ESCUELA DE POSGRADO
UNIDAD DE POSGRADO DE LA FACULTAD DE INGENIERÍA DE SISTEMAS E INFORMÁTICA
PROGRAMA EN MAESTRÍA EN CIENCIAS CON MENCIÓN EN TECNOLOGIA DE LA INFORMACIÓN

Tesis

Sistema de gestión para la seguridad de la información y la confidencialidad de la información, Hospital II-1 Moyobamba, 2024

Para optar el grado académico de Maestro en Ciencias con Mención en Tecnología de la Información

Autor:

Marco Heriberto Herrera Velásquez
https://orcid.org/0009-0009-5091-4111

Asesor:

Dr. Alberto Alva Arévalo
https://orcid.org/0000-0002-8392-3542

Co-Asesor:

Lic. Mg. Milagros Zevallos Ruiz
https://orcid.org/0000-0002-6030-0676

Tarapoto, Perú

2025

ESCUELA DE POSGRADO
UNIDAD DE POSGRADO DE LA FACULTAD DE INGENIERÍA DE SISTEMAS E INFORMÁTICA
PROGRAMA DE MAESTRÍA EN CIENCIAS CON MENCIÓN EN TECNOLOGÍA DE LA INFORMACIÓN

Tesis

Sistema de gestión para la seguridad de la información y la confidencialidad de la información, Hospital II-1 Moyobamba, 2024

Para optar el grado académico de Maestro en Ciencias con Mención en Tecnología de la Información

Autor:

Marco Heriberto Herrera Velásquez
https://orcid.org/0009-0009-5091-4111

Asesor:

Ing. Dr. Alberto Alva Arévalo
https://orcid.org/0000-0002-8392-3542

Co-Asesor:

Lic. Mg. Milagros Zevallos Ruiz
https://orcid.org/0000-0002-6030-0676

Tarapoto, Perú

2025

ESCUELA DE POSGRADO
UNIDAD DE POSGRADO DE LA FACULTAD DE INGENIERÍA DE SISTEMAS E INFORMÁTICA
PROGRAMA DE MAESTRÍA EN CIENCIAS CON MENCIÓN EN TECNOLOGÍA DE LA INFORMACIÓN

Tesis

Sistema de gestión para la seguridad de la información y la confidencialidad de la información, Hospital II-1 Moyobamba, 2024

Para optar el grado académico de Maestro en Ciencias con Mención en Tecnología de la Información

Autor:

Marco Heriberto Herrera Velásquez

Sustentado y aprobado el 13 de febrero del 2025, por los siguientes jurados:

Presidente de Jurado
Ing. Dr. Jorge Damián Valverde Iparraguirre

Secretario de Jurado
Ing. Dr. Juan Orlando Riascos Armas

Vocal de Jurado
Ing. Dr. Elmer Ruiz Trigozo

Asesor
Ing. Dr. Alberto Alva Arévalo

Coasesor
Lic. Mg. Milagros Zevallos Ruiz

Tarapoto, Perú

2025

ACTA DE SUSTENTACIÓN DE TESIS

Los Miembros del Jurado que suscriben, reunidos para estudiar y escuchar la sustentación y defensa del Trabajo de Tesis, modo presencial, presentado por:

Bach. Marco Heriberto Herrera Velásquez

Con el asesoramiento del Ing. Dr. Alberto Alva Arévalo.

"Sistema de gestión para la seguridad de la información y la confidencialidad de la información, en Hospital II-1 Moyobamba, 2024"

Teniendo en consideración los méritos del referido trabajo, así como los conocimientos demostrados por el sustentante, lo declaramos: APROBADO

Con el calificativo (*) MUY BUENO (18)

DIECIOCHO (18)

En consecuencia, queda en condición de ser considerado **APTO** por el Consejo Universitario y recibir el Grado Académico de **Maestro en Ciencias con mención en Tecnología de la Información**, de conformidad con lo estipulado en el Artículo 30° del Reglamento de Tesis de la Escuela de Posgrado de la UNSM.

Tarapoto, 13 de febrero de 2025.

Ing. Dr. Jorge Damián Valverde Iparraguirre
Presidente

Ing. Dr. Juan Orlando Riascos Armas
Secretario

Ing. Dr. Elmer Ruiz Trigozo
Miembro

Ing. Dr. Alberto Alva Arévalo
Asesor

Lic. Mg. Milagros Zevallos Ruiz
Co Asesor

(*) De acuerdo con el Artículo 40° del Reglamento General de Ciencia, Tecnología e Innovación (RG - CTI) la Universidad Nacional de San Martín - Tarapoto, estas deberán ser calificadas con términos de: BUENO, MUY BUENO, EXCELENTE, también considerar la nota

ESCUELA DE POSGRADO
UNIDAD DE POSGRADO DE LA FACULTAD DE INGENIERÍA DE SISTEMAS E INFORMÁTICA
PROGRAMA DE MAESTRÍA EN CIENCIAS CON MENCIÓN EN TECNOLOGÍA DE LA INFORMACIÓN

Tesis

Sistema de gestión para la seguridad de la información y la confidencialidad de la información, Hospital II-1 Moyobamba, 2024

Para optar el grado académico de Maestro en Ciencias con Mención en Tecnología de la Información

El suscrito declara que el presente trabajo de tesis es original, en su contenido y forma

Ejecutor
Marco Heriberto Herrera Velásquez

Asesor
Ing. Dr. Alberto Alva Arévalo

Co - Asesor
Lic. Mg. Milagros Zevallos Ruiz

Tarapoto, Perú

2025

Declaratoria de autenticidad

Yo, **Marco Heriberto Herrera Velásquez**, identificado con DNI N° **46231580**, egresado de la Escuela de Posgrado de la Universidad Nacional de San Martín, Unidad de Posgrado de la Facultad de Ingeniería de Sistemas e Informática, Programa de Maestría en Ciencias con Mención en Tecnología de la Información, con la tesis titulada: **Sistema de gestión para la seguridad de la información y la confidencialidad de la información, Hospital II-1 Moyobamba, 2024.**

Declaro bajo juramento que:

1. Declaro que he redactado completamente esta tesis.
2. Todas las fuentes consultadas están debidamente citadas y referenciadas según estándares internacionales, asegurando que no he plagiado parte alguna de la tesis.
3. Este trabajo no ha sido publicado ni usado para otro título académico.
4. Los resultados son auténticos y no han sido alterados, duplicados ni tomados de otras fuentes, representando contribuciones originales a la investigación realizada.

En caso de que considere que el estudio contiene un error crítico, como información falsa, evidencias manipuladas, o plagio (ya sea al no citar adecuadamente las fuentes o al presentar trabajos ajenos como propios o plagiar ideas de otros, asumo las consecuencias y sanciones de mis actos, acatando las normas de la Universidad Nacional de San Martín.

Tarapoto, 13 de febrero del 2025

Marco Heriberto Herrera Velásquez
DNI N° 46231580

Ficha de identificación

Título del proyecto Sistema de gestión de seguridad de la información y la confidencialidad de la información, Hospital II-1 Moyobamba, 2024	**Área de investigación:** Ciencias de Sistemas e Informática **Línea de investigación:** Estrategias de tecnologías de información y comunicación (TIC) y sistemas constructivos convencionales y no convencionales para el desarrollo sostenible. **Sublínea de investigación:** **Grupo de investigación:** Resolución de Consejo Directivo Nº 0265-2024-UNSM/EPG-CD **Tipo de investigación:** Básica ☐, Aplicada ☒, Desarrollo experimental ☐

Autor: Marco Heriberto Herrera Velásquez	Facultad de Ingeniería de Sistemas e Informática Escuela Profesional de Ingeniería de Sistemas e Informática https://orcid.org/0009-0009-5091-4111
Asesor: Ing. Dr. Alberto Alva Arévalo	**Dependencia local de soporte:** Facultad de Ingeniería de Sistemas e Informática Escuela Profesional de Ingeniería de Sistemas e Informática Unidad o Laboratorio Ingeniería de Sistemas e Informática https://orcid.org/0000-0002-8392-3542
Co-Asesor: Lic. Mg. Milagros Zevallos Ruiz	**Dependencia local de soporte:** Programa de Doctorado en Gestión Universitaria Escuela de Posgrado Unidad o Laboratorio Escuela de Posgrado https://orcid.org/0000-0002-6030-0676

Dedicatoria

Dedico este trabajo con todo mi amor a mi querida hija **Zoe Khaleesi Herrera Díaz**, quien ha sido el motor que me ha impulsado a seguir adelante, a luchar cada día por alcanzar mis sueños y a nunca rendirme, sin importar los obstáculos. Eres mi fuente constante de inspiración y la razón por la que todo esfuerzo tiene sentido.

A mi madre, **Yolanda Velázquez Medina**, por su amor incondicional, su fortaleza y su ejemplo de vida. Gracias por enseñarme que el trabajo, la dedicación y el compromiso son los pilares fundamentales para alcanzar cualquier meta.

Y a mi padre, **Domitilo Herrera Olivera**, que ahora descansa en el cielo, pero cuya sabiduría y valores continúan guiándome. Gracias por mostrarme que con esfuerzo y perseverancia se pueden lograr todos los objetivos, y por ser el ejemplo de lucha que sigue iluminando mi camino.

Este trabajo es el reflejo de su amor, enseñanza y sacrificio. ¡Gracias por todo lo que me han dado!

Marco Heriberto Herrera Velásquez

Agradecimiento

A lo largo de este proceso de investigación y redacción de mi tesis, he recibido el apoyo incondicional de muchas personas a quienes deseo expresar mi más sincero agradecimiento. Sin ellas, este trabajo no habría sido posible.

En primer término, deseo expresar mi más sincero agradecimiento a **mi hija Zoe Khaleesi Herrera Díaz**, quien ha sido mi mayor fuente de motivación. Su amor y energía me han impulsado a seguir adelante, incluso en los momentos más difíciles. Cada paso que doy es por ella, y por su felicidad.

A mis padres, **Yolanda Velázquez Medina** y **Domitilo Herrera Olivera**, por su apoyo constante, por creer en mí, y por enseñarme con su ejemplo que con trabajo, dedicación y perseverancia se puede alcanzar cualquier objetivo. A mi padre, que desde el cielo sigue guiándome, le agradezco por sus lecciones de vida que continúan siendo mi faro.

A mi asesor **Ing. Dr. Alberto Alva Arévalo**, por su invaluable guía, su paciencia y su respaldo a lo largo de todo el proceso de investigación. Su conocimiento y su disposición para guiarme han sido fundamentales para el desarrollo de este trabajo.

A los integrantes del **comité revisor** por su generosidad al compartir su experiencia y sabiduría, y por ayudarme a mejorar mis ideas y enfoques. Sus recomendaciones siempre fueron acertadas y me permitieron crecer tanto académica como profesionalmente.

A mis amigos y compañeros de estudio, por su camaradería, por su comprensión en los momentos de estrés, y por ser una fuente constante de apoyo y ánimo.

Finalmente, agradezco al personal del Hospital II-1 Moyobamba que han colaborado de alguna manera en el desarrollo de este trabajo, ya sea mediante la provisión de recursos, información o el brindarme su tiempo para compartir sus experiencias.

Este trabajo es un reflejo de todo lo que he aprendido de ustedes y de todo el apoyo que he recibido. A todos ustedes, mi más profundo agradecimiento.

Marco Heriberto Herrera Velásquez

Índice general

Índice de tablas

Índice de figuras

RESUMEN

La presente investigación tuvo como objetivo determinar la relación entre el sistema de gestión de seguridad de la información y la confidencialidad de la información en el Hospital II-1 – Moyobamba, 2024. Se desarrolló una investigación de tipo aplicada, enfoque cuantitativo, método deductivo, alcance relacional y diseño no experimental transversal. La muestra estuvo conformada por 16 trabajadores de la institución. Se aplicó la encuesta, mientras que el instrumento usado fue el cuestionario. Los resultados muestran que, el sistema de gestión de seguridad de la información en el Hospital II-1 – Moyobamba es eficiente con 62.5%. El grado de privacidad de los datos en el Hospital II-1 – Moyobamba es considerado alto, con un 56.3%. La efectividad de los controles de seguridad implementados en el hospital muestra una correlación significativa positiva en las dimensiones tecnológicas y de procesos y políticas, pero no en la dimensión cultural y organizacional, lo que indica una debilidad en esta última. Se llegó a concluir que hay una correlación positiva y significativa entre el sistema de administración de seguridad de la información y la confidencialidad de la información (Rho = 0.757 y $p < 0.05$), lo que confirma que un sistema bien gestionado contribuye a mejorar la confidencialidad de la información en el hospital

Palabras clave: Gestión de la seguridad de la información, confidencialidad, políticas, procesos y cultura organizacional

ABSTRACT

The objetive of this research was to determine the relationship between the information security management system and the confidentiality of information at Hospital II-1 – Moyobamba, 2024. An applied type of research was developed, with a quantitative approach, deductive method, relational scope and non-experimental transversal design. The sample consisted of 16 workers of the institution. The survey was applied, while the instrument used was the questionnaire. The results show that the information security management system at Hospital II-1 – Moyobamba is efficient with 62.5%. The degree of data privacy at Hospital II-1 – Moyobamba is considered high, with 56.3%. The effectiveness of the security controls implemented in the hospital shows a significant positive correlation in the technological and process and policy dimensions, but not in the cultural and organizational dimension, which indicates a weakness in the latter. It was concluded that there is a positive and significant correlation between the information security management system and the confidentiality of information (Rho = 0.757 and $p < 0.05$), which confirms that a well-managed system contributes to improving the confidentiality of information in the hospital.

Keywords: Information security management, confidentiality, policies, processes and organizational culture

CAPÍTULO I
INTRODUCCIÓN A LA INVESTIGACIÓN

Desde tiempos remotos, la información ha sido valorada como uno de los recursos más esenciales dentro de una organización, ya que en función de ella se toman decisiones que pueden influir de manera directa o indirecta en la vida de las personas. Con el transcurso del tiempo, los métodos para gestionarla y resguardarla han experimentado transformaciones y avances, adaptándose a las diversas tendencias que han surgido y se han implementado conforme a las necesidades específicas de cada entidad (Altamirano-de-la-Borda, 2021). No obstante, los niveles de competitividad y los altos requerimientos de un mundo cada vez más globalizado, exige a todos el uso obligatorio de herramientas de gestión que les permitan manejar grandes cantidades de información, para de este modo ser más competentes y eficientes en su labor (Santellán et al., 2022).

La seguridad de la información es clave para el crecimiento empresarial, ya que protege los datos y activos tecnológicos mediante principios de confidencialidad, integridad y disponibilidad (Martelo et al., 2015). Según Figueroa-Suárez et al. (2018), la seguridad de la información abarca la protección de datos en cualquier formato, mientras que la seguridad informática, como parte de ella, se centra en resguardar la infraestructura tecnológica y la información digital (Enrique et al., 2010).

Por el contrario, 8 de cada 10 ejecutivos a nivel global afirman que el COVID-19 obligó a las organizaciones a flexibilizar sus procesos de ciberseguridad (Mishima, 2021). Por otro lado, a medida que la tecnología va innovando los ciberataques también se vuelven más sofisticados. Los sectores que más se ven perjudicados por estos ataques son el retail, construcción y financiero (Enrique et al., 2006); sin embargo, existen industrias como salud y automotriz que también son vulnerables (Rodríguez Zambrano & Moreno Tamayo, 2024).

El 76 % de las empresas líderes de TI han experimentado una pérdida grave de datos críticos durante el último año y El 45 % de ellos perdió datos de forma permanente. Siendo, la confidencialidad, uno de las consecuencias de pérdidas económicas, debido a que las filtraciones de datos no sólo ponen en riesgo su reputación y a sus clientes. También agotan sus recursos financieros. Desde los costos de recuperación hasta la pérdida de ingresos, una infracción de este tipo tiene el poder de erosionar incluso los resultados de una gran empresa. Según el informe de IBM de 2023, el coste medio

global de una filtración de datos es 4,45 millones de dólares. Esto supone un aumento del 15 % en los últimos tres años y una buena razón por la que ninguna organización debería dejar sus datos en juego (Nuvo, 2023).

Según la Encuesta de Seguridad de la Información de EY (2020), el 51 % de las empresas en Perú carece de medidas de ciberseguridad. En 2021, otro estudio de EY reveló que los CISO enfrentan constantes desafíos ante amenazas digitales. El 60 % del empresariado está preocupado por los ciberataques, el 47 % ve el cumplimiento normativo como un reto estresante, el 39 % carece de presupuesto suficiente y el 64 % considera excesivo el gasto en tecnología.

En el Hospital II-1 de Moyobamba, se ha identificado una serie de deficiencias en la gestión de la seguridad de la información y protección de la confidencialidad de la misma. Estas deficiencias han surgido debido a una combinación de factores, que incluyen la falta de actualización tecnológica, procesos y políticas obsoletos, y una cultura organizacional que no promueve activamente la protección de la información. La ausencia de un sistema de gestión de seguridad de la información efectivo y la baja confidencialidad de la información en el Hospital II-1 de Moyobamba están poniendo pone en peligro la exactitud, accesibilidad y reserva de la información sensibles de los pacientes y del propio hospital. La información confidencial no está siendo debidamente protegida, lo que aumenta el riesgo de acceso no autorizado, filtraciones de datos y otros incidentes de seguridad. Las consecuencias de esta situación pueden ser graves, incluyendo la pérdida de la confianza del público en el hospital, violaciones de la privacidad de los pacientes, posibles multas por incumplimiento de normativas de protección de datos, y la pérdida de datos críticos que podrían afectar negativamente la provisión de atención médica.

En ese sentido, el propósito de este estudio es determinar la relación entre el sistema de gestión de seguridad de la información y la confidencialidad de la información en el Hospital II-1 de Moyobamba en el año 2024. Para lograr este objetivo, se llevará a cabo un análisis exhaustivo del sistema de gestión de seguridad de la información en el hospital, se identificará el nivel de confidencialidad de la información y se evaluará la efectividad de la implementación de controles de seguridad en la protección de la información ante amenazas tecnológicas, de procesos y políticas, y culturales y organizacionales.

Frente a ello, se formuló la pregunta general ¿Qué relación existe entre el sistema de gestión de seguridad de la información y la confidencialidad de la información en el Hospital II-1 – Moyobamba, 2024? Para la cual, se definió como objetivo general;

Determinar la relación entre el sistema de gestión de seguridad de la información y la confidencialidad de la información en el Hospital II-1 – Moyobamba, 2024. Y como objetivos específicos; a. Analizar el sistema de gestión de seguridad de la información en el Hospital II-1 – Moyobamba, 2024. b) Identificar el nivel de confidencialidad de la información en el Hospital II-1 – Moyobamba, 2024. c) Analizar la efectividad de la implementación de controles de seguridad en la protección de la información ante amenazas tecnológicas, de procesos y políticas, y culturales y organizacionales en el Hospital II-1 – Moyobamba, 2024.

Finalmente, se estableció como hipótesis alterna Ha: El sistema de gestión de seguridad de la información se relaciona significativamente con la confidencialidad de la información en el Hospital II-1 – Moyobamba, 2024. Y como hipótesis nula H0: El sistema de gestión de seguridad de la información no se relaciona significativamente con la confidencialidad de la información en el Hospital II-1 – Moyobamba, 2024.

CAPÍTULO II
MARCO TEÓRICO

2.1. Antecedentes

Zapata Chasiguasin (2020) en su estudio destaca que, para implementar un Sistema de Gestión de Seguridad de la Información según las Normas ISO/IEC 27001, se aplicó una metodología de investigación y evaluación en TI. Se concluyó que, además de definir políticas para los usuarios, es clave aplicarlas a los sistemas de información para reforzar la protección ante vulnerabilidades y amenazas.

Por otro lado, Rodriguez et al. (2020), en su investigación tuvo como objetivo analizar cómo la adopción de la norma ISO 27001 afecta la seguridad de la información en una empresa privada. Para ello, realizaron un estudio con enfoque cuantitativo, empleando un diseño preexperimental. La muestra estuvo conformada por 30 colaboradores, y los resultados evidenciaron, de manera cuantitativa, la influencia de la aplicación de la norma en sus tres dimensiones fundamentales: confidencialidad, integridad y disponibilidad de la información.

Paredes et al. (2019) en su investigación tuvo como objetivo analizar el uso de normas y protocolos de seguridad informática en PYMES de Quevedo, a través de un estudio en 30 empresas. Los resultados abrieron la posibilidad de futuros proyectos y se identificaron herramientas de marketing digital en crecimiento. Se ofrecieron recomendaciones para mejorar el uso de las TIC con seguridad informática, buscando aumentar la estabilidad y competitividad mediante soluciones innovadoras.

Silva Guerrero (2021), en su investigación tuvo el objetivo de poner en marcha un sistema de administración de Seguridad de la Información [SGSI], para mejorar la Seguridad de la Información o SI en una empresa MYPE. En el cual, empleó La autora aplicó la NTP-ISO/IEC 27001:2014, que establece pautas para gestionar el SGSI con mejora continua y enfoque en riesgos. Concluyó que esta norma protege la privacidad, precisión y acceso a la información en la organización.

Castro Rios (2022) manifiesta en su investigación que tuvo como finalidad establecer el vínculo entre la protección de datos y la administración de riesgos en una institución del sistema electoral. El estudio, de enfoque numérico y diseño no experimental, analizó a 45 empleados de la entidad electoral en 2021. Se utilizaron herramientas validadas con alta confiabilidad (Alfa de Cronbach: 0,965 y 0,905). Los resultados mostraron una fuerte

relación positiva entre seguridad de la información y gestión de riesgos (Rho de Spearman: 0,924**, p = 0,000).

Rojas Bustamante & Chura Chura (2022), evaluaron la Norma Técnica Peruana 27001:2014 ISO-IEC en relación con la protección de los sistemas de información en la Municipalidad Gregorio Albarracín, utilizando un enfoque cuantitativo y diseño no experimental. Se seleccionó una muestra de 80 trabajadores, concluyendo que existe una relación entre la norma y la seguridad de los sistemas.

García Cruz (2020) en su investigación tuvo como objetivo proponer la implementación de un sistema de gestión de seguridad de la información basado en la Norma ISO 27001 en la oficina de tecnologías del Gobierno Regional de Piura, buscando minimizar la pérdida de datos. Con un enfoque cuantitativo y diseño descriptivo no experimental, se encuestó a 23 trabajadores, de los cuales el 91 % expresó insatisfacción con la situación actual, mientras que el 100 % consideró necesaria la aplicación de la norma. La investigación destacó la importancia de preservar la confidencialidad, integridad y disponibilidad de la información. En conclusión, se determinó que la propuesta contribuyó a mejorar los procesos de seguridad y comunicación de la información en la entidad.

Flores Vasquez & Varas Valles (2023), implementaron un plan de gobierno de datos en los establecimientos de salud de la Región San Martín (2023) para fortalecer la confidencialidad de la información. Con un diseño preexperimental y 50 colaboradores, los resultados mostraron mejoras en acceso, seguridad, almacenamiento, políticas y auditoría (0,000 < 0,05), concluyendo que la iniciativa optimiza significativamente la protección de la información.

Shuña Pérez (2021), investigó la relación entre la gestión de la información y la toma de decisiones en el Hospital II-2 de Tarapoto (2020). Con una muestra de 30 funcionarios, utilizó una metodología básica, diseño correlacional y encuesta como técnica. Los resultados indicaron que no había relación significativa (p=0.617), aceptándose la hipótesis nula, con una correlación positiva muy baja (Rho de Spearman = 0.095).

2.2. Fundamentos teóricos

2.2.1. SGSI

Es un marco organizativo, técnico y operativo diseñado para garantizar la protección de la información mediante el análisis de la situación planificada, la implementación de

controles, la evaluación de su desempeño y la aplicación de mejoras y correcciones (González Hernández, 2023).

Son procedimientos documentados que protegen la información y establecen medidas preventivas en una organización. Según Duménigo (2012), el ISMS es parte del sistema de gestión de una organización e incluye políticas, procesos y recursos para proteger la información (Panaqué Dominguez et al., 2023).

La información que maneja una organización es su activo más valioso y debe ser protegida para evitar riesgos que comprometan su confidencialidad, accesibilidad e integridad, ya que cualquier vulnerabilidad afectaría a diversas áreas (Donoso Vargas et al., 2023). Si bien existen mecanismos de alerta para protegerla, es crucial contar con un sistema integral que incorpore controles y evalúe los riesgos a los que la organización puede estar expuesta (Chilán & Pionce, 2017). Lluch (2012) afirma que los Sistemas de Gestión de Seguridad de la Información basados en ISO 27001 siguen la mejora continua para optimizar la seguridad organizacional.

Seguridad de la Información

Según Duménigo (2012), La seguridad de la información protege datos y sistemas con medidas técnicas preventivas y reactivas. González Hernández (2023) afirma que “La seguridad de la información es la protección de la integridad, disponibilidad y confidencialidad de la información, según el nivel requerido para los objetivos de negocio de la empresa”.

Evaluar la seguridad de la información implica analizar eventos que puedan comprometer los datos (Martín, 2021). Es clave registrarlos y clasificarlos para una respuesta adecuada (Blandón Jaramillo & Benavides Sepúlveda, 2018).

Secretaría de Gobierno Digital (2018) señala que “La seguridad de la información es el conjunto de medidas preventivas y reactivas de las organizaciones que permiten resguardar y proteger la información buscando mantener las dimensiones (confidencialidad, disponibilidad e integridad) de la misma”.

La seguridad de la información engloba todo tipo de datos, ya sean impresos, manuscritos, registrados con soporte técnico, enviados por correo electrónico, almacenados digitalmente, publicados en sitios web, presentados en videos corporativos o comunicados verbalmente en conversaciones (Bustamante Maldonado & Osorio Cano, 2014).

Secretaría de Gobierno Digital (2018) señalan que: La protección de la información debe integrarse en todos los procesos empresariales, ya sean manuales o automatizados, dado que la información de la organización constituye un elemento clave en cada uno de ellos (Valencia-Duque & Orozco-Alzate, 2017). Estos procesos implican la interacción de personas, tecnologías y vínculos con socios comerciales, clientes o terceros, lo que resalta la importancia de garantizar su seguridad (Vega Velasco, 2008).

Los mercados actuales impulsan la interconexión, exigiendo adaptación, intercambio de información y respuesta a las necesidades (Coronel Suárez & Quirumbay Yagual, 2022). Además, deben diferenciarse de la competencia. En este contexto, la preocupación de las empresas no se limita solo a la productividad o a la innovación en productos y servicios, sino también a la protección frente a posibles ataques informáticos (Marreros et al., 2024). Asimismo, deben garantizar que, a pesar de estos incidentes, la continuidad operativa de sus procesos esenciales se mantenga dentro de los niveles acordados (Rodriguez Baca et al., 2020).

2.2.2. Confidencialidad de la Información

Duménigo (2012) señala que la confidencialidad consiste en evitar el acceso no autorizado a la información, permitiendo su uso solo a personas autorizadas (Alemán Novoa & Rodríguez Barrera, 2015). Este principio clave de la seguridad de la información busca restringir el acceso indebido y proteger los datos sensibles (Ortiz Vasquez, 2022)|.

La confidencialidad es la “cualidad de un mensaje, comunicación o datos, para que solo se entiendan de manera comprensible o sean leídos, por la persona o sistema que esté autorizado, comprende por tanto la privacidad o protección de dicho mensaje y datos que contiene” (Salazar-Lazo & Avila-Correa, 2024).

La confidencialidad es una propiedad que asegura el acceso restringido a la información, impidiendo su divulgación no autorizada a usuarios no identificados (Yory, 2006).

“La confidencialidad en todas las etapas del procesamiento de la información está protegida contra accesos no autorizados que pueden derivar en la alteración o robo de información confidencial” (Urbina, 2015).

“La confidencialidad es la propiedad que impide la divulgación de información a personas o sistemas no autorizados. A grandes rasgos, asegura el acceso a la información únicamente a aquellas personas que cuenten con la debida autorización” (Secretaría de Gobierno Digital, 2018).

Esta propiedad de la información garantiza la prevención de su divulgación a personas no autorizadas.

“La confidencialidad es la garantía de que la información no es conocida por personas, organizaciones o procesos que no disponen de la autorización necesaria” (Secretaría de Gobierno Digital, 2018).

CAPÍTULO III
MATERIALES Y MÉTODOS

3.1. Ámbito de la investigación

3.1.1. Ubicación experimental

La investigación se realizó en el Hospital II-1 de la ciudad de Moyobamba, región de San Martín, Perú.

3.1.2. Ubicación geográfica

Distrito de Moyobamba, provincia Moyobamba y región San Martín, Perú.

3.1.3. Periodo de ejecución

La tesis fue desarrollada durante enero a agosto del 2024.

3.1.4. Aplicación de principios éticos internacionales

El estudio se desarrolló con rectitud y profesionalismo, siguiendo lineamientos nacionales e internacionales que garantizaron su solidez ética. La información fue gestionada con precisión y compromiso, asegurando su autenticidad y exactitud. Se protegió la independencia de los involucrados, evitando cualquier impacto perjudicial para ellos, ya que los hallazgos fueron empleados únicamente con propósitos académicos. Además, se reconoció y documentó a los autores conforme a los estándares internacionales establecidos en la séptima edición de la norma APA.

3.2. Sistema de variables

Variable 1:

- X: Sistema de gestión de seguridad de la información

Variable 2:

- Y: Confidencialidad de la información.

Tabla 1

Descripción de variables por objetivo específico

Objetivo específico N.º 1: Analizar el sistema de gestión de seguridad de la información en el Hospital II-1 – Moyobamba, 2024.			
Variable abstracta	**Variable concreta**	**Medio de registro**	**Unidad de medida**
Análisis de la administración de la protección de datos.	Sistema de gestión de seguridad de la información	Cuestionario	01 trabajador administrativo
Objetivo específico N.º 2: Identificar el nivel de confidencialidad de la información en el Hospital II-1 – Moyobamba, 2024.			
Variable abstracta	**Variable concreta**	**Medio de registro**	**Unidad de medida**
Nivel de confidencialidad de la información	Confidencialidad de la información	Cuestionario	01 trabajador
Objetivo específico N.º 3: Analizar la efectividad de la implementación de controles de seguridad en la protección de la información ante amenazas tecnológicas, de procesos y políticas, y culturales y organizacionales en el Hospital II-1 – Moyobamba, 2024.			
Variable abstracta	**Variable concreta**	**Medio de registro**	**Unidad de medida**
Efectividad de la aplicación de medidas de protección en la protección de la información ante amenazas tecnológicas, de procesos y políticas, y culturales y organizacionales	Modelo de administración para la protección de datos Amenazas tecnológicas Amenazas de procedimientos y normativas Amenazas culturales y organizacionales	Archivo SPSS	Cuantificación total variable “Sistema de gestión de seguridad de la información” Cuantificación de las dimensiones “Tecnológica”, “Procesos y políticas” y “Cultural organizacional”

3.3. Procedimientos de la investigación

Tipo y nivel de la investigación

Aplicada. Según Hernández Sampieri et al. (2014), el estudio aplicado tiene como propósito resolver dificultades específicas mediante el uso del conocimiento existente. En ese sentido, se buscó generar nueva información respecto a las variables de estudio. En la que se determinó la relación del SGSI en la confidencialidad de la información en el Hospital II-1 de Moyobamba.

El alcance será descriptivo relacional. Descriptivo, ya que, fundamentándose en la literatura existente, se pretende especificar el entorno y las particularidades de este estudio. Relacional, ya que buscará medir el vínculo entre los factores del estudio, y dimensiones.

Población y muestra

Población

La población lo conformaron 16 trabajadores en el Hospital II-1 de Moyobamba. Asimismo, la investigación tuvo una muestra igual a la población, en otras palabras, no

se utilizó ningún muestreo estadístico (Cisneros González, 2017). Por lo tanto, se investigó con la participación de los 16 trabajadores en el Hospital II-1 de Moyobamba 2024.

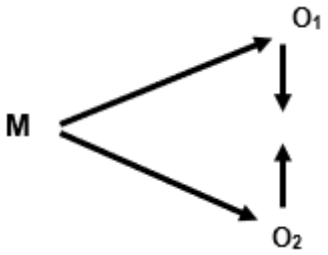
Unidad de análisis

Un trabajador.

Diseño analítico, muestral y experimental

El respectivo diseño de investigación fue no experimental transversal. En este diseño de estudio, no existe la intención deliberada de manipular variables y demostrar cambios mediante experimentos. Además, de que la recolección de los datos fue en una única vez (Ñaupas Paitán et al., 2018).

La investigación estuvo representada mediante el siguiente diseño:



Dónde:

M: Muestra de estudio

O_1: Sistema de gestión de seguridad de la información

O_2: Confidencialidad de la información

R: Relación entre O1 y O2

Técnicas e instrumentos de recolección de datos

Se utilizó la técnica de la encuesta, que consiste en preguntas dirigidas a un grupo seleccionado para recolectar información primaria (Vera et al., 2018). Como instrumento, se emplearon dos cuestionarios basados en las variables del estudio.

Técnicas de procesamiento y análisis de datos

Para el análisis de los datos se emplearon los programas Microsoft Excel 2019 y el software estadístico IBM SPSS Statistics v25, tras la recopilación de información obtenida de la muestra de estudio. Asimismo, se utilizaron medidas de tendencia central, como la media, mediana y moda, junto con medidas de dispersión, como la varianza y la desviación estándar. Para evaluar el grado de correlación entre las variables y sus

dimensiones, se aplicó el coeficiente Rho de Spearman, debido a que los datos no presentaron una distribución normal.

Para medir la significancia de la relación se tendrá en cuenta la siguiente tabla:

Tabla 2
Valoración del grado de correlación de variables

Valor de r	Significado
-0.9	"Correlación negativas muy fuertes"
- 0.75	"Correlación negativas considerables
- 0.5	"Correlación negativas medias
- 0.25	"Correlación negativas débiles
- 0.1	"Correlación negativas muy débiles
0.00	"No existe correlación entre las variables
0.1	"Correlación positivas muy débiles
0.25	"Correlación positivas débiles
0.5	"Correlación positivas medias
0.7	"Correlación positivas considerables
0.9	"Correlación positivas muy fuertes
1	"Correlación positivas perfectas

Fuente: (Hernández Sampieri et al., 2014)

3.1.1. Actividades del objetivo específico 1

Analizar el sistema de gestión de seguridad de la información en el Hospital II-1 – Moyobamba, 2024.

- Elaboración y validación de instrumentos de recolección de datos.
- Aplicación de prueba de confiabilidad.
- Aplicación de encuesta
- Recojo de datos
- Análisis estadístico descriptivo.
- Presentación de resultados

3.1.2. Actividades del objetivo específico 2

Identificar el nivel de confidencialidad de la información en el Hospital II-1 – Moyobamba, 2024.

- Elaboración y validación de instrumentos de recolección de datos.
- Aplicación de prueba de confiabilidad.
- Aplicación de encuesta
- Recojo de datos

- Análisis estadístico descriptivo.
- Presentación de resultados.

3.1.3. Actividades del objetivo específico 3

Analizar la efectividad de la implementación de controles de seguridad en la protección de la información ante amenazas tecnológicas, de procesos y políticas, y culturales y organizacionales en el Hospital II-1 – Moyobamba, 2024.

Actividades realizadas:

- Análisis estadístico inferencial.
- Presentación de resultados.

CAPÍTULO IV
RESULTADO Y DISCUSIÓN

4.1. Resultado objetivo específico 1

Analizar el sistema de gestión de seguridad de la información en el Hospital II-1 – Moyobamba, 2024.

Tabla 3
Evaluación SGSI en Hospital II-1 Moyobamba, 2024

Dimensión/ Variable	Deficiente		Regular		Eficiente		Total	
	N.º	%	N.º	%	N.º	%	N.º	%
Seguridad	1	6.3%	5	31.3%	10	62.5%	16	100%
Gestión	2	12.5%	3	18.8%	11	68.8%	16	100%
Implantación	3	18.8%	4	25.0%	9	56.3%	16	100%
Sistema de gestión de seguridad de la información	**2**	12.5%	**4**	25.0%	**10**	62.5%	**16**	**100%**

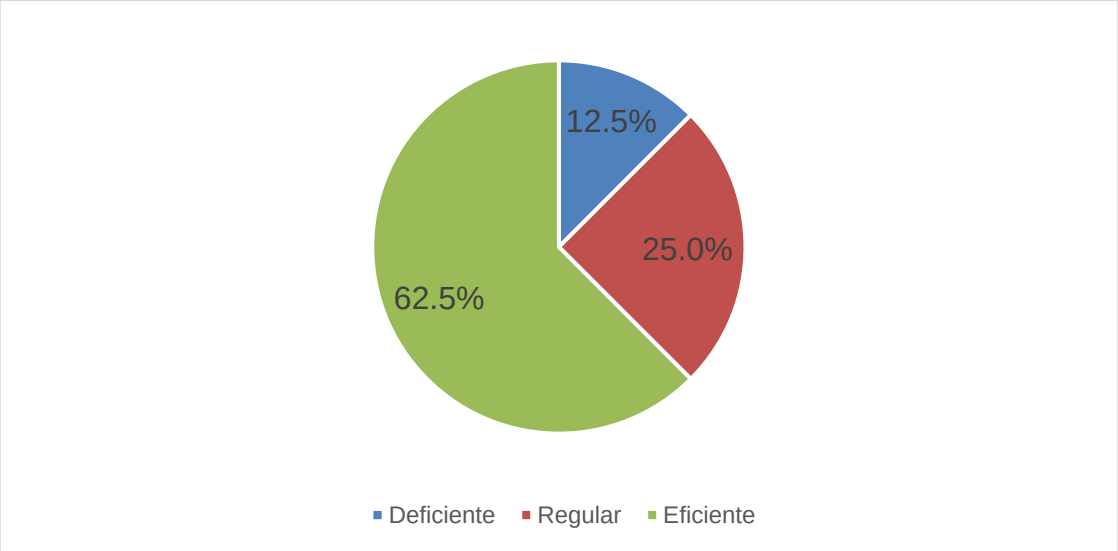


Figura 1
Evaluación de seguridad de la información - Hospital II-1 Moyobamba, 2024

De acuerdo a la tabla 5 y figura 1, se evidencia que el modelo de administración para la protección de datos en el Hospital II-1 – Moyobamba, 2024 es eficiente con una aprobación del 62.5 % de los trabajadores, seguido de una evaluación regular con 25 % y deficiente con 12.5 %. Según dimensiones, la gestión es la de mayor valoración con una aprobación del 68.8 % de los trabajadores, seguido de la seguridad con 62.5 % y finalmente, está la implantación con 56.3 % de aceptación.

4.2. Resultado objetivo específico 2

Identificar el nivel de confidencialidad de la información en el Hospital II-1 – Moyobamba, 2024.

Tabla 4

Nivel de confidencialidad de la información en el Hospital II-1 – Moyobamba, 2024

Dimensión/ Variable	Bajo		Medio		Alto		Total	
	N.º	%	N.º	%	N.º	%	N.º	%
Tecnológica	2	12.5%	6	37.5%	8	50.0%	16	100%
Procesos y políticas	3	18.8%	5	31.3%	8	50.0%	16	100%
Cultural y organizacional	1	6.3%	4	25.0%	11	68.8%	16	100%
Confidencialidad de la información	**2**	12.5%	**5**	31.3%	**9**	56.3%	**16**	**100%**

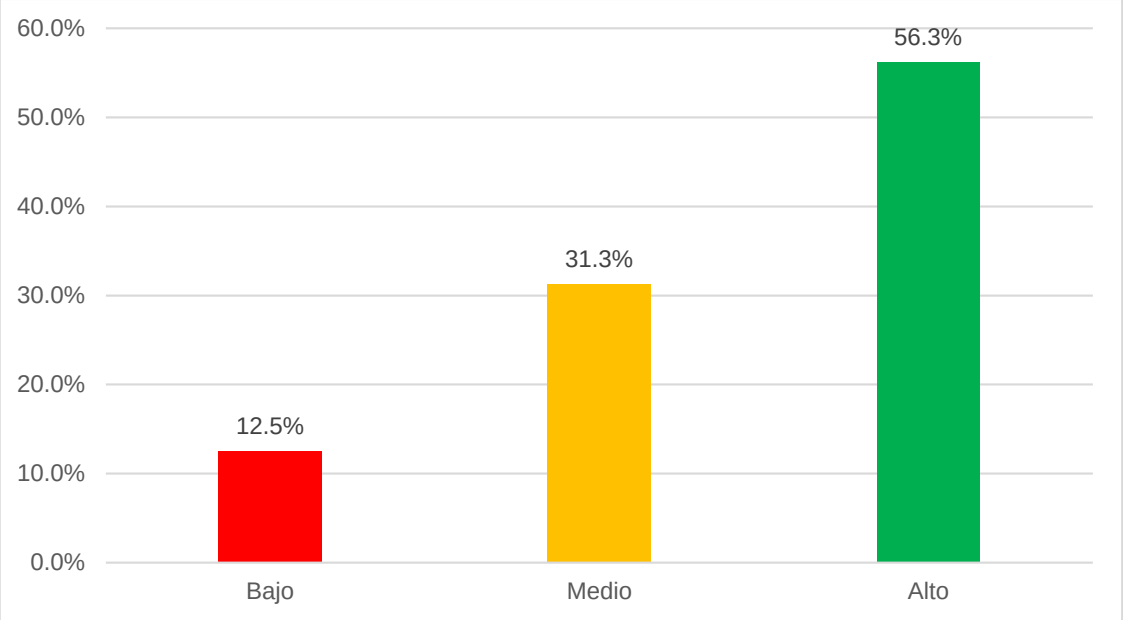


Figura 2

Nivel de confidencialidad de la información en el Hospital II-1 – Moyobamba, 2024

De acuerdo a dicha tabla 6 e figura 2, demuestran que el rango de confidencialidad de la información en el Hospital II-1 – Moyobamba, 2024 es alto con una aceptación del 56.3 % de los trabajadores, Posteriormente, se encuentra un nivel intermedio con un 31.3 % y un nivel bajo con un 12.5 %. De acuerdo con las dimensiones, cultural y organizacional adquiere un nivel superior con una aceptación del 68.8 % en un nivel alto, en tanto, las dimensiones tecnológicas, y procesos y políticas comparten el mismo nivel de aceptación, ambos con 50 % en un nivel alto.

4.3. Resultado objetivo específico 3

Analizar la efectividad de la implementación de controles de seguridad en la protección de la información ante amenazas tecnológicas, de procesos y políticas, y culturales y organizacionales en el Hospital II-1 – Moyobamba, 2024.

Tabla 5

Normalidad de los datos del SGSI y confidencialidad.

	Shapiro Wilk		
	Estadístico	gl	p
Sistema de gestión de seguridad de la información	,832	16	,007
Tecnológica	,912	16	,125
Procesos y políticas	,869	16	,026
Cultural y organizacional	,919	16	,161

Fuente: Datos propios de la investigación

Descripción

Los datos de la variable Sistema de gestión de seguridad de la información no están distribuidos normalmente, el p valor es menor a 0.05, lo mismo, con los datos de la dimensión procesos y políticas. En tanto, los datos de las dimensiones tecnológica, y cultural y organizacional si están distribuidos de manera normal. No obstante, al ser la variable el factor común, no es posible aplicar prueba paramétrica, en consecuencia, se empleó el análisis no paramétrico de asociación Rho de Spearman.

Tabla 6

Correlación entre SGSI y confidencialidad.

			Tecnológica	Procesos y políticas	Cultural y organizacional
Rho de Spearman	Sistema de gestión de seguridad de la información	Rho	,832**	,771**	,488
		p	,000	,000	,055
		N	16	16	16

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

Los datos de la tabla 8 muestra una conexión positiva significativa entre el sistema de seguridad de información con las dimensiones tecnológica y procesos y políticas, más no tiene relación significativa con la dimensión cultural y organizacional. Estos datos indican que los controles de seguridad de los sistemas de información implementados en el Hospital II-1 – Moyobamba, 2024 tienen efectividad significativa en las

dimensiones tecnológica, y en los procesos y políticas, más no es efectivo como tal con la dimensión cultural y organizacional.

4.4. Resultado objetivo general

Determinar la relación entre el sistema de gestión de seguridad de la información y la confidencialidad de la información en el Hospital II-1 – Moyobamba, 2024.

Tabla 7

Prueba de normalidad de datos entre las variables del estudio.

	Shapiro-Wilk		
	Estadístico	gl	p
Sistema de gestión de seguridad de la información	,832	16	,007
Confidencialidad de la información	,870	16	,028

Descripción

En la tabla se visualiza que el valor de significancia de las dos variables (0.007 y 0.028) son menores a 0.05 (margen de error); en consecuencia, se infiere que los datos expuestos no siguen una distribución normal; por lo que el coeficiente de correlación que se utilizó fue la rho de Spearman.

Contraste de hipótesis

Hipótesis alterna (Ha):

El sistema de gestión de seguridad de la información se relaciona significativamente con la confidencialidad de la información en el Hospital II-1 – Moyobamba, 2024.

Hipótesis nula (H0):

El sistema de gestión de seguridad de la información no se relaciona significativamente con la confidencialidad de la información en el Hospital II-1 – Moyobamba, 2024.

Regla de decisión:

Si Sig. (bilateral) > 0.05, aceptamos (H_o).

Pero si Sig. (bilateral) < 0.05, aceptamos (H_a).

Tabla 8

Seguridad y confidencialidad de la información – Hospital II-1 Moyobamba, 2024

			Sistema de gestión de seguridad de la información	Confidencialidad de la información
Rho de Spearman	Sistema de gestión de seguridad de la información	Rho	1,000	,757**
		p	.	,001
		N	16	16
	Confidencialidad de la información	Rho	,757**	1,000
		p	,001	.
		N	16	16

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

De acuerdo a la tabla 10, un coeficiente Rho igual a 0.757 indica relación positiva fuerte y un p igual a 0.001 indica que la relación es significativa. Entonces, según la regla de decisión el valor p es menor al nivel de significancia (0.001 < 0.05), en consecuencia, se aprobó la hipótesis alternativa del estudio y se negó la nula, en consecuencia, se afirma que existe suficiente evidencia estadística para concluir que el modelo de administración para la protección de datos tiene una relación significativa con la confidencialidad de la información en el Hospital II-1 – Moyobamba, 2024.

A modo de discusión, respecto a los resultados encontrados en la presente investigación, empezando con analizar el SGSI en el Hospital II-1 – Moyobamba, 2024. El sistema es percibido como eficiente por la mayoría de los trabajadores, con un 62.5% de ellos calificándolo positivamente. Sin embargo, hay una porción significativa que lo ve como regular (25%) y un pequeño grupo que lo considera deficiente (12.5%). El hecho de que el 62.5% de los trabajadores consideren el sistema eficiente indica que la mayoría confía en su capacidad para administrar la protección de los datos de manera adecuada. Esto sugiere que el sistema cumple con las expectativas en gran medida, aunque no de manera perfecta. No obstante, el 25% de evaluación regular y el 12.5% de evaluación deficiente reflejan que hay áreas dentro del sistema que no están funcionando tan bien como podrían. Estas cifras sugieren la presencia de desafíos o puntos débiles que requieren atención para evitar que la percepción de eficiencia disminuya. Ahora, en cuanto a sus dimensiones, la gestión dentro del modelo de protección de datos es el aspecto más valorado, con un 68.8% de aprobación. Esto significa que los procesos administrativos y de supervisión relacionados con la seguridad son vistos como sólidos y efectivos. En tanto, la seguridad, con un 62.5% de aprobación, indica que los mecanismos para proteger la información son relativamente robustos, pero podrían beneficiarse de mejoras. Por último, la implantación es la

dimensión con la menor aprobación (56.3%), lo que sugiere que la implementación de políticas, procedimientos o tecnologías no ha sido tan exitosa como otros aspectos del sistema. Esta dimensión muestra que la ejecución práctica del sistema tiene deficiencias que podrían estar relacionadas con problemas de capacitación, recursos insuficientes o falta de alineación entre las políticas y su aplicación.

El estudio quiere decir que, aunque el sistema es en su mayoría eficiente, existen áreas que no alcanzan el mismo nivel de desempeño, especialmente en lo que respecta a la implantación. La variabilidad en la percepción de eficiencia refleja la existencia de desigualdades en cómo diferentes partes del sistema están funcionando. El alto porcentaje de aprobación en la gestión sugiere que las políticas y procedimientos están bien diseñados, pero su implementación práctica no siempre es consistente o efectiva, lo que podría estar creando frustraciones o desafíos para los trabajadores.

Al comparar con resultados de otros estudios, se destacan el estudio de García Cruz (2020), quién determinó que la adopción de un SGSI basado en la norma ISO 27001 optimizó los procedimientos de protección de datos, con una alta aceptación por parte de los trabajadores. Además, del estudio de Bernaldo (2018), autor que demostró que la implementación del SGSI fortaleció la administración de riesgos de los activos de datos, aumentando la madurez de 3.65 a 5.22. Ambos estudios y el presente coinciden en que la adopción de un SGSI optimiza la protección de los datos. Los resultados sugieren que estos sistemas son generalmente efectivos, aunque siempre hay espacio para mejorar en áreas específicas. No obstante, la diferencia se encuentra en la evaluación del grado de eficiencia. Mientras que este estudio destaca áreas de mejora, los estudios de García y Bernaldo muestran mejoras significativas sin enfatizar tanto en las deficiencias. Además, estas diferencias en la evaluación de la eficiencia podrían deberse a los diferentes estándares y expectativas de cada organización, o a la fase en la que se encontraba la implementación del SGSI durante la realización de los estudios.

Continuando con el grado de privacidad de los datos en el Hospital II-1 – Moyobamba, 2024. En general, los empleados consideran que la privacidad de los datos está bien protegida, con un 56.3% que califica este aspecto como alto. Sin embargo, hay una variación significativa en la percepción de este nivel de confidencialidad, con un 31.3% que lo considera medio y un 12.5% que lo percibe como bajo. El hecho de que más de la mitad de los trabajadores (56.3%) considere que el nivel de confidencialidad es alto indica que la mayoría percibe que la información está adecuadamente protegida. No obstante, la existencia de un 31.3% que lo ve como medio y un 12.5% que lo ve como bajo sugiere que no todos los aspectos de la confidencialidad están igualmente bien

gestionados. Ahora, en cuanto a sus dimensiones, cultural y organizacional, esta dimensión tiene la mayor aceptación, con un 68.8% de los empleados, evaluándola en un nivel elevado. Esto significa que las normas, valores y comportamientos dentro del hospital, que contribuyen al resguardo de la privacidad de los datos, están bien establecidos y son efectivos. No obstante, tecnológica, procesos y políticas, ambas dimensiones tienen un nivel alto de aceptación del 50%, lo que indica que, aunque son vistas como relativamente sólidas, no alcanzan el mismo nivel de confianza que la dimensión cultural y organizacional. Esto sugiere que hay espacio para mejoras, especialmente en cómo las tecnologías y los procesos apoyan la confidencialidad.

Al comparar con resultados de otros estudios, se destacan el de Rodriguez et al. (2020), quienes encontraron que la implementación de la norma ISO 27001 impacta positivamente en la confidencialidad, integridad y accesibilidad de los datos. Además, el estudio de Moreira (2019), autor que identificó que la falta de procedimientos formales representa una amenaza significativa para la protección de los datos. Tanto este estudio como los de Rodriguez et al. y Moreira reconocen la importancia de las dimensiones tecnológicas y de procesos en la seguridad de la información. Todos coinciden en que estos aspectos son fundamentales para mantener la confidencialidad. No obstante, mientras que este estudio identifica áreas de mejora en tecnología y procesos, Rodriguez et al. concluyeron que la aplicación de la ISO 27001 es suficiente para mejorar estos aspectos. En tanto, Moreira se enfoca en la detección de amenazas por falta de procedimientos formales. Estas diferencias pueden deberse a la madurez del sistema de gestión en cada organización. En este estudio, las áreas de mejora pueden estar relacionadas con la fase de implementación o con la falta de recursos. En contraste, los estudios que encontraron resultados más positivos podrían haber contado con sistemas más avanzados o recursos mejor gestionados.

Acerca de la eficiencia en la aplicación de medidas de protección en la protección de la información ante amenazas tecnológicas, de procesos y políticas, y culturales y organizacionales en el Hospital II-1 – Moyobamba, 2024. Existe una relación positiva significativa entre el sistema de seguridad de la información del Hospital II-1 – Moyobamba, 2024 y dos de las dimensiones evaluadas: la tecnológica y la de procesos y políticas. Sin embargo, no se encontró un vínculo relevante entre el modelo de seguridad de la información y la dimensión cultural y organizacional. La relación positiva significativa con las dimensiones tecnológica y de procesos y políticas indica que el sistema de seguridad de la información es efectivo en estos ámbitos. Es decir, las herramientas tecnológicas y los procedimientos establecidos para proteger la información funcionan bien y están alineados con los objetivos de seguridad del hospital.

Esto sugiere que los controles de seguridad implementados en estas áreas son adecuados y contribuyen de manera importante a la protección de la información. Sin embargo, la ausencia de una relación significativa con la dimensión cultural y organizacional indica que el sistema de seguridad de la información no está teniendo el mismo impacto en la cultura y organización del hospital. Esto sugiere que, aunque los controles técnicos y de procesos son efectivos, no están integrados o respaldados adecuadamente por la cultura organizacional. Dicho de otro modo, la eficiencia del modelo de seguridad podría estar limitada porque no está siendo suficientemente adoptada o internalizada por los empleados y la estructura organizacional.

El estudio quiere decir que, aunque el sistema de seguridad de la información es robusto en una perspectiva técnico y procedimental, su efectividad se ve limitada en su dimensión cultural y organizacional. Esto podría ser una señal de que la seguridad de la información no está completamente incorporada en la cultura de trabajo del hospital, lo que podría manifestarse en comportamientos o actitudes que no apoyan plenamente las políticas de seguridad. En otras palabras, es probable que el hospital haya invertido más recursos y atención en la implementación de controles técnicos y en el desarrollo de políticas y procedimientos, lo que explica la fuerte relación en estas áreas. Sin embargo, puede haber subestimado la importancia de cultivar una cultura organizacional que respalde estas medidas de seguridad.

Al comparar con resultados de otros estudios, se destacan el de Zapata Chasiguasin (2020), autor que resaltó la importancia de aplicar políticas tanto a usuarios como a sistemas de información para enfrentar amenazas. Además, el estudio de Niño (2018), quién enfatizó la importancia de un programa para la administración de amenazas que incluya aspectos culturales y organizacionales. Ambos estudios, al igual que el desarrollado, reconocen la importancia de los aspectos tecnológicos y procedimentales. También coinciden en la necesidad de integrar la cultura organizacional en la administración de la protección. Este estudio destaca una debilidad en la dimensión cultural y organizacional, mientras que Niño Morante subraya la necesidad de fortalecer esta área, sugiriendo que es una preocupación común, aunque con diferentes enfoques. La debilidad en la dimensión cultural y organizacional podría ser una problemática general en muchas organizaciones, no solo en el Hospital II-1. Es posible que las empresas inviertan más en tecnología y procesos formales, descuidando la importancia de una cultura organizacional fuerte que respalde estas políticas.

Por último, sobre determinar la relación entre el sistema de gestión de seguridad de la información y la confidencialidad de la información en el Hospital II-1 – Moyobamba,

2024. Basada en el análisis estadístico, se establece que existe una relación significativa y fuerte entre el sistema de gestión de seguridad de la información y la confidencialidad de la información en el Hospital II-1 – Moyobamba, 2024. Este resultado se basa en un coeficiente Rho de Spearman de 0.757 y un valor p de 0.001. El coeficiente Rho de 0.757 indica una relación positiva fuerte entre las variables analizadas. En este contexto, significa que a medida que el SGSI mejora o se fortalece, también aumenta la confidencialidad de la información. Un coeficiente cercano a 1, como en este caso, señala que hay una correspondencia directa y consistente entre la calidad del sistema de seguridad y el nivel de confidencialidad. Por su parte, el valor p es una medida que ayuda a determinar la significancia estadística de los resultados. En este caso, un valor p de 0.001, que es inferior al umbral de significancia comúnmente utilizado (0.05), indica que la probabilidad de que la vinculación identificada entre el modelo de administración para la protección de datos y la confidencialidad de la información se deba al azar es extremadamente baja. Esto refuerza la confianza en que la relación observada es real y significativa.

Lo que el estudio quiere decir es que hay evidencia estadística sólida para afirmar que la calidad y efectividad del SGSI en el Hospital II-1 – Moyobamba está directamente relacionada con el nivel de privacidad de los datos. Un modelo de administración para la protección de la información bien implementado y gestionado mejora significativamente la protección de la información confidencial en el hospital.

Al respecto, al comparar estos resultados con las de otras investigaciones, se puede destacar que, Castro Rios (2022), encontró una relación totalmente positiva entre la protección de los datos y la administración de riesgos (Rho = 0.924**). Mientras que Shuña Pérez (2021), concluyó que no se evidencia un vínculo relevante entre la administración de los datos y la toma de decisiones en un contexto hospitalario (p=0.617). En resultados similares, claramente está el de Castro, ya que ambos estudios encontraron una fuerte correlación entre variables clave relacionadas con la seguridad de la información. Esto sugiere que un buen modelo de protección mejora otros aspectos críticos, como la confidencialidad o la gestión de riesgos. Por otro lado, la diferencia principal radica en el estudio de Shuña, que no encontró relación significativa, lo que contrasta con la fuerte correlación encontrada en tu estudio. Estas diferencias pueden atribuirse a las particularidades de cada organización y los diferentes enfoques metodológicos utilizados. Mientras que este estudio y el de Castro se centraron en aspectos directamente vinculados a la seguridad y la gestión de riesgos, el estudio de Shuña exploró la relación entre gestión de información y toma de decisiones, lo que puede ser menos directo o estar influenciado por factores externos no considerados.

En fin, los hallazgos de esta investigación coinciden con los resultados de otros estudios en la medida en que subrayan la importancia de un sistema de gestión de seguridad de la información robusto para mejorar la confidencialidad y la seguridad general de la información. Sin embargo, también revelan áreas específicas que requieren más atención, como la integración del entorno corporativo en la protección de los datos.

CONCLUSIONES

1. Se evidencia un vínculo positivo y relevante entre el modelo de administración para la protección de datos y la confidencialidad de la información (Rho = 0.757 y $p < 0.05$), lo que confirma que un sistema bien gestionado contribuye a mejorar la confidencialidad de la información en el hospital.

2. El sistema de gestión de seguridad de la información en el Hospital II-1 – Moyobamba es eficiente, con una aprobación del 62.5% por parte de los trabajadores. Sin embargo, la implantación de este sistema muestra áreas de mejora, dado que solo obtuvo un 56.3% de aceptación.

3. El grado de privacidad de los datos en el Hospital II-1 – Moyobamba es considerado alto, con un 56.3% de aceptación entre los trabajadores. No obstante, existe una menor confianza en los aspectos tecnológicos y de procesos y políticas, que requieren mayor atención para asegurar su efectividad.

4. La eficiencia de las medidas de protección implementados en el hospital muestra una correlación significativa positiva en las dimensiones tecnológicas y de procesos y políticas, pero no en la dimensión cultural y organizacional, lo que indica una debilidad en esta última.

RECOMENDACIONES

1. Para la Alta Dirección del Hospital: Es recomendable continuar invirtiendo en el fortalecimiento del sistema de gestión de seguridad de la información, asegurando que todos sus componentes estén alineados y operen de manera efectiva para preservar y fortalecer la privacidad de los datos.

2. Para la Dirección del Hospital: Se recomienda implementar programas de formación y mejora continua centrados en la implementación del modelo de protección de datos. Esto fortalecerá las áreas menos valoradas y mejorará la eficacia general del sistema.

3. Para el Departamento de TI y Gestión de la Información: Es crucial reforzar las medidas tecnológicas y las políticas de procesos para asegurar un alto nivel de confidencialidad en todas las dimensiones. Esto podría incluir la actualización de tecnologías y la revisión periódica de políticas de seguridad.

4. Para el CSI, es esencial diseñar una estrategia de acción enfocada en fortalecer la cultura empresarial en relación con la seguridad de la información. Esto puede incluir la organización de capacitaciones, iniciativas de concienciación y la incorporación de la protección de datos dentro de los principios fundamentales de la institución.

REFERENCIAS BIBLIOGRÁFICAS

Alemán Novoa, H., & Rodríguez Barrera, C. (2015). Metodologías para el análisis de riesgos en los sgsi. *Publicaciones e Investigación*, *9*, 73. https://doi.org/10.22490/25394088.1435

Altamirano-de-la-Borda, K. J. (2021). *La seguridad de la información en la administración pública*. 77–95. https://doi.org/10.26439/ciis2020.5480

Blandón Jaramillo, C. A., & Benavides Sepúlveda, A. M. (2018). Modelo sistema de gestión de seguridad de la información para instituciones educativas de nivel básico. *Scientia et Technica*, *23*(1), 85–92. https://doi.org/10.22517/23447214.15861

Bustamante Maldonado, G., & Osorio Cano, J. A. (2014). Metodología de la seguridad de la información como medida de protección en pequeñas empresas. *Cuaderno Activa*, *6*, 71–77. http://ojs.tdea.edu.co/index.php/cuadernoactiva/article/view/202/206

Castro Rios, H. (2022). *Seguridad de la información y gestión del riesgo en una entidad del sistema electoral, año 2021*.

Chilán, E. I., & Pionce, W. F. (2017). Apuntes teóricos introductorios sobre la seguridad de la información. *Dominio de Las Ciencias*, *3*(4), 285–295.

Cisneros González, R. (2017). Trilogía de la investigación. In *Entretextos* (Vol. 9, Issue 25). https://doi.org/10.59057/iberoleon.20075316.201725338

Coronel Suárez, I., & Quirumbay Yagual, D. (2022). Seguridad informática, metodologías, estándares y marco de gestión en un enfoque hacia las aplicaciones web. *Revista Científica y Tecnológica UPSE*, *9*(2), 97–108. https://doi.org/10.26423/rctu.v9i2.672

Donoso Vargas, D., Calahorrano Recalde, C., & Donoso Vargas, S. (2023). Application of the Iso 27001 Isms in the Social Rehabilitation System of Ecuador. *Universidad y Sociedad*, *15*(2), 274–284.

Duménigo, D. (2012). Sistemas de información, aplicación en empresas. *Universidad Central Marta Abreu de Las Villas*, 16. http://www.eumed.net/ce/2012/ddb.html

Enrique, L., Crespo, S., Fernández-Medina, E., & Piattini, M. (2006). *Modelos de madurez para SGSI desde un enfoque práctico Hybrid classical-quantum computing View project*. https://www.researchgate.net/publication/272089072

Enrique, L., Crespo, S., Santos, A., Parra, O., Fernández-Medina, E., & Piattini, M. (2010). *Características deseables para un SGSI orientado a PYMES Hybrid classical-quantum computing View project ArchiRev View project*. 978–987. https://www.researchgate.net/publication/232252352

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

Flores Vasquez, L., & Varas Valles, T. (2023). *Implementación de un plan de gobierno de datos para garantizar la confidencialidad de la información en establecimientos de salud, San Martín 2023*.

García Cruz, R. A. (2020). Propuesta de un sistema de gestion de seguridad de la informacion basado en la norma ISO 27001 para la oficina de Tecnologias de Informacion del Gobierno Regional Piura; 2020. *Univerisidad Catolica Los Ángeles de Chimbote*, *9*, 102. http://repositorio.uladech.edu.pe/handle/123456789/20291

González Hernández, I. (2023). Protección de datos y seguridad de la información. *Revista Canaria de Administración Pública*, *1 SE-Protección de datos y seguridad de la información*, 285–311. https://doi.org/10.36151/RCAP.2023.9

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, P. (2014). Metodología de la Investigación. Sexta Edición. Editorial McGraw-Hill. *México. Recuperado de: Http://Observatorio. Epacartagena. Gov. Co/Wpcontent/Uploads/2017/08/Metodologia-de-La-Investigación-Sexta-Edicion. Compressed. Pdf*.

Lluch, C. (2012). Guía de iniciación a actividad profesional implantación de SGSI según la norma ISO 27001. *Coit*, 46. https://www.coit.es/sites/default/files/informes/pdf/implantacion_de_sistemas_de_gestion_de_la_seguridad_de_la_informacion_sgsi_segun_la_norma_iso_27001.pdf

Marreros, J., Acosta, D., & Mendoza, A. (2024). Mecanismos de seguridad de la información en una organización: una revisión sistemática. *Revista Científica Ciencias Ingenieriles*, *4*(1), 79–90. https://doi.org/10.54943/ricci.v4i1.384

Martelo, R. J., Madera, J. E., & Betín, A. D. (2015). Software para Gestión Documental, un Componente Modular del Sistema de Gestión de Seguridad de la Información (SGSI). *Información Tecnológica*, *26*(2), 129–134. https://doi.org/10.4067/S0718-

07642015000200015

Martín, T. (2021). *Automation of an information security management system based on the ISO / IEC 27001 Standard*. *13*, 495–506.

Ñaupas Paitán, H., Valdivia Dueñas, M. R., Palacios Vilela, J. J., & Romero Delgado, H. E. (2018). Metodología de la investigación cuantitativa-cualitativa y redacción de la tesis. In 5ta Edición (Ed.), *Journal of Chemical Information and Modeling* (Vol. 53, Issue 9). Ediciones de la U. https://doi.org/10.1017/CBO9781107415324.004

Ortiz Vasquez, S. (2022). *Sistema de Gestión de Seguridad de la Información (SGSI) Para Planeta, Proyectos y Obras S.A.S.* http://hdl.handle.net/11349/31371

Panaqué Dominguez, J. A., Lizárraga Caipo, Y. G., & Mendoza De los Santos, A. (2023). Efectos de la implementación de un SGSI basado en la norma ISO 27001 para las organizaciones. *Perfiles de Ingeniería*, *18*(18), 67–74. https://doi.org/10.31381/perfilesingenieria.v18i18.5399

Raquel, A., Paredes, Z., Mecías, I., Quevedo, S., Javier, L., & Chalacán, M. (2019). Seguridad informática en las PyMES de la ciudad de Quevedo. *Journal of Business and Entrepreneurial*, *4*(2), 1–10. https://doi.org/10.37956/jbes.v4i2.971.1.1http://journalbusinesses.com/index.php/revistaeISSN:2576-0971

Rodriguez, B. L. S., Puente De La Vega, C. C. F., Mejía, C. C., & Alarcón, D. M. A. (2020). Aplicación de ISO 27001 y su influencia en la seguridad de la información de una empresa privada peruana Application of ISO 27001 and its influence on the information security of a Peruvian private company. *Propósitos y Representaciones*, *8*, 786. http://dx.doi.org/10.20511/pyr2020.v8n3.786ORCID:https://orcid.org/0000-0003-1850-615XORCID:https://orcid.org/0000-0001-7471-3140http://dx.doi.org/10.20511/pyr2020.v8n3.786

Rodriguez Baca, L. S., Cruzado Puente de la Vega, C. F., Mejía Corredor, C., & Alarcón Diaz, M. A. (2020). Aplicación de ISO 27001 y su influencia en la seguridad de la información de una empresa privada peruana. *Propósitos y Representaciones*, *8*(3 SE-Notas de investigación), e786. https://doi.org/10.20511/pyr2020.v8n3.786

Rodríguez Zambrano, H. M., & Moreno Tamayo, C. H. (2024). Seguridad de la información y ciberseguridad: su importancia para los Estados, empresas y las personas, una revisión sistemática. *Estudios y Perspectivas Revista Científica y*

Académica, *4*(1), 159–178. https://doi.org/10.61384/r.c.a..v4i1.90

Rojas Bustamante, J. J., & Chura Chura, A. W. (2022). *Norma técnica peruana 27001: 2014 ISO-IEC y seguridad en sistemas de información de la Municipalidad Gregorio Albarracín, Tacna 2022*.

Salazar-Lazo, C., & Avila-Correa, B. (2024). Estándares de Ciberseguridad Aplicables a los Sistemas Informáticos Sanitarios para Proteger los Datos Personales. *593 Digital Publisher CEIT*, *9*(1), 88–102. https://doi.org/10.33386/593dp.2024.1.2156

Santellán, K., Palomino, G., & Whittembury, K. (2022). Gestión de la información y comunicación para un hospital público del Perú. *Revista San Gregorio*, *1*(52), 37–50. http://scielo.senescyt.gob.ec/scielo.php?script=sci_arttext&pid=S2528-79072022000400037&lng=es&nrm=iso&tlng=es

Secretaría de Gobierno Digital. (2018). Lineamientos para la Formulación del Plan de Gobierno Digital en el Perú - PGD. *Secretaría de Gobierno Digital*, 35. https://cdn.www.gob.pe/uploads/document/file/356863/Anexo_I_Lineamientos_PGD.pdf?v=1567095341

Shuña Pérez, R. (2021). *Gestión de la información y toma de decisiones en las referencias y contrareferencias del Hospital II–2, Tarapoto, 2020*.

Silva Guerrero, A. R. (2021). *Implementación de un sistema de gestión de seguridad de la información para mejorar la seguridad de la información en una empresa MyPE, 2021*.

Urbina, G. B. (2015). *Proyectos de sistemas de información*. Grupo Editorial Patria.

Valencia-Duque, F. J., & Orozco-Alzate, M. (2017). Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000. *RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao*, *22*, 73–88. https://doi.org/10.17013/risti.22.73-88

Vega Velasco, W. (2008). Politicas Y Seguridad De La Informacion. *Fides Et Ratio*, *2*(2), 63–69.

Vera, J., Castaño, R., & Torres, Y. (2018). Fundamentos de metodología de la investigación científica. In *Fundamentos de metodología de la s Grupo de capacitación e investigación pedagógica investigación científica: Vol. Primera ed*. http://142.93.18.15:8080/jspui/bitstream/123456789/274/3/libro.pdf

Yory, J. (2006). Un acercamiento a las mejores prácticas de seguridad de información

internacionalmente reconocidas en el estándar ISO 17799:2005. *Mva*, 30.

Zapata Chasiguasin, K. B. (2020). Sistema De Gestión De Seguridad De La Información Basado En Las Normas Iso/Iec 27001, En El Departamento De Tecnologias De La Informacion Del Gobierno Autonomo Descentralizado De La Municipalidad De Ambato. *Universidad Técnica De Ambato*, 1–155. https://repositorio.uta.edu.ec/jspui/bitstream/123456789/30694/3/Tesis_t1661si.pdf

ANEXOS

Anexo 1. Matriz de consistencia

Título: Sistema de Gestión para la seguridad de la información y la confidencialidad de la información en Hospital II-1 - Moyobamba, 2024

Formulación del problema

General

¿Qué relación existe entre el sistema de gestión de seguridad de la información y la confidencialidad de la información en el Hospital II-1 – Moyobamba, 2024?

Objetivo

General

Determinar la relación entre el sistema de gestión de seguridad de la información y la confidencialidad de la información en el Hospital II-1 – Moyobamba, 2024.

Específicos

- Analizar el sistema de gestión de seguridad de la información en el Hospital II-1 – Moyobamba, 2024.
- Identificar el nivel de confidencialidad de la información en el Hospital II-1 – Moyobamba, 2024.
- Analizar la efectividad de la implementación de controles de seguridad en la protección de la información ante amenazas tecnológicas, de procesos y políticas, y culturales y organizacionales en el Hospital II-1 – Moyobamba, 2024.

Hipótesis

General

El sistema de gestión de seguridad de la información se relaciona significativamente con la confidencialidad de la información en el Hospital II-1 – Moyobamba, 2024.

Tipo, nivel y diseño de investigación

El tipo de investigación es Aplicada
Diseño no experimental
Nivel de investigación descriptivo relacional

Población y muestra

Población

La población estará comprendida por 16 trabajadores en el Hospital II-1 de Moyobamba.

Muestra:

La muestra está representada por 16 trabajadores en el Hospital II-1 de Moyobamba.

Variable de estudio

Variable	Dimensiones
Sistema de gestión de seguridad de la información.	Seguridad
	Gestión.
	Implantación
Confidencialidad de la información	Tecnológica
	Procesos y políticas
	Cultural y organizacional

Técnicas e instrumentos

Técnica: Encuesta
Instrumento: Cuestionario

Anexo 2. Instrumento de recolección de datos

UNIVERSIDAD NACIONAL DE SAN MARTIN – TARAPOTO
ESCUELA DE POSGRADO
FACULTAD DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

TEMA: **"Sistema de gestión de seguridad de la información y la confidencialidad de la información, Hospital II-1 Moyobamba, 2024"**

Cuestionario "Sistema de gestión de seguridad de la información"

Instrucciones: A continuación, se le presenta una serie de preguntas que deberá responder de acuerdo a su punto de vista.

Estimado colaborador, a continuación, tienes 18 preguntas sobre el Sistema de Gestión para la seguridad de la Información, para lo cual debes marcar con el número de la tabla la opción que consideras correcta:

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

N		1	2	3	4	5
Dimensión: Seguridad						
1	La información confidencial está protegida adecuadamente en nuestra institución.					
2	Se aplican políticas y procedimientos claros para el acceso y manejo de la información confidencial.					
3	Existe un control eficiente para prevenir accesos no autorizados a la información sensible.					
4	Nuestro sistema de seguridad de la información se actualiza regularmente para hacer frente a las nuevas amenazas.					
5	Se realizan auditorías periódicas para evaluar la efectividad de nuestras medidas de seguridad de la información.					
6	La formación sobre seguridad de la información es adecuada y se imparte regularmente al personal.					
Dimensión: Gestión						
7	La alta dirección muestra un compromiso claro con la seguridad de la información.					

8	Existe un responsable designado para la gestión de la seguridad de la información en nuestra institución.					
9	Se asignan recursos adecuados para implementar y mantener el sistema de gestión de seguridad de la información.					
10	Se establecen objetivos claros para mejorar continuamente la seguridad de la información.					
11	Las responsabilidades del personal en relación con la seguridad de la información están definidas y comunicadas.					
12	Se realizan revisiones periódicas del sistema de gestión de seguridad de la información para garantizar su efectividad.					
Dimensión: Implantación						
13	Se cuenta con los recursos tecnológicos necesarios para garantizar la seguridad de la información.					
14	La documentación relacionada con la seguridad de la información está actualizada y disponible para el personal.					
15	Los incidentes de seguridad de la información se registran, investigan y gestionan adecuadamente.					
16	Existe un plan de respuesta a incidentes de seguridad de la información y se prueba regularmente.					
17	Se realizan copias de seguridad periódicas de la información crítica y se almacenan de forma segura.					
18	Se realizan pruebas de seguridad de manera regular para evaluar la robustez del sistema de gestión de seguridad de la información.					

UNIVERSIDAD NACIONAL DE SAN MARTIN – TARAPOTO
ESCUELA DE POSGRADO
FACULTAD DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

TEMA: **"Sistema de gestión de seguridad de la información y la confidencialidad de la información, Hospital II-1 Moyobamba, 2024"**

Cuestionario "Confidencialidad de la información"

Instrucciones: A continuación, se le presenta una serie de preguntas que deberá responder de acuerdo a su punto de vista.

Estimado colaborador, a continuación, tienes 18 preguntas sobre la confidencialidad de la Información en la organización, para lo cual debes marcar con el número de la tabla la opción que consideras correcta:

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

N		1	2	3	4	5
Dimensión: Tecnológica						
1	Los sistemas de cifrado se utilizan adecuadamente para proteger la información confidencial en nuestra institución.					
2	Nuestros sistemas de seguridad de la información, como firewalls y detección de intrusos, son efectivos para prevenir accesos no autorizados.					
3	Se utiliza un control de acceso adecuado para restringir quién puede ver y modificar la información confidencial.					
4	Los sistemas informáticos están actualizados regularmente para protegerse contra nuevas amenazas de seguridad.					
5	Se realizan copias de seguridad de la información confidencial de manera regular y se almacenan de forma segura.					
6	Se llevan a cabo pruebas de seguridad de manera periódica para evaluar la efectividad de nuestras medidas de seguridad tecnológica.					
Dimensión: Procesos y políticas						
7	Se aplican políticas claras para el manejo de la información confidencial en nuestra institución.					
8	Existen procedimientos establecidos para garantizar que solo el personal autorizado tenga acceso a la información confidencial.					

9	La documentación relacionada con la seguridad de la información está actualizada y disponible para el personal.					
10	Se realizan auditorías periódicas para evaluar el cumplimiento de las políticas de seguridad de la información.					
11	Se lleva a cabo una formación regular sobre seguridad de la información para todo el personal.					
12	Se lleva a cabo una formación regular sobre seguridad de la información para todo el personal.					
Dimensión: Cultural y organizacional						
13	Existe un compromiso claro por parte de la dirección con la seguridad de la información.					
14	Se fomenta una cultura de seguridad de la información en nuestra institución.					
15	Los empleados entienden la importancia de mantener la información confidencial segura.					
16	Se promueve la responsabilidad individual en la protección de la información confidencial.					
17	La seguridad de la información se considera como parte integral de nuestra cultura corporativa.					
18	La dirección de la institución apoya activamente las iniciativas para mejorar la seguridad de la información.					

Anexo 3. Validación de instrumentos

INFORME DE OPINIÓN SOBRE INSTRUMENTO DE INVESTIGACIÓN CIENTÍFICA

I. DATOS GENERALES

Apellidos y nombres del experto : Dr. Wilson Torres Delgado
Institución donde labora : Universidad Nacional de San Martín - Tarapoto
Especialidad : Licenciado en estadística – COESPE 380
Instrumento de evaluación de la información : Cuestionario: Sistema de gestión de seguridad de la información
Autor (s) del instrumento (s) : Marco Heriberto Herrera Velásquez

II. ASPECTOS DE VALIDACIÓN

MUY DEFICIENTE (1) DEFICIENTE (2) ACEPTABLE (3) BUENA (4) EXCELENTE (5)

CRITERIOS	INDICADORES	1	2	3	4	5
CLARIDAD	Los ítems están redactados con lenguaje apropiado y libre de ambigüedades acorde con los sujetos muestrales.					X
OBJETIVIDAD	Las instrucciones y los ítems del instrumento permiten recoger la información objetiva sobre la variable, en todas sus dimensiones en indicadores conceptuales y operacionales.					X
ACTUALIDAD	El instrumento demuestra vigencia acorde con el conocimiento científico, tecnológico, innovación y legal inherente a la variable: Sistema de gestión de seguridad de la información.				X	
ORGANIZACIÓN	Los ítems del instrumento reflejan organicidad lógica entre la definición operacional y conceptual respecto a la variable, de manera que permiten hacer inferencias en función a las hipótesis, problema y objetivos de la investigación.					X
SUFICIENCIA	Los ítems del instrumento son suficientes en cantidad y calidad acorde con la variable, dimensiones e indicadores.				X	
INTENCIONALIDAD	Los ítems del instrumento son coherentes con el tipo de investigación y responden a los objetivos, hipótesis y variable de estudio: Sistema de gestión de seguridad de la información				X	
CONSISTENCIA	La información que se recoja a través de los ítems del instrumento, permitirá analizar, describir y explicar la realidad, motivo de la investigación.				X	
COHERENCIA	Los ítems del instrumento expresan relación con los indicadores de cada dimensión de la variable: Sistema de gestión de seguridad de la información					X
METODOLOGÍA	La relación entre la técnica y el instrumento propuestos responden al propósito de la investigación, desarrollo tecnológico e innovación.					X
PERTINENCIA	La redacción de los ítems concuerda con la escala valorativa del instrumento.					X
PUNTAJE TOTAL		46				

(Nota: Tener en cuenta que el instrumento es válido cuando se tiene un puntaje mínimo de 41 “Excelente”; sin embargo, un puntaje menor al anterior se considera al instrumento no válido ni aplicable)

III. OPINIÓN DE APLICABILIDAD

Establecido los valores de aplicabilidad se llegó a determinar que el instrumento de recolección de datos se encuentra listo para su ejecución con validación obtenida de “Excelente”

PROMEDIO DE VALORACIÓN: **46**

Tarapoto 13 de mayo de 2024

INFORME DE OPINIÓN SOBRE INSTRUMENTO DE INVESTIGACIÓN CIENTÍFICA

I. DATOS GENERALES

Apellidos y nombres del experto : Dr. Andi Lozano Chung
Institución donde labora : Universidad Nacional de San Martín
Especialidad : Docente en la Universidad Nacional de San Martín
Instrumento de evaluación : Cuestionario: Sistema de gestión de seguridad de la información
Autor (s) del instrumento (s) : Marco Heriberto Herrera Velásquez

II. ASPECTOS DE VALIDACIÓN

MUY DEFICIENTE (1) DEFICIENTE (2) ACEPTABLE (3) BUENA (4) EXCELENTE (5)

CRITERIOS	INDICADORES	1	2	3	4	5
CLARIDAD	Los ítems están redactados con lenguaje apropiado y libre de ambigüedades acorde con los sujetos muestrales.				X	
OBJETIVIDAD	Las instrucciones y los ítems del instrumento permiten recoger la información objetiva sobre la variable, en todas sus dimensiones en indicadores conceptuales y operacionales.					X
ACTUALIDAD	El instrumento demuestra vigencia acorde con el conocimiento científico, tecnológico, innovación y legal inherente a la variable: Sistema de gestión de seguridad de la información.					X
ORGANIZACIÓN	Los ítems del instrumento reflejan organicidad lógica entre la definición operacional y conceptual respecto a la variable, de manera que permiten hacer inferencias en función a las hipótesis, problema y objetivos de la investigación.					X
SUFICIENCIA	Los ítems del instrumento son suficientes en cantidad y calidad acorde con la variable, dimensiones e indicadores.					X
INTENCIONALIDAD	Los ítems del instrumento son coherentes con el tipo de investigación y responden a los objetivos, hipótesis y variable de estudio: Sistema de gestión de seguridad de la información				X	
CONSISTENCIA	La información que se recoja a través de los ítems del instrumento, permitirá analizar, describir y explicar la realidad, motivo de la investigación.					X
COHERENCIA	Los ítems del instrumento expresan relación con los indicadores de cada dimensión de la variable: Sistema de gestión de seguridad de la información				X	
METODOLOGÍA	La relación entre la técnica y el instrumento propuestos responden al propósito de la investigación, desarrollo tecnológico e innovación.					X
PERTINENCIA	La redacción de los ítems concuerda con la escala valorativa del instrumento.					X
PUNTAJE TOTAL		**47**				

(Nota: Tener en cuenta que el instrumento es válido cuando se tiene un puntaje mínimo de 41 “Excelente”; sin embargo, un puntaje menor al anterior se considera al instrumento no válido ni aplicable)

III. OPINIÓN DE APLICABILIDAD

Aplicable y Coherente.

PROMEDIO DE VALORACIÓN:

47

Tarapoto 13 de mayo de 2024

INFORME DE OPINIÓN SOBRE INSTRUMENTO DE INVESTIGACIÓN CIENTÍFICA

I. DATOS GENERALES

Apellidos y nombres del experto : Ing. MBA. Ángel Cárdenas García
Institución donde labora : Universidad Nacional de San Martín
Especialidad : Docente en Metodología - UNSM
Instrumento de evaluación : Cuestionario: Sistema de gestión de seguridad de la información
Autor (s) del instrumento (s) : Marco Heriberto Herrera Velásquez

II. ASPECTOS DE VALIDACIÓN

MUY DEFICIENTE (1) DEFICIENTE (2) ACEPTABLE (3) BUENA (4) EXCELENTE (5)

CRITERIOS	INDICADORES	1	2	3	4	5
CLARIDAD	Los ítems están redactados con lenguaje apropiado y libre de ambigüedades acorde con los sujetos muestrales.				X	
OBJETIVIDAD	Las instrucciones y los ítems del instrumento permiten recoger la información objetiva sobre la variable, en todas sus dimensiones en indicadores conceptuales y operacionales.				X	
ACTUALIDAD	El instrumento demuestra vigencia acorde con el conocimiento científico, tecnológico, innovación y legal inherente a la variable: Sistema de gestión de seguridad de la información.					X
ORGANIZACIÓN	Los ítems del instrumento reflejan organicidad lógica entre la definición operacional y conceptual respecto a la variable, de manera que permiten hacer inferencias en función a las hipótesis, problema y objetivos de la investigación.				X	
SUFICIENCIA	Los ítems del instrumento son suficientes en cantidad y calidad acorde con la variable, dimensiones e indicadores.					X
INTENCIONALIDAD	Los ítems del instrumento son coherentes con el tipo de investigación y responden a los objetivos, hipótesis y variable de estudio: Sistema de gestión de seguridad de la información					X
CONSISTENCIA	La información que se recoja a través de los ítems del instrumento, permitirá analizar, describir y explicar la realidad, motivo de la investigación.					X
COHERENCIA	Los ítems del instrumento expresan relación con los indicadores de cada dimensión de la variable: Sistema de gestión de seguridad de la información.					X
METODOLOGÍA	La relación entre la técnica y el instrumento propuestos responden al propósito de la investigación, desarrollo tecnológico e innovación.					X
PERTINENCIA	La redacción de los ítems concuerda con la escala valorativa del instrumento.				X	
PUNTAJE TOTAL		**46**				

(Nota: Tener en cuenta que el instrumento es válido cuando se tiene un puntaje mínimo de 41 “Excelente”; sin embargo, un puntaje menor al anterior se considera al instrumento no válido ni aplicable)

III. OPINIÓN DE APLICABILIDAD

Excelente para su aplicación.

IV. PROMEDIO DE VALORACIÓN: 46

Tarapoto 13 de mayo de 2024

INFORME DE OPINIÓN SOBRE INSTRUMENTO DE INVESTIGACIÓN CIENTÍFICA

I. DATOS GENERALES

Apellidos y nombres del experto : Dr. Wilson Torres Delgado
Institución donde labora : Universidad Nacional de San Martín - Tarapoto
Especialidad : Licenciado en estadística – COESPE 380
Instrumento de evaluación : Cuestionario: Confidencialidad de la información
Autor (s) del instrumento (s) : Marco Heriberto Herrera Velásquez

II. ASPECTOS DE VALIDACIÓN

MUY DEFICIENTE (1) DEFICIENTE (2) ACEPTABLE (3) BUENA (4) EXCELENTE (5)

CRITERIOS	INDICADORES	1	2	3	4	5
CLARIDAD	Los ítems están redactados con lenguaje apropiado y libre de ambigüedades acorde con los sujetos muestrales.					X
OBJETIVIDAD	Las instrucciones y los ítems del instrumento permiten recoger la información objetiva sobre la variable, en todas sus dimensiones en indicadores conceptuales y operacionales.					X
ACTUALIDAD	El instrumento demuestra vigencia acorde con el conocimiento científico, tecnológico, innovación y legal inherente a la variable: Confidencialidad de la información.					X
ORGANIZACIÓN	Los ítems del instrumento reflejan organicidad lógica entre la definición operacional y conceptual respecto a la variable, de manera que permiten hacer inferencias en función a las hipótesis, problema y objetivos de la investigación.				X	
SUFICIENCIA	Los ítems del instrumento son suficientes en cantidad y calidad acorde con la variable, dimensiones e indicadores.					X
INTENCIONALIDAD	Los ítems del instrumento son coherentes con el tipo de investigación y responden a los objetivos, hipótesis y variable de estudio: Confidencialidad de la información				X	
CONSISTENCIA	La información que se recoja a través de los ítems del instrumento, permitirá analizar, describir y explicar la realidad, motivo de la investigación.					X
COHERENCIA	Los ítems del instrumento expresan relación con los indicadores de cada dimensión de la variable: Confidencialidad de la información					X
METODOLOGÍA	La relación entre la técnica y el instrumento propuestos responden al propósito de la investigación, desarrollo tecnológico e innovación.					X
PERTINENCIA	La redacción de los ítems concuerda con la escala valorativa del instrumento.					X
PUNTAJE TOTAL		48				

(Nota: Tener en cuenta que el instrumento es válido cuando se tiene un puntaje mínimo de 41 “Excelente”; sin embargo, un puntaje menor al anterior se considera al instrumento no válido ni aplicable)

III. OPINIÓN DE APLICABILIDAD

Establecido los valores de aplicabilidad se llegó a determinar que el instrumento de recolección de datos se encuentra listo para su ejecución con validación obtenida de “Excelente”

PROMEDIO DE VALORACIÓN: **48**

Tarapoto 13 de mayo de 2024

INFORME DE OPINIÓN SOBRE INSTRUMENTO DE INVESTIGACIÓN CIENTÍFICA

I. DATOS GENERALES

Apellidos y nombres del experto : Dr. Andi Lozano Chung
Institución donde labora : Universidad Nacional de San Martín
Especialidad : Docente en la Universidad Nacional de San Martín
Instrumento de evaluación : Cuestionario: Confidencialidad de la información
Autor (s) del instrumento (s) : Marco Heriberto Herrera Velásquez

II. ASPECTOS DE VALIDACIÓN

MUY DEFICIENTE (1) DEFICIENTE (2) ACEPTABLE (3) BUENA (4) EXCELENTE (5)

CRITERIOS	INDICADORES	1	2	3	4	5
CLARIDAD	Los ítems están redactados con lenguaje apropiado y libre de ambigüedades acorde con los sujetos muestrales.					X
OBJETIVIDAD	Las instrucciones y los ítems del instrumento permiten recoger la información objetiva sobre la variable, en todas sus dimensiones en indicadores conceptuales y operacionales.				X	
ACTUALIDAD	El instrumento demuestra vigencia acorde con el conocimiento científico, tecnológico, innovación y legal inherente a la variable: Confidencialidad de la información.					X
ORGANIZACIÓN	Los ítems del instrumento reflejan organicidad lógica entre la definición operacional y conceptual respecto a la variable, de manera que permiten hacer inferencias en función a las hipótesis, problema y objetivos de la investigación.				X	
SUFICIENCIA	Los ítems del instrumento son suficientes en cantidad y calidad acorde con la variable, dimensiones e indicadores.					X
INTENCIONALIDAD	Los ítems del instrumento son coherentes con el tipo de investigación y responden a los objetivos, hipótesis y variable de estudio: Confidencialidad de la información				X	
CONSISTENCIA	La información que se recoja a través de los ítems del instrumento, permitirá analizar, describir y explicar la realidad, motivo de la investigación.					X
COHERENCIA	Los ítems del instrumento expresan relación con los indicadores de cada dimensión de la variable: Confidencialidad de la información.					X
METODOLOGÍA	La relación entre la técnica y el instrumento propuestos responden al propósito de la investigación, desarrollo tecnológico e innovación.					X
PERTINENCIA	La redacción de los ítems concuerda con la escala valorativa del instrumento.					X
PUNTAJE TOTAL		**47**				

(Nota: Tener en cuenta que el instrumento es válido cuando se tiene un puntaje mínimo de 41 “Excelente”; sin embargo, un puntaje menor al anterior se considera al instrumento no válido ni aplicable)

IV. OPINIÓN DE APLICABILIDAD

Aplicable y Coherente.

PROMEDIO DE VALORACIÓN:

47

Tarapoto 13 de mayo de 2024

INFORME DE OPINIÓN SOBRE INSTRUMENTO DE INVESTIGACIÓN CIENTÍFICA

I. DATOS GENERALES

Apellidos y nombres del experto : Ing. MBA. Ángel Cárdenas García
Institución donde labora : Universidad Nacional de San Martín
Especialidad : Docente en Metodología - UNSM
Instrumento de evaluación : Cuestionario: Confidencialidad de la información
Autor (s) del instrumento (s) : Marco Heriberto Herrera Velásquez

II. ASPECTOS DE VALIDACIÓN

MUY DEFICIENTE (1) DEFICIENTE (2) ACEPTABLE (3) BUENA (4) EXCELENTE (5)

CRITERIOS	INDICADORES	1	2	3	4	5
CLARIDAD	Los ítems están redactados con lenguaje apropiado y libre de ambigüedades acorde con los sujetos muestrales.					X
OBJETIVIDAD	Las instrucciones y los ítems del instrumento permiten recoger la información objetiva sobre la variable, en todas sus dimensiones en indicadores conceptuales y operacionales.					X
ACTUALIDAD	El instrumento demuestra vigencia acorde con el conocimiento científico, tecnológico, innovación y legal inherente a la variable: Confidencialidad de la información.				X	
ORGANIZACIÓN	Los ítems del instrumento reflejan organicidad lógica entre la definición operacional y conceptual respecto a la variable, de manera que permiten hacer inferencias en función a las hipótesis, problema y objetivos de la investigación.					X
SUFICIENCIA	Los ítems del instrumento son suficientes en cantidad y calidad acorde con la variable, dimensiones e indicadores.				X	
INTENCIONALIDAD	Los ítems del instrumento son coherentes con el tipo de investigación y responden a los objetivos, hipótesis y variable de estudio: Confidencialidad de la información					X
CONSISTENCIA	La información que se recoja a través de los ítems del instrumento, permitirá analizar, describir y explicar la realidad, motivo de la investigación.					X
COHERENCIA	Los ítems del instrumento expresan relación con los indicadores de cada dimensión de la variable: Confidencialidad de la información.					X
METODOLOGÍA	La relación entre la técnica y el instrumento propuestos responden al propósito de la investigación, desarrollo tecnológico e innovación.					X
PERTINENCIA	La redacción de los ítems concuerda con la escala valorativa del instrumento.					X
PUNTAJE TOTAL		**48**				

(Nota: Tener en cuenta que el instrumento es válido cuando se tiene un puntaje mínimo de 41 “Excelente”; sin embargo, un puntaje menor al anterior se considera al instrumento no válido ni aplicable)

V. OPINIÓN DE APLICABILIDAD

Excelente para su aplicación.

PROMEDIO DE VALORACIÓN: **48**

Tarapoto 13 de mayo de 2024

Anexo 4. Confiabilidad del instrumento

Cuestionario “Sistema de gestión de seguridad de la información”

La confiabilidad del instrumento se calculó a través del Índice de confiabilidad - Alfa de Cronbach, teniendo como muestra piloto a 16 sujetos; y del análisis de los 18 ítems del instrumento de evaluación se obtuvo como resultado un índice de **0,791** que se encuentra dentro del rango “Aceptable” de confiabilidad, por lo tanto, el instrumento de medición es muy confiable para su aplicación.

A través del Alfa de Cronbach

$$\alpha = \frac{K}{K-1}\left[1-\frac{\sum S_i^2}{S_T^2}\right]$$

Nivel de confiabilidad del coeficiente alfa de Cronbach

Rango	**Nivel**
0,9 – 1,0	Excelente
0,8 – 0,9	Muy bueno
0,7 – 0,8	Aceptable
0,6 – 0,7	Cuestionable
0,5 – 0,6	Pobre
0,0 – 0,5	No aceptable

Fuente: George y Mallery (2003).

Resumen del procesamiento de los casos

		N	%
Casos	Válido	16	100,0
	Excluido[a]	0	,0
	Total	16	100,0

a. La eliminación por lista se basa en todas las variables del procedimiento.

Fuente: SPSS ver 25.

Estadísticas de total de elemento

	Media de escala si el elemento se ha suprimido	Varianza de escala si el elemento se ha suprimido	Correlación total de elementos corregida	Alfa de Cronbach si el elemento se ha suprimido
item1	49,31	105,296	,670	,758
item2	49,00	122,667	,190	,791
item3	49,13	119,983	,245	,789
item4	48,81	113,896	,472	,775
item5	49,63	121,450	,161	,795
item6	49,44	114,263	,422	,777
item7	49,19	114,962	,353	,782
item8	49,69	117,029	,313	,785
Item9	49,00	116,133	,400	,779
item10	49,06	119,796	,302	,785
item11	49,06	115,796	,378	,780
item12	49,06	107,796	,604	,763
item13	49,31	111,029	,510	,771
item14	49,69	106,496	,648	,760
item15	49,63	110,250	,586	,766
item16	49,50	122,267	,146	,795
item17	49,31	111,829	,554	,769
item18	49,38	132,117	-,176	,823

Fuente: SPSS v27

Estadísticas de fiabilidad

Alfa de Cronbach	N de elementos
,791	18

Fuente: SPSS

Bibliografía de Referencia:

George, D., y Mallery, P. (2003). SPSS for Windows step by step: A simple guide and reference. 11.0 update (4th ed.). Boston: Allyn y Bacon.

Cuestionario "Confidencialidad de la información"

La confiabilidad del instrumento se calculó a través del Índice de confiabilidad - Alfa de Cronbach, teniendo como muestra piloto a 16 sujetos; y del análisis de los 18 ítems del instrumento de evaluación se obtuvo como resultado un índice de **0,828** que se encuentra dentro del rango "Muy bueno" de confiabilidad, por lo tanto, el instrumento de medición es muy confiable para su aplicación.

A través del Alfa de Cronbach

$$\alpha = \frac{K}{K-1}\left[1-\frac{\sum S_i^2}{S_T^2}\right]$$

Nivel de confiabilidad del coeficiente alfa de Cronbach

Rango	**Nivel**
0,9 – 1,0	Excelente
0,8 – 0,9	Muy bueno
0,7 – 0,8	Aceptable
0,6 – 0,7	Cuestionable
0,5 – 0,6	Pobre
0,0 – 0,5	No aceptable

Fuente: George y Mallery (2003).

Resumen del procesamiento de los casos

		N	%
Casos	Válido	16	100,0
	Excluido[a]	0	,0
	Total	16	100,0

a. La eliminación por lista se basa en todas las variables del procedimiento.

Fuente: SPSS ver 25.

Estadísticas de total de elemento

	Media de escala si el elemento se ha suprimido	Varianza de escala si el elemento se ha suprimido	Correlación total de elementos corregida	Alfa de Cronbach si el elemento se ha suprimido
item1	52,06	125,529	,607	,811
item2	52,06	130,063	,487	,817
item3	52,00	127,200	,566	,813
item4	51,94	118,996	,818	,798
item5	52,50	132,533	,258	,829
item6	52,19	127,629	,441	,818
item7	52,06	128,329	,424	,819
item8	52,25	137,933	,097	,837
Item9	52,06	123,929	,607	,810
item10	51,94	139,129	,118	,833
item11	52,13	132,650	,298	,826
item12	52,25	126,333	,435	,819
item13	52,31	123,829	,625	,809
item14	52,75	122,867	,500	,815
item15	52,38	118,250	,727	,801
item16	52,25	134,067	,260	,828
item17	52,50	122,000	,629	,808
item18	52,69	148,362	-,213	,854

Fuente: SPSS v27

Estadísticas de fiabilidad

Alfa de Cronbach	N de elementos
,828	18

Fuente: SPSS

Bibliografía de Referencia:

George, D., y Mallery, P. (2003). SPSS for Windows step by step: A simple guide and reference. 11.0 update (4th ed.). Boston: Allyn y Bacon.

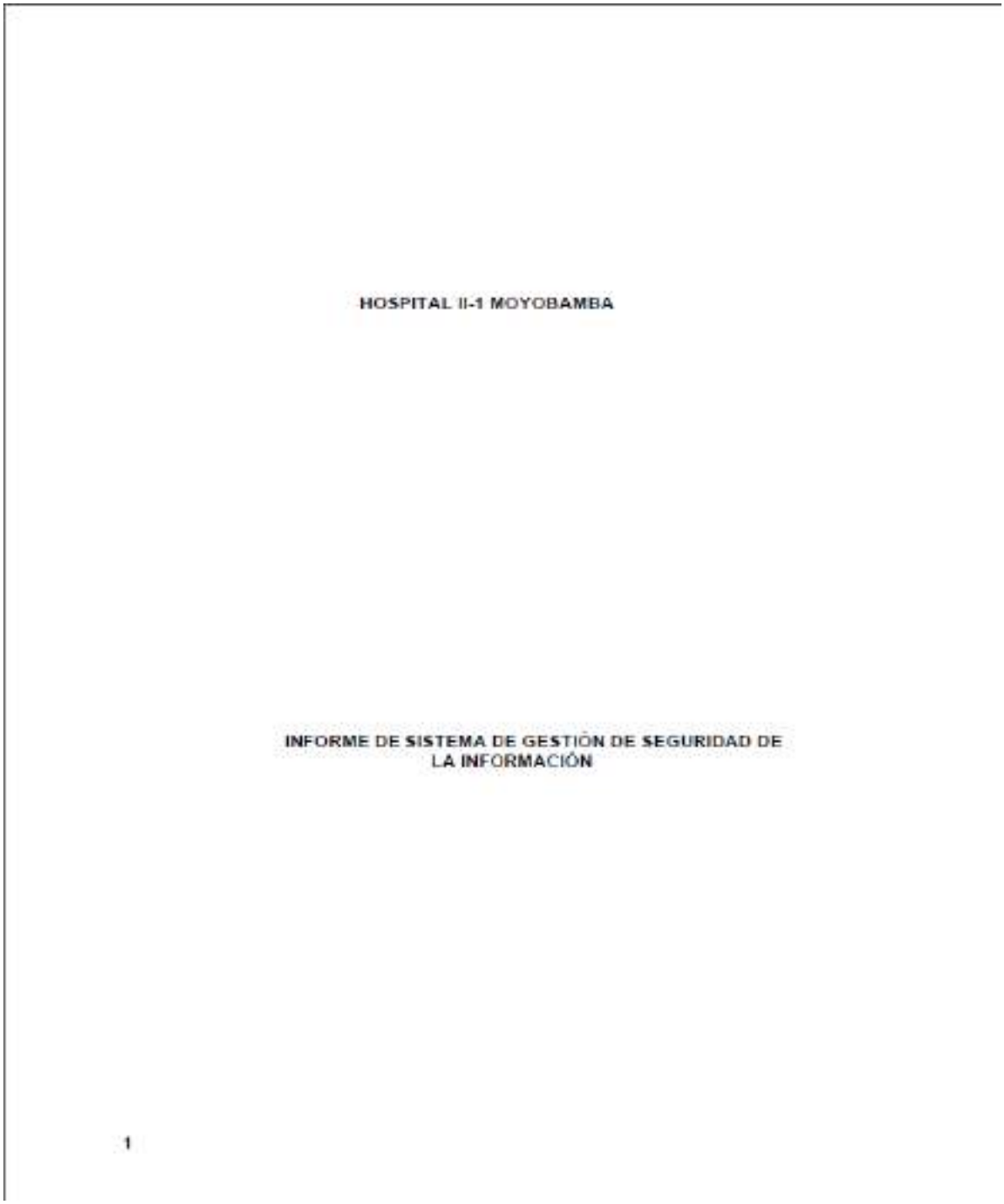
Anexo 5. Base de datos estadístico

N.º	Seguridad	Gestión	Implantación	**Sistema de gestión de seguridad de la información**	Tecnológica	Procesos y políticas	Cultural y organizacional	**Confidencialidad de la información**
1	25	29	25	79	21	20	25	66
2	28	30	22	80	28	26	22	76
3	24	29	26	79	22	25	30	77
4	22	30	24	76	28	29	25	82
5	17	20	20	57	17	16	15	48
6	19	17	7	43	15	9	19	43
7	28	22	29	79	24	28	27	79
8	29	26	24	79	28	26	25	79
9	24	27	26	77	29	27	28	84
10	6	13	10	29	9	13	13	35
11	24	30	15	69	17	15	27	59
12	25	23	28	76	24	27	30	81
13	21	9	13	43	9	9	18	36
14	14	15	21	50	18	14	20	52
15	18	22	20	60	16	16	30	62
16	26	29	28	83	29	28	25	82

Anexo 6. informe del Sistema de gestión de seguridad de la información del Hospital II-1 Moyobamba

Ingresar:

https://drive.google.com/file/d/1E94NpxUm6ErpExl2KpejSxi8JnY5Zloq/view?usp=sharing



HOSPITAL II-1 MOYOBAMBA

INFORME DE SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

1

Sistema de gestión para la seguridad de la información y la confidencialidad de la información, Hospital II-1 Moyobamba, 2024

por Marco Heriberto Herrera Velásquez

Fecha de entrega: 18-mar-2025 10:17a.m. (UTC-0500)
Identificador de la entrega: 2618229416
Nombre del archivo: TESIS_HERIBERTO_16-03-2025.docx (1.62M)
Total de palabras: 13188
Total de caracteres: 74535

Sistema de gestión para la seguridad de la información y la confidencialidad de la información, Hospital II-1 Moyobamba, 2024

INFORME DE ORIGINALIDAD

20%	17%	10%	13%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	repositorio.unjfsc.edu.pe Fuente de Internet	2%
2	Submitted to Universidad Cesar Vallejo Trabajo del estudiante	2%
3	hdl.handle.net Fuente de Internet	2%
4	repositorio.espe.edu.ec Fuente de Internet	1%
5	Submitted to Morgan Park High School Trabajo del estudiante	1%
6	upc.aws.openrepository.com Fuente de Internet	1%
7	www.risti.xyz Fuente de Internet	1%
8	ciencia.lasalle.edu.co Fuente de Internet	1%