FACULTAD DE INGENIERÍA DE SISTEMAS E INFORMÁTICA
ESCUELA PROFESIONAL DE INGENERÍA DE SISTEMAS E INFORMÁTICA

Tesis

Seguridad de información y protección de activos según ISO 27001 en INNOTEC: eficiente gestión para salvaguardar datos y recursos

Para optar el título profesional de Ingeniero de Sistemas e Informática

Autor:

Edward Hans Pinchi Núñez
https://orcid.org/0000-0003-4087-3300

Asesora:
Dra. Janina Cotrina Linares de Quezada
https://orcid.org/0000-0002-9097-2430

Tarapoto, Perú

2025

FACULTAD DE INGENIERÍA DE SISTEMAS E INFORMÁTICA
ESCUELA PROFESIONAL DE INGENERÍA DE SISTEMAS E INFORMÁTICA

Tesis

Seguridad de información y protección de activos según ISO 27001 en INNOTEC: eficiente gestión para salvaguardar datos y recursos

Para optar el título profesional de Ingeniero de Sistemas e Informática

Autor:

Edward Hans Pinchi Núñez

Sustentado y aprobado el 17 de octubre del 2025, por los siguientes jurados:

Presidente de Jurado Dr. Andy Hirvyn Rucoba Reátegui	**Secretario de Jurado** Ing. M. Sc. Pamela Magnolia Granda Milón
Vocal de Jurado Dr. Wilson Torres Delgado	**Asesora** Dra. Janina Cotrina Linares de Quezada

Tarapoto, Perú

2025

Universidad Nacional de San Martín
Facultad de Ingeniería de Sistema e Informática
Ciudad Universitaria - Jr. Amorarca # 315 - Morales

ACTA DE SUSTENTACIÓN
PARA OPTAR EL TÍTULO DE INGENIERO DE SISTEMAS E INFORMÁTICA

Resolución Nº 048-2025-UNSM/FISI-D (13.10.2025)

FACULTAD DE INGENIERÍA DE SISTEMAS E INFORMÁTICA – ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

A las 11:00 horas del día viernes, 17 de octubre del año 2025, se inició el acto público de sustentación de la tesis titulada: SEGURIDAD DE INFORMACIÓN Y PROTECCIÓN DE ACTIVOS SEGÚN ISO 27001 EN INNOTEC: EFICIENTE GESTIÓN PARA SALVAGUARDAR DATOS Y RECURSOS, presentado por el Bach. EDWARD HANS PINCHI NUÑEZ con el Asesor: Ing. Dr. Janina Cotrina Linares de Quezada.

Instalado los miembros de jurado calificador conformado por:

Presidente	:	Ing. Dr. Andy Hirvyn Rucoba Reátegui
Secretario	:	Ing. M. Sc. Pamela Magnolia Granda Milon
Vocal	:	Lic. Dr. Wilson Torres Delgado

El presidente del jurado dirigió brevemente unas palabras y a continuación el secretario dio lectura a la Resolución Nº 048-2025-UNSM/FISI-D.

Seguidamente el autor expuso el trabajo de investigación y el jurado realizó las preguntas pertinentes, respondidas por el sustentante y eventualmente por el asesor, con la venia del jurado.

Una vez terminada la ronda de preguntas el jurado procedió a deliberar para determinar la calificación final, para lo cual dispuso un receso de quince (15) minutos, con participación del asesor con voz, pero sin voto y sin la presencia del sustentante y otros participantes del acto público.

Luego de aplicar los criterios de calificación con estricta observancia del principio de objetividad y de acuerdo con los puntajes en escala vigesimal (de 0 a 20), según el Anexo 4.2. del RG-CTI, la nota de sustentación otorgada resultante del promedio aritmético de los calificativos emitidos por cada uno de los miembros del jurado fue .dieciséis. (16).

De acuerdo con el Artículo 40° del RG – CTI, la nota obtenida es .....Aprobatoria..... y correspondiente a la calificación de .....Bueno.....; leído este resultado en presencia de todos los participantes del acto de sustentación, el secretario dio lectura a las observaciones subsanables al informe final que el autor deberá corregir y alcanzar al jurado en un plazo máximo de treinta (30) días calendario.

Firman los integrantes del jurado calificador, asesor y el autor de la tesis en señal de conformidad, dando por concluido el acto a las ...12:30...horas, el mismo día 17 de octubre del 2025.

Ing. Dr. Andy Hirvyn Rucoba Reátegui
Presidente

Ing. M. Sc. Pamela Magnolia Granda Milon
Secretario

Lic. Dr. Wilson Torres Delgado
Vocal

Ing. Dr. Janina Cotrina Linares de Quezada
Asesor

Bach. Edward Hans Pinchi Nuñez
Autor

Declaratoria de autenticidad

Yo, **Edward Hans Pinchi Núñez**, con DNI N° 45874181, egresado de la Escuela Profesional de Ingeniería de Sistemas e Informática de la Facultad de Ingeniería de Sistemas e Informática de la Universidad Nacional de San Martín, autor de la tesis titulada: **Seguridad de información y protección de activos según ISO 27001 en INNOTEC: eficiente gestión para salvaguardar datos y recursos.**

Declaro bajo juramento que:

1. La tesis presentada es de mi autoría
2. La redacción fue realizada respetando las citas y referencia de las fuentes bibliográficas consultadas, siguiendo las normas APA actuales
3. Toda información que contiene la tesis no ha sido plagiada;
4. Los datos presentados en los resultados son reales, no han sido alterados ni copiados, por tanto, la información de esta investigación debe considerarse como aporte a la realidad investigada.

Por lo antes mencionado, asumo bajo responsabilidad las consecuencias que deriven de mi accionar, sometiéndome a las leyes de mi país y normas vigentes de la Universidad Nacional de San Martín.

Tarapoto, 17 de octubre de 2025.

Edward Hans Pinchi Núñez
DNI. Nº 45874181

Ficha de identificación

Título: Seguridad de información según ISO 27001 y la protección de activos en INNOTEC: eficiente gestión para salvaguardar datos y recursos	**Área de investigación:** Ingeniería y Tecnología. **Línea de investigación:** Ingeniería de Sistemas y Comunicaciones. **Sublínea de investigación:** Sistemas de información. **Grupo de investigación:** Innuva (Resolución Nº 390-2022-UNSM/CU-R) **Tipo de investigación:** Básica ☒, Aplicada ☐, Desarrollo experimental ☐

Autor: Edward Hans Pinchi Nuñez	Facultad de Ingeniería de Sistemas e Informática Escuela Profesional de Ingeniería de Sistemas e Informática https://orcid.org/0000-0003-4087-3300

Asesora: Dra. Janina Cotrina Linares de Quezada	**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/0000-0002-9097-2430

Dedicatoria

A mis padres, Sr. Segundo Limber Pinchi García y Sra. Gloria Luz Núñez Lomas, por su amor sin límites y su constante respaldo, por mostrarme a través de su ejemplo, que la constancia y el esfuerzo son fundamentales para lograr las metas más difíciles.

A mi hermana, Rita Vanessa, quien ha sido mi primera amiga y compañera en este camino de vida, por su cariño y apoyo incondicional han sido fundamentales en cada etapa que he recorrido.

Edward

Agradecimientos

Agradezco a Dios por brindarme luz, fortaleza y la capacidad necesaria para comprender y analizar los conceptos desarrollados en esta tesis.

Expreso mi más sincero agradecimiento a los miembros del jurado, cuyo conocimiento, compromiso y dedicación fueron fundamentales para la culminación de este trabajo: al Dr. Andy Hirvyn Rucoba Reátegui, a la Ing. M. Sc. Pamela Magnolia Granda Milón y al Dr. Wilson Torres Delgado, por sus valiosas contribuciones y su constante búsqueda de la excelencia académica.

Asimismo, manifiesto mi especial gratitud a la Dra. Janina Cotrina Linares de Quezada, mi asesora, por su orientación, sabiduría y compromiso, los cuales fueron esenciales para el desarrollo y la calidad de este proyecto.

El autor

Índice general

Índice de tablas

Índice de figuras

RESUMEN

Seguridad de información según ISO 27001 y la protección de activos en INNOTEC: eficiente gestión para salvaguardar datos y recursos.

En la actualidad, tanto las organizaciones del ámbito público como las del ámbito privado otorgan prioridad a la salvaguarda de la información, considerándola como uno de sus activos más valiosos para garantizar la continuidad operativa y destacar frente a la competencia. Esta investigación titulada “Seguridad de información según ISO 27001 y la protección de activos en INNOTEC: eficiente gestión para salvaguardar datos y recursos” mediante su objetivo principal buscó determinar la relación entre la seguridad de la información según la ISO 27001 y la protección de activos en la empresa INNOTEC - Tarapoto, 2023. Para ende, se realizó una investigación básica, no experimental, con un enfoque descriptivo - correlacional. En la población se consideró a todos los 25 miembros del personal que labora en la empresa INNOTEC en Tarapoto. Asimismo, se empleó 2 cuestionarios como técnicas para recolectar datos. Entre sus principales resultados se destacan que el nivel de la seguridad de la información en la empresa INNOTEC - Tarapoto se encuentra en un nivel predominantemente regular, con un 52%. Asimismo, la protección de los activos en la empresa INNOTEC - Tarapoto se encuentra mayormente con un 64% en el mismo nivel. Se concluye que, que existe una relación muy alta y significativa entre la seguridad de la información según la norma ISO 27001 y la protección de activos en la empresa INNOTEC – Tarapoto, con un coeficiente de correlación obtenido de 0.841, un coeficiente de determinación del 71%, lo que evidencia que la seguridad de la información explica en gran medida la variabilidad en la protección de los activos. Con un valor p de 0.000, confirmando que la relación es significativa.

Palabras clave: Seguridad de información, protección, confiabilidad, integridad, disponibilidad.

ABSTRACT

Information Security According to ISO 27001 and Asset Protection at INNOTEC: Efficient Management to Safeguard Data and Resources

Currently, both public and private organizations prioritize the safeguarding of information, considering it one of their most valuable assets for ensuring operational continuity and maintaining competitive advantage. This study, entitled *"Information Security According to ISO 27001 and Asset Protection at INNOTEC: Efficient Management to Safeguard Data and Resources,"* aimed to determine the relationship between information security in accordance with ISO 27001 and asset protection at the company INNOTEC – Tarapoto, in 2023. For this purpose, a basic, non-experimental study was conducted using a descriptive–correlational approach. The population consisted of all 25 staff members working at INNOTEC in Tarapoto. Data were collected using two questionnaires as research instruments. Among the main results, it was observed that the level of information security at INNOTEC – Tarapoto was predominantly at a moderate level, accounting for 52%. Likewise, asset protection at the company was mostly classified at the same level, representing 64%. It is concluded that there is a very high and statistically significant relationship between information security in accordance with the ISO 27001 standard and asset protection at INNOTEC – Tarapoto, with a correlation coefficient of 0.841 and a coefficient of determination of 71%, indicating that information security largely explains the variability in asset protection. A p-value of 0.000 confirms that this relationship is statistically significant.

***Keywords*:** Information security, protection, reliability, integrity, availability

CAPÍTULO I
INTRODUCCIÓN A LA INVESTIGACIÓN

En la actualidad, tanto las organizaciones del ámbito público como las del ámbito privado otorgan prioridad a la salvaguarda de la información, considerándola como uno de sus activos más valiosos para garantizar la continuidad operativa y destacar frente a la competencia. La seguridad de la información en el contexto empresarial abarca diversos aspectos, como el control de acceso, la protección de dispositivos, la gestión de contraseñas y la supervisión de vulnerabilidades, entre otros (Vega, 2021). Cada uno de estos aspectos demanda un análisis detallado, una asignación presupuestaria y la implementación de medidas preventivas o correctivas en relación con los posibles riesgos de seguridad identificados. Asimismo, la creación de sistemas completamente seguros resulta un desafío constante, dado que continuamente se descubren nuevas amenazas en distintos niveles (Ramírez & Rinconc, 2022).

Las amenazas cibernéticas emergentes en las empresas se manifiestan en la rápida evolución tecnológica y la creciente interconexión global, lo que aumenta las oportunidades para los actores maliciosos. La causa principal es la dependencia creciente de las organizaciones en la tecnología digital, que amplía las superficies de ataque, conduciendo a la pérdida de datos, interrupciones operativas y daño a la reputación. La falta de conciencia y preparación adecuada también contribuye a la vulnerabilidad, destacando la necesidad urgente de implementar medidas preventivas y estrategias de respuesta para proteger los activos digitales de las empresas (Tonysé, 2021).

Otro de los problemas es la controversia constante en torno a la seguridad de la información en medios digitales, específicamente en relación con la privacidad y los datos personales. La disciplina jurídica se ve desafiada por debates continuos en el ciberespacio sobre la protección de la información que se convierte en una referencia esencial en el ámbito empresarial, señalando que las empresas enfrentan desafíos significativos en la gestión de la seguridad de la información (Donoso et al., 2023). La necesidad de abordar eficazmente estas preocupaciones legales y éticas destaca la importancia de analizar medidas efectivas para garantizar la privacidad y los datos personales en el entorno digital.

Las dificultades en la aplicación efectiva de los controles y requisitos de la norma ISO 27001 a menudo surgen por la falta de comprensión y compromiso del personal, debido a insuficiente capacitación y recursos asignados. Esto puede generar vulnerabilidades

en la seguridad de la información, aumentando el riesgo de brechas y comprometiendo la integridad de los datos. Además, la no conformidad con la norma puede resultar en la pérdida de certificaciones, dañar la reputación y tener repercusiones financieras negativas (Yungán & Narváez, 2022).

Así como también, en Perú, nos encontramos ante el desafío crucial de la insuficiente protección digital de datos, donde numerosas empresas no reconocen o subestiman la importancia de implementar políticas de seguridad adecuadas. Esta falta de conciencia lleva a que estas compañías dirijan considerables sumas de dinero hacia áreas que no son prioritarias, generando pérdidas significativas debido a la magnitud de este problema. Este escenario refleja la problemática generalizada, su origen en la falta de reconocimiento y atención hacia la seguridad digital, y sus consecuencias perjudiciales para las empresas y la integridad de los datos (Rodriguez et al., 2020).

Por otro lado, en la región de San Martín, se identificaron importantes deficiencias en la seguridad de la información. Estas falencias podrían haber resultado en una pérdida significativa de control empresarial, colocando a la empresa en una posición desventajosa en el mercado y, en situaciones extremas, llevándola a la insolvencia. Dado que la información desempeña un papel crucial en los objetivos y riesgos de una organización, resultaba imperativo que las empresas implementaran medidas para salvaguardar tanto sus propios datos como los de sus clientes (Mamani, 2020).

La empresa INNOTEC, dedicada al desarrollo de software, venta de equipos de cómputo, redes informáticas y servicio técnico especializado, enfrenta un contexto en el que la protección de la información constituye un activo esencial para garantizar la continuidad de sus operaciones. Sin embargo, la organización se ve afectada por la creciente exposición a amenazas cibernéticas emergentes y por las limitaciones en la gestión de la seguridad de la información, problemática que se intensifica en el contexto peruano debido a la escasa cultura y protección digital existente.

En San Martín, donde la empresa desarrolla sus actividades, se evidencian deficiencias significativas en los mecanismos de seguridad informática, lo que incrementa el riesgo de pérdida de datos, filtración de información sensible y disminución del control operativo. Estas vulnerabilidades no solo comprometen la confianza de los clientes, sino que también colocan a INNOTEC en una posición competitiva desfavorable, pudiendo incluso amenazar su sostenibilidad económica. Por ello, resulta urgente y prioritario que la empresa adopte estrategias y medidas integrales de protección de la información, orientadas a fortalecer su infraestructura tecnológica, minimizar riesgos y garantizar la seguridad y confidencialidad de los datos tanto corporativos como de sus clientes.

De acuerdo con lo expuesto, la formulación de la pregunta general se consideró: ¿Cuál es la relación entre la gestión de la seguridad de la información según la ISO 27001 y la protección de activos en la empresa INNOTEC - Tarapoto, 2023?. Asimismo, como objetivo general: Determinar la relación entre la seguridad de la información según la ISO 27001 y la protección de activos en la empresa INNOTEC - Tarapoto, 2023. En efecto, como objetivos específicos: a) Analizar el nivel de la seguridad de la información según la ISO 27001 en la empresa INNOTEC - Tarapoto, 2023. b) Analizar el nivel de protección de los activos en la empresa INNOTEC - Tarapoto, 2023. c) Determinar la relación entre las dimensiones de la seguridad de la información basados en la norma ISO 27001 y la protección de activos en la empresa INNOTEC - Tarapoto, 2023. En definitiva, la hipótesis general fue: Existe una relación significativa entre la seguridad de la información según la ISO 27001 y la protección de activos en la empresa INNOTEC - Tarapoto, 2023.

CAPÍTULO II
MARCO TEÓRICO

2.1. Antecedentes de la investigación

2.1.1. A nivel internacional

Lopes et al. (2019) en su artículo sobre la implementación de normas ISO 27001 como facilitador de cumplimiento del Reglamento General de Protección de Datos (GDPR) evaluó en qué medida la implementación de los estándares ISO 27001 pueden facilitar el cumplimiento del Reglamento General de Protección de Datos (GDPR) de la UE. La metodología implica analizar sitios web, principalmente de empresas de consultoría, para identificar aspectos facilitadores en la implementación del GDPR. Se concluye que la adopción de la norma ISO 27001 podría desempeñar un papel clave en simplificar el cumplimiento con el GDPR, ofreciendo a las organizaciones una guía práctica para abordar los desafíos de protección de datos personales.

Por otro lado, Latinovic et al. (2020) en su investigación propusieron la implementación del estándar ISO / IEC 27001 para la gestión de seguridad de la información. La metodología priorizó la evaluación de riesgos antes de establecer sistemas de seguridad, buscando un equilibrio entre eficacia en costos y velocidad de implementación. El resultado destacó la necesidad de evitar una planificación excesiva y una amplia gama de sistemas de seguridad, ya que podrían obstaculizar la implementación efectiva, generando costos desproporcionados. El estudio también exploró la dinámica actual en la aplicación de estándares en diversas áreas industriales, subrayando la distribución e implementación como aspectos cruciales del análisis.

En Indonesia, Jevelin y Faza (2023) en su investigación buscaron evaluar el Sistema de Gestión de Seguridad de la Información (SGSI) de un contratista privado para obtener la certificación ISO 27001, abordando la necesidad apremiante de seguridad de datos. La metodología empleada fue un enfoque de métodos mixtos, combinando el índice KAMI para evaluar la madurez cuantitativa con conocimientos cualitativos obtenidos mediante entrevistas y revisión de la literatura. Los resultados revelan una madurez del SGSI en los niveles I+ a II, indicando un déficit en el cumplimiento de ISO 27001. La discusión destaca la eficacia del ciclo PDCA en la implementación del SGSI, pero subraya la necesidad de mejoras para cumplir con los requisitos de certificación.

2.1.2. **A nivel nacional**

Bustamante et al. (2021) en su estudio sobre la implementación de políticas basadas en la ISO 27001:2013 en una municipalidad distrital peruana, se investigó cómo estas políticas mejoraron la gestión de la seguridad de la información. Se realizó una investigación preexperimental con 30 trabajadores, quienes evaluaron su satisfacción mediante un cuestionario. Los resultados mostraron que más del 90 % de los encuestados reconocieron mejoras significativas, aumentando del 49 % al 96 % entre el pre y postest. Se concluyó que el modelo de políticas de seguridad, centrado en la confidencialidad, integridad y disponibilidad, logró mejorar de manera efectiva la gestión de seguridad de la información, garantizando la adecuada protección de los datos.

Además, Rodriguez et al. (2020) en su artículo científico, analizaron cómo la aplicación de la norma ISO 27001 impacta la seguridad de la información en una empresa privada en Lima, Perú. Para abordar este objetivo, se empleó un enfoque cuantitativo mediante un estudio preexperimental que involucró a 30 empleados de la empresa seleccionada. Este método evaluó cómo la norma ISO 27001 impacta la confidencialidad, integridad y disponibilidad de la información. Los resultados mostraron que la norma mejora la seguridad de la información, destacando su importancia para proteger los intereses estratégicos de las empresas en el entorno tecnológico actual.

Asimismo, Apahuasco (2020) en su tesis, evaluó la gestión de la seguridad de la información en la empresa de distribución de bebidas Disav SAC a través de la implementación de los lineamientos del estándar ISO 27001. Se llevó a cabo un análisis detallado de la seguridad de la información en dispositivos y entre el personal, utilizando preguntas específicas. Posteriormente, se aplicaron controles, capacitando al personal y ajustando dispositivos informáticos. La evaluación con SPSS v.24 demostró la eficacia al reducir satisfactoriamente las vulnerabilidades. Desde un enfoque cuantitativo, la encuesta reflejó la disminución de vulnerabilidades y la seguridad de la información crítica de la empresa.

Finalmente, Risco (2020) en su tesis, evaluó el impacto de un sistema de gestión de seguridad de la información basado en ISO 27001:2013 en la Empresa Constructora Pérez & Pérez SAC, que tenía vulnerabilidades en sus procesos. Se usó una metodología cuantitativa con un diseño preexperimental y una muestra de 20 registros por indicador. Los resultados mostraron mejoras notables en la seguridad de la información: la vulnerabilidad en confidencialidad bajó de 68,85% a 15,40%, en integridad de la información de 52,60% a 11,40%, y en disponibilidad de la información de 47,15% a 11,95%. En conjunto, estas medidas elevaron la seguridad de la

información de la empresa del 80% al 90%. En conclusión, la implementación del sistema de gestión ISO 27001 resultó beneficiosa para la Empresa Constructora Pérez & Pérez SAC.

2.2. Fundamentos teóricos

2.2.1. **Seguridad de la información**

La seguridad de la información es cada vez más relevante en nuestra sociedad hiperconectada debido al uso generalizado de las TIC. Hoy en día, interactuar con computadoras y dispositivos móviles en casi todos los aspectos de la vida diaria, desde el trabajo y el estudio en línea hasta las compras por internet y la gestión de finanzas y salud a través de aplicaciones móviles (Vega, 2021). Para asegurar la integridad y resguardo de su información, hemos implementado diversas medidas preventivas y correctivas. En términos simples, nuestras normativas y procedimientos de uso impactan directamente en la gestión de datos dentro de nuestra empresa (Zevallos, 2019).

La salvaguarda de la información y de los sistemas contra accesos no autorizados, uso indebido, divulgación, interrupción, alteración y destrucción se lleva a cabo mediante procesos, mejores prácticas y metodologías vigentes en la actualidad (Morales et al., 2020). Según esta premisa, resulta imperativo salvaguardar los datos y recursos tecnológicos contra cualquier uso no autorizado. Según la ISO/IEC (2016), la seguridad de la información se centra en proteger los datos y sistemas contra accesos no autorizados y abusos. La norma ISO 27001 destaca la importancia de garantizar la confidencialidad, integridad y disponibilidad de la información clave para la organización.

2.2.1.1. Gestión de Seguridad de la Información

Para Podrecca et al. (2022) la gestión de la seguridad de la información es clave para la integridad de la empresa. En un entorno corporativo caracterizado por la digitalización y el crecimiento de la conectividad, este aspecto se ha convertido en un desafío significativo. A diario, se registran diversos incidentes en los cuales la confidencialidad de los datos se ve comprometida, permitiendo que numerosas personas no autorizadas accedan a la información. Sin embargo, esta proximidad y facilidad de uso de la tecnología plantea riesgos reales para las empresas, interfiriendo con el correcto funcionamiento de las actividades empresariales y exacerbando las amenazas que surgen en el entorno que pueden causar problemas comerciales, lo que hace que las empresas sean cada vez más vulnerables.

2.2.1.2. **Bases Internacionales ISO/IEC 27001**

En octubre de 2005, se llevó a cabo la distribución con la planificación de los criterios previos para un Sistema de Gestión de Seguridad de la Información (SGSI). Este constituye la regla fundamental en la presente serie, fundamentada en la norma previa BS 7799-2:2002.

2.2.1.3. Norma ISO 27001

La seguridad de la información, esencial para preservar la integridad corporativa, se ve amenazada por riesgos informáticos constantes. La alineación de la seguridad de datos con las estrategias empresariales y la evaluación de un Sistema de Gestión de Seguridad de la Información (SGSI) bajo la norma ISO 27001 marcan el inicio de una mejora continua. Supervisado por el modelo PDCA, este proceso establece una conexión integral entre la seguridad de la información y las estrategias corporativas, generando un impulso transformador en su evolución.

La norma ISO 27001, desarrollada por la Organización Internacional de Normalización (ISO), proporciona un marco normativo para que las empresas gestionen la seguridad de la información mediante procedimientos que buscan implementar, mantener y mejorar constantemente la seguridad de los datos, ofreciendo ventajas significativas para fortalecer y optimizar la seguridad de la información de manera continua en la organización (Tonysé, 2021). Las más importantes son las siguientes son:

a) La mejora continua

Este aspecto de la norma no solo permite implantar procedimientos que promuevan la construcción de una cultura de seguridad dentro de una organización, sino que también establece controles paso a paso para garantizar el desarrollo y la mejora continua de la seguridad de la información.

b) Adaptación a las necesidades de cada organización

La norma promueve la implantación progresiva de criterios para reforzar la seguridad de la información apoyando el desarrollo de metodologías de análisis de riesgos de seguridad adaptadas a las circunstancias específicas de cada empresa.

c) Controles adecuados para la seguridad de la información

Se utilizará un estudio científico para establecer las medidas de seguridad que deben ejecutarse mediante la implantación de un sistema de gestión SGSI para examinar cómo afectan los riesgos y amenazas a la seguridad de la información, a los requisitos de cada empresa.

d) Integración de los sistemas de información

Es fácil integrar muchos sistemas de gestión en una empresa porque la norma de seguridad de la información tiene la misma estructura que las normas ISO 9001 de Gestión de la Calidad o ISO 14001 de Gestión Medioambiental.

e) Confidencialidad

La confidencialidad en el contexto de la norma ISO 27001 se refiere a la protección de la información para garantizar que solo aquellos autorizados tengan acceso a ella. Esta norma establece que las organizaciones deben identificar y clasificar la información según su importancia y sensibilidad, determinando quiénes son los usuarios o entidades que tienen el derecho de acceder a dicha información (Damian, 2023). También, la confidencialidad implica implementar medidas de seguridad adecuadas, como controles de acceso, cifrado y políticas de gestión de contraseñas, con el objetivo de prevenir accesos no autorizados y proteger la información contra divulgaciones indebidas (Astudillo & Cabrera, 2019).

Para lograr la confidencialidad, la ISO 27001 sugiere la implementación de un Sistema de Gestión de la Seguridad de la Información (SGSI), que incluye la definición de políticas claras, la asignación de roles y responsabilidades, la realización de evaluaciones de riesgos y la implementación de controles de seguridad específicos. Además, se destaca la importancia de la concientización y capacitación del personal para fomentar la cultura de la seguridad de la información en toda la organización (Mora et al., 2020). La confidencialidad, como uno de los pilares fundamentales de la ISO 27001, busca asegurar que la información crítica se mantenga protegida y solo sea accesible por aquellos que cuenten con los permisos adecuados (Rojas et al., 2020).

f) Disponibilidad

La disponibilidad es clave para la seguridad de la información, ya que asegura que los servicios críticos y las funciones del sistema estén siempre accesibles. Esto requiere medidas para prevenir y corregir interrupciones, garantizando la continuidad operativa en cualquier situación (Carvajal et al., 2019).

La norma ISO 27001 recomienda controles como la redundancia de sistemas, la gestión de capacidad, la gestión de incidentes y la planificación de la continuidad del negocio para asegurar la disponibilidad. Estos controles buscan mitigar riesgos que podrían afectar la disponibilidad, como fallos en hardware, ataques cibernéticos, desastres naturales u otros eventos que podrían impactar la infraestructura tecnológica. La gestión proactiva de la disponibilidad contribuye a fortalecer la resiliencia de los sistemas de información, mejorando la capacidad de la organización para mantener la continuidad

de las operaciones y proteger sus activos de información críticos (Diamantopoulou et al., 2020).

g) Integridad

Esta es una forma de asegurarse de que los datos no se hayan modificado sin permiso desde que se crearon. Esta característica es muy importante, por ejemplo, al realizar operaciones bancarias a través de Internet. Su función es velar por la veracidad y el cumplimiento de la información y sus prácticas de gestión (CEUPE, 2020). Para Rodriguez et al. (2020), es la capacidad de impedir que los datos se alteren de forma no deseada o ilícita. Esto puede referirse a la modificación o supresión no autorizada de datos o fragmentos de datos, así como a la modificación o supresión autorizada pero no deseada de datos. Según la fuente mencionada, para mantener la integridad es necesario tener tanto la capacidad de deshacer las modificaciones permitidas que deben deshacerse como una forma de detener los cambios no autorizados en los datos.

2.2.1.4. **Estructura normativa ISO 27001**

Según Andrés y Gómez (2009), La norma está compuesta por dos organismos que colaboran para lograr el objetivo de crear un sistema de gestión de la seguridad de la información.

- **ISO 27001:** Esta norma específica los requisitos y autoriza el uso de sistemas de seguridad de la información.
- **ISO 27002:** Manual de buenas prácticas para implantar un SGSI Se trata de un manual que enumera todos los controles y mecanismos de control previamente identificados y creados especialmente para hacer frente a los problemas o peligros relacionados con la Seguridad de los datos.

2.2.1.5. **Etapas y cronogramas de un SGSI según el estándar ISO 27001**

Las etapas donde la ejecución del SGSI está coordinada por la norma 27001, según Castillo et al. (2023) son las siguientes:

- ETAPA I: Se inicia con la organización de proyectos, seguida de un examen de la circunstancia de la norma mediante un análisis de brechas. Esta etapa también incluye la definición del significado de la sociedad de seguridad de datos, que establece el marco y el alcance del SGSI.
- ETAPA II: En esta etapa, se realiza una auditoría de riesgos para identificar amenazas y vulnerabilidades, seguido de una evaluación de riesgos y la creación de un plan para abordar las áreas detectadas.
- ETAPA III: Esta etapa se centra en la implementación, que incluye rastrear estrategias para asegurar la correspondencia y la preparación del SGSI. Se evalúa el

control funcional, se asegura la disponibilidad de los indicadores del tablero de control y se aplica todo lo planificado anteriormente.

- ETAPA IV: En esta fase, se revisan los indicadores para evaluar el desempeño del SGSI y se realiza una auditoría interna para verificar la conformidad y eficacia del sistema implementado.
- ETAPA V: Finalmente, se procede a rectificar y modificar la situación de la administración del SGSI, ajustando y mejorando el sistema según los resultados de las auditorías y evaluaciones previas para asegurar su continua efectividad y adecuación.

2.2.1.6. **Familia ISO/IEC 27000**

La norma ISO/27000 está relacionada con los Sistemas de Gestión de Seguridad de la Información (SGSI), abarcando aspectos específicos numerados del 27000 al 27019, y del 27030 al 27044. Esta normativa, lanzada en el año 2009, proporciona un esquema integral de la serie 27000, detallando los términos y condiciones esenciales que deben ser comprendidos de manera definitiva (Herrera, 2020).

2.2.1.7. **Identificación de vulnerabilidades**

Importante darse cuenta de las debilidades que podría tomar por los peligros reconocidos en el pasado mandado. Cuando hablamos de debilidades no solo nos referimos a aquellas que influyen en los marcos, hay debilidades que influyen en otros activos como fundaciones, profesores, etc. Al igual que con los peligros, debemos tener una lista de las debilidades de cuáles nos encontramos expuestos a los peligros que hemos señalado en ese punto. Según Ramírez y Rinconc (2022) el control es un movimiento de carácter gerencial que acciona la exhibición de capacidades dentro de una organización tratando de subsanar las deficiencias mientras son vitales; siendo considerada como una interacción administrativa.

De igual forma, los recursos fijos direccionan parte de los recursos dentro de una organización, y su devaluación influye fundamentalmente en lo que está pasando la organización en la parte monetaria y monetaria a través de los gastos de los artículos vendidos (Guerra et al., 2021). Por otro lado, son aquellos bienes o mercancías materiales de la asociación que no se espera estén disponibles para ser comprados, sino que constituyen una 19 parte del legado y deben ser utilizados para la creación de artículos para su posterior compraventa. Es la disposición de los recursos reales de una organización que serán utilizados para el mejoramiento de sus ejercicios funcionales para el desarrollo del trabajo y los productos.

En cuanto al Control de recursos fijos, son procesos que permiten a la organización tener la opción de dar de alta tanto los pasajes como las salidas de los recursos fijos,

con el objetivo de que la organización cuente con un stock que refleje la realidad y evalúe la condición de protección de los mismos recursos fijos. Por otro lado, Cruz et al. (2023) mencionan que el control de recursos es importante porque ayuda a la organización a tomar medidas correctivas en caso de cualquier problema para que ninguna región resulte dañada y se acceda a información veraz.

Asimismo, García et al. (2022) afirma que la pericia en el control de los recursos propios de una asociación permite la satisfacción de los fines que la acompañan: Poner los recursos del patrimonio en un lugar protegido. Permite obtener datos suficientes en el momento necesario, mejorando la competencia funcional y animando la consistencia con las estrategias de los ejecutivos. Muestran que parten de un stock real, adquisición y utilización del gran, y para su identificación se requerirá una marca o placa, según lo indicado por lo sugerido.

Esta es una forma de asegurarse de que los datos no se hayan modificado sin permiso desde que se crearon. Esta característica es muy importante, por ejemplo, al realizar operaciones bancarias a través de Internet. Su función es velar por la veracidad y el cumplimiento de la información y sus prácticas de gestión (CEUPE, 2020). Para Rodriguez et al. (2020), es la capacidad de evitar alteraciones no deseadas o ilegales en los datos, incluyendo modificaciones o eliminaciones no autorizadas o no deseadas. Según la fuente mencionada, para mantener la integridad es necesario tener tanto la capacidad de deshacer las modificaciones permitidas que deben deshacerse como una forma de detener los cambios no autorizados en los datos.

2.2.1.8. Beneficios que aporta la norma a la Organización

Para el autor los beneficios son los siguientes:

- Confirma la efectividad de los controles internos y el cumplimiento de criterios de gestión y continuidad operativa.
- Verifica el cumplimiento de leyes y regulaciones de forma independiente.
- Ofrece una ventaja competitiva al cumplir con acuerdos contractuales y priorizar la seguridad de la información.
- Confirma la adecuada gestión de riesgos y la formalización de procesos y documentación de seguridad.
- Demuestra el compromiso de la alta dirección con la seguridad de la información.
- Las evaluaciones periódicas ayudan a monitorear y mejorar continuamente el desempeño.

2.2.1.9. **Organismos responsables de estandarizaciones.**

También llamada IEC, es el órgano encargado de crear las directrices electrotécnicas y electrónicas, al igual que la ISO, cuenta con una obligación específica en cuanto a normalizaciones (García et al., 2018).

2.2.2. **Protección de activos**

Referente a la protección de activos, García et al. (2018) señalan que, actualmente las empresas dedican importantes esfuerzos a preservar su información, considerada como su activo más valioso. Para lograrlo, implementan estrategias de gestión de riesgos con el objetivo de prevenir posibles consecuencias negativas, tales como grandes pérdidas financieras o la vulneración de la confidencialidad de datos sensibles.

La protección de activos en las empresas es esencial para garantizar su continuidad y éxito a largo plazo. Los activos empresariales abarcan desde propiedades y tecnología hasta datos, reputación y recursos humanos. Salvaguardar estos elementos críticos implica la implementación de medidas de seguridad efectivas y políticas robustas. Sin embargo, es fundamental identificar y evaluar los activos críticos para la operación de la empresa, comprendiendo su importancia en términos de funcionamiento y rentabilidad (Macías, 2022). A continuación, se deben establecer protocolos de seguridad, incluyendo controles de acceso, cifrado de datos y sistemas de monitoreo, para proteger estos activos contra amenazas internas y externas. La conciencia y capacitación del personal son aspectos cruciales, ya que la adopción y comprensión de prácticas de seguridad deben ser universales entre los empleados.

Implementar políticas de gestión de riesgos es clave para anticipar y manejar amenazas antes de que se conviertan en problemas serios (Sabillón & Cano, 2019). Asimismo, contar con un plan de respuesta a incidentes es clave para actuar rápidamente en caso de violaciones de seguridad o emergencias. La protección de activos no solo busca prevenir pérdidas financieras, sino también preservar la confianza del cliente y la reputación de la empresa en el mercado. En última instancia, una estrategia integral de protección de activos contribuye a la resiliencia y sostenibilidad de la empresa en un entorno empresarial cada vez más complejo y dinámico (Álvarez et al., 2021).

2.2.2.1. **La protección de activos de acuerdo según Magerit V.3:**

a) Información

Es el uso de datos y conocimientos para salvaguardar los recursos valiosos de una organización. Esto incluye la protección de bienes físicos, como equipos y propiedades, así como activos intangibles, como la propiedad intelectual y la información confidencial. La información relevante puede provenir de una variedad de fuentes, incluyendo

informes de seguridad, evaluaciones de riesgos y datos operativos, y su adecuada gestión es esencial para mantener la integridad y el valor de estos activos (Najar & Suárez, 2015).

b) Software

Es el valor económico que el software representa para una organización, considerándolo no solo como una herramienta operativa, sino como un recurso valioso que contribuye al éxito y la competitividad de la empresa. En este contexto, el software es tratado como un activo intangible que puede influir directamente en la eficiencia, productividad y capacidad de innovación de la empresa. Su valor no solo radica en su funcionalidad inmediata, sino también en su potencial para generar beneficios a largo plazo (Stallman, 2020).

Este concepto implica que el software debe ser gestionado, evaluado y contabilizado adecuadamente en los informes financieros de la empresa. Los activos de software pueden incluir aplicaciones comerciales, sistemas personalizados, y licencias, entre otros. La adecuada gestión de estos activos asegura que se maximicen sus beneficios, se optimicen los costos asociados y se minimicen los riesgos relacionados con su uso y mantenimiento (Camacho et al., 2021).

Además, el tratamiento del software como activo también requiere una estrategia de mantenimiento y actualización para asegurar que siga siendo relevante y útil. Esto incluye la inversión en mejoras, la capacitación de los usuarios y la gestión de las licencias. Reconocer el software como un activo estratégico permite a las empresas tomar decisiones informadas sobre sus inversiones en tecnología, alineándolas con sus objetivos generales y asegurando que el software continúe aportando valor a la organización (Lanzas, 2018).

c) Físicos

Los activos físicos de software de una empresa se refieren a todos los elementos tangibles que son necesarios para la operatividad y funcionalidad del software dentro de la organización. Esto incluye los servidores, computadoras, dispositivos de almacenamiento, y cualquier otro hardware que aloje o ejecute aplicaciones y programas de software. Estos activos físicos son fundamentales para garantizar que el software pueda funcionar de manera eficiente y efectiva, proporcionando la infraestructura necesaria para el procesamiento de datos, el almacenamiento seguro de información, y la ejecución de aplicaciones críticas para el negocio (Arévalo & Gámez, 2021).

Además, los activos físicos de software también comprenden los medios físicos donde se almacenan las licencias de software, como discos duros, CDs, DVDs, o unidades USB. La correcta gestión y mantenimiento de estos activos físicos es crucial para asegurar que las licencias de software sean válidas y estén actualizadas, evitando problemas legales y de cumplimiento. La integridad de estos medios también es vital para la recuperación en caso de fallos o pérdidas, permitiendo la reinstalación y el funcionamiento continuo del software en situaciones de emergencia (Linares et al., 2023).

La protección y el mantenimiento de los activos físicos de software requieren una inversión en medidas de seguridad y en la actualización constante del hardware. La empresa debe implementar políticas de seguridad física, como el control de acceso y la vigilancia, para proteger estos activos de daños, robos o manipulaciones no autorizadas. Asimismo, es necesario planificar y ejecutar un programa de actualización de hardware que garantice que todos los equipos sean compatibles con las versiones más recientes del software y puedan soportar futuras actualizaciones y expansiones tecnológicas (Ferruzola et al., 2019).

d) Servicios

Los activos de servicio de una empresa son aquellos recursos tangibles e intangibles utilizados para proporcionar servicios a los clientes. Estos activos pueden incluir equipos, software, infraestructuras, habilidades y conocimientos del personal, así como procesos y sistemas que permiten la entrega eficiente y efectiva de servicios. En esencia, son los elementos que permiten a una empresa cumplir con sus promesas de servicio y satisfacer las necesidades de sus clientes (Jácome et al., 2021).

Estos activos son cruciales para el éxito y la competitividad de una empresa de servicios. Por ejemplo, en una empresa de tecnología de la información, los activos de servicio podrían incluir servidores, redes, aplicaciones de software y el conocimiento especializado de los técnicos. En una empresa de servicios financieros, los activos de servicio podrían incluir sistemas de gestión de datos, herramientas de análisis financiero y la experiencia de sus asesores. La gestión efectiva de estos activos permite a la empresa mantener altos niveles de calidad y consistencia en la entrega de sus servicios (Cabrejos, 2020).

La inversión y mantenimiento de los activos de servicio son esenciales para asegurar la sostenibilidad a largo plazo de la empresa. Esto implica no solo la adquisición de nuevos activos cuando sea necesario, sino también la actualización y mejora continua de los activos existentes. Además, la formación y desarrollo del personal, así como la

implementación de procesos eficientes, son fundamentales para maximizar el valor de estos activos. Una gestión adecuada de los activos de servicio contribuye a la optimización de costos, la mejora de la satisfacción del cliente y, en última instancia, el crecimiento y éxito de la empresa en el mercado competitivo (Alvarado et al., 2018).

e) Personas

El capital humano es un recurso intangible clave que mejora la productividad, fomenta la innovación y aumenta la competitividad. Su éxito depende del desempeño de todas las personas en la organización, quienes aportan habilidades, conocimientos y valores esenciales (Gallego & Naranjo, 2020).

Las personas dentro de una organización son las que deciden cómo, cuándo y dónde utilizar sus capacidades. Los recursos humanos se convierten así en una fuente de ventaja competitiva para las organizaciones. Es crucial que las empresas reconozcan el valor de sus empleados y trabajen en potenciarlo. Esto no solo mejora el rendimiento organizacional, sino que también incrementa el valor de la empresa para sus empleados (Díaz & Toscano, 2022).

Para atraer y retener a los mejores talentos, las empresas deben identificar y maximizar el valor que cada persona aporta. Además, es importante que las organizaciones aumenten su atractivo para los empleados, reduciendo así el riesgo de perder un activo tan valioso como el capital humano. Esto asegura que el conocimiento y las habilidades esenciales permanezcan dentro de la empresa, fortaleciendo su posición competitiva (Bernal et al., 2020).

CAPÍTULO III
MATERIALES Y MÉTODOS

3.1. Ámbito y condiciones de la investigación

3.1.1. Contexto de la investigación

2.2.2.2. Ubicación política

Se realizó en el distrito de Tarapoto, Jr. Libertad 291, lugar donde se encuentra ubicada la empresa.

El distrito limita con:

- Morales, por el norte
- La Banda de Shilcayo, por el sur

2.2.2.3. Ubicación geográfica

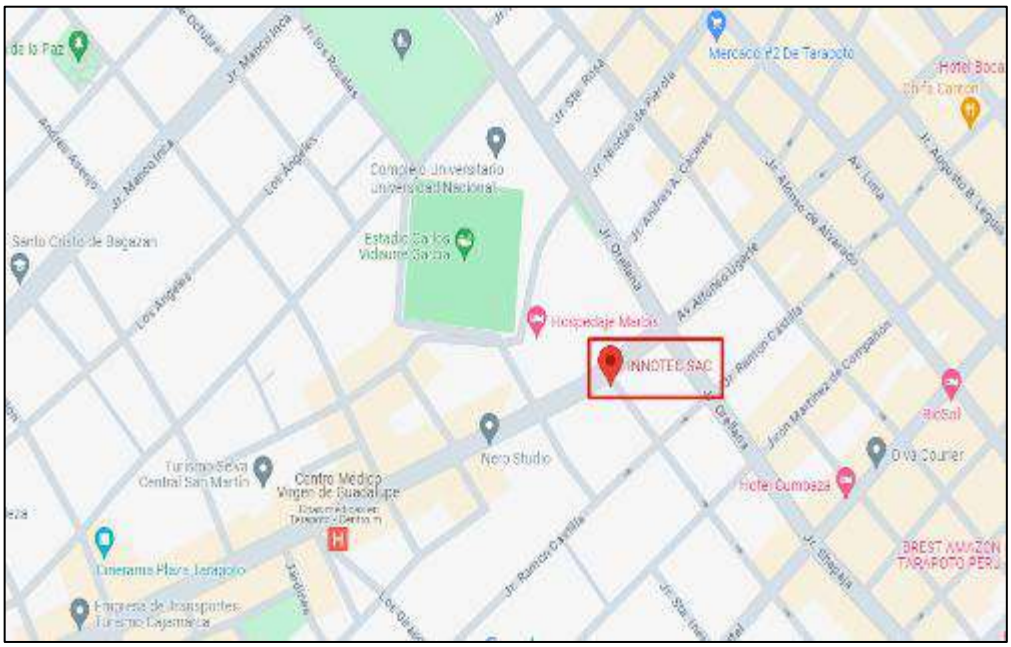


Figura 1
Ubicación geográfica de la empresa
Fuente: Google maps

3.1.2. Periodo de ejecución

La ejecución de tesis se llevó a cabo durante los meses comprendidos entre setiembre del 2024 a mayo del 2025. Específicamente siguiendo el siguiente cronograma.

Tabla 1

Cronograma de actividades

Objetivo 1: Analizar el nivel de la seguridad de la información según la ISO 27001 en la empresa INNOTEC - Tarapoto, 2023.

ACTIVIDADES	MESES								
	1	2		3	4	5	6	7	8	9
1. Recopilar información bibliográfica.	X		x							
2. Diseño de instrumento		X								
3. Validez y confiabilidad del instrumento.		X								
4. Aplicación de instrumento de recolección.				X						
5. Análisis descriptivo de los resultados.					X					

Objetivo 2: Analizar el nivel de protección de los activos en la empresa INNOTEC - Tarapoto, 2023.

ACTIVIDADES	MESES								
	1	2		3	4	5	6	7	8	9
1. Recopilar información bibliográfica.	X									
2. Diseño de instrumento		X								
3. Validez y confiabilidad del instrumento.		X								
4. Aplicación de instrumento de recolección.				X						
5. Análisis descriptivo de los resultados.					X					

Objetivo 3: Determinar la relación entre las dimensiones de la seguridad de la información basados en la norma ISO 27001 y la protección de activos en la empresa INNOTEC - Tarapoto, 2023.

ACTIVIDADES	MESES								
	1	2	3	4	5	6	7	8	9
1. Tabulación y recuentos de los datos.					X	X			
2. Análisis inferencial de los resultados.							X		
3. Presentación de resultados							X	X	
4. Recomendaciones								X	
5. Conclusiones									X

3.1.3. Autorizaciones y permisos

Se solicitaron permisos al gerente general de la empresa INNOTEC S.A.C, donde se llevó a cabo la investigación, asegurando su colaboración y apoyo para hacerla posible. Asimismo, se obtuvieron los consentimientos informados de los involucrados para participar en el estudio, explicándoles claramente los objetivos, procedimientos y posibles riesgos asociados. Estas autorizaciones fueron fundamentales para garantizar la validez, integridad y ética de la investigación, así como para proteger los derechos y el bienestar de todos los participantes.

3.1.4. Control ambiental y protocolos de bioseguridad

No se aplicó este paso.

3.1.5. Aplicación de principios éticos internacionales

En esta investigación se aplicaron los siguientes principios éticos: la investigación se llevó a cabo con la máxima integridad y profesionalismo, adhiriéndose a los principios

éticos tanto nacionales como internacionales. Estos principios aseguraron la calidad ética del estudio, manejando los datos con la debida seriedad. Se preservó la integridad y exactitud de la información, y se garantizó el respeto a la autonomía de los participantes, evitando cualquier consecuencia negativa. Los resultados fueron utilizados exclusivamente con fines académicos y se realizó una referencia y citación adecuada de los autores, siguiendo las Normas APA, séptima edición de 2019.

- Respeto a las personas: Se garantizó un trato equitativo y considerado hacia los colaboradores de INNOTEC, reconociendo su papel crucial en la implementación y evaluación de las prácticas de seguridad de la información. Este respeto se reflejó en una comunicación abierta y transparente, asegurando que cada miembro del equipo comprendiera la finalidad y los beneficios del estudio.
- Conveniencia: Este estudio sobre la seguridad de la información y la protección de activos en INNOTEC representó una iniciativa estratégica de gran relevancia, ya que proporcionó una visión detallada y actualizada del estado de las prácticas de seguridad de la información en la empresa, permitiendo identificar áreas de mejora y optimización. La evaluación comparativa ofreció una perspectiva integral de cómo las prácticas actuales influían en la eficiencia operativa y la gestión de recursos tecnológicos, facilitando la mejora continua en la protección de activos.
- Totalidad/Integridad: Dado el papel fundamental de la seguridad de la información en las operaciones empresariales, fue crucial garantizar que las prácticas de protección de activos estuvieran alineadas con los mejores estándares de la industria. Este estudio permitió identificar posibles brechas en la gestión de seguridad y proponer estrategias de mejora para optimizar la protección de datos y recursos en INNOTEC.
- Beneficencia: La investigación analizó de manera integral la eficacia y eficiencia de las prácticas de seguridad de la información en INNOTEC. A través de datos objetivos, los resultados facilitaron la toma de decisiones estratégicas, fortaleciendo la seguridad y optimización de los procesos. Esto permitió mejorar la protección de activos, garantizar la continuidad operativa y potenciar la productividad empresarial.

3.2. Sistema de variables

3.2.1. Variables principales

Variable independiente: La seguridad de la información.

Variable dependiente: La protección de los activos.

Descripción de variables por objetivo específico:

Tabla 2

Descripción de variables por objetivo específico 1

Objetivo específico 1: Analizar el nivel de la seguridad de la información según la ISO 27001 en la empresa INNOTEC - Tarapoto, 2023.			
Variable abstracta	**Variable concreta**	**Medio de registro**	**Unidad de medida**
Seguridad de la información	• Disponibilidad • Confidencialidad • Integridad	• Encuesta (Cuestionario) • Hoja de cálculo Excel	Ordinal

Tabla 3

Descripción de variables por objetivo específico 2

Objetivo específico № 2: Analizar el nivel de protección de los activos en la empresa INNOTEC - Tarapoto, 2023.			
Variable abstracta	**Variable concreta**	**Medio de registro**	**Unidad de medida**
Protección de los activos	• Los tipos de activos de la empresa (información, software, físicos, servicios, personal)	• Encuesta (Cuestionario) • Hoja de cálculo Excel	Ordinal

3.2.2. Variables secundarias

No se pudo evidenciar variables de esta naturaleza, solo se consideró las variables establecidas en el estudio.

3.3. Procedimientos de la investigación

Para la evaluación de las dos variables se tomó como referencia los contenidos vertidos en el proyecto de investigación

3.3.1. Diseño de la investigación

Tipo de investigación: Fue básica. Según Cívicos y Hernández (2007), también denominada investigación fundamental, exacta o pura, se enfocó en el objeto de estudio sin buscar una aplicación inmediata. No obstante, sus resultados y descubrimientos pudieron generar nuevos productos y avances científicos. En este sentido, se desarrolló la investigación con propósitos de exploración, descripción y establecimiento de relaciones.

Nivel de investigación: Se clasificó como un estudio descriptivo correlacional. De acuerdo con Carrasco (2019), este tipo de investigación tuvo como objetivo describir los elementos de las variables en relación con sus características específicas, proporcionando una visión detallada de cómo se presentaron y comportaron ciertos fenómenos. El propósito principal de este estudio fue comprender la relación o grado de asociación entre dos o más variables o categorías dentro de un contexto o muestra particular.

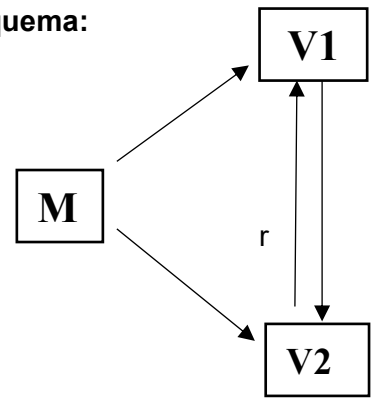
Población: Es la totalidad de los individuos que participaron en el fenómeno seleccionado y delimitado para el análisis de la problemática de estudio (Otzen & Manterola, 2017). En este caso, la población estuvo conformada por un grupo de 25 miembros del personal de INNOTEC-Tarapoto.

Muestra: Refiere a una fracción de la población que se elige cuidadosamente para obtener información relevante relacionada al problema que se pretende resolver (Ñaupas et al., 2018). En este caso, la muestra del estudio estuvo integrada por el total de la población ascendiendo a 25 miembros del personal de INNOTEC-Tarapoto.

Muestreo: Para la elección de la muestra se aplicó un muestreo no probabilístico a conveniencia del investigador. Según la definición de Cuesta y Herrero (2010), este tipo de muestreo no probabilístico implica la selección de participantes principalmente basada en el acceso y criterio personal e intencional del investigador.

Diseño: La investigación tuvo un diseño no experimental de tipo transversal, el cual, según la definición de Hernández et al. (2014), implica la observación en el contexto real sin manipulación deliberada de variables. Además, el estudio adopta un diseño transversal al limitarse a un único periodo de estudio. El esquema metodológico es de la siguiente manera:

Esquema:



Dónde:

M = Muestra de la investigación.

V_1 = Gestión de la seguridad de la información

V_2 = Protección de activos

r = Relación de las variables involucradas

3.3.2. Actividades del objetivo específico 1: Analizar el nivel de la seguridad de la información según la ISO 27001 en la empresa INNOTEC - Tarapoto, 2023

Para medir la seguridad de la información en el contexto de la norma ISO 27001, se siguió un conjunto de procedimientos estructurados. En primer lugar, se llevó a cabo una exhaustiva revisión de la literatura para identificar conceptos clave, estudios previos y enfoques metodológicos relacionados con la seguridad de la información, la norma ISO 27001 y sus dimensiones de confidencialidad, integridad y disponibilidad. Esta revisión proporcionó una base teórica sólida para el diseño del instrumento de recolección de datos.

Posteriormente, con base en la información recopilada, se diseñó una encuesta estructurada en torno a las tres dimensiones principales de la seguridad de la información. Cada dimensión se midió a través de indicadores específicos, tales como la efectividad de la formación en confidencialidad, la adecuación de los procesos de control de cambios y la percepción de la estabilidad de los sistemas. Para garantizar la validez del instrumento, se utilizó la técnica de juicio de expertos, mientras que su confiabilidad se evaluó mediante el coeficiente Alfa de Cronbach.

Una vez validado el instrumento, este fue aplicado a la población objetivo, asegurando que los encuestados comprendieran correctamente las preguntas y proporcionaran respuestas precisas y útiles para el análisis. Posteriormente, se realizó un análisis descriptivo de los datos recolectados, lo que permitió identificar tendencias, fortalezas y áreas de mejora en la gestión de la seguridad de la información, según las dimensiones de confidencialidad, integridad y disponibilidad. Los resultados obtenidos ofrecieron una visión clara sobre la percepción e implementación de la seguridad de la información en la organización.

Para el procesamiento y análisis de los datos, se utilizó Microsoft Excel, lo que permitió evaluar de manera eficiente las características de la variable seguridad de la información según la norma ISO 27001 en la empresa INNOTEC.

3.3.3. Actividades del objetivo específico 2: Analizar el nivel de protección de los activos en la empresa INNOTEC - Tarapoto, 2023

Para analizar el nivel de protección de los activos en la empresa INNOTEC en 2023, se siguió un conjunto de procedimientos estructurados. En primer lugar, se realizó una investigación exhaustiva sobre la protección de activos, con un enfoque particular en Magerit V.3. Además, se elaboró un listado detallado de los activos presentes en la empresa, los cuales fueron clasificados en cinco categorías: Información, Software,

Físicos, Servicios y Personal. Este listado permitió identificar y evaluar las medidas de protección necesarias para cada tipo de activo.

A partir de la información recopilada y del listado de activos, se diseñó un cuestionario para evaluar el nivel de protección de los activos en INNOTEC. La encuesta se estructuró en torno a las cinco categorías mencionadas, asegurando un enfoque integral en la evaluación de las medidas de seguridad implementadas en la empresa. Para garantizar la validez del cuestionario, se utilizó la técnica de juicio de expertos, en la cual especialistas en la materia revisaron y aprobaron el instrumento. Asimismo, para evaluar la confiabilidad o consistencia del cuestionario, se calculó el coeficiente Alfa de Cronbach, lo que permitió medir la coherencia interna de los ítems y garantizar que estos reflejaran de manera fiable las dimensiones de protección de activos.

Una vez validado y comprobado su nivel de confiabilidad, el cuestionario fue aplicado a los miembros del personal de INNOTEC-Tarapoto. Durante la aplicación, se aseguraron condiciones adecuadas para que los encuestados comprendieran claramente las preguntas y proporcionaran respuestas precisas y útiles sobre las medidas de protección implementadas en la empresa. Posteriormente, se llevó a cabo un análisis descriptivo de los datos recolectados, lo que permitió evaluar el nivel de protección de los activos en la organización. Este análisis facilitó la identificación de fortalezas y áreas de mejora en la seguridad de la información, el software, los activos físicos, los servicios y el personal, proporcionando una visión integral del estado de protección de los activos en INNOTEC.

Finalmente, el procesamiento y análisis de datos se realizó utilizando Microsoft Excel, lo que permitió evaluar de manera eficiente las características de la variable protección de activos, facilitando la identificación de áreas críticas y la implementación de mejoras efectivas.

3.3.4. Actividades del objetivo específico 3: Determinar la relación entre las dimensiones de la seguridad de la información basados en la norma ISO 27001 y la protección de activos en la empresa INNOTEC - Tarapoto, 2023

Para determinar la relación entre las dimensiones de la seguridad de la información, basadas en la norma ISO 27001, y la protección de activos en la empresa INNOTEC en 2023, se llevaron a cabo diversas actividades metodológicas. En primer lugar, se realizó la tabulación y recuento de los datos recolectados a través de los cuestionarios. Durante este proceso, la información fue organizada y resumida, permitiendo identificar la frecuencia de las respuestas en cada categoría y dimensión. Se elaboraron tablas y gráficos que facilitaron la visualización de la distribución de los datos, reflejando de

manera clara la relación entre las dimensiones de confidencialidad, integridad y disponibilidad con la protección de activos.

Posteriormente, se efectuó un análisis estadístico inferencial con el objetivo de identificar y evaluar relaciones significativas entre las dimensiones de la seguridad de la información y la protección de activos. Para ello, se aplicaron pruebas de correlación que permitieron medir el grado de asociación entre las variables en estudio, proporcionando evidencia sobre cómo las prácticas de seguridad influían en la protección de los activos dentro de la empresa.

A partir de los resultados obtenidos, se redactaron las conclusiones del estudio, en las que se resumieron los principales hallazgos respecto a la relación entre la seguridad de la información y la protección de activos. Estas conclusiones destacaron la efectividad de las prácticas de seguridad implementadas en INNOTEC y sus implicaciones para la mejora de la gestión de activos.

Finalmente, se elaboraron recomendaciones específicas orientadas a fortalecer la protección de los activos en la empresa, alineándolas con las dimensiones de la seguridad de la información establecidas por la norma ISO 27001. Estas sugerencias se enfocaron en mejorar las prácticas actuales y optimizar los procesos de seguridad.

Para el procesamiento y análisis de los datos, se emplearon técnicas estadísticas especializadas. En primer lugar, se aplicó la prueba de Shapiro-Wilk para determinar si los datos seguían una distribución normal, lo que resultó fundamental para seleccionar el análisis estadístico más adecuado. Dado que los datos no presentaron una distribución normal, se utilizó la prueba de correlación de Spearman para evaluar la asociación entre las variables. Estas pruebas permitieron cuantificar la relación entre las dimensiones de la seguridad de la información y la protección de activos, proporcionando una visión detallada sobre cómo las medidas de seguridad impactaban en la gestión de los activos dentro de INNOTEC.

CAPÍTULO IV
RESULTADOS Y DISCUSIÓN

4.1. Resultado específico 1: nivel de la seguridad de la información según la ISO 27001

Tabla 4

Puntajes establecidos para la variable seguridad de la información y sus dimensiones

Dimensiones / Variable	Deficiente	Regular	Bueno
	Puntaje	Puntaje	Puntaje
Confidencialidad	6 a 14	15 a 22	23 a 30
Integridad	6 a 14	15 a 22	23 a 30
Disponibilidad	6 a 14	15 a 22	23 a 30
Seguridad de la información	18 a 42	43 a 66	67 a 90

Fuente: Datos propios de la investigación.

La tabla 4 presenta la baremación para evaluar la variable seguridad de la información y sus dimensiones: confidencialidad, integridad y disponibilidad. Cada dimensión se clasifica en tres niveles: deficiente, regular y bueno, según los puntajes obtenidos. En todas las dimensiones, un puntaje entre 6 y 14 indica un nivel deficiente, entre 15 y 22 corresponde a un nivel regular, y entre 23 y 30 se considera bueno. De la variable seguridad de la información se evalúa en un rango de 18 a 90, donde un puntaje de 18 a 42 representa una seguridad deficiente, de 43 a 66 es regular, y de 67 a 90 es buena.

Tabla 5

Evaluación del nivel de la seguridad de la información según la ISO 27001 en la empresa INNOTEC - Tarapoto, 2023.

Dimensiones / Variable	Deficiente		Regular		Bueno		Total	
	N°	%	N°	%	N°	%	N°	%
Confidencialidad	3	12,0	3	12,0	19	76,0	25	100
Integridad	3	12,0	18	72,0	4	16,0	25	100
Disponibilidad	3	12,0	18	72,0	4	16,0	25	100
Seguridad de la información	3	12,0	13	52,0	9	36,0	25	100

Fuente: Datos propios de la investigación.

La tabla 4 muestra la evaluación del nivel de seguridad de la información en la empresa INNOTEC - Tarapoto, 2023, considerando sus dimensiones: confidencialidad, integridad y disponibilidad. Se observa que la confidencialidad presenta un nivel mayormente bueno (76%), mientras que la integridad y la disponibilidad tienen una mayor proporción en el nivel regular (72% en ambos casos). En cuanto a la seguridad de la información en general, el 52% la percibe como regular, el 36 % como buena y el 12 % como deficiente.

4.2. Resultado específico 2: nivel de protección de los activos

Tabla 6

Puntajes establecidos para la variable protección de los activos y sus dimensiones

Dimensiones / Variable	Deficiente	Regular	Bueno
	Puntaje	Puntaje	Puntaje
Información	3 a 7	8 a 11	12 a 15
Software	4 a 9	10 a 15	16 a 20
Físicos	5 a 11	12 a 18	19 a 25
Servicios	2 a 4	5 a 7	8 a 10
Personal	2 a 4	5 a 7	8 a 10
Protección de los activos	16 a 37	38 a 59	60 a 80

Fuente: Datos propios de la investigación.

La tabla 6 presenta la baremación para evaluar el nivel de protección de los activos en la empresa INNOTEC - Tarapoto. En la dimensión información, los puntajes de 3 a 7 indican un nivel deficiente, de 8 a 11 es regular y de 12 a 15 es bueno. Para el software, un puntaje entre 4 y 9 es deficiente, entre 10 y 15 es regular y entre 16 y 20 es bueno. En los activos físicos, los puntajes de 5 a 11 representan un nivel deficiente, de 12 a 18 es regular y de 19 a 25 es bueno. Tanto en servicios como en personal, los valores de 2 a 4 corresponden a un nivel deficiente, de 5 a 7 a regular, y de 8 a 10 a bueno. Finalmente, la variable protección de los activos se evalúa en puntajes de 16 a 37 indican una protección deficiente, de 38 a 59 es regular, y de 60 a 80 es buena.

Tabla 7

Evaluación del nivel de protección de los activos en la empresa INNOTEC - Tarapoto, 2023.

Dimensiones / Variable	Deficiente		Regular		Bueno		Total	
	N°	%	N°	%	N°	%	N°	%
Información	5	20,0	18	72,0	2	8,0	25	100
Software	2	8,0	13	52,0	10	40,0	25	100
Físicos	2	8,0	6	24,0	17	68,0	25	100
Servicios	1	4,0	2	8,0	22	88,0	25	100
Personal	17	68,0	8	32,0	0	0,0	25	100
Protección de los activos	2	8,0	16	64,0	7	28,0	25	100

Fuente: Datos propios de la investigación.

En la tabla 7 se observa que la dimensión de los servicios es la más alta, con un 88 % en el nivel bueno, seguida de la dimensión activos físicos con un 68 % en el nivel de Bueno. En cuanto al software, el 40% lo percibe como bueno, mientras que la mayoría lo evalúa como regular (52%). La información tiene un 72 % en nivel regular, pero un 20% aún la considera deficiente. La dimensión más crítica es personal, con un 68 % en nivel deficiente y sin registros en la categoría bueno. En general, la protección de los activos es considerada mayormente regular (64%), con un 28% que la evalúa como buena.

4.3. Resultado específico 3: relación entre las dimensiones de la seguridad de la información basados en la norma ISO 27001 y la protección de activos

Tabla 8

Prueba de normalidad.

Variables	Shapiro-Wilk		
	Estadístico	gl	Sig.
Confidencialidad	0,848	25	0,002
Integridad	0,848	25	0,002
Disponibilidad	0,920	25	0,052
Seguridad de la información	0,802	25	0,000
Protección de los activos	0,848	25	0,002

Se realizó la prueba de Shapiro-Wilk para verificar la distribución normal de los datos obtenidos de los 25 miembros del personal de INNOTEC-Tarapoto que completaron los cuestionarios. Los resultados de esta prueba, presentados en la Tabla 7, indican que ambas variables analizadas no siguen una distribución normal, ya que los valores de p obtenidos fueron inferiores a 0.05. En consecuencia, se concluye que las mediciones de las dimensiones de la seguridad de la información basadas en la norma ISO 27001 y la protección de activos en la muestra estudiada no provienen de una distribución normal, por lo que se empleará una prueba no paramétrica para el análisis.

Tabla 9

Correlación no paramétrica de Spearman para las dimensiones de la seguridad de la información basados en la norma ISO 27001 y la protección de activos en la empresa INNOTEC - Tarapoto, 2023.

Rho de Spearman		Protección de activos
Confidencialidad	Coeficiente de correlación	,788**
	Coeficiente de determinación	62%
	Sig. (bilateral)	0,000
	N	25
Integridad	Coeficiente de correlación	,702**
	Coeficiente de determinación	49%
	Sig. (bilateral)	0,000
	N	25
Disponibilidad	Coeficiente de correlación	,525**
	Coeficiente de determinación	28%
	Sig. (bilateral)	0,007
	N	25

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

La Tabla 8 presenta los resultados de la correlación no paramétrica de Spearman entre las dimensiones de la seguridad de la información, según la norma ISO 27001, y la protección de activos en la empresa INNOTEC - Tarapoto, 2023. Se observa que todas las dimensiones presentan una correlación positiva y significativa con la protección de activos ($p < 0.01$). La confidencialidad muestra una correlación alta ($\rho = 0.788$), con un 62% de coeficiente de determinación, lo que indica que esta dimensión explica en gran

medida la variabilidad en la protección de activos. La integridad presenta una correlación alta (ρ = 0.702), con un 49% de coeficiente de determinación. Finalmente, la disponibilidad tiene una correlación moderada (ρ = 0.525) y un 28% de coeficiente de determinación, lo que indica una influencia más limitada. En general, los resultados evidencian que mejorar la seguridad de la información, especialmente la confidencialidad e integridad, contribuye significativamente a la protección de los activos en la empresa.

4.4. Resultado general: relación entre la seguridad de la información según la ISO 27001 y la protección de activos en la empresa INNOTEC - Tarapoto, 2023

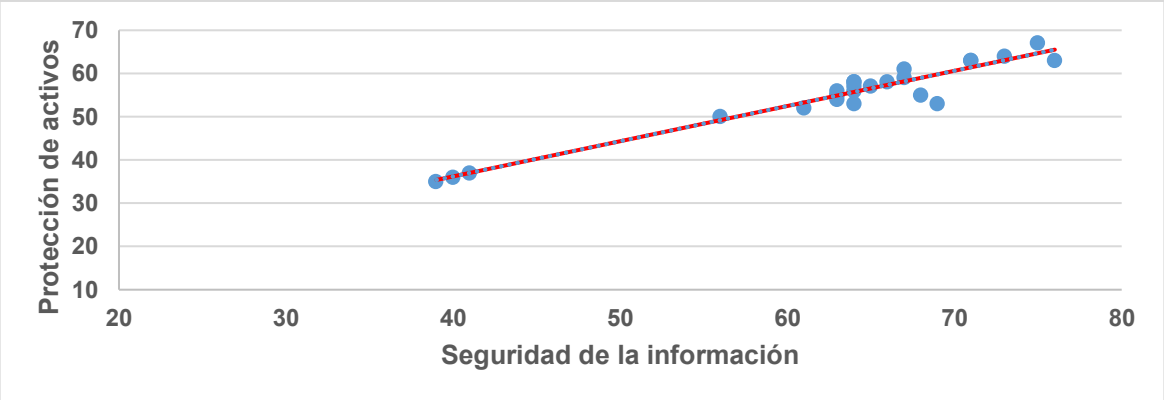


Figura 2
Gráfico de dispersión entre la seguridad de la información según la ISO 27001 y la protección de activos en la empresa INNOTEC - Tarapoto, 2023.

La Figura 2 muestra un gráfico de dispersión que representa la relación entre la seguridad de la información según la ISO 27001 y la protección de activos en la empresa INNOTEC - Tarapoto, 2023. Se observa una tendencia positiva, lo que indica que a medida que aumenta el nivel de seguridad de la información, también mejora la protección de los activos. La presencia de una línea de tendencia ajustada a los datos refuerza esta correlación, evidenciando que existe una relación directa entre ambas variables.

Tabla 10
Correlación no paramétrica de Spearman entre la seguridad de la información según la ISO 27001 y la protección de activos en la empresa INNOTEC - Tarapoto, 2023

Rho de Spearman		Protección de activos
Seguridad de la información	Coeficiente de correlación	,841**
	Coeficiente de determinación	71%
	Sig. (bilateral)	0,000
	N	25

**. La correlación es significativa en el nivel 0,01 (bilateral).
Fuente: Datos propios de la investigación.

4.4.1. Contrastación de prueba de hipótesis

Hipótesis alterna (Ha): Existe una relación significativa entre la seguridad de la información según la ISO 27001 y la protección de activos en la empresa INNOTEC - Tarapoto, 2023.

Hipótesis nula (Ho): No existe una relación significativa entre la seguridad de la información según la ISO 27001 y la protección de activos en la empresa INNOTEC - Tarapoto, 2023.

4.4.1.1. Nivel de significación

Para el análisis es del 5%, lo que corresponde a un nivel de confianza del 95%. Esto se debe a que se emplea un nivel de significancia teórica de α igual a 0,05, lo que implica que se acepta una probabilidad del 5% de cometer un error al rechazar una hipótesis nula verdadera.

4.4.1.2. Regla decisiva

- Si el valor p es mayor o igual a 0,05, se acepta la Hipótesis Nula (H0). En cambio, si el valor p es menor o igual a 0,05, se rechaza la Hipótesis Nula y, en consecuencia, se acepta la Hipótesis Alterna (Ha).

4.4.1.3. Interpretación

Se obtiene de la tabla 9 que la relación de Spearman entre las variables revela que la seguridad de la información según la ISO 27001 posee una correlacion muy alta con la protección de activos en la empresa INNOTEC - Tarapoto, especificamente con un coeficiente de correlación de 0.841. Además, con un p valor igual a 0.000, y un coeficiente de determinación del 71%. Este hallazgo fortalece aún más la aceptacion de la hipótesis alterna. En otras palabras, existe una relación significativa entre la seguridad de la información según la ISO 27001 y la protección de activos en la empresa INNOTEC - Tarapoto, 2023. Esto implica que fortalecer la seguridad de la información contribuye a una mejor protección de los activos dentro de la empresa.

4.5. Discusión

Objetivo específico 1: Los hallazgos de Bustamante et al. (2021) demuestran que la implementación de políticas basadas en la ISO 27001:2013 puede generar mejoras sustanciales en la seguridad de la información, reflejadas en un aumento del 49 % al 96 % en la satisfacción de los trabajadores tras aplicar dichas directrices. Esta efectividad se explica por el enfoque integral que abarca la confidencialidad, la integridad y la disponibilidad, lo cual coincide con la importancia de estas tres dimensiones en la evaluación de la seguridad de la información. En este sentido, el estudio de Bustamante

et al. sugiere que el éxito de la norma ISO 27001:2013 radica en la adopción de políticas claras, la formación continua del personal y la supervisión constante de su cumplimiento, aspectos que resultaron decisivos para reforzar la gestión de seguridad en la municipalidad distrital analizada.

En contraste, los resultados de la empresa INNOTEC - Tarapoto evidencian que, si bien la confidencialidad presenta un nivel bueno (76 %), tanto la integridad como la disponibilidad continúan en un nivel predominantemente regular (72 % cada una). Este escenario plantea la necesidad de reforzar la implementación y el seguimiento de los controles establecidos por la norma ISO 27001, tal como lo hizo la municipalidad peruana estudiada por Bustamante et al. (2021). La adopción sistemática de estas políticas, complementada con capacitación y monitoreo, podría impulsar a INNOTEC a evolucionar desde un 52 % de nivel regular en seguridad de la información hacia indicadores más cercanos a los resultados favorables observados en la investigación previa.

Al comparar ambos estudios, se observa que la implementación exhaustiva de los lineamientos de la norma ISO 27001 conduce a mejoras sustanciales en la seguridad de la información. En el caso de la municipalidad analizada por Bustamante et al. (2021), la satisfacción de los trabajadores se elevó de 49 % a 96 %, lo que evidencia una adopción exitosa de políticas claras y una capacitación efectiva. En contraste, INNOTEC - Tarapoto presenta un nivel predominantemente regular (52 %) y deficiencias particulares en la integridad y la disponibilidad (ambas con 72 % en nivel regular), lo que indica la necesidad de reforzar las estrategias de aplicación de la norma y de profundizar en la sensibilización y formación continua del personal. De este modo, la empresa podría alinear sus resultados con los logros documentados por Bustamante et al., impulsando la madurez de su sistema de gestión de seguridad de la información.

Objetivo específico 2: En la investigación de Apahuasco (2020), la implementación de los lineamientos del estándar ISO 27001 en la empresa Disav SAC evidenció la importancia de reforzar la seguridad de la información tanto en los dispositivos como entre el personal. A través de un análisis detallado y la aplicación de controles específicos, se capacitó a los colaboradores y se ajustaron los equipos informáticos, lo que contribuyó a la disminución de vulnerabilidades. El enfoque cuantitativo, complementado por el uso del software SPSS v.24, permitió medir de manera objetiva la efectividad de dichas intervenciones, confirmando que la reducción de brechas de seguridad está asociada a la adecuada formación del personal y a la correcta implementación de medidas técnicas.

De manera similar, los resultados de la empresa INNOTEC - Tarapoto ponen de relieve la necesidad de fortalecer la protección de sus activos, especialmente ante la prevalencia del nivel regular (64%) en la mayoría de las dimensiones evaluadas. Aunque las áreas de servicios y activos físicos presentan porcentajes más favorables, persisten oportunidades de mejora significativas, particularmente en el resguardo de la información (72% en nivel regular y 20% en nivel deficiente) y del software (52% regular). Destaca, sobre todo, la dimensión del personal, que alcanza un 68% en nivel deficiente, lo que indica que este factor humano requiere intervenciones decididas, tal como evidenciaron los hallazgos del estudio de la empresa Disav SAC.

Ambos escenarios coinciden en subrayar que la optimización de la seguridad de la información no solo depende de la adquisición o actualización de herramientas tecnológicas, sino también de la formación continua y la concientización del personal para minimizar riesgos. La experiencia de Disav SAC demuestra que la aplicación sistemática de controles y la capacitación son estrategias efectivas para reducir vulnerabilidades, mientras que en INNOTEC - Tarapoto se hace evidente la necesidad de incorporar enfoques similares para mejorar las capacidades de su capital humano y, con ello, aumentar el nivel de protección de todos sus activos.

Objetivo específico 3: En el estudio de Rodríguez et al. (2020), se destaca que la aplicación de la norma ISO 27001 en una empresa privada de Lima contribuyó significativamente a mejorar la gestión de la seguridad de la información, centrándose en las dimensiones de confidencialidad, integridad y disponibilidad. A través de un enfoque cuantitativo y un diseño preexperimental con 30 empleados, se evidenció que la adopción de la norma influyó de manera positiva en la protección de los datos corporativos, minimizando los riesgos en un entorno tecnológico cada vez más complejo y competitivo.

De manera similar, los hallazgos en la empresa INNOTEC - Tarapoto refuerzan la relevancia de fortalecer dichas dimensiones para optimizar la protección de los activos. Al analizar la relación entre la seguridad de la información y la protección de activos, se obtuvo una correlación significativa, particularmente en la confidencialidad ($\rho = 0.788$) y la integridad ($\rho = 0.702$), lo que demuestra que el cumplimiento de los lineamientos de la norma ISO 27001 es determinante para reducir vulnerabilidades y salvaguardar los recursos críticos de la organización. Asimismo, aunque la disponibilidad mostró un coeficiente de correlación menor ($\rho = 0.525$), sigue siendo un componente esencial para la continuidad de las operaciones.

La coincidencia en la importancia de la norma ISO 27001 en ambos contextos –una empresa privada en Lima y la organización INNOTEC– pone de relieve la necesidad de adoptar un enfoque integral de seguridad, donde la formación y concientización del personal, junto a políticas y controles claramente definidos, resultan fundamentales para reforzar la confidencialidad, integridad y disponibilidad de la información. En conjunto, estos estudios evidencian que la aplicación efectiva de la norma no solo protege los intereses estratégicos de las empresas, sino que incide positivamente en la confianza de las partes interesadas y en la estabilidad de las operaciones a largo plazo.

Objetivo general: En concordancia con la investigación de Risco (2020), quien evidenció una reducción significativa de las vulnerabilidades en confidencialidad, integridad y disponibilidad tras implementar un sistema de gestión de seguridad de la información basado en ISO 27001:2013, los resultados obtenidos en la empresa INNOTEC - Tarapoto refuerzan la efectividad de esta norma. Risco (2020) reportó que las acciones orientadas a la adopción de ISO 27001 disminuyeron las vulnerabilidades de casi un 70% a valores cercanos al 11-15% y elevaron la seguridad global del 80% al 90%. Del mismo modo, en INNOTEC se comprobó que un mayor nivel de seguridad de la información, fundamentado en los lineamientos de ISO 27001, se asocia de forma muy significativa con la protección de los activos ($\rho = 0.841$), indicando que las organizaciones que aplican rigurosamente estos controles son capaces de mitigar riesgos y salvaguardar sus recursos críticos.

La coincidencia entre ambas investigaciones radica en la importancia de combinar la adopción de políticas claras, la capacitación continua del personal y la evaluación constante de los procesos para optimizar los niveles de confidencialidad, integridad y disponibilidad de la información. Así como en la Empresa Constructora Pérez & Pérez SAC se observaron mejoras sustanciales en la gestión de la seguridad tras implementar la norma ISO 27001, en INNOTEC se evidencia la pertinencia de reforzar dichas estrategias para maximizar la protección de sus activos. Estas observaciones confirman que, mediante un enfoque sistemático y estandarizado, se puede alcanzar un grado más alto de preparación frente a eventuales amenazas, minimizando vulnerabilidades y asegurando la continuidad de las operaciones.

CONCLUSIONES

1º. Los resultados evidenciaron que existe una relación muy alta y significativa entre la seguridad de la información según la norma ISO 27001 y la protección de activos en la empresa INNOTEC - Tarapoto. El análisis del gráfico de dispersión mostró una clara tendencia positiva, indicando que un mayor nivel de seguridad de la información se asocia con una mejor protección de los activos. Asimismo, la correlación no paramétrica de Spearman arrojó un coeficiente de ρ = 0.841, con un coeficiente de determinación del 71%, lo que evidencia que la seguridad de la información explica en gran medida la variabilidad en la protección de los activos. Con un valor p de 0.000, mostrando que la relación existente es significativa.

2º. La seguridad de la información en la empresa INNOTEC - Tarapoto se encuentra en un nivel predominantemente regular, con un 52% en esta categoría. El 36% se ubica en un nivel bueno, mientras que el 12% es deficiente. En cuanto a las dimensiones evaluadas, la confidencialidad muestra el mejor desempeño, con un 76% en nivel bueno. Sin embargo, tanto la integridad como la disponibilidad presentan un nivel mayoritariamente regular, con un 72% en ambos casos.

3º. La protección de los activos en la empresa INNOTEC - Tarapoto se encuentra mayormente en un nivel regular, con un 64% en esta categoría. El 28% se ubica en un nivel bueno, mientras que el 8% es deficiente. La dimensión mejor valorada es la de servicios, con un 88% en nivel bueno, seguida de activos físicos con un 68%. Sin embargo, la información presenta una mayor proporción en nivel regular (72%) y un 20% en nivel deficiente. La protección del software también muestra oportunidades de optimización, con un 52% en nivel regular y solo un 40% en nivel bueno. La dimensión más crítica es la del personal, con un 68% en nivel deficiente y sin registros en la categoría de bueno.

4º. Los resultados demostraron una relación positiva y significativa entre las dimensiones de la seguridad de la información, según la norma ISO 27001, y la protección de activos en la empresa INNOTEC - Tarapoto. Se encontró que la confidencialidad presentó la correlación más alta (ρ = 0.788) con un coeficiente de determinación del 62%, seguida de la integridad (ρ = 0.702) con un 49% y la disponibilidad (ρ = 0.525) con un 28%. Estos resultados evidencian que el fortalecimiento de la seguridad de la información, especialmente en las dimensiones de confidencialidad e integridad, influye directamente en la mejora de la protección de los activos de la empresa.

RECOMENDACIONES

1. A la empresa INNOTEC, se recomienda reforzar la implementación de la norma ISO 27001 en la empresa INNOTEC - Tarapoto, priorizando las prácticas y controles que contribuyan a la protección de activos. Además, se sugiere realizar auditorías periódicas para evaluar la efectividad de las medidas de seguridad implementadas y su impacto en la protección de los activos.
2. La empresa INNOTEC debe fortalecer las dimensiones de integridad y disponibilidad de la información. Para ello, se recomienda implementar controles más rigurosos en la gestión y verificación de datos, garantizar la trazabilidad de la información y optimizar los mecanismos de respaldo y recuperación ante incidentes. Asimismo, es fundamental fomentar una cultura organizacional de seguridad a través de capacitaciones constantes y la implementación de normativas internas.
3. A la empresa INNOTEC, se recomienda priorizar el fortalecimiento de la seguridad en la dimensión de personal, a través de capacitaciones especializadas y la implementación de controles más estrictos. Asimismo, es crucial mejorar la protección del software mediante actualizaciones periódicas, monitoreo constante y el uso de herramientas de seguridad avanzadas.
4. A la empresa INNOTEC, se recomienda focalizar los esfuerzos en mejorar la seguridad de la información en las dimensiones de confidencialidad e integridad, ya que tienen un impacto directo en la protección de activos. Para ello, se pueden implementar mecanismos de encriptación de datos, políticas de acceso restringido y una supervisión constante de los protocolos de seguridad dentro de la organización.

REFERENCIAS BIBLIOGRÁFICAS

Alvarado, J., Pacheco, J., & Martillo, I. (2018). El análisis y gestión de riesgos en gobiernos de ti desde el enfoque de la metodología MAGERIT. *Contribuciones a Las Ciencias Sociales*. https://www.eumed.net/rev/cccss/2018/11/gestion-riesgos-magerit.html

Álvarez Magaña, K. N., Martínez Prats, G., & García Álvarez, A. D. (2021). La importancia del control interno en el área de ingresos de una empresa comercial. *Publicaciones e Investigación*, *15*(1), 1–11. https://doi.org/10.22490/25394088.4692

Andrés, A., & Gómez, L. (2009). Guía de aplicación de la Norma UNE-ISO / IEC 27001 sobre seguridad en sistemas de información para pymes. *AENOR (Asociación Española de Normalización y Certificación)*, 1–135. https://varios.cen7dias.es/documentos/documentos/90/iso.pdf

Apahuasco Saccaco, E. J. (2020). Evaluación del sistema de seguridad de la información en la organización Disav SAC aplicando lineamientos ISO 27001. *Repositorio Institucional de La Universidad Nacional José María Arguedas*. https://hdl.handle.net/20.500.14168/496

Arévalo Mora, K. T., & Restrepo Gámez, B. J. (2021). Análisis de riesgos al Sistema de información Transaccional (TSP) en su elemento software para la empresa de servicios públicos del municipio de Arauca Emserpa E.I.C.E. E.S.P. bajo el estándar ISO 27001:2013 y la metodología Magerit. *Repositorio Institucional Universidad Cooperativa de Colombia*. https://hdl.handle.net/20.500.12494/32776

Astudillo-García, C. W., & Cabrera-Duffaut, A. E. (2019). Políticas de gestión de seguridad de la información, fundamentadas en la norma ISO/IEC 27001, centro de datos diseñado con el estándar ANSI/TIA 942. *Dominio de Las Ciencias*, *5*(3), 132. https://doi.org/10.23857/dc.v5i3.929

Bernal González, I., Pedraza Melo, N. A., & Castillo Hernandez, L. (2020). El capital humano y su relación con el desempeño organizacional. *Revista Espacios*, *41*(22), 1–15. https://www.revistaespacios.com/a20v41n22/20412214.html

Bustamante García, S., Valles Coral, M. Á., Cuellar Rodríguez, I. E., & Lévano Rodríguez, D. (2021). Políticas basadas en la ISO 27001:2013 y su influencia en

la gestión de seguridad de la información en municipalidades de Perú. *Enfoque UTE*, *12*(2), 69–79. https://doi.org/10.29019/enfoqueute.743

Cabrejos Torres, R. (2020). Influencia de la metodología Magerit V3 en la seguridad de información de la empresa Deco Interiors SAC. *Repositorio Institucional USS*. https://hdl.handle.net/20.500.12802/7573

Camacho Zapata, A. S., Ríos Baldovino, J. P., Mojica Herazo, J., & Rojas Millán, R. (2021). Importancia de la gestión de inventario en empresa de Manufacura. *Boletín de Innovación, Logística y Operaciones*, *2*(2), 37–42. https://doi.org/10.17981/bilo.02.02.2020.05

Carrasco Díaz, S. (2019). Metodología de la investigación científica: Pautas metodológicas para diseñar y elaborar el proyecto de investigación. *San Cristobal*. https://www.sancristoballibros.com/libro/metodologia-de-la-investigacion-cientifica_45761

Carvajal Portilla, D. L., Cardona Londoño, A., & Valencia Duque, F. J. (2019). Una propuesta de gestión de la seguridad de la información aplicado a una entidad pública colombiana. *Entre Ciencia e Ingeniería*, *13*(25), 68–76. https://doi.org/10.31908/19098367.4016

Castillo Durán, E. F., Fernando Illescas Peña, F., & Quevedo Sacoto, A. S. (2023). Fase de análisis para la implementación de un Sistema de Gestión de Seguridad de la Información (S.G.S.I.) basado en ISO 27001. Orientado a los medios de comunicación. *ConcienciaDigital*, *6*(4.1), 31–50. https://doi.org/10.33262/concienciadigital.v6i4.1.2725

Cívicos Juárez, A., & Hernández Hernández, M. (2007). Algunas reflexiones y aportaciones en torno a los enfoques teóricos y prácticos de la investigación en Trabajo Social. *Acciones e Investigaciones Sociales*, *23*(23), 25. https://doi.org/10.26754/ojs_ais/ais.200723306

Cruz Lucas, G. I., Figueroa Rodríguez, E. L., Cruz Lucas, N. I., & Abad Parrales, W. M. (2023). Vulnerabilidad de datos en los sistemas información basado en la norma ISO 27001. *Journal TechInnovation*, *2*(2 SE-Artículos de Investigación), 54–59. https://doi.org/10.47230/Journal.TechInnovation.v2.n2.2023.54-59

Cuesta, M., & Herrero, F. (2010). Introducción al muestreo. *Universidad de Oviedo, Depto. de Psicología.* http://www.psico.uniovi.es/Dpto_Psicologia/metodos/tutor.7/.

Damian Vasquez, J. (2023). ISO/IEC 27000. *HIGH TECH-ENGINEERING JOURNAL*, *3*(2), 80–84. https://doi.org/10.46363/high-tech.v3i2.3

Diamantopoulou, V., Tsohou, A., & Karyda, M. (2020). From ISO/IEC 27002:2013 Information Security Controls to Personal Data Protection Controls: Guidelines for GDPR Compliance. In *Computer Security* (pp. 238–257). https://doi.org/10.1007/978-3-030-42048-2_16

Díaz Díaz, A. A., & Toscano Moctezuma, J. A. (2022). El capital humano y la productividad de las empresas. *Revista Torreón Universitario*, *11*(30), 123–130. https://doi.org/10.5377/rtu.v11i30.13427

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. http://scielo.sld.cu/scielo.php?script=sci_abstract&pid=S2218-36202023000200274&lng=es&nrm=iso&tlng=en

Ferruzola Gómez, E., Duchimaza S., J., Ramos Holguín, J., & Alejandro Lindao, M. (2019). Plan de contingencia para los equipos y sistemas informáticos utilizando la metodología MAGERIT. *Revista Científica y Tecnológica UPSE*, *6*(1), 34–41. https://doi.org/10.26423/rctu.v6i1.429

Gallego-Giraldo, C., & Naranjo-Herrera, C. G. (2020). El capital humano de la empresa: una propuesta de medición. *Entramado*, *16*(2), 70–89. https://doi.org/10.18041/1900-3803/entramado.2.6544

García, M. K., Venegas, E., Aguilera, E., Panizo, J. M., Kelly, C., & Serrano, D. (2022). Digital onboarding in finance: a novel model and related cybersecurity risks. *Open Research Europe*, *1*, 149. https://doi.org/10.12688/openreseurope.14289.2

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

George, D., & Mallery, P. (2003). SPSS for Windows step by step: A simple guide and reference. 11.0 update (4thed.). *Casa Del Libro*. https://books.google.com.pe/books/about/SPSS_for_Windows_Step_by_Step.html?id=AghHAAAAMAAJ&redir_esc=y

Guerra, E., Neira, H., Díaz, J. L., & Patiño, J. (2021). Desarrollo de un sistema de gestión

para la seguridad de la información basado en metodología de identificación y análisis de riesgo en bibliotecas universitarias. *Información Tecnológica*, *32*(5), 145–156. https://doi.org/10.4067/S0718-07642021000500145

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, P. (2014). Metodología de la investigación. In *McGraw-Hill - Edición 6* (Vol. 6). McGraw-Hill / Interamericana Editores, S.A. https://www.esup.edu.pe/wp-content/uploads/2020/12/2. Hernandez, Fernandez y Baptista-Metodología Investigacion Cientifica 6ta ed.pdf

Herrera Córdoba, J. (2020). Propuesta de implementación de un Sistema Gestor de Seguridad de la Información, basados en INTE/ISO/IEC 27001:2014 en el departamento de TI para Almacenes El Rey, en el año 2021. *Revista de La Facultad de Ingenierías y Tecnologías de La Información y Comunicación*, 27–32. https://revistas.ulatina.ac.cr/index.php/tecnologiavital/article/view/464

Jácome Segovia, D., Castillo Fiallos, J., Mantilla Cabrera, C., & Vaca Barahona, B. E. (2021). Aplicación de MAGERIT para reducir riesgos en servicios Web en un contexto académico en Ecuador. *AlfaPublicaciones*, *3*(2.2), 66–82. https://doi.org/10.33262/ap.v3i2.2.60

Jevelin, J., & Faza, A. (2023). Evaluation the Information Security Management System: A Path Towards ISO 27001 Certification. *Journal of Information Systems and Informatics*, *5*(4), 1240–1256. https://doi.org/10.51519/journalisi.v5i4.572

Lanzas Duque, Á. M. (2018). Modelo de generación de valor mediante el capital intelectual en empresas de base tecnológica de software. *Contaduría y Administración*, *65*(2), 166. https://doi.org/10.22201/fca.24488410e.2018.1897

Latinovic, T., & Sikman, L. (2020). *ISO 27001 – Information systems security, development, trends, technical and economic challenges, Journal Annals of Hunedoara*. *July*. https://www.researchgate.net/publication/342955172_ISO_27001_-_INFORMATION_SYSTEMS_SECURITY_DEVELOPMENT_TRENDS_TECHNICAL_AND_ECONOMIC_CHALLENGES_Journal_Annals_of_Hunedoara

Linares Fernández, E., Balverdi Cruz, L. H., & Cuellar, I. (2023). Políticas de seguridad de la información y metodología Magerit en la empresa Induamerica Chiclayo S.A.C. *Revista Científica Pakamuros*, *10*(2). https://doi.org/10.37787/ggpbfw19

Lopes, I. M., Guarda, T., & Oliveira, P. (2019). Implementation of ISO 27001 Standards

as GDPR Compliance Facilitator. *Journal of Information Systems Engineering & Management*, *4*(2). https://doi.org/10.29333/jisem/5888

Macías Rivas, A. I. (2022). Control interno en empresas comerciales nacientes en Ecuador. *Polo Del Conocimiento*, *7*(9), 336–360. https://doi.org/10.23857/pc.v7i9

Mamani Ventura, W. (2020). Análisis de riesgo de la información según la norma iso 27001:2013: previo a una implementación. *RENATI*. http://repositorio.upeu.edu.pe/handle/20.500.12840/3734

Mora Secaira, J., Díaz Ocampo, R., Zhuma Mera, E., & Díaz Kovalenko, I. E. (2020). El sistema de gestión de seguridad de la información bajo la norma NTE ISO/IEC 27001 en instituciones de Educación Superior (Ecuador). *Revista Científico - Educaciones de La Provincia de Granma*, *16*, 546–559. https://dialnet.unirioja.es/servlet/articulo?codigo=7414351

Morales, F., Toapanta, S., & Toasa, R. (2020). Implementación de un sistema de seguridad perimetral como estrategia de seguridad de la información. *Revista Ibérica de Sistemas e Tecnologias de Informação Lousada*, *E27*, 553–565. https://www.proquest.com/openview/35d3af032ceee8d79daf8a813e2c7967/1?pq-origsite=gscholar&cbl=1006393

Najar Pacheco, J. C., & Suárez Suárez, N. E. (2015). La seguridad de la información: un activo valioso de la organización. *Revista Vinculos*, *12*(1), 89–97. https://revistas.udistrital.edu.co/index.php/vinculos/article/view/10518

Ñaupas, H., Valdivia, M., Palacios, J., & Romero, H. (2014). Summary for Policymakers. In 5ta Edición (Ed.), *Climate Change 2013 – The Physical Science Basis* (Vol. 53, Issue 9, pp. 1–30). Cambridge University Press. https://doi.org/10.1017/CBO9781107415324.004

Otzen, T., & Manterola, C. (2017). *International Journal of Morphology*. https://doi.org/http://dx.doi.org/10.4067/S0717-95022017000100037.

Podrecca, M., Culot, G., Nassimbeni, G., & Sartor, M. (2022). Information security and value creation: The performance implications of ISO/IEC 27001. *Computers in Industry*, *142*, 103744. https://doi.org/10.1016/j.compind.2022.103744

Ramírez Camargo, E. A., & Rinconc Pinzon, M. A. (2022). La importancia de la seguridad de la información en el sector público en Colombia. *RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação*, *46*, 87–99. https://doi.org/10.17013/risti.46.87-99

Risco Villarreal, E. G. (2020). Sistema de gestión para la seguridad de la informacion basado en la Norma ISO/IEC 27001:2013 en la empresa constructora perez & perez SAC, moyobamba, san martin, 2021. *Universidad Andina Del Cusco*, 1–118. https://dialnet.unirioja.es/servlet/articulo?codigo=7861273

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 Application of ISO 27001 and its influence on the information security of a Peruvian private company. *Propósitos y Representaciones*, *8*, 786. http://www.scielo.org.pe/scielo.php?script=sci_arttext&pid=S2307-79992020000400011

Rojas Pupo, Y., Tamayo Garcia, P. F., & Moreno Pino, M. (2020). Metodología para la Gestión de la Seguridad de la Información basada en los aspectos más relevantes de la norma Cubana NC ISO IEC 27001:2016. *RILCO - Revista de Desarrollo Sustentable, Negocios, Emprendimiento y Educación*, 12. https://www.eumed.net/rev/rilcoDS/12/gestion-seguridad-informacion.pdf

Sabillón, R., & Cano, J. (2019). Auditorías en Ciberseguridad: Un modelo de aplicación general para empresas y naciones. *RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação*, *32*, 33–48. https://doi.org/10.17013/risti.32.33-48

Stallman, R. (2020). La definición de Software libre The definition of Free Software. *MIT (Massachusetts Institute of Technology)*, 151–154. https://revistascientificas.us.es/index.php/Communiars/article/download/12773/11048/43146

Tonysé De la Rosa, M. (2021). Automatización de un sistema de gestión de seguridad de la información basado en la Norma ISO/IEC 27001. In *Revista Universidad y Sociedad* (Vol. 13, pp. 495–506). https://rus.ucf.edu.cu/index.php/rus/article/view/2260

Vega Briceño, E. (2021). *Seguridad de la información*. Editorial Científica 3Ciencias. https://doi.org/10.17993/tics.2021.4

Yungán Cazar, J. C., & Narváez Contero, C. V. (2022). Aplicación de la Norma ISO 27001 para la seguridad de los Sistemas de Información. *Dominio De Las Ciencias*, *8*(3), 1025–1041. https://dominiodelasciencias.com/ojs/index.php/es/article/view/2854

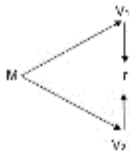
Zevallos Morales, M. N. (2019). Modelo de gestión de riesgos de seguridad de la información: Una revisión del estado del arte. *Revista Peruana de Computación y Sistemas*, *2*(1), 43–60. https://revistasinvestigacion.unmsm.edu.pe/index.php/rpcsis/article/view/17103

ANEXOS

Anexo 01: Matriz de consistencia

<table>
<tr><th colspan="5">“Seguridad de información según ISO 27001 y la protección de activos en INNOTEC: eficiente gestión para salvaguardar datos y recursos”</th></tr>
<tr><th>Formulación del problema general</th><th>Objetivos</th><th>Hipótesis</th><th>Tipo, nivel y diseño de investigación</th><th>Población y muestra</th></tr>
<tr>
<td>¿Cuál es la relación entre la gestión de la seguridad de la información según la ISO 27001 y la protección de activos en la empresa INNOTEC - Tarapoto, 2023?</td>
<td><u>General</u>
Determinar la relación entre la seguridad de la información según la ISO 27001 y la protección de activos en la empresa INNOTEC - Tarapoto, 2023.

<u>Específicos</u>
1. Analizar el nivel de la seguridad de la información según la ISO 27001 en la empresa INNOTEC - Tarapoto, 2023.
2. Analizar el nivel de protección de los activos en la empresa INNOTEC - Tarapoto, 2023.
3. Determinar la relación entre las dimensiones de la seguridad de la información basados en la norma ISO 27001 y la protección de activos en la empresa INNOTEC - Tarapoto, 2023.</td>
<td><u>Hi</u>
Existe una relación significativa entre la seguridad de la información según la ISO 27001 y la protección de activos en la empresa INNOTEC - Tarapoto, 2023.

<u>Ho</u>
No existe una relación significativa entre la seguridad de la información según la ISO 27001 y la protección de activos en la empresa INNOTEC - Tarapoto, 2023.</td>
<td>El tipo de investigación
Básica
Nivel de la investigación
Descriptivo - Correlacional
Diseño
No experimental
Esquema:
 
Dónde:
M = Muestra de estudio.
V_1 = Seguridad de información
V_2 = Protección de activos
r = Relación entre las variables.</td>
<td>Población
La población estará conformada por 25 miembros del personal de INNOTEC - Tarapoto.
Muestra:
La muestra estará conformada por la totalidad de la población con un total de 25 miembros del personal de INNOTEC-Tarapoto.
Muestreo:
Para la elección de la muestra se aplicará un muestreo no probabilístico seleccionado por el investigador de acuerdo con las necesidades y propósito de la investigación.
Técnicas e instrumentos
Técnica: Encuesta.
Instrumento: Cuestionario.</td>
</tr>
</table>

Anexo 02: Operacionalización de las variables

Variables	Definición conceptual	Definición operacional	Dimensión	Indicadores	Escala de medición
Seguridad de información según ISO 27001	Según la norma ISO 27001, se enfoca en garantizar la confidencialidad, integridad y disponibilidad de la información y datos cruciales para la organización.	La seguridad de la información se medirá en el contexto de la norma ISO 27001 que asegura la confidencialidad, disponibilidad e integridad de la información y los sistemas que la procesan, integrando la seguridad en el marco de gestión organizacional.	Confidencialidad	- Efectividad de la formación en confidencialidad. - Conocimiento sobre políticas de confidencialidad. - Seguridad en el manejo de información personal.	Escala Ordinal
			Integridad	- Adecuación de los procesos de control de cambios. - Efectividad de los procesos de verificación de datos. - Satisfacción con la precisión de los datos.	
			Disponibilidad	- Efectividad de las estrategias de recuperación. - Satisfacción con el tiempo de respuesta a incidentes. - Percepción de la estabilidad de los sistemas	
Protección de activos	Asegurar propiedades, tecnología, datos, reputación y recursos humanos mediante medidas de seguridad y políticas adecuadas para garantizar la continuidad y éxito a largo plazo de la organización (Macías, 2022).	Se medirá la protección de los activos de la empresa en estudio de acuerdo a los tipos de activos consideradas por Magerit V.3 y que se encuentran presentes en la empresa INNOTEC.	Información	- Copias de respaldo - Información escrita - Código fuente de los sistemas de información	Escala Ordinal
			Software	- Sistema de gestión de base de datos - Antivirus - Ofimática - Sistema operativo	
			Físicos	- Equipo de procesamiento - Equipo de comunicaciones - Medio de almacenamiento - Equipos de escritorio - Impresoras y escáner	
			Servicios	- Procesamiento y comunicaciones - Correo electrónico	
			Personal	- Administrador de sistemas - Personal interno	

Anexo 03: Instrumento de recolección de datos

UNIVERSIDAD NACIONAL DE SAN MARTÍN - TARAPOTO

FACULTAD DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

Título: "Seguridad de información y la protección de activos según ISO 27001 en INNOTEC: eficiente gestión para salvaguardar datos y recursos"

CUESTIONARIO 1

- Este cuestionario es anónimo y tiene como objetivo recolectar información sobre el nivel de la seguridad de la información según las directrices establecidas en ISO 27001 en INNOTEC Tarapoto; para ello se responderá a los ítems considerando la siguiente escala valorativa.

Estimado/a participante:

Esta es una investigación llevada a cabo en la ciudad de Tarapoto; los datos recopilados son anónimos, serán tratados de forma confidencial y tienen finalidad netamente académica. Por tanto, en forma voluntaria; SÍ ( ) NO ( ) doy mi consentimiento para continuar con la investigación que tiene por objetivo "Determinar la relación entre la seguridad de la información según la ISO 27001 y la protección de activos en INNOTEC Tarapoto".

Cualquier duda que les surja al contestar esta encuesta puede enviarla al correo: hpinchin@alumno.unsm.edu.pe

Agradecemos por anticipado su valiosa participación y ayuda, motivo por el que los resultados del estudio de investigación científica.

INSTRUCCIONES:

El cuestionario consta de 9 ítems. Cada ítem incluye cinco alternativas de respuestas. Lea con mucho cuidado cada ítem y las opciones de las repuestas. Para cada ítem marque solo una respuesta con una (x) en el recuadro que considere que se aproxime más según su discernimiento.

Totalmente en desacuerdo	En desacuerdo	Ni en acuerdo, ni en desacuerdo	De acuerdo	Totalmente de acuerdo
1	2	3	4	5

N°	ÍTEMS	1	2	3	4	5
DIMENSIÓN 01: CONFIDENCIALIDAD						
01	La formación que ha recibido sobre políticas de confidencialidad es clara y fácil de entender.					
02	La formación en confidencialidad me ha proporcionado los conocimientos necesarios para proteger la información adecuadamente.					
03	Existe un conocimiento sólido y claro sobre las políticas de confidencialidad de la empresa.					
04	La empresa proporciona suficientes recursos para asegurar que todos los empleados conozcan y comprendan las políticas de confidencialidad.					
05	Considera que la empresa maneja de manera segura la información de sus clientes y personal.					
06	Considera que la información personal de la empre está protegida adecuadamente por la empresa.					
DIMENSIÓN: INTEGRIDAD						
07	Los procesos de control de cambios en la empresa son adecuados para mantener la integridad de los datos.					
08	Los controles establecidos para gestionar cambios en los datos son efectivos y confiables.					
09	Confío en que los procedimientos de verificación de datos aseguran que los datos sean precisos.					
10	Los procedimientos de verificación de datos son adecuados para garantizar la integridad de la información.					
11	Estoy satisfecho/a con la precisión de los datos que recibo y manejo en mi trabajo.					
12	Los datos que se me proporcionan son precisos y están actualizados.					
DIMENSIÓN: DISPONIBILIDAD						
13	Las estrategias de recuperación de datos en caso de incidentes son efectivas.					
14	Los planes de recuperación ante incidentes aseguran una rápida restauración de los datos.					
15	Estoy satisfecho/a con el tiempo que toma la empresa para responder a los incidentes que afectan la disponibilidad.					
16	La empresa responde de manera oportuna a los incidentes que afectan la disponibilidad de la información.					
17	La infraestructura tecnológica de la empresa es estable y rara vez experimenta fallos.					
18	La estabilidad del sistema asegura un acceso continuo a la información sin interrupciones.					

¡Muchas gracias por su colaboración!

UNIVERSIDAD NACIONAL DE SAN MARTÍN - TARAPOTO

FACULTAD DE INGENIERÍA DE SISTEMAS E INFORMÁTICA
ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

Título: "Seguridad de información y la protección de activos según ISO 27001 en INNOTEC: eficiente gestión para salvaguardar datos y recursos."

CUESTIONARIO 2

- Este cuestionario es anónimo y tiene como objetivo recolectar información sobre el nivel de protección de activos en INNOTEC; para ello se responderá a los ítems considerando la siguiente escala valorativa.

Estimado/a participante:

Esta es una investigación llevada a cabo en la ciudad de Tarapoto; los datos recopilados son anónimos, serán tratados de forma confidencial y tienen finalidad netamente académica. Por tanto, en forma voluntaria; SÍ ( ) NO ( ) doy mi consentimiento para continuar con la investigación que tiene por objetivo "Determinar la relación entre la gestión de la seguridad de la información según la ISO 27001 y la protección de activos en INNOTEC Tarapoto".

Cualquier duda que les surja al contestar esta encuesta puede enviarla al correo: hpinchin@alumno.unsm.edu.pe

Agradecemos por anticipado su valiosa participación y ayuda, motivo por el que los resultados del estudio de investigación científica.

INSTRUCCIONES:

El cuestionario consta de 16 ítems. Cada ítem incluye cinco alternativas de respuestas. Lea con mucho cuidado cada ítem y las opciones de las repuestas. Para cada ítem marque sólo una respuesta con una (x) en el recuadro que considere que se aproxime más según su discernimiento.

Muy baja	Baja	Media	Alta	Muy alta
1	2	3	4	5

N°	ÍTEMS	1	2	3	4	5

DIMENSIÓN 01: INFORMACIÓN						
1	¿Con qué frecuencia se realizan copias de respaldo de la información crítica en su organización? • Muy baja: No se realizan copias de respaldo • Baja: Ocasionalmente • Media: Mensualmente • Alta: Semanalmente • Muy alta: Diariamente					
2	¿Qué nivel de seguridad se aplica a la información escrita (documentos físicos) en su organización? • Muy baja: No se aplican medidas de seguridad. • Baja: Se almacenan en escritorios accesibles a todos. • Media: Se almacenan en archivos cerrados con acceso limitado. • Alta: Se almacenan en una sala segura con acceso restringido. • Muy alta: Se almacenan en una sala segura con controles de acceso y monitoreo.					
3	¿Qué nivel de protección tiene el código fuente de los sistemas de información en su organización? • Muy baja: No se toman medidas específicas para proteger el código. • Baja: Código fuente disponible para todos los empleados. • Media: Acceso controlado sin repositorios específicos. • Alta: Control de acceso restringido y versiones guardadas en repositorios seguros. • Muy alta: Control de acceso restringido, repositorios seguros y auditorías regulares.					
DIMENSIÓN 02: SOFTWARE						
4	¿Qué nivel de protección tiene el sistema de gestión de bases de datos en su organización? • Muy baja: No se aplican medidas de seguridad específicas. • Baja: Acceso abierto con contraseñas estándar. • Media: Contraseñas básicas y acceso controlado. • Alta: Contraseñas fuertes, cifrado y acceso restringido. • Muy alta: Contraseñas fuertes, cifrado, acceso restringido y auditorías regulares.					
5	¿Qué nivel de protección antivirus se utiliza en su organización? • Muy baja: No se utiliza antivirus) • Baja: Solo en servidores críticos) • Media: Software antivirus en algunos dispositivos) • Alta: Software antivirus actualizado en todos los dispositivos) • Muy alta: Software antivirus actualizado y monitoreado en todos los dispositivos)					
6	¿Qué nivel de seguridad se aplica al software de ofimática (como procesadores de texto, hojas de cálculo) en su organización? • Muy baja: No se aplican medidas de seguridad. • Baja: Protección mínima sin actualizaciones. • Media: Actualizaciones manuales y protección con contraseña. • Alta: Actualizaciones automáticas y protección con contraseña. • Muy alta: Actualizaciones automáticas, protección con contraseña y cifrado.					

7	¿Qué nivel de protección se asegura en el sistema operativo de su organización? • Muy baja: No se aplican medidas de seguridad. • Baja: Solo actualizaciones básicas. • Media: Actualizaciones manuales y configuración básica. • Alta: Actualizaciones automáticas y configuraciones de seguridad ajustadas. • Muy alta: Actualizaciones automáticas, configuraciones de seguridad ajustadas y monitoreo continuo.					
DIMENSIÓN 03: FÍSICOS						
8	¿Qué nivel de protección se aplica al equipo de procesamiento (computadoras, servidores) en su organización? • Muy baja: No se aplican medidas de seguridad. • Baja: Solo medidas básicas de seguridad física. • Media: Seguridad física básica sin monitoreo. • Alta: Seguridad física con controles de acceso y monitoreo. • Muy alta: Seguridad física avanzada con controles de acceso, monitoreo y auditorías regulares.					
9	¿Qué nivel de seguridad se aplica al equipo de comunicaciones (routers, switches)? • Muy baja: sin seguridad. • Baja: seguridad mínima. • Media: seguridad moderada. • Alta: seguridad alta. • Muy alta: máxima seguridad.					
10	¿Qué nivel de protección tienen los medios de almacenamiento (discos duros, unidades flash)? • Muy baja: sin protección. • Baja: protección mínima. • Media: protección moderada. • Alta: protección alta. • Muy alta: máxima protección.					
11	¿Qué nivel de seguridad se aplica a los equipos de escritorio? • Muy baja: sin seguridad. • Baja: seguridad mínima. • Media: seguridad moderada. • Alta: seguridad alta. • Muy alta: máxima seguridad.					
12	¿Qué nivel de seguridad se aplica al acceso a impresoras y escáneres? • Muy baja: sin seguridad. • Baja: seguridad mínima. • Media: seguridad moderada. • Alta: seguridad alta. • 5Muy alta: máxima seguridad.					
DIMENSIÓN 04: SERVICIOS						
13	¿Qué nivel de seguridad se aplica al procesamiento y comunicaciones de datos? • Muy baja: sin seguridad. • Baja: seguridad mínima.					

	• Media: seguridad moderada. • Alta: seguridad alta. • Muy alta: máxima seguridad.					
14	¿Qué nivel de seguridad se aplica al correo electrónico? • Muy baja: sin protección. • Baja: protección mínima. • Media: protección moderada. • Alta: protección alta. • Muy alta: máxima protección.					
DIMENSIÓN 05: PERSONAL						
15	¿Qué nivel de control de acceso tiene el administrador de sistemas? • Muy bajo: sin control. • Bajo: control mínimo. • Medio: control moderado. Alto: control alto. • Muy alto: máximo control.					
16	¿Qué nivel de seguridad se aplica al acceso del personal interno a los sistemas y datos? • Muy baja: sin seguridad. • Baja: seguridad mínima. • Media: seguridad moderada. • Alta: seguridad alta. • Muy alta: máxima seguridad.					

¡Muchas gracias por su colaboración!

Anexo 04: Validación de los instrumentos de recolección de datos

INFORME DE OPINIÓN SOBRE INSTRUMENTO DE INVESTIGACIÓN CIENTÍFICA

I. DATOS GENERALES

Apellidos y nombres del experto: García Castro Juan Carlos
Institución donde labora : UNSM
Especialidad : Ing. de Sistemas
Instrumento de evaluación : **Cuestionario 1:** Nivel de la seguridad de la información según ISO 27001 en INNOTEC.
Autor del Instrumento : Edward Hans Pinchi Núñez

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: Seguridad de información según ISO 27001, 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: Seguridad de información según ISO 27001.					X
ORGANIZACIÓN	Los ítems del instrumento reflejan organicidad lógica entre la definición operacional y conceptual respecto a la variable: Seguridad de información según ISO 27001, 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.				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: Seguridad de información según ISO 27001.					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

Instrumento coherente y aplicable

Tarapoto, Julio del 2024.

IV. PROMEDIO DE VALORACIÓN:

47

INFORME DE OPINIÓN SOBRE INSTRUMENTO DE INVESTIGACIÓN CIENTÍFICA

I. DATOS GENERALES

Apellidos y nombres del experto: Garcia Cantu Juan Carlos
Institución donde labora : UNSM
Especialidad : Ing. en Sistemas
Instrumento de evaluación : **Cuestionario 2:** Nivel de protección de activos en INNOTEC.
Autor del instrumento : Edward Hans Pinchi Núñez

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: Protección de activos, 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: Protección de activos.					X
ORGANIZACIÓN	Los ítems del instrumento reflejan organicidad lógica entre la definición operacional y conceptual respecto a la variable: Protección de activos, 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.				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: Protección de activos					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					40	

(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

Instrumento coherente y aplicable

Tarapoto, Julio del 2024.

IV. PROMEDIO DE VALORACIÓN:

4.8

INFORME DE OPINIÓN SOBRE INSTRUMENTO DE INVESTIGACIÓN CIENTÍFICA

I. DATOS GENERALES

Apellidos y nombres del experto: Valverde Iparraguirre Jorge Damian
Institución donde labora : UNSM
Especialidad : Ingeniero de Computación y Sistemas
Instrumento de evaluación : **Cuestionario 1**: Nivel de la seguridad de la información según ISO 27001 en INNOTEC.
Autor del instrumento : Edward Hans Pinchi Núñez

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: Seguridad de información según ISO 27001, 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: Seguridad de información según ISO 27001.					X
ORGANIZACIÓN	Los ítems del instrumento reflejan organicidad lógica entre la definición operacional y conceptual respecto a la variable: Seguridad de información según ISO 27001, 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.					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: Seguridad de información según ISO 27001.					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

Instrumento coherente y aplicable

IV. PROMEDIO DE VALORACIÓN: 4.7

Tarapoto, Julio del 2024.

Ing. Dr. Jorge Valverde I.

INFORME DE OPINIÓN SOBRE INSTRUMENTO DE INVESTIGACIÓN CIENTÍFICA

I. DATOS GENERALES

Apellidos y nombres del experto: Valverde Iparraguirre Jorge Damian
Institución donde labora : UNSM
Especialidad : Ingeniero de Computación y Sistemas.
Instrumento de evaluación : **Cuestionario 2:** Nivel de protección de activos en INNOTEC.
Autor del instrumento : Edward Hans Pinchi Núñez

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: Protección de activos, 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: Protección de activos.					X
ORGANIZACIÓN	Los ítems del instrumento reflejan organicidad lógica entre la definición operacional y conceptual respecto a la variable: Protección de activos, 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.					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: Protección de activos					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

Instrumento coherente y aplicable

IV. PROMEDIO DE VALORACIÓN: 4.8

Tarapoto, Julio del 2024.

Ing. Dr. Jorge Valverde I.

INFORME DE OPINIÓN SOBRE INSTRUMENTO DE INVESTIGACIÓN CIENTÍFICA

I. DATOS GENERALES

Apellidos y nombres del experto: Cárdenas García Angel
Institución donde labora : UNSM-T
Especialidad : Ing. de Sistemas - Tecnología de la investigación
Instrumento de evaluación : **Cuestionario 1**: Nivel de la seguridad de la información según ISO 27001 en INNOTEC.
Autor del instrumento : Edward Hans Pinchi Núñez

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: Seguridad de información según ISO 27001, 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: Seguridad de información según ISO 27001.					X
ORGANIZACIÓN	Los ítems del instrumento reflejan organicidad lógica entre la definición operacional y conceptual respecto a la variable: Seguridad de información según ISO 27001, 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.				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: Seguridad de información según ISO 27001.				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

Instrumento coherente y aplicable

IV. PROMEDIO DE VALORACIÓN: 4.6

Tarapoto, Julio del 2024.

INFORME DE OPINIÓN SOBRE INSTRUMENTO DE INVESTIGACIÓN CIENTÍFICA

I. DATOS GENERALES

Apellidos y nombres del experto: Córdova Horna Jhael
Institución donde labora : UNSM-T
Especialidad : Ing. de Sistemas - Metodología de la Investigación
Instrumento de evaluación : **Cuestionario 2:** Nivel de protección de activos en INNOTEC.
Autor del instrumento : Edward Hans Pinchi Núñez

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: Protección de activos, 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: Protección de activos.					X
ORGANIZACIÓN	Los ítems del instrumento reflejan organicidad lógica entre la definición operacional y conceptual respecto a la variable: Protección de activos, de maners 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.					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: Protección de activos					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						49

(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

Instrumento coherente y aplicable

IV. PROMEDIO DE VALORACIÓN: 4.9

Tarapoto, Julio del 2024.

Anexo 05: Confiabilidad del instrumento

Cuestionario 1: Nivel de la seguridad de la información según las directrices establecidas en ISO 27001 en INNOTEC Tarapoto.

La confiabilidad del **Cuestionario 1**: Se calculó a través del Índice de confiabilidad - Alfa de Cronbach, y del análisis de los 18 ítems del cuestionario se obtuvo como resultado un índice de 0,865 que se ubica en el nivel “Muy bueno” de fiabilidad, por lo tanto, el instrumento de medición es 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 de procesamiento de casos

		N	%
Casos	Válido	25	100,0
	Excluido[a]	0	,0
	Total	25	100,0

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

Número de preguntas (18)

Tabla 1
Confiabilidad del número de preguntas

Estadísticas de fiabilidad	
Alfa de Cronbach	N de elementos
,865	18

Fuente: SPSS ver 27

Confiabilidad del Cuestionario 1 por el número de ítems

Es importante ofrecer una descripción detallada de la relación de cada ítem del cuestionario, ya que esto facilitará una comprensión más profunda de los resultados y reforzará la validez del estudio.

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
Pregunta 01: La formación que ha recibido sobre políticas de confidencialidad es clara y fácil de entender.	59,0000	79,833	0,791	0,844
Pregunta 02: La formación en confidencialidad me ha proporcionado los conocimientos necesarios para proteger la información adecuadamente.	59,3600	82,990	0,686	0,849
Pregunta 03: Existe un conocimiento sólido y claro sobre las políticas de confidencialidad de la empresa.	58,8000	85,500	0,564	0,855
Pregunta 04: La empresa proporciona suficientes recursos para asegurar que todos los empleados conozcan y comprendan las políticas de confidencialidad.	59,2800	82,293	0,618	0,851
Pregunta 05: Considera que la empresa maneja de manera segura la información de sus clientes y personal.	59,3200	80,143	0,729	0,846
Pregunta 06: Considera que la información personal de la empre está protegida adecuadamente por la empresa.	59,3600	83,240	0,579	0,853
Pregunta 07: Los procesos de control de cambios en la empresa son adecuados para mantener la integridad de los datos.	60,2400	89,607	0,326	0,863
Pregunta 08: Los controles establecidos para gestionar cambios en los datos son efectivos y confiables.	60,0400	90,290	0,287	0,865
Pregunta 09: Confío en que los procedimientos de verificación	60,2000	91,083	0,286	0,864

de datos aseguran que los datos sean precisos.				
Pregunta 10: Los procedimientos de verificación de datos son adecuados para garantizar la integridad de la información.	59,1200	85,110	0,556	0,855
Pregunta 11: Estoy satisfecho/a con la precisión de los datos que recibo y manejo en mi trabajo.	59,4000	87,917	0,406	0,860
Pregunta 12: Los datos que se me proporcionan son precisos y están actualizados.	59,3200	84,727	0,622	0,852
Pregunta 13: Las estrategias de recuperación de datos en caso de incidentes son efectivas.	60,4000	90,750	0,299	0,864
Pregunta 14: Los planes de recuperación ante incidentes aseguran una rápida restauración de los datos.	59,8800	82,693	0,530	0,856
Pregunta 15: Estoy satisfecho/a con el tiempo que toma la empresa para responder a los incidentes que afectan la disponibilidad.	59,8000	86,333	0,347	0,865
Pregunta 16: La empresa responde de manera oportuna a los incidentes que afectan la disponibilidad de la información.	60,4400	92,173	0,094	0,876
Pregunta 17: La infraestructura tecnológica de la empresa es estable y rara vez experimenta fallos.	59,2800	92,960	0,124	0,870
Pregunta 18: La estabilidad del sistema asegura un acceso continuo a la información sin interrupciones.	59,1200	79,110	0,699	0,847

Cuestionario 2: Nivel de protección de activos en INNOTEC.

La confiabilidad del **Cuestionario 2**: Se calculó a través del Índice de confiabilidad - Alfa de Cronbach, y del análisis de los 16 ítems del cuestionario se obtuvo como resultado un índice de 0,910 que se ubica en el nivel “Excelente” de fiabilidad, por lo tanto, el instrumento de medición es 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 de procesamiento de casos

		N	%
Casos	Válido	25	100,0
	Excluido[a]	0	,0
	Total	25	100,0

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

Número de preguntas (16)

Tabla 1
Confiabilidad del número de preguntas

Estadísticas de fiabilidad	
Alfa de Cronbach	N de elementos
,910	16

Fuente: SPSS ver 27

Confiabilidad del Cuestionario 2 por el número de ítems

Es importante ofrecer una descripción detallada de la relación de cada ítem del cuestionario, ya que esto facilitará una comprensión más profunda de los resultados y reforzará la validez del estudio.

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
Pregunta 01: ¿Con qué frecuencia se realizan copias de respaldo de la información crítica en su organización?	56,6800	82,143	0,359	0,911

Pregunta 02: ¿Qué nivel de seguridad se aplica a la información escrita (documentos físicos) en su organización?	56,3200	80,560	0,575	0,906
Pregunta 03: ¿Qué nivel de protección tiene el código fuente de los sistemas de información en su organización?	56,1600	78,307	0,614	0,904
Pregunta 04: ¿Qué nivel de protección tiene el sistema de gestión de bases de datos en su organización?	55,3600	79,740	0,448	0,909
Pregunta 05: ¿Qué nivel de protección antivirus se utiliza en su organización?	55,1200	74,527	0,738	0,899
Pregunta 06: ¿Qué nivel de seguridad se aplica al software de ofimática (como procesadores de texto, hojas de cálculo) en su organización?	56,7200	74,877	0,497	0,911
Pregunta 07: ¿Qué nivel de protección se asegura en el sistema operativo de su organización?	55,6400	76,657	0,610	0,904
Pregunta 08: ¿Qué nivel de protección se aplica al equipo de procesamiento (computadoras, servidores) en su organización?	55,6800	76,477	0,652	0,902
Pregunta 09: ¿Qué nivel de seguridad se aplica al equipo de comunicaciones (routers, switches)?	55,7200	79,293	0,493	0,907
Pregunta 10: ¿Qué nivel de protección tienen los medios de almacenamiento (discos duros, unidades flash)?	55,1600	75,140	0,710	0,900
Pregunta 11: ¿Qué nivel de seguridad se aplica a los equipos de escritorio?	54,9600	74,207	0,807	0,897
Pregunta 12: ¿Qué nivel de seguridad se aplica al acceso a impresoras y escáneres?	56,3600	81,323	0,272	0,916
Pregunta 13: ¿Qué nivel de seguridad se aplica al procesamiento y comunicaciones de datos?	54,9200	75,993	0,772	0,899
Pregunta 14: ¿Qué nivel de seguridad se aplica al correo electrónico?	55,0000	77,667	0,660	0,902
Pregunta 15: ¿Qué nivel de control de acceso tiene el administrador de sistemas?	54,9200	75,660	0,797	0,898

Pregunta 16: ¿Qué nivel de seguridad se aplica al acceso del personal interno a los sistemas y datos?	55,0800	77,327	0,709	0,901

Anexo 06: Constancia de autorización

AUTORIZACIÓN DE USO DE INFORMACIÓN DE EMPRESA

Yo, Nelson Ramos Eduen identificado con DNI N° 80671130, en mi calidad de Gerente General de la Empresa **INNOTEC S.A.C.**, con R.U.C N° 20494004209, ubicada en el Jr. Prolong. Libertad N° 991, distrito de Tarapoto, provincia de San Martin y departamento de San Martin.

OTORGO LA AUTORIZACIÓN,

Al señor **Edward Hans Pinchi Núñez**, Identificada con DNI N° 45874181 de la Carrera profesional de Ingeniería de Sistemas e Informática, para que pueda usar información de empresa de la Empresa INNOTEC S.A.C., con la finalidad de que pueda desarrollar su ( ) Informe estadístico, ( ) Trabajo de Investigación, (X) Tesis para optar el Título Profesional.

(X) Publique los resultados de la investigación en el repositorio institucional.

( ) Mantener en reserva el nombre o cualquier distintivo de la empresa; o

(X) Mencionar el nombre de la empresa.

INNOTEC S.A.C.
NELSON RAMOS EDUEN
REPRESENTANTE LEGAL

(Gerente General)
DNI N° 80671130

El Estudiante declara que los datos emitidos en esta carta y en el Trabajo de Investigación, en la Tesis son auténticos. En caso de comprobarse la falsedad de datos, el Estudiante será sometido al inicio del procedimiento disciplinario correspondiente, asimismo, asumirá toda la responsabilidad ante posibles acciones legales que la empresa, otorgante de información, pueda ejecutar.

Edward Hans Pinchi Núñez
DNI N° 45874181

Anexo 07: Base de datos

Seguridad de la información																		
	Confidencialidad							Integridad					Disponibilidad					
N°	it1	it2	it3	it4	it5	it6	it7	it8	it9	it10	it11	it12	it13	it14	it15	it16	it17	it18
1	5	4	5	4	3	5	3	2	4	4	5	3	2	2	3	3	3	5
2	4	3	5	3	3	3	2	4	3	4	3	4	4	2	3	4	5	4
3	4	3	5	5	4	5	3	3	3	3	5	4	3	2	2	3	3	4
4	4	5	4	4	4	4	4	4	4	3	3	4	3	2	5	3	4	5
5	5	4	5	5	3	5	2	2	4	5	3	5	4	5	5	3	5	3
6	5	4	5	5	4	3	4	4	3	5	3	4	2	4	2	2	4	5
7	5	4	3	4	4	4	3	3	2	4	4	4	3	3	3	4	3	4
8	5	3	4	3	5	5	2	4	3	3	3	3	2	4	3	4	4	4
9	5	5	3	4	4	3	4	4	3	4	5	3	4	5	5	2	4	4
10	4	3	5	3	5	5	3	3	4	5	4	4	2	4	3	2	3	5
11	2	2	3	1	2	2	3	2	3	1	3	2	2	2	2	2	4	1
12	4	4	4	3	3	3	2	2	4	5	3	4	3	2	5	1	4	5
13	2	3	3	2	3	4	2	3	2	4	4	4	3	2	4	1	5	5
14	4	5	5	5	5	5	4	4	3	4	5	4	2	5	4	4	3	5
15	5	3	5	5	5	3	4	3	2	4	3	3	3	4	4	2	3	5
16	4	4	5	5	4	3	2	2	3	4	5	5	2	4	2	4	4	5
17	2	2	3	3	2	2	2	3	2	3	2	2	2	2	2	2	3	1
18	4	5	5	4	4	3	2	2	3	5	4	4	2	3	4	1	5	4
19	5	4	5	3	3	3	4	2	2	4	4	5	3	5	2	1	5	3
20	5	5	5	4	5	5	3	3	3	4	5	4	3	5	5	2	4	5
21	4	3	3	4	4	5	2	4	3	4	3	4	2	2	5	4	4	3
22	5	5	5	5	5	4	4	4	2	5	3	4	4	3	2	4	3	4
23	2	3	3	3	1	2	2	2	2	3	3	2	2	2	2	3	2	2
24	4	4	4	3	4	4	3	4	2	4	3	4	3	3	2	4	4	4
25	4	3	5	5	5	3	2	3	3	5	4	5	2	3	3	1	4	4

Protección de los activos

	Información			Software				Físicos					Servicios		Personal	
N°	Pr1	Pr2	Pr3	Pr4	Pr5	Pr6	Pr7	Pr8	Pr9	Pr10	Pr11	Pr12	Pr13	Pr14	Pr15	Pr16
1	3	3	3	5	5	3	3	4	4	4	5	2	5	4	4	4
2	2	3	4	3	4	4	3	4	3	5	4	3	5	5	5	5
3	3	4	3	3	4	3	4	4	4	4	4	3	4	5	5	5
4	3	2	3	4	5	1	4	4	3	4	4	2	5	5	4	5
5	3	4	4	4	5	4	3	4	5	5	5	4	5	4	5	5
6	2	2	3	5	5	1	3	3	5	5	5	1	5	5	4	4
7	3	3	2	5	5	3	4	5	4	4	4	1	5	4	5	5
8	2	3	3	5	4	1	3	4	3	5	5	2	4	5	5	5
9	4	3	4	4	4	3	4	5	4	5	5	4	4	5	4	5
10	2	3	4	3	4	5	5	4	4	5	5	3	5	4	5	5
11	2	2	2	2	2	1	2	2	2	2	3	3	3	3	2	3
12	2	3	3	4	5	1	5	3	3	5	4	1	4	5	4	4
13	2	3	2	3	4	1	4	4	3	4	4	3	4	4	4	4
14	3	4	5	5	5	4	4	3	3	4	5	4	5	5	5	4
15	2	3	4	4	5	4	5	3	4	4	4	3	5	4	5	4
16	3	3	3	3	5	3	5	3	4	5	5	4	5	4	4	4
17	2	3	2	3	2	1	2	2	2	2	2	3	3	3	3	2
18	2	3	3	4	5	3	4	5	3	4	5	4	4	4	4	5
19	2	3	3	5	4	1	3	4	4	4	5	4	4	5	5	4
20	5	4	4	5	4	4	5	5	4	4	5	4	5	5	5	4
21	3	2	2	5	4	2	3	3	5	4	5	3	5	4	5	4
22	3	4	4	4	5	4	4	4	3	4	5	5	5	5	5	5
23	3	2	3	3	2	3	2	2	3	2	2	2	2	2	3	3
24	2	3	3	4	4	3	4	4	3	5	5	3	4	4	5	4
25	3	3	3	4	4	2	4	3	5	5	4	3	5	5	5	4

Edward pinchi

Seguridad de información y protección de activos según ISO 27001 en INNOTEC: eficiente gestión para salvaguardar datos...

Revisión de Tesis final - Unidad de Investigación FISI

Detalles del documento

Identificador de la entrega
trn:oid:::3117:557787775

Fecha de entrega
17 feb 2026, 7:12 GMT-5

Fecha de descarga
17 feb 2026, 7:21 GMT-5

Nombre del archivo
INFORME TESIS - HANS_TERMINADO.pdf

Tamaño del archivo
2.2 MB

77 páginas

19.760 palabras

109.331 caracteres

18% Similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para ca...

Filtrado desde el informe

- Bibliografía
- Texto citado
- Texto mencionado
- Coincidencias menores (menos de 10 palabras)

Fuentes principales

15% Fuentes de Internet
8% Publicaciones
10% Trabajos entregados (trabajos del estudiante)

Marcas de integridad

N.º de alertas de integridad para revisión

Los algoritmos de nuestro sistema analizan un documento en profundidad para buscar inconsistencias que permitirían distinguirlo de una entrega normal. Si advertimos algo extraño, lo marcamos como una alerta para que pueda revisarlo.

Una marca de alerta no es necesariamente un indicador de problemas. Sin embargo, recomendamos que preste atención y la revise.