

Figura 6

Gráfico de columnas de dimensión 1: Disponibilidad



Dimensión 2: Adaptabilidad

Tabla 4

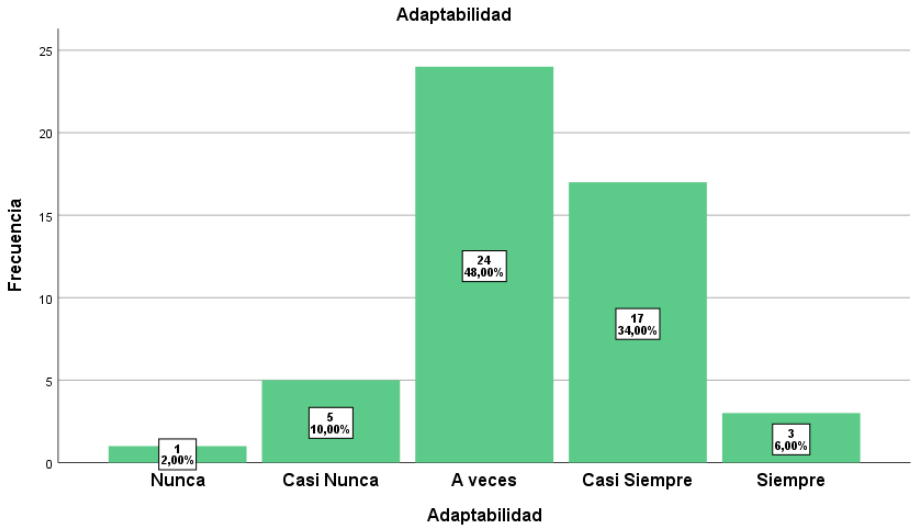
Frecuencia dimensión 2: Adaptabilidad

		Frecuencia	%	% válido	% acumulado
Válido	Nunca	1	2,0	2,0	2,0
	Casi Nunca	5	10,0	10,0	12,0
	A veces	24	48,0	48,0	60,0
	Casi Siempre	17	34,0	34,0	94,0
	Siempre	3	6,0	6,0	100,0
	Total	50	100,0	100,0	

Se analizaron los datos recopilados a través de una encuesta en línea y los resultados se presentaron de manera visual mediante la tabla 4 y figura 7, se manifiesta que 3 colaboradores del área TI representa el 6,00% tiene un nivel de siempre, a su vez, 17 colaboradores que representa el 34,00% tiene un nivel de casi siempre, asimismo 24 colaboradores que representa un 48,0% tiene un nivel de a veces, otros 5 colaboradores que representa el 10,00% tiene un nivel de casi nunca y 1 colaborador que representa el 2,00% tiene un nivel de nunca.

Figura 7

Gráfico de columnas de dimensión 2: Adaptabilidad



Dimensión 3: Accesibilidad

Tabla 5

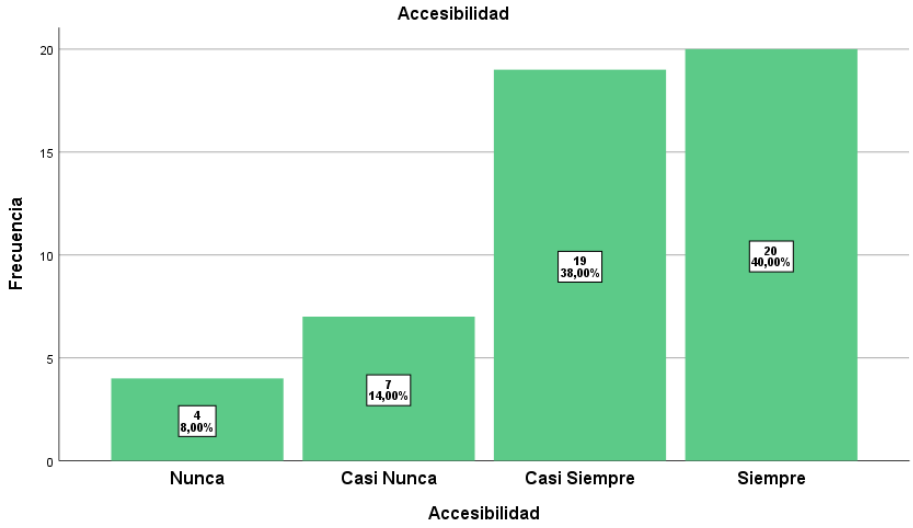
Frecuencia dimensión 3: Accesibilidad

		Frecuencia	%	% válido	% acumulado
Válido	Nunca	4	8,0	8,0	8,0
	Casi Nunca	7	14,0	14,0	22,0
	Casi Siempre	19	38,0	38,0	60,0
	Siempre	20	40,0	40,0	100,0
	Total	50	100,0	100,0	

Se analizaron los datos recopilados a través de una encuesta en línea y los resultados se presentaron de manera visual mediante la tabla 5 y figura 8, se manifiesta que 20 colaboradores del área TI representa el 40,00% tiene un nivel de siempre, a su vez, 19 colaboradores que representa el 38,00% tiene un nivel de casi siempre, asimismo 7 colaboradores que representa un 14,0% tiene un nivel de casi nunca, y 4 colaboradores que representa el 8,00% tiene un nivel de nunca.

Figura 8

Gráfico de columnas de dimensión 3: Accesibilidad



Dimensión 4: Resguardo

Tabla 6

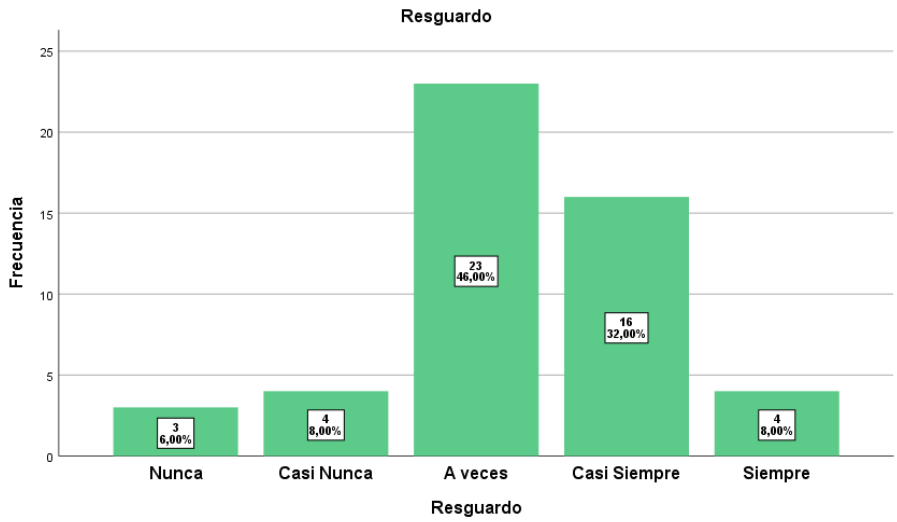
Frecuencia dimensión 4: Resguardo

		Frecuencia	%	% válido	% acumulado
Válido	Nunca	3	6,0	6,0	6,0
	Casi Nunca	4	8,0	8,0	14,0
	A veces	23	46,0	46,0	60,0
	Casi Siempre	16	32,0	32,0	92,0
	Siempre	4	8,0	8,0	100,0
	Total	50	100,0	100,0	

Se analizaron los datos recopilados a través de una encuesta en línea y los resultados se presentaron de manera visual mediante la tabla 6 y figura 9, se manifiesta que 4 colaboradores del área TI representa el 8,00% tiene un nivel de siempre, a su vez, 16 colaboradores que representa el 32,00% tiene un nivel de casi siempre, asimismo 23 colaboradores que representa un 46,0% tiene un nivel de a veces, otros 4 colaboradores que representa el 8,00% tiene un nivel de casi nunca y 3 colaborador que representa el 6,00% tiene un nivel de nunca.

Figura 9

Gráfico de columnas de dimensión 4: Resguardo



Prueba de confiablidad

Es el valor utilizado para evaluar el nivel de confianza de un instrumento. Además, se comprobó la fiabilidad de Alfa de Cronbach para establecer la confianza en los instrumentos que emplearon la Escala de Likert.

Tabla 7

Escala alfa de Cronbach

Escala	Intensidad
> 0.90	Muy Alta
0.80 a 0.90	Alta
0.70 a 0.79	Moderada
0.60 a 0.69	Baja
0.50 a 0.59	Muy Baja
< 0.50	Inaceptable

La tabla 7 es un indicador usado para estimar la fiabilidad interna de un instrumento, evaluando el grado en que los elementos o preguntas del mismo se correlacionan entre sí.

Tabla 8

Credibilidad de la encuesta

Alfa de Cronbach	N de elementos
,803	43

Contiene 43 interrogantes, se alcanzó un coeficiente de 0.803, el valor es calificado “Moderada”, por lo tanto, se concluye que el instrumento es confiable y adecuado para recopilar datos en el estudio.

Prueba de normalidad

Tabla 9

Prueba de normalidad Variable independiente y Variable dependiente

	Kolmogorov-Smirnov[a]		
	Estadístico	gl	Sig.
Variable independiente	,276	50	,000
Variable dependiente	,280	50	,000

En la tabla número 9, se visualiza que los hallazgos obtenidos generales al momento llevar a cabo la prueba de normalidad Kolmogórov, que se empleará ya que nuestra población es superior a 50. Como p = 0 < 0.05, entonces se refuta la hipótesis y se aprueba la hipótesis, en resumen, los hallazgos no cumplen con una distribución normal. Se optó por utilizar métodos estadísticos no paramétricos.

Dimensión 1: Disponibilidad

Tabla 10

Prueba de normalidad Disponibilidad.

	Kolmogorov Smirnov		
	Estad.	gl	Sig.
Disponibilidad	,273	50	,000

En la tabla número 10, se aprecia que los resultados obtenidos de la dimensión disponibilidad al momento llevar a cabo la prueba de normalidad Kolmogórov, que se empleará ya que nuestra población es superior a 50. Como p = 0 < 0.05, entonces se refuta la hipótesis y se aprueba la hipótesis, en resumen, los hallazgos no cumplen con una distribución normal. Se optó por utilizar métodos estadísticos no paramétricos.

Dimensión 2: Adaptabilidad

Tabla 11

Prueba de normalidad Adaptabilidad.

	Kolmogorov-Smirnov		
	Estad.	Gl	Sig.
Adaptabilidad	,252	50	,000

En la tabla número 11, se visualiza que los hallazgos obtenidos de la dimensión adaptabilidad al momento llevar a cabo la prueba de normalidad Kolmogórov, que se empleará ya que nuestra población es superior a 50. Como $p = 0 < 0.05$, entonces se refuta la hipótesis y se aprueba la hipótesis, en resumen, los hallazgos no cumplen con una distribución normal. Se optó por utilizar métodos estadísticos no paramétricos.

Dimensión 3: Accesibilidad

Tabla 12

Prueba de normalidad Accesibilidad.

	Kolmogorov-Smirnov		
	Estad.	Gl	Sig.
Accesibilidad	,317	50	,000

En la tabla número 12, se visualiza que los datos obtenidos de la dimensión accesibilidad al momento llevar a cabo la prueba de normalidad Kolmogórov, que se empleará ya que nuestra población es superior a 50. Como $p = 0 < 0.05$, entonces se refuta la hipótesis y se aprueba la hipótesis, en resumen, los hallazgos no cumplen con una distribución normal. Se optó por utilizar métodos estadísticos no paramétricos.

Dimensión 4: Resguardo

Tabla 13

Prueba de normalidad Resguardo.

	Kolmogorov-Smirnov		
	Estad.	gl	Sig.
Resguardo	,244	50	,000

En la tabla número 13, se visualiza que los hallazgos obtenidos de la dimensión resguardo al momento llevar a cabo la prueba de normalidad Kolmogórov, que se empleará ya que nuestra población es superior a 50. Como $p = 0 < 0.05$, entonces se refuta la hipótesis y se aprueba la hipótesis, es decir, en resumen, los hallazgos no cumplen con una distribución normal. Se optó por utilizar métodos estadísticos no paramétricos.

Contrastación de hipótesis

Hipótesis general:

Ho: El ISO 27001 no mejora significativamente la gestión de seguridad de la información en las áreas de tecnología de la información (TI) de la institución pública.

H1: El ISO 27001 mejora significativamente la gestión de seguridad de la información en las áreas de tecnología de la información (TI) de la institución pública.

Tabla 14

Prueba Spearman entre Variable 1 independiente y Variable 2 dependiente

			Variable indep	Variable depen
Spearman	Variable indep	Coef. de Corr.	1,000	,882**
		Sig. (Bilat.)	.	,000
		N	50	50
	Variable depen	Coef. de Corr.	,882**	1,000
		Sig. (Bilat.)	,000	.
		N	50	50

Se observó una correlación alta de 0. 882 de los datos y sig. p = 0 < 0.05, lo que demuestra una conexión sólida entre las variables analizadas.

Cuando el sig. p = 0 < 0.05, se descarta la hipótesis nula (Ho), se desestima la hipótesis nula Ho: El ISO 27001 no mejora significativamente la gestión de seguridad de la información en el área de TI de la institución pública

Por lo tanto, se acepta H1: El ISO 27001 mejora significativamente la gestión de seguridad de la información en el área de TI de la institución pública.

Hipótesis Específica 1:

Ho: El ISO 27001 no mejora significativamente la disponibilidad de la información para la gestión seguridad de la información en el área de TI de la institución pública.

H1: El ISO 27001 mejora significativamente la disponibilidad de la información para la gestión seguridad de la información en el área de TI de la institución pública.

Tabla 15

Prueba Spearman entre *Variable 2* y Disponibilidad

			Variable 2	Disponibilidad
Spearman	Variable 2	Coef. de Corr.	1,000	,532**
		Sig. (Bilat.)	.	,000
		N	50	50
	Disponibilidad	Coef. de Corr.	,532**	1,000
		Sig. (Bilat.)	,000	.
		N	50	50

Se observó una correlación alta de 0. 532 de los datos y sig. p = 0 < 0.05, lo que demuestra una conexión sólida entre la variable dependiente y la dimensión disponibilidad.

Cuando el sig. p = 0 < 0.05, se descarta la hipótesis nula (Ho), se desestima la hipótesis nula Ho: El ISO 27001 no mejora significativamente la disponibilidad de la información para la gestión seguridad de la información en el área de TI de la institución pública.

Por lo tanto, se acepta H1: El ISO 27001 mejora significativamente la disponibilidad de la información para la gestión seguridad de la información en el área de TI de la institución pública.

Hipótesis Específica 2:

Ho: El ISO 27001 no mejora significativamente la adaptabilidad de la información para la gestión seguridad de la información en el área de TI de la institución pública.

H1: El ISO 27001 mejora significativamente la adaptabilidad de la información para la gestión seguridad de la información en el área de TI de la institución pública.

Tabla 16

Prueba Spearman entre Variable 2 y adaptabilidad

			Variable 2	Adaptabilidad
Spearman	Variable 2	Coef. de Corr.	1,000	,364**
		Sig. (Bilat.)	.	,009
		N	50	50
	Adaptabilidad	Coef. de Corr.	,364**	1,000
		Sig. (Bilat.)	,009	.
		N	50	50

Se observó una correlación alta de 0. 364 de los datos y sig. p = 0 < 0.05, lo que demuestra una conexión sólida entre la variable dependiente y la dimensión adaptabilidad.

Cuando el sig. p = 0 < 0.05, se descarta la hipótesis nula (Ho), se desestima la hipótesis nula Ho: El ISO 27001 no mejora significativamente la adaptabilidad de la información para la gestión seguridad de la información en el área de TI de la institución pública.

Por lo tanto, se acepta H1: El ISO 27001 mejora significativamente la adaptabilidad de la información para la gestión seguridad de la información en el área de TI de la institución pública.

Hipótesis Específica 3:

Ho: El ISO 27001 no mejora significativamente la accesibilidad de la información para la gestión seguridad de la información en el área de TI de la institución pública.

H1: El ISO 27001 mejora significativamente la accesibilidad de la información para la gestión seguridad de la información en el área de TI de la institución pública

Tabla 17

Prueba Spearman entre Variable 2 y accesibilidad

			Variable 2	accesibilidad
Spearman	Variable 2	Coef. de Corr.	1,000	,417**
		Sig. (Bilat.)	.	,003
		N	50	50
	accesibilidad	Coef. de Corr.	,417**	1,000
		Sig. (Bilat.)	,003	.
		N	50	50

Se observó una correlación alta de 0. 417 de los datos y sig. p = 0 < 0.05, lo que demuestra una conexión sólida entre la variable dependiente y la dimensión accesibilidad.

Cuando el sig. p = 0 < 0.05, se descarta la hipótesis nula (Ho), se desestima la hipótesis nula Ho: El ISO 27001 no mejora significativamente la accesibilidad de la información para la gestión seguridad de la información en el área de TI de la institución pública.

Por lo tanto, se acepta H1: El ISO 27001 mejora significativamente la accesibilidad de la información para la gestión seguridad de la información en el área de TI de la institución pública.

Hipótesis Específica 4:

Ho: El ISO 27001 no mejora significativamente el resguardo de la información para la gestión seguridad de la información en el área de TI de la institución pública.

H1: El ISO 27001 mejora significativamente el resguardo de la información para la gestión seguridad de la información en el área de TI de la institución pública

Tabla 18

Prueba Spearman entre Variable 2 y resguardo

			Variable 2	Resguardo
Spearman	Variable 2	Coef. de Corr.	1,000	,297*
		Sig. (Bilat.)	.	,037
		N	50	50
	Resguardo	Coef. de Corr.	,297*	1,000
		Sig. (Bilat.)	,037	.
		N	50	50

Se observó una correlación alta de 0. 297 de los datos y sig. p = 0 < 0.05, lo que demuestra una conexión sólida entre la variable dependiente y la dimensión resguardo.

Cuando el sig. p = 0 < 0.05, se descarta la hipótesis nula (Ho), se desestima la hipótesis nula Ho: El ISO 27001 no mejora significativamente el de la información para la gestión seguridad de la información en el área de TI de la institución pública.

Por lo tanto, se acepta H1: El ISO 27001 mejora significativamente el resguardo de la información para la gestión seguridad de la información en el área de TI de la institución pública.

V. DISCUSIÓN

A causa de los hallazgos conseguidos en este estudio, se evidenció un progreso relevante en las dimensiones relacionadas con la variable dependiente después de ejecutar la ISO 27001 en la Institución Pública. La hipótesis principal planteada sostiene que la ISO 27001 mejora la Gestión de Seguridad de la Información en una Institución Pública. Los resultados, con el nivel de sig. $p = 0 < 0.05$, desestiman la hipótesis nula y respaldan la hipótesis alternativa, lo que indica que ISO 27001 efectivamente mejora la gestión de seguridad de la información en el área de tecnología de la información (TI) de la institución pública. Además, el estudio revela que la ejecución de la ISO 27001 implica un mayor control, salvaguardar y privacidad de datos de la institución.

Tras la aplicación de la norma ISO 27001, se observó un incremento en la apreciación acerca de la adecuada gestión de seguridad de la información, según los datos obtenidos. El estudio descriptivo de la disponibilidad se llevó a cabo a través de encuestas realizadas a un total de 50 profesionales.

Se observo las virtudes del despliegue de la ISO 27001, un 2 % obtuvo una apreciación “Nunca” ,10% la apreciación de “Casi Nunca”, 2% la apreciación de “A veces”, 17% la apreciación de “Casi Siempre” y un 20% la apreciación de “Siempre” referente a la disponibilidad para la gestión de seguridad de la información.

En el análisis inferencial, se utilizó el test de Kolmogorov para evaluar la normalidad de los datos, la cual indicó que los datos examinados muestran una distribución no paramétrica. Para contrastar las hipótesis, se utilizó la prueba de correlación de Spearman, obteniendo un valor de significación estadística bilateral 0,000 y la medida de relación de 0,532. Estos hallazgos confirman el descarte de la hipótesis nula y la confirmación de la hipótesis alternativa, lo que lleva a la conclusión de que la ejecución de la ISO 27001 mejora significativamente la disponibilidad.

Los resultados encontrados están relacionados con el estudio realizada por Mejía (2020), que mostró una relevancia propicia del 60% al ejecutar la ISO 27001 para afianzar la disponibilidad. En la evaluación previa, se obtuvo una apreciación del 11%, mientras que en la evaluación final fue del 71%. Además, al utilizar la

prueba de hipótesis de Kolmogorov con la prueba de Wilcoxon, se confirmó la aprobación de la hipótesis alternativa. Esto indica que la ejecución de la ISO 27001:2013, facilita reducir las amenazas en la disponibilidad, puesto que hubo una media de 0.236 en la evaluación previa y 0.347 en la evaluación final. Es importante destacar que se utilizó un diseño experimental en el cual, en la prueba no paramétrica, obteniendo un valor de significación estadística bilateral inferior a 0.05, lo que condujo admitir la hipótesis alternativa.

Por otra parte, en el estudio llevado a cabo por Quintana (2019), cuya idea principal fue aplicar la ISO 27001 para garantizar la disponibilidad, al realizar la verificación de las pruebas de hipótesis, se constató la comprobación de la hipótesis alternativa. Se alcanzó una media superior a 0,05, con un valor de p=0,61 en el pretest y p=0,52 en el post-test. Esto lleva a la conclusión de que la disponibilidad mejora después de implementar la norma ISO 27001. Es importante destacar que se utilizó un diseño experimental en el cual, la prueba no paramétrica obteniendo un valor de significación estadística bilateral inferior a 0.05, lo que llevó a corroborar la hipótesis alternativa.

Como efecto de los resultados obtenidos al aplicar la ISO 27001, se observó un incremento en la percepción acerca de la adecuada adaptación para la gestión de la seguridad de la información. El estudio descriptivo de la adaptabilidad se llevó a cabo a través de encuestas realizadas a un total de 50 profesionales.

Se registraron los resultados de conformidad con la norma ISO 27001, donde se observó que el 2% de los participantes indicaron una percepción de 'Nunca', el 10% expresó una percepción de 'Casi Nunca', el 48% manifestó una percepción de 'A veces', el 34% mostró una percepción de 'Casi Siempre', y el 20% indicó una percepción de 'Siempre' en relación con la adaptabilidad.

En la evaluación inferencial, se utilizó el test de Kolmogorov para evaluar la normalidad de los datos, la cual indicó que los datos examinados muestran una distribución no paramétrica. Para medir las hipótesis, se empleó la prueba de correlación de Spearman, obteniendo un valor de significación estadística bilateral 0,000 y la medida 0,634. Estos resultados sustentan la desestimación de la hipótesis nula y la admisión de la hipótesis alternativa, lo que conduce a la

conclusión de que la implementación de la norma ISO 27001 influye notablemente en la mejora de la adaptabilidad.

Estas conclusiones guardan estudios similares, obtenido por Atencio (2019), en el cual se encontró que al ejecutar la ISO 27001, un progreso positivo del 69% en cuanto a la adaptabilidad. En la evaluación inicial, se obtuvo una percepción del 8%, mientras que en la evaluación final fue del 77%. Además, al utilizar la prueba de hipótesis de Kolmogorov con la prueba de Wilcoxon, se admitió la hipótesis alternativa, lo cual indica que la ejecución de la ISO 27001 ayuda a reducir los riesgos en la adaptabilidad. Se observó una media de 0,125 en la evaluación inicial y 0,156 en la evaluación final. Es importante destacar que se utilizó un diseño experimental de prueba no paramétrica y obteniendo un valor de significación estadística bilateral inferior a 0.05, lo que llevó a admitir la hipótesis alternativa. Esto resalta la relevancia de abordar y mejorar la adaptabilidad.

En otro estudio realizado por Córdova (2021), la idea principal fue ejecutar la ISO 27001 para mejorar la adaptabilidad, de igual manera que se reconocieron las múltiples amenazas económicos y administrativos a los que se enfrentaría la entidad universitaria. Además, se observó que el 63% del personal de sistemas e Informática tenía un conocimiento deficiente de la ISO 27001. Esto resalta la importancia de plasmar y gestionar como una herramienta para optimizar el procedimiento de adaptabilidad en la organización.

Se efectuó una evaluación descriptiva de la tercera dimensión mediante encuestas dirigidas a un grupo de 50 expertos. Se analizó la accesibilidad después de implementar la ISO 27001.

Se percibió los valores de la ISO 27001, donde se encontró que el 8% de los participantes indicaron una percepción de "Nunca", el 14% manifestó una percepción de "Casi Nunca", el 38% expresó una percepción de "Casi Siempre", y el 40% indicó una percepción de "Siempre" en relación con la accesibilidad para la gestión de la seguridad de la información.

En el análisis estadístico, se empleó la prueba de rangos de Wilcoxon con la prueba de Kolmogorov-Smirnov para determinar la distribución de los datos, revelando que los datos analizados siguen una distribución no paramétrica. Para

medir las hipótesis, se empleó la prueba de correlación de Spearman, obteniendo un valor de significación estadística bilateral 0,000 y la medida 0,417. Estos resultados sustentan la desestimación de la hipótesis nula y la admisión de la hipótesis alternativa, lo que lleva a la conclusión de que la implementación de la norma ISO 27001 tiene un impacto notablemente en la mejora de la accesibilidad.

Estos datos están relacionados con la investigación llevada a cabo por Guardia (2022), donde se mostró un progreso positivo del 72% al implementar la ISO 27001 para mejorar la accesibilidad. En la prueba inicial, se logró una apreciación del 8%, mientras que en la prueba final fue del 80%. Además, al utilizar la prueba de rangos de Wilcoxon con la prueba de Kolmogorov-Smirnov, se confirmó la admisión de la hipótesis alternativa, lo cual indicó que la ejecución de la ISO 27001:2013 ayuda a reducir los riesgos en la accesibilidad. Se observó una media de 0.324 en la prueba inicial y 0.298 en la prueba final. Es importante destacar que se utilizó un diseño experimental en el cual, en la prueba no paramétrica, obteniendo un valor de significación estadística bilateral inferior a 0.05, lo que condujo admitir la hipótesis alternativa.

En otro estudio realizado por Nacipucha (2019), se encontró que al ejecutar ISO 27001:2013 para mejorar la accesibilidad, se obtuvo una tasa de aprobación del 78% en la evaluación final, mientras en la prueba inicial con el 15%. Al efectuar la comprobación de las pruebas de hipótesis, se estableció la admisión de la hipótesis alternativa. Se alcanzó una media superior a 0.05. En la prueba inicial, se obtuvo un valor de p=0.74, mientras que en la prueba final fue de p=0.91. Además, se concluyó que la accesibilidad mejora después de la puesta en marcha de la ISO 27001:2013.

En otro estudio realizado, se encontraron resultados diferentes a los obtenidos por Cueva y Ríos (2017), se procedió a realizar un análisis de la ciberseguridad basado en los controles establecidos en la ISO 27001. Los resultados indicaron que se está cumpliendo con un 43% de los controles de acceso, lo cual evidencia la urgencia de llevar a cabo intervenciones para potenciar esta área. Sin embargo, se identificó que un 10% de los controles se encuentra en una etapa de maduración, lo que implica un cumplimiento parcial en la actualidad. Por otro lado, se observó que un 33% de los controles aún no se cumplen o se

hallan en una fase inicial de implementación. Esta situación se debe a las múltiples exigencias normativas que EsSalud debe cumplir de acuerdo con las regulaciones del estado peruano. Además, se destacó que el control con menor grado de implementación se encuentra vinculado a la seguridad del equipo de trabajo. Esto se atribuye a la falta de capacitaciones organizacional sólida en cuanto a la ciberseguridad, la cual EsSalud debe fomentar e implementar en su personal.

Como efecto de los resultados obtenidos al aplicar la ISO 27001, se observó el grado de resguardo y salvaguarda de los datos después de ejecutar la ISO 27001. El estudio descriptivo del resguardo se llevo a cabo a través de encuestas realizadas a un total de 50 profesionales.

Se percibió los valores de la ISO 27001, donde se encontró que el 6% de los participantes indicaron una percepción de "Nunca", el 8% manifestó una percepción de "Casi Nunca", el 46% expresó una percepción de "A veces", el 32% indicó una percepción de "Casi Siempre", y el 80% indicó una percepción de "Siempre" en relación con el resguardo de la ciberseguridad.

En la evaluación inferencial, se empleó la prueba de Kolmogorov-Smirnov para evaluar la normalidad de los datos, la cual indicó que los datos examinados muestran una distribución no paramétrica. Para medir las hipótesis, se empleó la prueba de correlación de Spearman, obteniendo un valor de significación estadística bilateral 0,000 y la medida 0,297. Estos resultados sustentan la desestimación de la hipótesis nula y la admisión de la hipótesis alternativa, lo que conduce a la conclusión de que la implementación de la norma ISO 27001 tiene un impacto significativo en la mejora del resguardo.

Estos datos están relacionados con el estudio efectuado por Chicaiza (2022), donde se observó un progreso positivo del 80% al ejecutar la ISO 27001:2013 para el resguardo. En la evaluación inicial se obtuvo una percepción del 5%, mientras que en la evaluación final fue del 85%. Además, al utilizar la prueba de hipótesis Kolmogorov con la prueba de Wilcoxon, se admitió la hipótesis alternativa, lo cual indicó que la ejecución de la ISO 27001:2013 ayuda a reducir los riesgos en el resguardo de la información. Se observó una media de 0.567 en la evaluación inicial y 0.442 en la evaluación final. Es importante destacar que se utilizó un diseño

experimental de prueba no paramétrica y obteniendo un valor de significación estadística bilateral inferior a 0.05, lo que llevó a admitir la hipótesis alternativa. Esto resalta la relevancia del resguardo mejora después de la ejecucion de la norma.

De igual modo, Álvarez y Andrade (2020) mencionó que alcanzó realizar una tasa de aprobación del 76% en la prueba final al ejecutar el ISO 27001 para el resguardo, en a diferencia del 7% en la prueba inicial. Durante la corroboración de las hipótesis, se constató la conformidad de la hipótesis alternativa, evidenciando la media superior a 0,05 en la prueba inicial, se obtuvo un valor de p=0,221, mientras que en la prueba final se registró un valor de p=0,855. Por lo tanto, se concluye que el resguardo mejoro después de implementar la norma ISO 27001. Es importante mencionar que se aplicó un enfoque experimental, donde el nivel de confianza estadística fue por debajo a 0,05, por lo cual se respaldó la aceptación de la hipótesis alternativa.

VI. CONCLUSIONES

1. Se concluyó que el objetivo general, mediante resultados de Spearman, la medida de relación es de 0,882 y significación estadística bilateral 0.000, indicando que mejora significativamente y positiva, por consiguiente, se validó la hipótesis alternativa (H1) y se descartó la hipótesis nula (H0), lo cual quiere decir que el ISO 27001 mejora significativamente para la gestión de seguridad de la información en el área de TI de la institución pública.

2. Se concluyó que el objetivo específico uno, mediante resultados de Spearman, la medida de relación es de 0,532 y significación estadística bilateral de 0.000, indicando que es moderada y positiva, por consiguiente, se validó la hipótesis alternativa (H1) y se descartó la hipótesis nula (H0), lo cual quiere decir que el ISO 27001 mejora significativamente la disponibilidad para la gestión de seguridad de la información en el área de TI de la institución pública.

3. Se concluyó que el objetivo específico dos, mediante resultados de Spearman, la medida de relación es de 0,882 y significación estadística bilateral de 0.000, indicando que mejora significativamente y positiva, por consiguiente, se validó la hipótesis alternativa (H1) y se descartó la hipótesis nula (H0), lo cual quiere decir que el ISO 27001 mejora significativamente la adaptabilidad para la gestión de seguridad de la información en el área de TI de la institución pública.

4. Se concluyó que el objetivo específico tres, mediante resultados de Spearman, la medida de relación es de 0,417 y significación estadística bilateral de 0.003, indicando que es moderada y positiva, por consiguiente, se validó la hipótesis alternativa (H1) y se descartó la hipótesis nula (H0), lo cual quiere decir que el ISO 27001 mejora significativamente la accesibilidad para la gestión de seguridad de la información en el área de TI de la institución pública.

5. Finalmente, el objetivo específico cuatro, mediante resultados de Spearman, la medida de relación es de 0,297 y significación estadística bilateral de 0.037, indicando que es moderada y positiva, por consiguiente, se validó la hipótesis alternativa (H1) y se descartó la hipótesis nula (H0), lo cual quiere decir el ISO 27001 mejora significativamente el resguardo para la gestión de seguridad de la información en el área de TI de la institución pública.

VII. RECOMENDACIONES

1. Se recomienda al coordinador del área, llevar a cabo auditorías de seguimiento tras de la adopción de la norma ISO27001, con el propósito de lograr un mejoramiento continuo para la gestión informática y asegurar una mayor seguridad. La adopción de la norma 27001 garantizará un nivel alto de resguardo y eficiencia en vínculo con la protección de la información.

2. Se recomienda al coordinador del área, llevar a cabo auditorías de seguimiento para evaluar la evolución de los estándares aplicados, se obtendrá garantizar el resguardo de la información. Se podrá afrontar los riesgos y ciberataques que surjan. Realizar estas auditorías periódicas permitirá mantener un control efectivo y asegurar la seguridad de los datos de manera constante.

3. Se recomienda al coordinador del área, que establezca manuales de procedimientos para promover la adaptabilidad de la información. Esto tiene lograr que la institución sea dinámica y flexible en términos. La implementación de estos manuales permitirá establecer pautas claras y procesos definidos para garantizar que puedan adaptarse de manera efectiva a los cambios. De ese modo se fomentará una cultura organizacional que valore y priorice la adaptabilidad en este ámbito crucial.

4. Se recomienda al coordinador del área que desarrolle tácticas de respuesta para complementar eventuales controles ausentes en relación a la accesibilidad. Esta medida beneficiará tanto a los usuarios como a la institución, ya que al tener datos en tiempo real se podrán optimizar los procesos de decisión estratégica de manera significativa. Al implementar planes de acción para fortalecer la accesibilidad de la información, se garantizará que los usuarios tengan un acceso rápido y confidencial a la información crucial, aquello que favorecerá una deliberación más segura y operativa.

5. Se recomienda al coordinador del área estructurar de acción basado en un análisis de riesgo para el resguardo de la información. Esto reducirá la desaparición de datos clave y mejorará la efectividad de los flujos de información para los clientes.

REFERENCIAS

Agustino, D. P. (2018). *Information Security Management System Analysis Menggunakan ISO/IEC 27001 (Studi Kasus: STMIK STIKOM Bali)*. Jurnal Eksplora Informatika, 8(1), 1-5. https://doi.org/10.30864/eksplora.v8i1.130

Alexei, A. (2021). *Ensuring information security in public organizations in the Republic of Moldova through the ISO 27001 standard*. Journal of Social Sciences, 4(1), 84-94. https://doi.org/10.52326/jss.utm.2021.4(1).11

Álvarez, L., & Andrade, M. (2020). Políticas de Seguridad de la Información bajo la Norma ISO 27002:2013 para el Gobierno Autónomo Descentralizado del *Cantón Biblián. Polo del Conocimiento, 5(11),* 591-621. https://polodelconocimiento.com/ojs/index.php/es/article/download/2011/4004

Ari, K., Rizal, I., & Aris, P. W. (2018). *Assessment of Information Security Management System based on ISO/IEC 27001:2013 On Subdirectorate of Data Center and Data Recovery Center in Ministry of Internal Affairs*. E3S Web of Conferences, 31, 11013. https://doi.org/10.1051/e3sconf/20183111013

Arias, J. (2021). Diseño y metodología de la investigación. *Enfoques Consulting EIRL*. https://repositorio.concytec.gob.pe/handle/20.500.12390/2260

Atencio, E. L. (2019*). Diseño de un sistema de gestión de seguridad de la información basado en la NTP-ISO/IEC 27001:2014 para la dirección general de informática y estadística de la Universidad Nacional Daniel Alcides Carrión Pasco Perú* [Tesis de posgrado, Universidad Nacional Daniel Alcides Carrión]. Repositorio Institucional de la Universidad Nacional Daniel Alcides Carrión. http://repositorio.undac.edu.pe/handle/undac/1474

Bai, H. (2022). *Legal Management of Network Information Security Based on Embedded Real-Time Task Processing*. Computational Intelligence and Neuroscience, 2022, 2379274. https://doi.org/10.1155/2022/2379274

Bailon, L. (2019). Gestión de riesgos del área informática de las empresas exportadoras de pesca blanca de Manta y Jaramijó. Polo del Conocimiento: Revista científico-profesional, 4(8), 165-189. https://dialnet.unirioja.es/servlet/articulo?codigo=7164331

Bertalanffy, L. (1976). Teoría General de los Sistemas: Fundamentos, desarrollo, aplicaciones. *Fondo de Cultura Económica*. https://fad.unsa.edu.pe/bancayseguros/wp-content/uploads/sites/4/2019/03/Teoria-General-de-los-Sistemas.pdf

Bongiovanni, I. (2019). The least secure places in the universe? A systematic literature review on information security management in higher education. *Computers & Security, 86*, 350-357. https://doi.org/10.1016/j.cose.2019.07.003

Bustamante, S., Valles, M. A., Cuellar, I. E., & Lévano, D. (2021*). Políticas basadas en la ISO 27001: 2013 y su influencia en la gestión de seguridad de la información en municipalidades de Perú*. Enfoque UTE, 12(2), pp. 69 - 79. https://doi.org/10.29019/enfoqueute.743

Cardona, J. & Restrepo, R. (2020). *Evaluación de la implementación de la norma ISO 27001 en empresas del sector privado, bajo un enfoque cultural. Tecnológico de Antioquia*, Institución Universitaria. https://dspace.tdea.edu.co/handle/tdea/921

Chen, H. Y., Wu, Z. Y., Chen, T. L., Huang, Y. M., & Liu, C. H. (2021). *Security Privacy and Policy for Cryptographic Based Electronic Medical Information System*. Sensors (Basel, Switzerland), 21(3), 713. https://doi.org/10.3390/s21030713

Chen, L., Xie, Z., Zhen, J., & Dong, K. (2022). The Impact of Challenge Information Security Stress on Information Security Policy Compliance: The Mediating Roles of Emotions. Psychology Research and Behavior Management, 15, 1177-1191. https://doi.org/10.2147/PRBM.S359277

Chicaiza, D. (2019). *Modelo de gestión de la seguridad de la información para pequeñas empresas*. [Tesis de maestría, Universidad Técnica de Ambato]. https://repositorio.uta.edu.ec/jspui/handle/123456789/29348

Chu, A. M., & So, M. K. (2020). Organizational Information Security Management for Sustainable Information Systems: An Unethical Employee Information Security Behavior Perspective. *Sustainability, 12*(8), 3163. https://doi.org/10.3390/su12083163

Córdova, J. (2021). *Diseño de un sistema automatizado de gestión de la seguridad de la información basado en la Norma ISO/IEC 27001:2013 para dar cumplimiento a la Ley 1581 de 2012 de protección de datos personales en el departamento de sistemas de una institución universitaria en Colombia*. [Tesis Maestría]. Universidad Peruana Unión. http://hdl.handle.net/20.500.12840/4789

Cueva, P., & Rios, J. (2017). Gestión de la historia clínica y la seguridad de la información del Hospital II Cajamarca - ESSALUD bajo la NTP-ISO/IEC 27001:2014. [Tesis de maestría, Universidad Privada del Norte]. https://hdl.handle.net/11537/13676

Di, Z., Liu, Y., & Li, S. (2022). Networked Organizational Structure of Enterprise Information Security Management Based on Digital Transformation and Genetic Algorithm. *Frontiers in public health, 10*, 921632. https://doi.org/10.3389/fpubh.2022.921632

Díaz, L. V. (2021). Percepción de la implementación de la NTP-ISO/IEC 27001:2014 en base a la información documentada del gobierno central del Perú, año 2021. Tesis de Maestría en Gestión de Tecnologías de la Información, Universidad César Vallejo, Perú.https://repositorio.ucv.edu.pe/handle/20.500.12692/76216

Ferreira, R. S., Frogeri, R. F., Coelho, A., & Piurcosky, F. (2018). Prácticas de gestión de la seguridad de la información: Estudio de los factores que influyen en una institución de la Fuerza Aérea brasileña. *JISTEM - Revista de Sistemas de Información y Gestión de Tecnologías, 15*. https://doi.org/10.4301/S1807-1775201815005

Figueroa, J., Rodríguez, R., Bone, C., & Saltos, J. (2018). La seguridad informática y la seguridad de la información. *Polo del Conocimiento, 2*(12), 145-155. https://doi.org/10.23857/pc.v2i12.420

García, J. C., Huamani, S. C., & Lomparte, R. F. (2018). Modelo de gestión de riesgos de seguridad de la información para PYMES peruanas. *Revista Peruana De Computación Y Sistemas, 1*(1), 47–56. https://doi.org/10.15381/rpcs.v1i1.14856

Guardia, R. (2020). *Diseño de un modelo de seguridad de la información para minimizar los riesgos informáticos en la gestión académica del instituto de educación superior tecnológico público "ELEAZAR GUZMAN BARRON" - HUARAZ" – 2018.* [Tesis de maestría, Universidad Nacional Santiago Antúnez de Mayolo]. http://repositorio.unasam.edu.pe/handle/UNASAM/4212

Handayani, N. U., Wibowo, M. A., Sari, D. P., Satria, Y., & Gifari, A. R. (2019). Risk Assessment of Information System of Faculty of Engineering University Diponegoro Using Failure Mode Effect and Analysis Method based on Framework ISO 27001. *Teknik, 39*(2), 78-85. https://doi.org/10.14710/teknik.v39i2.15918

Hannigan, L., Deyab, G., Al Thani, A., Al Marri, A., & Afifi, N. (2019). The Implementation of an Integrated Management System at Qatar Biobank. Biopreservation and Biobanking, 17(6), 506-511. https://doi.org/10.1089/bio.2019.0076

Husaeni, F., Sulistiyowati, N., & Rizal, A. (2019). Evaluasi pengelolaan aset laboratorium komputer menggunakan standar ISO/IEC 27001. *Jurnal TAM, 9*(2), 101-105. https://ojs.stmikpringsewu.ac.id/index.php/JurnalTam/article/view/675

Jelovčan, L., Mihelič, A., & Prislan, K. (2022). Outsource or not? An AHP Based Decision Model for Information Security Management. *Organizacija, 55*(2), 142-159. https://doi.org/10.2478/orga-2022-0010

Kim, Y., & Kim, B. (2021). The Effective Factors on Continuity of Corporate Information Security Management: Based on TOE Framework. *Information, 12*(11), 446. https://doi.org/10.3390/info12110446

Ključnikov, A., Mura, L., & Sklenár, D. (2019). Information security management in SMEs: factors of success. *Entrepreneurship and Sustainability Issues, 6*(4), 2081-2093. https://doi.org/10.9770/jesi.2019.6.4(37)

Lopes, I. M., Guarda, T., & Oliveira, P. (2019). Implementation of ISO 27001 Standards as GDPR Compliance Facilitator. *Journal of Information Systems Engineering & Management, 4*(2), 21. https://doi.org/10.29333/jisem/5888

López, E., Vásquez, C., & Tapia, R. (2019). Propuesta para el diseño e implementación de un sistema de gestión de seguridad de la información en

instituciones públicas en el Perú. *Revista Científica de Ingeniería y Tecnología, 10(18), 53-67*. https://doi.org/10.35381/r.cit.2019.18.53-67

Lugo, P. J., Carrasquero, P. H., & Gómez, P. J. (2020). Evaluación de gestión de seguridad de la información en los sistemas de información gerencial como herramienta de competitividad en empresas de servicios de ensayos no destructivos en la ciudad de lima - Perú. *Revista Qualitas, 19*(19), 062-076. https://revistas.unibe.edu.ec/index.php/qualitas/article/view/42

Maingak, A. Z., Candiwan, C., & Harsono, L. D. (2018). *Information security assessment using ISO/IEC 27001:2013 standard on government institution*. Trikonomika, 17(1), 28-37. https://doi.org/10.23969/trikonomika.v17i1.1138

Mejía, B. (2020). *Implementación de los controles de la ISO/IEC 27002: 2013 para la gestión de la base de datos de los registros públicos de la Zona VII – Sede Huaraz, 2019*. [Tesis de maestría, Universidad Peruana de Ciencias e Informática]. http://repositorio.upci.edu.pe/handle/upci/151

Mohammed, T. J., & Jasim, N. A. (2022). *Designing a model to protect documented information according to the integration of some international standards (ISO 27001: 2013) (ISO 10013: 2021): A case study*. International Journal of Health Sciences, 6(S3), 10684–10697. https://doi.org/10.53730/ijhs.v6nS3.8376

Monev, V. (2020). Organisational *Information Security Maturity Assessment Based on ISO 27001 and ISO 27002*. In 2020 International Conference on Information Technologies (InfoTech) (pp. 1-5). Varna, Bulgaria. doi: 10.1109/InfoTech49733.2020.9211066.

Nacipucha, J. (2019). *Análisis y diseño para un modelo de gestión de seguridad de la información basados en normas ISO/IEC 27001:2013 para la empresa Artehogar en la ciudad de Guayaquil.* [Tesis doctorado, Universidad de Guayaquil]. http://repositorio.ug.edu.ec/handle/redug/44410

Niño, N. (2018). *Modelo de un sistema de gestión de seguridad de información – SGSI, para fortalecer la confidencialidad, integridad, disponibilidad y monitorear los activos de información para el Instituto Nacional de Estadística e Informática - INEI filial Lambayeque* [Tesis de posgrado, Universidad Nacional Pedro Ruiz Gallo"]. Repositorio Institucional de la Universidad Nacional Pedro Ruiz. https://hdl.handle.net/20.500.12893/5935

Ordoñez, J., Real, J., Gallardo, J., Alvarado, H., & Roby, A. (2018). Knowledge on sexual health and its relationship with sexual behavior in university students. *Anales de La Facultad de Medicina, 78*(4), 423. https://doi.org/10.15381/anales.v78i4.14264

Patel, M., & Patel, N. (2019). Exploring Research Methodology: Review Article. *International Journal of Research & Review, 6*(3),48-55. https://www.ijrrjournal.com/IJRR_Vol.6_Issue.3_March2019/IJRR0011.pdf

Peikari, H. R., Ramayah, T., Shah, M. H., & Lo, M. C. (2018). Patients' perception of the information security management in health centers: the role of organizational and human factors. *BMC Medical Informatics and Decision Making, 18*(1), 1-13. doi: 10.1186/s12911-018-0681-z.

Prasetyowati, D.D., Gamayanto, I., Wibowo, S., & Suharnawi, S. (2019). Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) Berdasarkan ISO/IEC 27001:2013 pada Politeknik Ilmu Pelayaran Semarang. *JOINS (Journal of Information System), 4*(1), 65-75. https://doi.org/10.33633/joins.v4i1.2429

Prislan, K., Mihelič, A., & Bernik, I. (2020). *A real-world information security performance assessment using a multidimensional socio-technical approach*. PLoS One, 15(9), e0238739. https://doi.org/10.1371/journal.pone.0238739

Qusef, A., & Alkilani, H. (2022). *The effect of ISO/IEC 27001 standard over open-source intelligence*. PeerJ Computer Science, 8, e810. https://doi.org/10.7717/peerj-cs.810

Revista Economía. (2021). *Ciberataques en el Perú incrementaron en un 15% durante el 2021*. Recuperado de https://www.revistaeconomia.com/ciberataques-en-el-peru-incrementaron-en-un-15-durante-el-2021/

Rincón, J. (2019). *Implantación de un sistema de gestión de la seguridad de la información según la norma ISO/IEC 27001 en una entidad financiera* [Tesis de Posgrado, Universitat Oberta de Catalunya]. Repositorio Institucional Universitat Oberta de Catalunya.http://hdl.handle.net/10609/107386

Safonova, O. M., & Kotelnikov, N. V. (2020). Modeling the information security management system (ISMS) of a medical organization. *E3S Web of Conferences, 224*, 01035. https://doi.org/10.1051/e3sconf/202022401035

Shannon, C. E., & Weaver, W. (1964). The mathematical theory of communication. *University of Illinois Press.* https://pure.mpg.de/rest/items/item_2383164/component/file_2383163/content

Sikman, L., Latinovic, T., & Sarajlic, N. (2022). Modelling of Fuzzy Expert System for an Assessment of Security Information Management System UIS (University Information System). *Tehnički Vjesnik, 29*(1), 60-65. https://doi.org/10.17559/TV-20200721154801

Silva, F., Segadas, L. y Kowask, E. (2019). Gestión de la seguridad de la información. *REDCEDIA*. https://www.cedia.edu.ec/assets/docs/publicaciones/libros/GTI8.pdf

Sun, H., & Bai, S. (2022). *Enterprise Information Security Management Using Internet of Things Combined with Artificial Intelligence Technology*. Computational Intelligence and Neuroscience, 2022, 7138515. https://doi.org/10.1155/2022/7138515

Tanadi, Y., Soeprajitno, R., Firmansah, G., & El Karima, T. (2021). ISO 27001 Information Security Management System: Effect of Firm Audits in Emerging Blockchain Technology. *Riset Akuntansi dan Keuangan Indonesia, 6*(2), 198-204. https://journals.ums.ac.id/index.php/reaksi/article/view/15146

Tanović, A., & Marjanovic, I. S. (2019). *Development of a new improved model of ISO 20000 standard based on recommendations from ISO 27001 standard. In 2019 42nd International Convention on Information and Communication Technology*, Electronics and Microelectronics (MIPRO) (pp. 1503-1508). Opatija, Croatia. doi: 10.23919/MIPRO.2019.8756843.

Thoyyibah, T. (2018). Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) berdasarkan ISO 27001:2013 Pada Pusat Informasi dan Pangkalan Data Perguruan Tinggi X. *Jurnal CoreIT: Jurnal Hasil Penelitian Ilmu Komputer dan Teknologi Informasi, 4(*2), 72-76. https://doi.org/10.24014/coreit.v4i2.6292

Toro, R., Peña, M., Avendaño, B. L., Mejía, S., & Bernal, A. (2022). Análisis Empírico del Coeficiente Alfa de Cronbach según Opciones de Respuesta, Muestra y Observaciones Atípicas. *Revista Iberoamericana de Diagnóstico y Evaluación - e Avaliação Psicológica, 2*(63), 17-30. https://www.redalyc.org/articulo.oa?id=459671926003

Vega, E.M., Delgado,J.R, & De los Santos, A. C. (2022). *Importancia de la gestión de seguridad de la información en instituciones educativas con ITIL e ISO 27001. Revista de investigación de Sistemas e Informática*, 15(1), 113-123. https://revistasinvestigacion.unmsm.edu.pe/index.php/sistem/article/view/23362/18739

Vela, O., Requejo, M., Cubillas, C., Pérez M y Alfaro, P. (2019). Análisis de la clasificación de normas técnicas para la gestión de infraestructuras y servicios de tecnologías de la información. *DINA, 94* (5), 484. https://doi.org/10.6036/9303

Velasco, J., Ullauri, R., Pilicita, L., Jácome, B., Saa, P., & Moscoso-Zea, O. (2018). *Benefits of Implementing an ISMS According to the ISO 27001 Standard in the Ecuadorian Manufacturing Industry*. In 2018 International Conference on Information Systems and Computer Science (INCISCOS) (pp. 294-300). Quito, Ecuador. doi: 10.1109/INCISCOS.2018.00049.

Vergara, O. H. (2019). *Mejorando la implantación de la ISO 27001 en las organizaciones*. Piloto de Colombia, Institución Universitaria Repositorio Institucional. http://repository.unipiloto.edu.co/handle/20.500.12277/6178

Wang, R., & Wang, Y. (2019). Compatible matrices of Spearman's rank correlation. Paper. *Statistics and Probability Letters, 151*(1), 67–72. https://doi.org/10.1016/j.spl.2019.03.015

Yang, M., & Wang, J. (2022). The Security of Student Information Management System Based upon Blockchain. *Journal of Electrical and Computer Engineering*, 2022. https://doi.org/10.1155/2022/8186189

Zhao, Y., Tian, B., Niu, Y., Zhang, H., Yi, Z., & Zeng, R. (2021). *A Security Management and Control Solution of Smart Park Based on Sensor Networks*. Sensors (Basel, Switzerland), 21(20), 6815. https://doi.org/10.3390/s21206815

ANEXOS

Anexo 1. Matriz de operacionalización de las variables

VARIABLES DE ESTUDIO	DEFINICIÓN CONCUPTUAL	DEFINICIÓN OPERACIONAL	DIMENSIÓN	INDICADORES	TÉCNICA	INSTRUMENTO	ESCALA DE MEDICIÓN
ISO 27001	Este manual promueve las mejores prácticas para fortalecer la seguridad de la información y, a su vez, asegura la estabilidad y competitividad corporativa en el mercado (Silva et al, 2019).	Implica aplicar conceptos de seguridad de la información en la empresa para desarrollar un plan de asesoría privada.	Planificación	a. Análisis de brecha inicial b. Compromiso de alta dirección c. Comprender el contexto de la organización d. Comprender necesidades y expectativas e. Determinar el alcance del SGSI f. Determinar políticas de SI	Encuesta	Cuestionario	Escala Likert 1 Muy Bajo 2 Bajo 3 Medio Bajo 4

				g. Determinar objetivos de SI h. Crear procedimiento de gestión de riesgos i. Crear procedimiento de gestión de incidencia j. Gestionar los riesgos k. Crear plan de tratamiento de riesgos l. Determinar la declaración de aplicabilidad m. Crear plan de capacitación y concientización			Medio 5 Medio Alto 6 Alto
			Ejecución	a. Implementar plan de tratamiento de riesgos			

				b. Implementar plan de capacitación y concientización			
			Verificación	a. Preparar la auditoría interna b. Ejecutar auditoria c. Revisar con la alta dirección los resultados obtenidos			
			Mejora Continua	a. Crear plan de acciones correctivas b. Implementar plan de acciones correctivas c. Análisis de brecha final			
VARIABLES DE ESTUDIO	**DEFINICIÓN CONCUPTUAL**	**DEFINICIÓN OPERACIONAL**	**DIMENSIÓN**	**INDICADORES**	**TÉCNICA**	**INSTRUMENTO**	**ESCALA DE MEDICIÓN**
Gestión de Seguridad de la Información	Busca proteger los activos de información empresariales, incluyendo	Se refiere al resguardo de la información, a través de las buenas prácticas definidas	Disponibilidad	a. Tiempos de acceso b. Tipos de acceso c. Políticas de acceso			Escala Likert 1 Nunca
			Adaptabilidad	a. Crecimiento de información			

	sistemas y datos, implementando políticas de seguridad TI para prevenir daños y reducir costos (Silva et al., 2019).	por diversas metodologías o normas ya consolidadas en el ámbito de la seguridad TI.		b. Adaptación de nuevas tecnologías c. Espacio disponible d. Capacidad de almacenamiento físico	Encuesta	Cuestionario	2 Casi Nunca 3 A veces 4 Casi Siempre 5 Siempre
			Accesibilidad	a. Acceso a consultas b. Tiempo de respuesta			
			Resguardo	a. Respaldo de seguridad b. Almacenamiento del respaldo de seguridad c. Acceso al respaldo de seguridad d. Seguridad física			

Anexo 2. Validación de expertos

Dimensiones del instrumento:

- **Primera dimensión**: Disponibilidad
- Objetivos de la Dimensión: (describa lo que mide el instrumento).

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Tiempos de acceso	1	4	4	4	
Tipos de acceso	2	4	4	4	
Políticas de acceso	3	4	4	4	

- **Segunda dimensión**: Adaptabilidad
- Objetivos de la Dimensión: (describa lo que mide el instrumento).

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Crecimiento de información	1	4	4	4	
Adaptación de nuevas tecnologías	2	4	4	4	
Espacio disponible	2	4	4	4	
Capacidad de almacenamiento físico	3	4	4	4	

- **Tercera dimensión**: Accesibilidad
- Objetivos de la Dimensión: (describa lo que mide el instrumento).

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Acceso a consultas	1	4	4	4	
Tiempo de respuesta	2	4	4	4	

- **Tercera dimensión**: Resguardo
- Objetivos de la Dimensión: (describa lo que mide el instrumento).

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Respaldo de seguridad	1	4	4	4	
Almacenamiento del respaldo de seguridad	2	4	4	4	
Acceso al respaldo de seguridad	3	4	4	4	
Seguridad física	4	4	4	4	

Observaciones (precisar si hay suficiencia):

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

Apellidos y nombres del juez validador: Dr. Acuña Benites, Marlon Frank

Especialidad del validador: METODÓLOGO

19 de mayo del 2023

[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

Dr. Marlon Acuña Benites
DNI: 42097456
Ing. de Sistemas / Investigador

Firma del Experto validador

Williams y Webb (1994) así como Powell (2003), mencionan que no existe un consenso respecto al número de expertos a emplear. Por otra parte, el número de jueces que se debe emplear en un juicio depende del nivel de experticia y de la diversidad del conocimiento. Así, mientras Gable y Wolf (1993), Grant y Davis (1997), y Lynn (1986) (citados en McGartland et al. 2003) sugieren un rango de **2** hasta **20 expertos**, Hyrkäs et al. (2003) manifiestan que **10 expertos** brindarán una estimación confiable de la validez de contenido de un instrumento (cantidad mínimamente recomendable para construcciones de nuevos instrumentos). Si un 80 % de los expertos han estado de acuerdo con la validez de un ítem éste puede ser incorporado al instrumento (Voutilainen & Liukkonen, 1995, citados en Hyrkäs et al. (2003).

Ver : https://www.revistaespacios.com/cited2017/cited2017-23.pdf entre otra bibliografía.

Dimensiones del instrumento:

- **Primera dimensión**: (Colocar el nombre de la dimensión)
- Objetivos de la Dimensión: (describa lo que mide el instrumento).

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Tiempos de acceso	1	4	4	4	
Tipos de acceso	2	4	4	4	
Políticas de acceso	3	4	4	4	

- **Segunda dimensión**: Adaptabilidad
- Objetivos de la Dimensión: (describa lo que mide el instrumento).

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Crecimiento de información	1	4	4	4	
Adaptación de nuevas tecnologías	2	4	4	4	
Espacio disponible	2	4	4	4	
Capacidad de almacenamiento físico	3	4	4	4	

- **Tercera dimensión**: Accesibilidad
- Objetivos de la Dimensión: (describa lo que mide el instrumento).

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Acceso a consultas	1	4	4	4	
Tiempo de respuesta	2	4	4	4	

- **Tercera dimensión**: Resguardo
- Objetivos de la Dimensión: (describa lo que mide el instrumento).

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Respaldo de seguridad	1	4	4	4	
Almacenamiento del respaldo de seguridad	2	4	4	4	
Acceso al respaldo de seguridad	3	4	4	4	
Seguridad física	4	4	4	4	

Observaciones (precisar si hay suficiencia):

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

Apellidos y nombres del juez validador: Fernando Mendoza Apaza

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

19 de mayo del 2023

Firma del Experto validador

Williams y Webb (1994) así como Powell (2003), mencionan que no existe un consenso respecto al número de expertos a emplear. Por otra parte, el número de jueces que se debe emplear en un juicio depende del nivel de experticia y de la diversidad del conocimiento. Así, mientras Gable y Wolf (1993), Grant y Davis (1997), y Lynn (1986) (citados en McGartland et al. 2003) sugieren un rango de **2** hasta **20 expertos**, Hyrkäs et al. (2003) manifiestan que **10 expertos** brindarán una estimación confiable de la validez de contenido de un instrumento (cantidad mínimamente recomendable para construcciones de nuevos instrumentos). Si un 80 % de los expertos han estado de acuerdo con la validez de un ítem éste puede ser incorporado al instrumento (Voutilainen & Liukkonen, 1995, citados en Hyrkäs et al. (2003).

Ver : https://www.revistaespacios.com/cited2017/cited2017-23.pdf entre otra bibliografía.

Dimensiones del instrumento:

- **Primera dimensión**: (Colocar el nombre de la dimensión)
- Objetivos de la Dimensión: (describa lo que mide el instrumento).

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Tiempos de acceso	1	4	4	4	
Tipos de acceso	2	4	4	4	
Políticas de acceso	3	4	4	4	

- **Segunda dimensión**: Adaptabilidad
- Objetivos de la Dimensión: (describa lo que mide el instrumento).

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Crecimiento de información	1	4	4	4	
Adaptación de nuevas tecnologías	2	4	4	4	
Espacio disponible	2	4	4	4	
Capacidad de almacenamiento físico	3	4	4	4	

- **Tercera dimensión**: Accesibilidad
- Objetivos de la Dimensión: (describa lo que mide el instrumento).

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Acceso a consultas	1	4	4	4	
Tiempo de respuesta	2	4	4	4	

- **Tercera dimensión**: Resguardo
- Objetivos de la Dimensión: (describa lo que mide el instrumento).

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Respaldo de seguridad	1	4	4	4	
Almacenamiento del respaldo de seguridad	2	4	4	4	
Acceso al respaldo de seguridad	3	4	4	4	
Seguridad física	4	4	4	4	

Observaciones (precisar si hay suficiencia):

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

Apellidos y nombres del juez validador: Núñez Marinovich Néstor Manuel

Especialidad del validador: Magister en Ingeniería de Sistemas e Informática con mención en Ingeniería de Software

19 de mayo del 2023

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

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

Firma del Experto validador

Williams y Webb (1994) así como Powell (2003), mencionan que no existe un consenso respecto al número de expertos a emplear. Por otra parte, el número de jueces que se debe emplear en un juicio depende del nivel de experticia y de la diversidad del conocimiento. Así, mientras Gable y Wolf (1993), Grant y Davis (1997), y Lynn (1986) (citados en McGartland et al. 2003) sugieren un rango de **2** hasta **20 expertos**, Hyrkäs et al. (2003) manifiestan que **10 expertos** brindarán una estimación confiable de la validez de contenido de un instrumento (cantidad mínimamente recomendable para construcciones de nuevos instrumentos). Si un 80 % de los expertos han estado de acuerdo con la validez de un ítem éste puede ser incorporado al instrumento (Voutilainen & Liukkonen, 1995, citados en Hyrkäs et al. (2003).

Ver : https://www.revistaespacios.com/cited2017/cited2017-23.pdf entre otra bibliografía.

Anexo 3. Instrumento de Recolección de Datos

Cuestionario ISO 27001

Fecha: / /

Sexo: Femenino [] Masculino []

Autor: Aleman Balladares Fernando Yasmani (2023) adaptado para la investigación.

Instrucciones: Marque con un aspa la respuesta que crea conveniente teniendo en consideración el puntaje que corresponda de acuerdo con la siguiente valoración:

Valoración
1 nunca
2 casi nunca
3 a veces
4 casi siempre
5 siempre

N.º	DIMENSION	PREGUNTA	1	2	3	4	5
1	Planificación	¿La dirección aprueba el cumplimiento de los objetivos de la seguridad de la información para la implementación de la ISO 27001?					
2		¿El equipo de proyecto asegura la integración de los requisitos para implementar la ISO 27001 en los procesos de la institución?					
3		¿Existe apoyo a los trabajadores para su contribución efectiva de la ISO 27001?					
4		¿Se ha establecido una política de seguridad de la información?					
5		¿Se ha definido roles y responsabilidades para la seguridad de información?					
6		¿La institución realiza análisis de riesgos de la seguridad de información?					
7		¿La institución define y aplica el proceso de valoración de riesgos de la seguridad de información?					
8		¿La institución tiene un plan de tratamiento de riesgos de la seguridad informática?					

9		¿La institución tiene documentado los objetivos de la seguridad de información?					
10		¿La institución cuenta con un plan de mejora en el cumplimiento de objetivos?					
11		¿La institución proporciona los recursos necesarios para la gestión de la seguridad informática?					
12		¿Existen evaluaciones de desempeño acerca de la seguridad de información?					
13		¿Existen políticas de seguridad de información?					
14		¿Se tiene definidos canales de atención para la seguridad de información?					
15		¿Se cuenta con documentación de la seguridad de información para asegurar la efectividad?					
16		¿Se controla que la información requerida para la gestión de la seguridad esté disponible y protegida?					
17		¿Existe una planificación, ejecución y control de procesos para la gestión de seguridad de información?					
18	Ejecución	¿Se llevan a cabo evaluaciones de riesgo planificados?					
19		¿La empresa cuenta con un plan de tratamiento de riesgos?					
20	Verificación	¿La institución realiza el seguimiento, análisis y evaluación de la gestión de seguridad de información?					
21		¿La institución realiza auditorías internas?					
22		¿La alta dirección revisa su gestión de seguridad de información para asegurar su eficacia?					
23		¿La alta dirección toma decisiones y medidas en base a los resultados obtenidos por la gestión de seguridad de información?					
24	Mejora Continua	¿La institución controla y corrige las normas de cumplimiento de la seguridad de información?					
15		¿La institución mejora continuamente la adecuación y efectividad de la gestión de la seguridad de información?					

Cuestionario Gestión de Seguridad de la Información

Fecha: / /

Sexo: Femenino [] Masculino []

Autor: Aleman Balladares Fernando Yasmani (2023) adaptado para la investigación.

Instrucciones: Marque con un aspa la respuesta que crea conveniente teniendo en consideración el puntaje que corresponda de acuerdo con la siguiente valoración:

Valoración
1 nunca
2 casi nunca
3 a veces
4 casi siempre
5 siempre

N.º	DIMENSION	PREGUNTA	1	2	3	4	5
1	Disponibilidad	¿La entidad cuenta con horarios establecidos para acceder al repositorio de información?					
2		¿Existen tipos de acceso para los usuarios?					
3		¿Existen políticas de acceso al repositorio de la información?					
4		¿Los usuarios cuentan con los mismos permisos para acceder a la información?					
5	Adaptabilidad	¿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 computadora asignado?					
9		¿Es necesario mejorar la capacidad física de la computadora asignado?					
10	Accesibilidad	¿Cualquier usuario puede acceder a toda la información del repositorio?					
11		¿Existen controles de acceso para ingresar a la computadora 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 óptimo?					
14	Resguardo	¿Se realizan copias de resguardo del repositorio de información?					
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 computadora 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?					

Anexo 4. Carta de presentación

UNIVERSIDAD CÉSAR VALLEJO

"Año de la unidad, la paz y el desarrollo"

Lima, 16 de mayo de 2023
Carta P. 0075-2023-UCV-VA-EPG-F01/J

Ingeniero de sistemas
Juan Williams Feliciano Barrera
Coordinador de Informática
PODER JUDICIAL

De mi mayor consideración:

Es grato dirigirme a usted, para presentar a TRUJILLO BAILON, FLAVIO CESAR; identificado con DNI N° 75401367 y con código de matrícula N° 6500066784; estudiante del programa de MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN quien, en el marco de su tesis conducente a la obtención de su grado de MAESTRO, se encuentra desarrollando el trabajo de investigación titulado:

ISO 27001 en la Gestión de Seguridad de la Información en el área TI en una Institución Pública, Lima 2023

Con fines de investigación académica, solicito a su digna persona otorgar el permiso a nuestro estudiante, a fin de que pueda obtener información, en la institución que usted representa, que le permita desarrollar su trabajo de investigación. Nuestro estudiante investigador TRUJILLO BAILON, FLAVIO CESAR asume el compromiso de alcanzar a su despacho los resultados de este estudio, luego de haber finalizado el mismo con la asesoría de nuestros docentes.

Agradeciendo la gentileza de su atención al presente, hago propicia la oportunidad para expresarle los sentimientos de mi mayor consideración.

Atentamente,

ESCUELA DE POSGRADO UCV JEFATURA CAMPUS LIMA NORTE

Dra. Helga R. Majo Marrufo
Jefe
Escuela de Posgrado UCV
Filial Lima Campus Los Olivos

PODER JUDICIAL
Ing. JUAN W. FELICIANO BARRERA
Coordinador de Informática
Unidad de Planeamiento y Desarrollo
CORTE SUPERIOR DE JUSTICIA DE LIMA

Recibido 18/05/2023

Somos la universidad de los que quieren salir adelante.

ucv.edu.pe

Anexo 5. Aspectos administrativos

Recursos y Presupuesto

Recursos Humanos

En el estudio realizado, se tuvieron en cuenta las actividades llevadas a cabo para su concreción, por lo que se incluyen los costos de los recursos humanos. Esto engloba las fuentes bibliográficas, la recogida, procesamiento e interpretación de los datos, y la movilidad debido a ciertas coordinaciones que se efectuaron de manera presencial. Cada uno de estos elementos se detalla en la Tabla 1.

Tabla 1

Presupuesto de Recursos Humanos

Recursos	Descripción		Monto
Referencia	Fuentes Bibliográficas	S/	100.00
Transporte	Movilidad	S/	80.00
Data	Recolección y procesamiento	S/	2,500.00
	Total	S/	2,680.00

Recursos de Hardware

Además, se tuvo en cuenta el equipo empleado para la ejecución del trabajo de investigación, en este contexto se utilizó una computadora de mesa, como se refleja en la Tabla 2.

Tabla 2

Presupuesto de Hardware

Recursos	Descripción		Monto
Equipo	Computadora (Core I7 3ra gene.)	S/	3,550.00
	Total	S/	3,550.00

Recursos de Software

Por otro lado, se tuvo en cuenta el software utilizado para llevar a cabo la investigación, los detalles se presentan en la Tabla 3.

Tabla 3

Presupuesto de Software

Recursos	Descripción	Monto
Licencia	Statistical Package for the Social Sciences (SPSS) v23.0	S/ 200.00
Licencia	Project	S/ 80.00
	Total	S/ 280.00

Presupuesto

Por último, se procede a calcular la suma de todos los presupuestos previamente mencionados para obtener el presupuesto total necesario para la investigación. Esto se muestra en la Tabla 4.

Tabla 4

Presupuesto Total

Sumatorio de costo	Monto
Recursos Humanos	S/ 2,680.00
Recursos de Hardware	S/ 3,000.00
Recursos de software	S/ 280.00
Total	S/ 5,960.00

Financiamiento

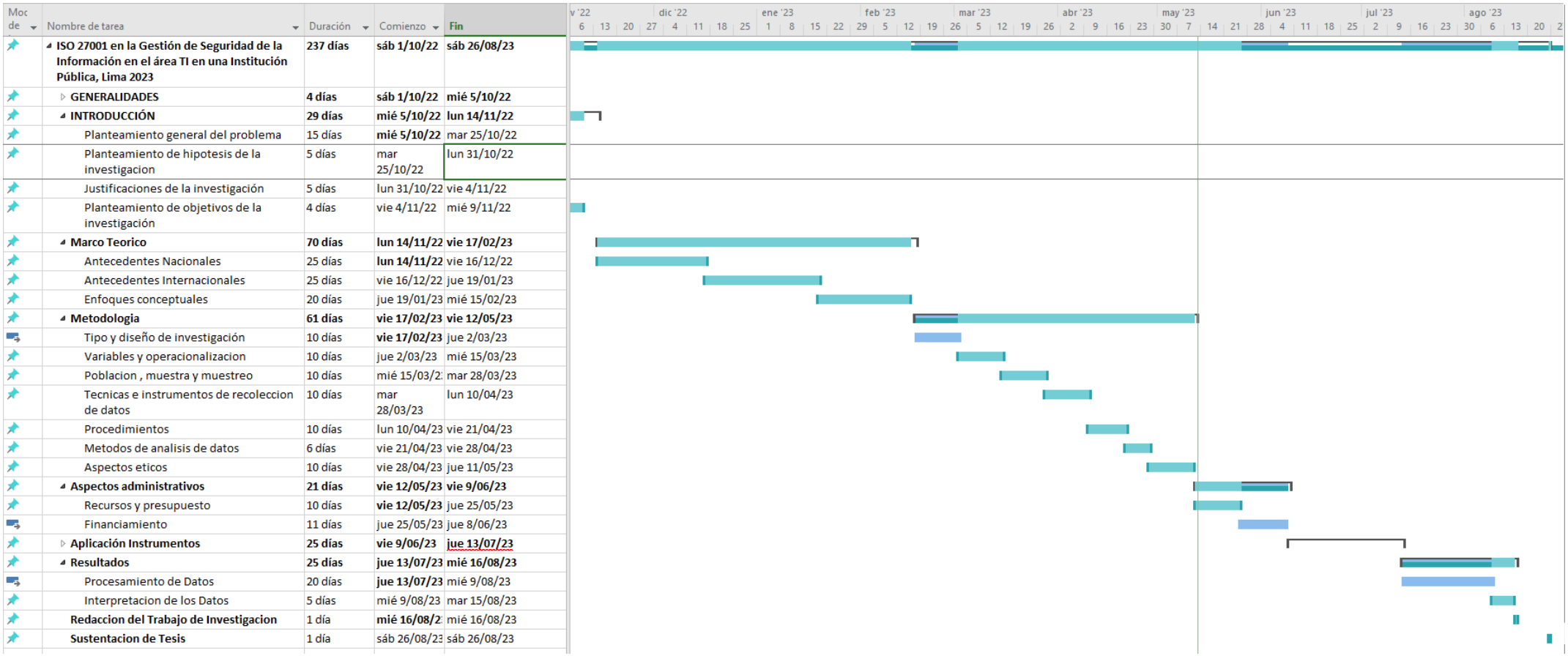
El presente estudio de investigación llevado a cabo en la Universidad César Vallejo tiene como objetivo fortalecer el conocimiento en el área correspondiente. Además, en relación a los presupuestos detallados, tanto el software, hardware y los recursos humanos fueron financiados internamente. Esto se muestra en la Tabla 5.

Tabla 5

Entidad financiadora	Monto	Porcentaje
Autofinanciado	S/ 7,000.00	100%

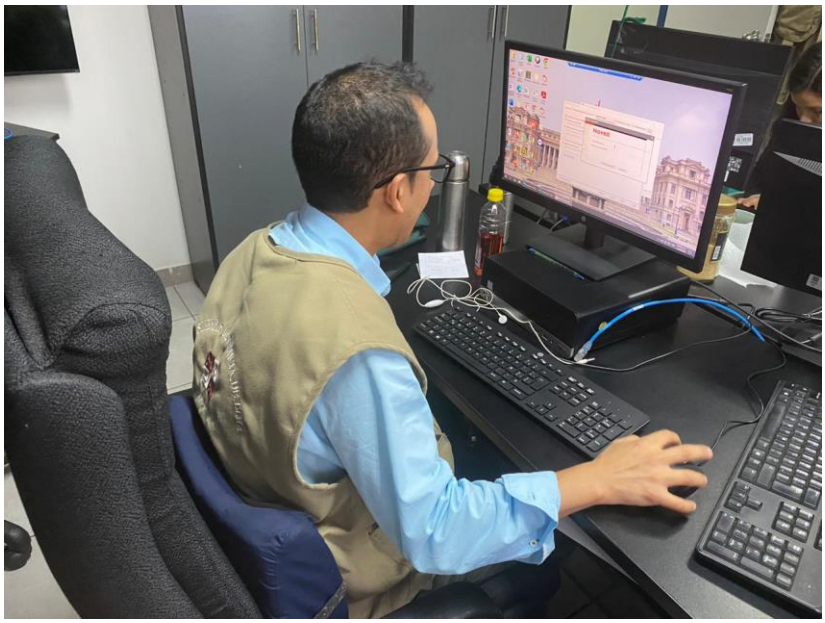
Cronograma de Ejecución

Cronograma de Ejecución

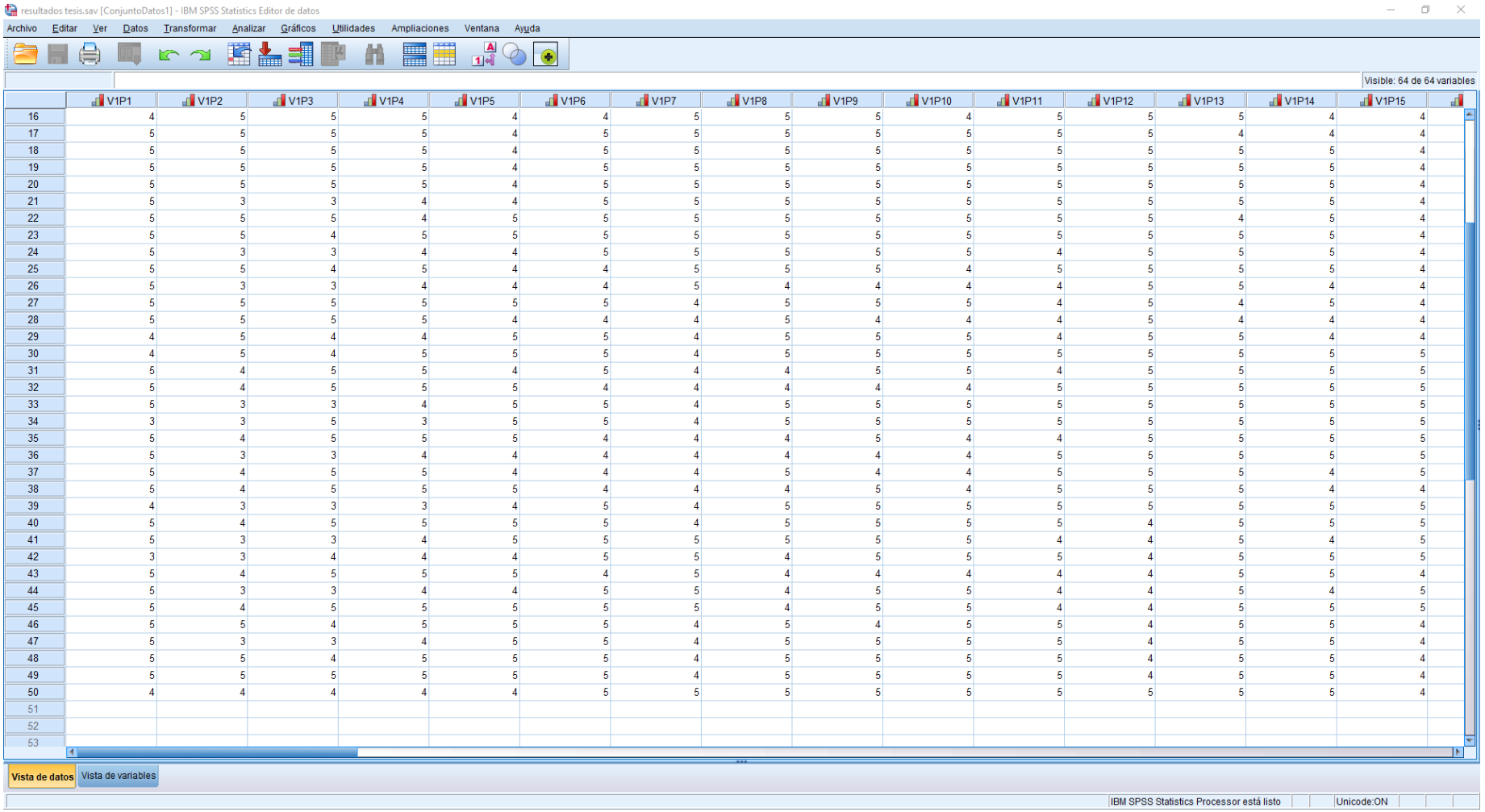


Moc de	Nombre de tarea	Duración	Comienzo	Fin
	ISO 27001 en la Gestión de Seguridad de la Información en el área TI en una Institución Pública, Lima 2023	**237 días**	**sáb 1/10/22**	**sáb 26/08/23**
	GENERALIDADES	**4 días**	**sáb 1/10/22**	**mié 5/10/22**
	INTRODUCCIÓN	**29 días**	**mié 5/10/22**	**lun 14/11/22**
	Planteamiento general del problema	15 días	**mié 5/10/22**	mar 25/10/22
	Planteamiento de hipotesis de la investigacion	5 días	mar 25/10/22	lun 31/10/22
	Justificaciones de la investigación	5 días	lun 31/10/22	vie 4/11/22
	Planteamiento de objetivos de la investigación	4 días	vie 4/11/22	mié 9/11/22
	Marco Teorico	**70 días**	**lun 14/11/22**	**vie 17/02/23**
	Antecedentes Nacionales	25 días	**lun 14/11/22**	vie 16/12/22
	Antecedentes Internacionales	25 días	vie 16/12/22	jue 19/01/23
	Enfoques conceptuales	20 días	jue 19/01/23	mié 15/02/23
	Metodologia	**61 días**	**vie 17/02/23**	**vie 12/05/23**
	Tipo y diseño de investigación	10 días	**vie 17/02/23**	jue 2/03/23
	Variables y operacionalizacion	10 días	jue 2/03/23	mié 15/03/23
	Poblacion , muestra y muestreo	10 días	mié 15/03/2	mar 28/03/23
	Tecnicas e instrumentos de recoleccion de datos	10 días	mar 28/03/23	lun 10/04/23
	Procedimientos	10 días	lun 10/04/23	vie 21/04/23
	Metodos de analisis de datos	6 días	vie 21/04/23	vie 28/04/23
	Aspectos eticos	10 días	vie 28/04/23	jue 11/05/23
	Aspectos administrativos	**21 días**	**vie 12/05/23**	**vie 9/06/23**
	Recursos y presupuesto	10 días	**vie 12/05/23**	jue 25/05/23
	Financiamiento	11 días	jue 25/05/23	jue 8/06/23
	Aplicación Instrumentos	**25 días**	**vie 9/06/23**	**jue 13/07/23**
	Resultados	**25 días**	**jue 13/07/23**	**mié 16/08/23**
	Procesamiento de Datos	20 días	**jue 13/07/23**	mié 9/08/23
	Interpretacion de los Datos	5 días	mié 9/08/23	mar 15/08/23
	Redaccion del Trabajo de Investigacion	1 día	**mié 16/08/2**	mié 16/08/23
	Sustentacion de Tesis	1 día	sáb 26/08/23	sáb 26/08/23

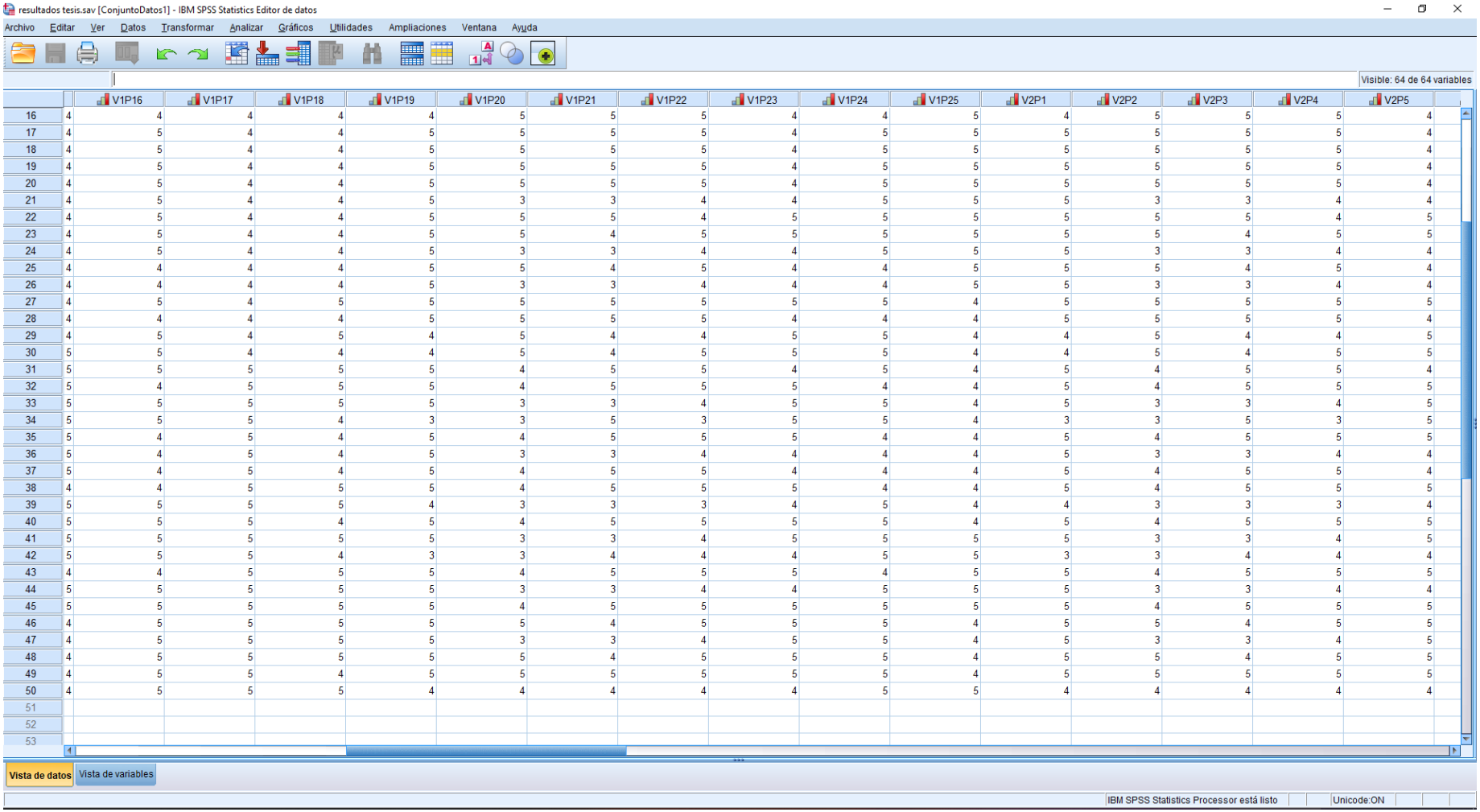
Anexo 6. Foto de implementación de accesos



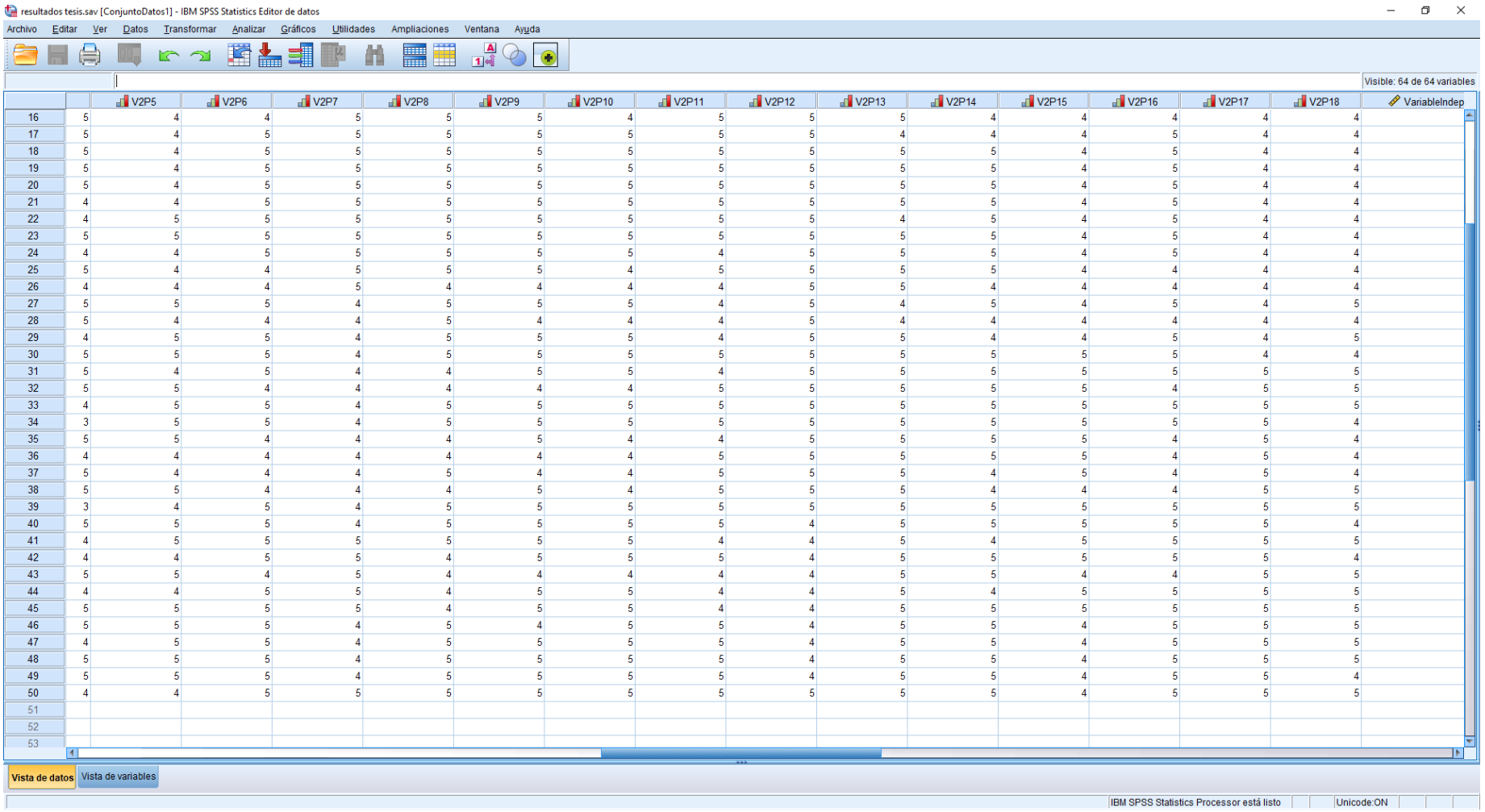
Anexo 7: Base datos en SPSS



	V1P1	V1P2	V1P3	V1P4	V1P5	V1P6	V1P7	V1P8	V1P9	V1P10	V1P11	V1P12	V1P13	V1P14	V1P15
16	4	5	5	5	4	4	5	5	5	4	5	5	5	4	4
17	5	5	5	5	4	5	5	5	5	5	5	5	4	4	4
18	5	5	5	5	4	5	5	5	5	5	5	5	5	5	4
19	5	5	5	5	4	5	5	5	5	5	5	5	5	5	4
20	5	5	5	5	4	5	5	5	5	5	5	5	5	5	4
21	5	3	3	4	4	5	5	5	5	5	5	5	5	5	4
22	5	5	5	4	5	5	5	5	5	5	5	5	4	5	4
23	5	5	4	5	5	5	5	5	5	5	5	5	5	5	4
24	5	3	3	4	4	5	5	5	5	5	4	5	5	5	4
25	5	5	4	5	4	4	5	5	5	4	5	5	5	5	4
26	5	3	3	4	4	4	5	4	4	4	4	5	5	4	4
27	5	5	5	5	5	5	4	5	5	5	4	5	4	5	4
28	5	5	5	5	4	4	4	5	4	4	4	5	4	4	4
29	4	5	4	4	5	5	4	5	5	5	4	5	5	4	4
30	4	5	4	5	5	5	4	5	5	5	5	5	5	5	5
31	5	4	5	5	4	5	4	4	5	5	4	5	5	5	5
32	5	4	5	5	5	4	4	4	4	4	5	5	5	5	5
33	5	3	3	4	5	5	4	5	5	5	5	5	5	5	5
34	3	3	5	3	5	5	4	5	5	5	5	5	5	5	5
35	5	4	5	5	5	4	4	4	5	4	4	5	5	5	5
36	5	3	3	4	4	4	4	4	4	4	5	5	5	5	5
37	5	4	5	5	4	4	4	5	4	4	5	5	5	4	5
38	5	4	5	5	5	4	4	4	5	4	5	5	5	4	4
39	4	3	3	3	4	5	4	5	5	5	5	5	5	5	5
40	5	4	5	5	5	5	4	5	5	5	5	4	5	5	5
41	5	3	3	4	5	5	5	5	5	5	4	4	5	4	5
42	3	3	4	4	4	5	5	4	5	5	5	4	5	5	5
43	5	4	5	5	5	4	5	4	4	4	4	4	5	5	4
44	5	3	3	4	4	5	5	4	5	5	4	4	5	4	5
45	5	4	5	5	5	5	5	4	5	5	4	4	5	5	5
46	5	5	4	5	5	5	4	5	4	5	5	4	5	5	4
47	5	3	3	4	5	5	4	5	5	5	5	4	5	5	4
48	5	5	4	5	5	5	4	5	5	5	5	4	5	5	4
49	5	5	5	5	5	5	4	5	5	5	5	4	5	5	4
50	4	4	4	4	4	5	5	5	5	5	5	5	5	5	4
51															
52															
53															



	V1P16	V1P17	V1P18	V1P19	V1P20	V1P21	V1P22	V1P23	V1P24	V1P25	V2P1	V2P2	V2P3	V2P4	V2P5
16	4	4	4	4	4	5	5	5	4	4	5	4	5	5	5	4
17	4	5	4	4	5	5	5	5	4	5	5	5	5	5	5	4
18	4	5	4	4	5	5	5	5	4	5	5	5	5	5	5	4
19	4	5	4	4	5	5	5	5	4	5	5	5	5	5	5	4
20	4	5	4	4	5	5	5	5	4	5	5	5	5	5	5	4
21	4	5	4	4	5	3	3	4	4	5	5	5	3	3	4	4
22	4	5	4	4	5	5	5	4	5	5	5	5	5	5	4	5
23	4	5	4	4	5	5	4	5	5	5	5	5	5	4	5	5
24	4	5	4	4	5	3	3	4	4	5	5	5	3	3	4	4
25	4	4	4	4	5	5	4	5	4	4	5	5	5	4	5	4
26	4	4	4	4	5	3	3	4	4	4	5	5	3	3	4	4
27	4	5	4	5	5	5	5	5	5	5	4	5	5	5	5	5
28	4	4	4	4	5	5	5	5	4	4	4	5	5	5	5	4
29	4	5	4	5	4	5	4	4	5	5	4	4	5	4	4	5
30	5	5	4	4	4	5	4	5	5	5	4	4	5	4	5	5
31	5	5	5	5	5	4	5	5	4	5	4	5	4	5	5	4
32	5	4	5	5	5	4	5	5	5	4	4	5	4	5	5	5
33	5	5	5	5	5	3	3	4	5	5	4	5	3	3	4	5
34	5	5	5	4	3	3	5	3	5	5	4	3	3	5	3	5
35	5	4	5	4	5	4	5	5	5	4	4	5	4	5	5	5
36	5	4	5	4	5	3	3	4	4	4	4	5	3	3	4	4
37	5	4	5	4	5	4	5	5	4	4	4	5	4	5	5	4
38	4	4	5	5	5	4	5	5	5	4	4	5	4	5	5	5
39	5	5	5	5	4	3	3	3	4	5	4	4	3	3	3	4
40	5	5	5	4	5	4	5	5	5	5	4	5	4	5	5	5
41	5	5	5	5	5	3	3	4	5	5	5	5	3	3	4	5
42	5	5	5	4	3	3	4	4	4	5	5	3	3	4	4	4
43	4	4	5	5	5	4	5	5	5	4	5	5	4	5	5	5
44	5	5	5	5	5	3	3	4	4	5	5	5	3	3	4	4
45	5	5	5	5	5	4	5	5	5	5	5	5	4	5	5	5
46	4	5	5	5	5	5	4	5	5	5	4	5	5	4	5	5
47	4	5	5	5	5	3	3	4	5	5	4	5	3	3	4	5
48	4	5	5	5	5	5	4	5	5	5	4	5	5	4	5	5
49	4	5	5	4	5	5	5	5	5	5	4	5	5	5	5	5
50	4	5	5	5	4	4	4	4	4	5	5	4	4	4	4	4
51																
52																
53																



	V2P5	V2P6	V2P7	V2P8	V2P9	V2P10	V2P11	V2P12	V2P13	V2P14	V2P15	V2P16	V2P17	V2P18	VariableIndep
16	5	4	4	5	5	5	4	5	5	5	4	4	4	4	4	
17	5	4	5	5	5	5	5	5	5	5	4	4	4	5	4	4	
18	5	4	5	5	5	5	5	5	5	5	5	4	5	4	4	
19	5	4	5	5	5	5	5	5	5	5	5	4	5	4	4	
20	5	4	5	5	5	5	5	5	5	5	5	4	5	4	4	
21	4	4	5	5	5	5	5	5	5	5	5	4	5	4	4	
22	4	5	5	5	5	5	5	5	5	4	5	4	5	4	4	
23	5	5	5	5	5	5	5	5	5	5	5	4	5	4	4	
24	4	4	5	5	5	5	5	4	5	5	5	4	5	4	4	
25	5	4	4	5	5	5	4	5	5	5	5	4	4	4	4	
26	4	4	4	5	4	4	4	4	5	5	4	4	4	4	4	
27	5	5	5	4	5	5	5	4	5	4	5	4	5	4	5	
28	5	4	4	4	5	4	4	4	5	4	4	4	4	4	4	
29	4	5	5	4	5	5	5	4	5	5	4	4	5	4	5	
30	5	5	5	4	5	5	5	5	5	5	5	5	5	4	4	
31	5	4	5	4	4	5	5	4	5	5	5	5	5	5	5	
32	5	5	4	4	4	4	4	5	5	5	5	5	4	5	5	
33	4	5	5	4	5	5	5	5	5	5	5	5	5	5	5	
34	3	5	5	4	5	5	5	5	5	5	5	5	5	5	4	
35	5	5	4	4	4	5	4	4	5	5	5	5	4	5	4	
36	4	4	4	4	4	4	4	5	5	5	5	5	4	5	4	
37	5	4	4	4	5	4	4	5	5	5	4	5	4	5	4	
38	5	5	4	4	4	5	4	5	5	5	4	4	4	5	5	
39	3	4	5	4	5	5	5	5	5	5	5	5	5	5	5	
40	5	5	5	4	5	5	5	5	4	5	5	5	5	5	4	
41	4	5	5	5	5	5	5	4	4	5	4	5	5	5	5	
42	4	4	5	5	4	5	5	5	4	5	5	5	5	5	4	
43	5	5	4	5	4	4	4	4	4	5	5	4	4	5	5	
44	4	4	5	5	4	5	5	4	4	5	4	5	5	5	5	
45	5	5	5	5	4	5	5	4	4	5	5	5	5	5	5	
46	5	5	5	4	5	4	5	5	4	5	5	4	5	5	5	
47	4	5	5	4	5	5	5	5	4	5	5	4	5	5	5	
48	5	5	5	4	5	5	5	5	4	5	5	4	5	5	5	
49	5	5	5	4	5	5	5	5	4	5	5	4	5	5	4	
50	4	4	5	5	5	5	5	5	5	5	5	4	5	5	5	
51																
52																
53																

Anexo 8. Matriz de consistencia

PROBLEMA	OBJETIVOS	HIPÓTESIS	Variable independiente: ISO 27001				
			DIMENSION	**INDICADORES**	**ÍTEMS**	**ESCALA DE MEDICIÓN**	**NIVELES RANGOS**
Problema General ¿Cómo mejorara el ISO 27001 en la gestión de seguridad de la información en las áreas de TI de la institución pública?	**Objetivo General** Determinar el ISO 27001 mejora en la gestión de seguridad de la información en el área TI de la institución pública.	**Hipótesis General** El ISO 27001 mejora significativamente la gestión de seguridad de la información en el área TI de la institución pública.	Planificación	a) Análisis de brecha inicial b) Compromiso de alta dirección c) Comprender el contexto de la organización d) Comprender necesidades y expectativas e) Determinar el alcance del SGSI f) Determinar políticas de SI g) Determinar objetivos de SI	1 - 16	Escala Likert 0 Muy Bajo 1 Bajo 2 Medio Bajo 3 Medio	0 – 22 % No existe 23 – 50 % Inicio 51 – 75 % En proceso 76 – 100 % Completo

Problema Especifico ¿Cómo mejorara el ISO 27001 la disponibilidad de información en la seguridad de la información en el área de TI de la institución pública? ¿Cómo mejorara el ISO 27001 la adaptabilidad de la información para la seguridad de la información en el área de TI de la institución pública?	**Objetivo Especifico** Determinar cómo mejora el ISO 27001 la disponibilidad de información en la seguridad de la información en el área de TI de la institución pública. Determinar cómo mejora el ISO 27001 la adaptabilidad de la información para la seguridad de la información en el área de TI de la institución pública. Determinar cómo mejora el ISO 27001 en la accesibilidad de la información para la	**Hipótesis Especifico** El ISO 27001 mejora significativamente la disponibilidad de la información para la gestión seguridad de la información en el área de TI de la institución pública. El ISO 27001 mejora significativamente la adaptabilidad de la información para la gestión seguridad de la información en el área de TI de la institución pública. El ISO 27001 mejora significativamente la accesibilidad de la información para la		h) Crear procedimiento de gestión de riesgos i) Crear procedimiento de gestión de incidencia j) Gestionar los riesgos k) Crear plan de tratamiento de riesgos l) Determinar la declaración de aplicabilidad m) Crear plan de capacitación y concientización		4 Medio Alto 5 Alto	
			Ejecución	c. Implementar plan de tratamiento de riesgos d. Implementar plan de capacitación y concientización	17 - 29		

¿Cómo el ISO 27001 en la accesibilidad de la información para la gestión de seguridad de la información en el área de TI de la institución pública? ¿Cómo el ISO 27001 en el resguardo de la información para la gestión de seguridad de la información en el área de TI de la institución pública?	gestión de seguridad de la información en el área de TI de la institución pública. Determinar cómo mejora el ISO 27001 en el resguardo de la información para la gestión de seguridad de la información en el área de TI de la institución pública.	gestión seguridad de la información en el área de TI de la institución pública. El ISO 27001 mejora significativamente el resguardo de la información para la gestión seguridad de la información en el área de TI de la institución pública.	Verificación	d. Preparar la auditoría interna e. Ejecutar auditoria f. Revisar con la alta dirección los resultados obtenidos	20 – 23		
			Mejora Continua	d. Crear plan de acciones correctivas e. Implementar plan de acciones correctivas f. Análisis de brecha final	24 - 25		

PROBLEMA	OBJETIVOS	HIPÓTESIS	DIMENSION	Variable Dependiente: Gestión de Seguridad de la Información			
				INDICADORES	ÍTEMS	ESCALA DE MEDICION	NIVELES RANGOS
			Disponibilidad	d. Tiempos de acceso e. Tipos de acceso f. Políticas de acceso	1-4	Escala Likert 0 Nunca 1 Casi Nunca 2 A veces	Muy Bajo 0 – 15 % Bajo 16 - 30 % Medio 31 – 60 % Alto 61 – 80 % Muy Alto - 100 %
			Adaptabilidad	e. Crecimiento de información f. Adaptación de nuevas tecnologías g. Espacio disponible h. Capacidad de almacenamiento físico	5-9		
			Accesibilidad	c. Acceso a consultas d. Tiempo de respuesta	10-13		
			Resguardo	e. Respaldo de seguridad f. Almacenamiento del respaldo de seguridad	14-18		

				g. Acceso al respaldo de seguridad h. Seguridad física		3 Casi Siempre 4 Siempre	