UNIVERSIDAD PARA EL DESARROLLO ANDINO

FACULTAD DE CIENCIAS E INGENIERÍA

ESCUELA PROFESIONAL DE INGENIERÍA INFORMÁTICA

TESIS

ISO/IEC 27001 PARA EVALUAR LA SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN EN INVERSIONES RMK, LIRCAY – 2025

Para optar el título profesional de:

Ingeniero Informático

Autor:

Samuel Huincho Taype

Asesor:

Mg. Rolando Yossef Bendezu Ureta

Lircay – Angaraes – Huancavelica – Perú

2026

METADATOS COMPLEMENTARIOS

Datos de Autor	
Nombres y apellidos	Samuel Huincho Taype
Tipo de documento de identidad	DNI
Número de documento de identidad	72275714
URL de ORCID	https://orcid.org/0009-0008-2105-758X
Datos del Asesor	
Nombres y apellidos	Mg. Rolando Yossef Bendezu Ureta
Tipo de documento de identidad	DNI
Número de documento de identidad	29673566
URL de ORCID	https://orcid.org/0000-0003-2974-7485
Datos de los Jurados	
Presidente	
Nombres y apellidos	Mg. Sonia Condori Benito
Tipo de documento de identidad	DNI
Número de documento de identidad	46902887
Secretario	
Nombres y apellidos	Mg. Ruben Tito De La Cruz
Tipo de documento de identidad	DNI
Número de documento de identidad	41413782
Vocal	
Nombres y apellidos	Mg. Jhony Bartolo Arche
Tipo de documento de identidad	DNI
Número de documento de identidad	72480371

DATOS DE INVESTIGACIÓN	
Línea de investigación	Normas y estándares informáticas
Grupo de investigación	No aplica
Agencia de financiamiento	No aplica
Ubicación geográfica de la investigación	País: Perú Departamento: Huancavelica Provincia: Angaraes Distrito: Lircay Calle: Jr. Libertad Nro. 259 Bellavista (Altura 4 Esquinas 2P Amarillo Celeste) Longitud: -74.724722
Año o rango de años en que se realizó la investigación	Abril 2025 – Mayo 2026
URL de disciplinas OCDE	Ciencias de la Información (OCDE 1.02.02) https://purl.org/pe-repo/ocde/ford#1.02.02

DEDICATORIA

A Dios, por ser la fuente de sabiduría y fortaleza que me permitió culminar con perseverancia cada etapa de este trabajo. A mis padres, cuyo esfuerzo, amor y ejemplo han sido el sostén fundamental en mi formación personal y profesional; en especial, a mi madre Hilda Taype Vásquez. A mi pareja Roxana Perla Chahuailacc Ichpas y a mi hijo Matteo Andrew Huincho Chahuailacc, por ser mi mayor inspiración y la razón principal para seguir esforzándome día a día. A mi asesor, Mg. Rolando Yossef Bendezu Ureta, por su guía y orientación académica que hizo posible la concreción de este trabajo.

AGRADECIMIENTO

A Dios, por devolverme la vida, la salud y la fortaleza, con las que puedo superar las adversidades y acabar con éxito en el desarrollo de esta investigación. A mis padres, por su amor incondicional y su sacrificio a través del apoyo, el cual ha sido la base fundamental en el desarrollo de mi vida personal y profesional. A mis amigos, por su compañía y los ánimos que tanto me brindaron en los momentos más difíciles y exigentes de este proceso académico.

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

La tesis titulada “ISO/IEC 27001 para evaluar la seguridad de los sistemas de información en Inversiones RMK, Lircay – 2025”, tuvo como objetivo evaluar la influencia de los criterios de la norma ISO/IEC 27001 en la seguridad de los sistemas de información en Inversiones RMK, Lircay – 2025. La investigación fue de tipo aplicada, nivel explicativo, con método científico y diseño no experimental de corte longitudinal (panel), con mediciones repetidas durante 90 días consecutivos.

La población y muestra constituida por los cinco sistemas de información operativos de la organización que han sido seleccionados mediante la técnica de muestreo censal. Las técnicas utilizadas fueron la observación y el análisis documental, empleando las fichas de observación y de análisis documental como instrumentos de trabajo. El análisis de tipo estadístico se realizó mediante la técnica de la regresión lineal. Los resultados indicaron que el cumplimiento de los criterios de la norma tenía una influencia estadísticamente significativa sobre la seguridad de los sistemas (β_1= 0.778; R^2= 0.636; $p < .001$), lo que significa que más del 60 % de la variabilidad de la seguridad de los sistemas se explicaba por la variable normativa. En las dimensiones confirmaban asociaciones estadísticamente significativas: confidencialidad (R^2= 0.491), integridad (R^2= 0.490) y disponibilidad (R^2= 0.545), lo que confirmó el efecto positivo de la norma sobre los pilares de la seguridad de la información. Se concluyó que el grado de cumplimiento de la norma ISO/IEC 27001 eleva de forma clara la seguridad de los sistemas de información en un entorno como el de la localización Lircay, ya que la heterogeneidad tecnológica y la falta de recursos obligaban a la priorización de controles normativos.

***Palabras clave**:* seguridad de la información, ISO/IEC 27001, confidencialidad, integridad, disponibilidad.

ABSTRACT

The thesis entitled "ISO/IEC 27001 to evaluate the security of information systems at Inversiones RMK, Lircay - 2025", aimed to evaluate the influence of the criteria of the ISO/IEC 27001 standard on the security of information systems at Inversiones RMK, Lircay - 2025. The research was applied, explanatory level, with a scientific method and a non-experimental longitudinal cross-sectional design (panel), with repeated measurements over 90 consecutive days.

A total of five operational information systems were part of the population and sample for this study. In this case, the sampling method employed was census sampling. The research methodology consisted of two types of techniques: observational and documentary analysis techniques. Both data collection and data analysis were conducted using two types of instruments, i.e., the observational and documentary analysis sheet. Data was analyzed statistically using linear regression analysis, with the outcome indicating that compliance with this standard's criteria will have a statistically significant impact on the security of these systems ($\beta_1 = 0.778$; $R^2 = 0.636$; $p < 0.001$), explaining over 60% of the variance in their respective security. The researcher also found that the standard had strong statistical relationships with confidentiality ($R^2 = 0.491$), integrity ($R^2 = 0.490$) and availability ($R^2 = 0.545$), all of which affirm that this standard positively affects the information security pillars. To summarize, the results indicate that compliance with ISO/IEC 27001 increases the level of protection of information systems operating within an environment like Lircay, where there is a large amount of technological diversity and limited resources. As a result, implementation of regulatory controls is a major consideration for managing information security within this type of environment.

Keywords: information security, ISO/IEC 27001, confidentiality, integrity, availability

CHINTI

Kay tesis sutichasqa “ISO/IEC 27001 para Evaluación de la Seguridad de Sistemas de Información en RMK Inversiones, Lircay – 2025” nisqa, criterios estándares ISO/IEC 27001 nisqapa influencianta chaninchanapaqmi karqa, RMK Inversiones, Lircay – 2025 nisqapi sistemas de información nisqapa seguridadninmanta, chay investigacionqa aplicasqa, sut’inchanapaq, hinaspa método científico nisqawan huk mana experimental ruway, suni tiempopi qhaway (panel nisqa), 90 punchaw hina kuti kuti tupuspa. Población y muestra nisqa empresapa pichqa sistemas de información operativa nisqamanta ruwasqa, muestreo censo nisqawan akllasqa. Qhaway, qillqa t’aqwiy ima, willay huñunapaq técnicas hina llamk’achikurqa, qhaway, qillqa t’aqwiy formulariokunata instrumentujina llamk’achispa. Análisis estadístico nisqa ruwakurqa regresión lineal nisqawan. Chay ruwasqakunam qawarichirqa chay criterios de estándar nisqawan hunt’ayqa anchata influyen chay sistemakunapa seguridadninpi ($\beta1 = 0,778$; $R2 = 0,636$; $p < .001$), chaymi sut’incharqa aswan 60% variabilidad nisqamanta. Asociaciones relevantes nisqakunam tarikurqa tukuy dimensiones nisqapi: confidencialidad ($R2 = 0,491$), integridad ($R2 = 0,490$), chaynallataq disponibilidad ($R2 = 0,545$), chaymi takyachirqa chay normapa allin ruwayninta pilares de seguridad de información nisqapi. Tukuchikunmi ISO/IEC 27001 nisqa kamachikuy hunt’akuyninqa sut’itan yapan sistemas de información nisqakunaq amachayninta Lircay hina pachamamapi, chaypin heterogeneidad tecnológica nisqa hinallataq pisi recursokuna necesitan controles regulatorios nisqakunata ñawpaqman churayta.

***Sapaq simikuna**:* willakuy waqaychasqa, ISO/IEC 27001, pakasqa, hunt'asqa, tarikuy

INTRODUCCIÓN

En la actualidad, la seguridad de los sistemas de información constituye un desafío prioritario para organizaciones públicas y privadas debido al incremento sostenido de los ciberataques y a la creciente dependencia tecnológica de los procesos operativos. La norma ISO/IEC 27001 ha adquirido un rol protagónico al establecer un marco formal para la gestión de riesgos, la protección de activos digitales y la continuidad del negocio, siendo adoptada por más de 60,000 organizaciones en el mundo. La aplicación de la norma en la región ha contribuido a disminuir los incidentes en áreas estratégicas, aunque aún hay limitaciones en infraestructura y cultura de seguridad, sobre todo en los países de desarrollo. Respecto del caso peruano, el número de ataques cibernéticos se consideró elevado, alcanzando más de 64 millones de registros entre 2023 y 2024, impactando de forma relevante a algunos sectores productivos, como el de la construcción. Esta realidad pone en evidencia la importancia de incrementar la gestión de seguridad de la información en organizaciones medianas y regionales que enfrentan altos riesgos sin contar con un desarrollo formal de la afectación. Inversiones RMK, ubicada en Lircay, constituye un ejemplo de esta problemática, al carecer de un sistema integral de seguridad que garantice la confidencialidad, integridad y disponibilidad de sus datos críticos.

Basándonos en la problemática descrita, se plantea el siguiente problema: ¿De qué manera los criterios de la norma ISO/IEC 27001 influyen en la seguridad de los sistemas de información en Inversiones RMK, Lircay – 2025? A partir de este contexto, la presente investigación plantea como objetivo general evaluar la influencia de los criterios de la norma ISO/IEC 27001 en la seguridad de los sistemas de información en Inversiones RMK, Lircay – 2025, considerando dimensiones específicas vinculadas a la confidencialidad, integridad y disponibilidad. Para ello, se desarrolló un estudio de tipo aplicado, nivel explicativo, con diseño no experimental, de corte longitudinal con alcance panel. La población y muestra estuvieron

constituidas por los cinco sistemas de información operativos de la empresa. Se emplearon como técnicas la observación y el análisis documental, utilizando fichas de registro validadas como instrumentos de recolección.

La investigación se organiza en cinco capítulos: El Capítulo I desarrolla el problema, objetivos, hipótesis y justificación. El Capítulo II contiene el marco teórico, en el que se presentan los antecedentes y las bases teóricas; el Capítulo III describe la metodología, la cual incluye el tipo, nivel y diseño de investigación, la especificación de la población y muestra, la definición de las técnicas e instrumentos para recolectar información, el procesamiento de información obtenido y las consideraciones éticas del estudio. El Capítulo IV presenta los resultados descriptivos, la contrastación de hipótesis y la discusión delos resultados; y el Capítulo V da cuenta de las conclusiones y las recomendaciones.

CAPÍTULO I

EL PROBLEMA DE INVESTIGACIÓN

1.1. Planteamiento del problema

En la actualidad, la seguridad de los sistemas de información representa un desafío global cada vez más complejo, tanto para organizaciones públicas como privadas. La creciente sofisticación de los ciberataques y la dependencia tecnológica de los procesos operativos han generado una preocupación constante sobre la protección de los datos. En este contexto, Arrieta (2024) destaca que la norma ISO/IEC 27001 ha cobrado un rol protagónico al proporcionar un marco estructurado para reducir riesgos, proteger los sistemas y garantizar la continuidad del negocio. Esta regulación, que tiene una implementación de más de 60,000 organizaciones en todo el mundo, se está convirtiendo en un recurso indispensable en el contexto de la multitud de amenazas que se están produciendo y de filtraciones de información.

Efectivamente, en el caso de Latinoamérica, el efecto de las normas ISO/IEC 27001 ha llegado a ser un fenómeno en las diferentes organizaciones que forman parte de sectores clave, tal y como nos indica Arrieta (2024), desde el año 2018 estas certificaciones asociadas a temas de seguridad, así como a gobernanza de datos, han aumentado un 28% y donde Brasil y México son líderes en la implementación. En el caso concreto del análisis en Brasil, este ha puesto de manifiesto que la adopción de la norma ISO/IEC 27001 ha ayudado a mitigar en un 40% la cantidad de incidentes cibernéticos que se producen en el sector IT. Torres (2025) añade que la última revisión de la norma, que reorganizó los controles de 114 en 14 dominios a 93 en 4 grandes categorías para permitir a las organizaciones latinoamericanas la puesta al día de sus sistemas en el sentido de los nuevos escenarios de riesgo, en particular la cadena de suministro y los entornos digitales híbridos.

Desde el punto de vista social, el caso peruano resulta más que preocupante. Según el autor Chavarría (2025) entre julio de 2023 y julio del 2024 ha habido más de 64,7 millones de

ataques de malware en el Perú, lo que representa un aumento del 2,9 % respecto al año anterior. Este problema ha impactado a sectores estratégicos como el sector de la construcción, donde hay un 5,14 % de incidencia reportada. En la línea aquí opina Solar (2025), el mismo año 2023 registra más de 5 mil millones de intentos de ataques cibernéticos contra el Perú, sea a través de ransomware, phishing y explotación. Estos datos revelan un entorno crítico en el que los sistemas públicos y privados particularmente los centralizados en Lima han sido blancos constantes de ataques que han comprometido datos financieros y operativos.

En cuanto al abordaje empresarial, Chavarría (2025) documenta que la empresa Cementos Pacasmayo se convirtió en la primera cementera del Perú en obtener la certificación ISO/IEC 27001, como parte de una estrategia integral para proteger sus activos informáticos. La empresa realizó un diagnóstico interno, auditorías exigentes y una validación externa que robusteció su postura de seguridad y la convirtió en un referente para otras empresas nacionales.

En una mirada crítica, Ruiz (2025) manifiesta que el enfoque tradicional que solo adquiría nuevas herramientas tecnológicas fue insuficiente. En 2024 las organizaciones implementaron una media de 120 soluciones de ciberseguridad diferentes. Lamentablemente, muchas tecnologías fueron no utilizadas o tan solo parcialmente utilizadas, creando flujos de trabajo desarticulados. La ausencia de una estrategia de gobernanza, junto a una poca madurez organizacional, minó la capacidad de respuesta ante incidentes. En este sentido, Ruiz (2025) explica que el NIST incorporó la función de “Gobernar” en su Cybersecurity Framework para establecer una gestión dinámica del riesgo y una toma de decisiones basada en la analítica de datos estratégicos.

En este contexto, la variable seguridad de la información debe ser entendida como la propia capacidad de proteger la confidencialidad, la integridad y la disponibilidad de la información en medios digitales, incluyendo todos los aspectos técnicos, como los organizacionales y los humanos, como por ejemplo la formación del personal, los accesos, o la

reacción ante incidentes. Por el lado contrario, la particular aplicación de la norma ISO/IEC 27001 debe ser entendida como un enfoque formal y sistemático con el que poder llevar a cabo una evaluación de riesgos, una definición de políticas de seguridad, así como un proceso de mejora continua de la gestión de la información.

Ambas variables se consultan directamente en la problemática que encuentra Inversiones RMK en Lircay. Esta organización, como muchas otras en el país, se ve sometida cada vez más a la exposición a ataques informáticos, y en contrapartida no mantiene una estructura de gestión formal de la seguridad informática. Es a partir de esta base que este estudio se plantea la necesidad de determinar en qué medida la aplicación de la norma ISO/IEC 27001 beneficiaría la seguridad de los sistemas de información, no solo como una medida de cumplimiento con lo normativo sino como un enfoque global para fortalecer la resiliencia operativa, minimizar riesgos y proteger los activos críticos de la organización.

1.2. Formulación del problema

1.2.1. Problema principal

¿De qué manera los criterios de la norma ISO/IEC 27001 influyen en la seguridad de los sistemas de información en Inversiones RMK, Lircay – 2025?

1.2.2. Problemas específicos

a) ¿De qué manera los criterios de la norma ISO/IEC 27001 influyen en la confidencialidad de los sistemas de información en Inversiones RMK, Lircay – 2025?
b) ¿De qué manera los criterios de la norma ISO/IEC 27001 influyen en la integridad de los sistemas de información en Inversiones RMK, Lircay – 2025?
c) ¿De qué manera los criterios de la norma ISO/IEC 27001 influyen en la disponibilidad de los sistemas de información en Inversiones RMK, Lircay – 2025?

1.3.Fundamentación

1.3.1. Fundamentación científica

La presente investigación se sustenta en los principios de la investigación aplicada, la cual, según Hadi et al. (2023), se fundamenta en teorías existentes para abordar problemas prácticos en campos como la ingeniería, donde la teoría se utiliza para generar soluciones aplicables. En este sentido, el estudio contribuye al conocimiento sobre la norma internacional ISO/IEC 27001 y su impacto en la seguridad de los sistemas de información, abordando un vacío empírico identificado por Culot et al. (2021), quienes señalan que, tras 15 años de investigación académica sobre el estándar, persisten interrogantes sobre su eficacia en contextos organizacionales específicos, especialmente en entornos con recursos limitados.

Al realizar un análisis sobre cómo se implementa la norma en Inversiones RMK, en Lircay, esta investigación da respuesta al requerimiento que hacen Kamil et al. (2023), quienes advierten que es necesario desarrollar alternativas metodológicas para validar las relevantes operaciones y medidas de seguridad, sobre todo en organizaciones pequeñas. Asimismo, se atendió el vacío que existe en los estudios de ciberseguridad en organizaciones peruanas medianas, sobre todo en departamentos las cuales no pertenecen a la capital; lo cierto es que la literatura especializada en esta problemática aún es limitada. Debemos tener en cuenta que, tal como plantea Chavarría (2025), entre julio de 2023 y julio de 2024 se produjeron más de 64.7 millones de ataques con malware en Perú, lo cual está afectando a sectores productivos, tal como la construcción, sector que corresponde con la empresa objeto del estudio.

1.3.2. Fundamentación teórica y relevancia disciplinar

Desde una perspectiva teórica, la investigación profundiza en las variables involucradas en la gestión de seguridad de la información, fortaleciendo el marco conceptual existente. Kitsios et al. (2023) hacen hincapié en que las organizaciones han de llegar a integrar correctamente las estrategias de seguridad para volverse más resilientes ante las amenazas

cibernéticas, para lo cual se necesitan no solamente controles técnicos, sino también un conocimiento profundo de los factores organizativos en la implementación

La norma ISO/IEC 27001 se orienta en convertirse en el núcleo y la referencia internacional para el diseño, la implantación y la mejora continua del Sistema de Gestión de la Seguridad de la Información (SGSI). Según Viteri (2022), este estándar permite a las organizaciones identificar, gestionar y reducir los riesgos relacionados con la información, protegiendo datos corporativos, información de clientes y propiedad intelectual. Por su parte, ISOTools (2022) destaca el carácter evolutivo de la norma, al definirla como una solución de mejora continua capaz de evaluar amenazas tanto internas como externas.

Credibilidad y validez metodológica

La validez del hallazgo se sostiene en un diseño metódico riguroso. La investigación, siguiendo a Hinojosa et al. (2024), presenta un nivel explicativo, que permite descubrir y explicar las causas y consecuencias de un hecho. La investigación, en el sentido que establecen Hernández-Sampieri y Mendoza (2018), se desarrolla con un diseño no experimental de corte longitudinal, con un alcance de serie temporal, favoreciendo la observación sistemática de las variables en su contexto natural, sin manipularlo por parte del investigador, de forma tal que se puede inferir la validez externa.

La consistencia de los instrumentos de recoger la información fue evaluada con el coeficiente Kuder-Richardson 20 (KR-20), obteniendo resultados cercanos a valores de 0.878 para la variable independiente y de 0.83 para la variable dependiente, asegurando ampliamente el umbral de 0.70 que se considera como aceptable (Kuder y Richardson, 1937). Este nivel de consistencia interna avala la calidad de los registros obtenidos a lo largo de los 90 días consecutivos de observación.

1.3.3. Fundamentación práctica y social

La investigación aborda un problema real en Inversiones RMK, relacionado con la falta de un sistema estructurado de protección de información, una situación que, según Ruiz (2025), es común en organizaciones que carecen de una estrategia clara de gobernanza en seguridad digital. Los resultados obtenidos no solo benefician a la empresa estudiada, sino que resultan útiles para otras organizaciones que enfrentan desafíos similares en contextos regionales.

De acuerdo con la tesis pendiente de Salas et al. (2024) en el caso ecuatoriano, esta investigación pone de manifiesto que la normativa ISO/IEC 27001 mejora la seguridad digital mediante la implementación de controles adecuados y la gestión de riesgos, además de enriquecer la cultura organizativa en torno a la protección de datos. Tal y como concluye Mirtsch (2023), se generan recomendaciones prácticas para mejorar la gestión de la información en entornos vulnerables, así como la adopción de estándares internacionales como una herramienta de diferenciación competitiva y como una práctica de protección estratégica.

1.3.4. Fundamentación metodológico y prospectivo

El enfoque metodológico empleado, basado en mediciones diarias durante 90 días consecutivos y análisis mediante regresión lineal, constituye un modelo replicable para futuras investigaciones en empresas similares. Jevelin y Faza (2023) sostienen que la evaluación de madurez de los SGSI requiere métodos mixtos que combinen evaluaciones cuantitativas con conocimientos cualitativos; en este sentido, el presente estudio aporta una aproximación sistemática que puede ser adaptada a distintos contextos organizacionales, contribuyendo así al desarrollo de la investigación en seguridad de la información en el ámbito nacional e internacional.

1.4. Objetivos de la investigación

1.4.1. Objetivo general

Evaluar la influencia de los criterios de la norma ISO/IEC 27001 en la seguridad de los sistemas de información en Inversiones RMK, Lircay – 2025.

1.4.2. Objetivos específicos

a) Evaluar la influencia de los criterios de la norma ISO/IEC 27001 en la confidencialidad de los sistemas de información en Inversiones RMK, Lircay – 2025.
b) Evaluar la influencia de los criterios de la norma ISO/IEC 27001 en la integridad de los sistemas de información en Inversiones RMK, Lircay – 2025.
c) Evaluar la influencia de los criterios de la norma ISO/IEC 27001 en la disponibilidad de los sistemas de información en Inversiones RMK, Lircay – 2025.

1.5. Hipótesis

1.5.1. Hipótesis general

El cumplimiento de los criterios de la norma ISO/IEC 27001 influye en la seguridad de los sistemas de información en Inversiones RMK, Lircay – 2025.

1.5.2. Hipótesis específicas

a) El cumplimiento de los criterios de la norma ISO/IEC 27001 influye en la confidencialidad de los sistemas de información en Inversiones RMK, Lircay – 2025.
b) El cumplimiento de los criterios de la norma ISO/IEC 27001 influye en la integridad de los sistemas de información en Inversiones RMK, Lircay – 2025.
c) El cumplimiento de los criterios de la norma ISO/IEC 27001 influye en la disponibilidad de los sistemas de información en Inversiones RMK, Lircay – 2025

CAPÍTULO II

MARCO TEÓRICO

2.1. Antecedentes de la investigación

2.1.1. Antecedentes internacionales

Salas et al. (2024) en el estudio *"Evaluación de la aplicación de la norma ISO 27001 en micro y pequeñas empresas del sur Quito"*. La metodología adoptada efectivamente incorporó la combinación de entrevistas y cuestionarios empleados para cada responsable de las áreas de seguridad de la información y tecnología de la información dentro de las empresas, la contemplación de los documentos de registros del Sistema de Gestión de la Seguridad de la Información (SGSI). La muestra de empresas pasó por un proceso ponderado, describiendo que la adopción de la norma fue en general dispar, presentándose empresas con una adopción activa y otras aún en las primeras etapas de implementación. Además, también se advirtieron otros obstáculos, como la ausencia de recursos humanos y financieros y de conocimientos tecnológicos y de seguridad de la información, la resistencia a los cambios en la organización, entre otros. Los resultados del presente trabajo apuntan a una última conclusión válida y objetiva; aunque la adopción de la norma ISO 27001 señala ser un reto importante para las micro y pequeñas empresas de la zona sur de Quito, los beneficios a medio-largo plazo, mediante la mayor protección de los datos más sensibles y la mayor confianza por parte de los clientes y socios de negocio son motivos suficientes para justificar la implementación de esfuerzos y recursos de inversión por parte de las empresas.

Mirtsch (2023), en su investigación *"Adoption of the information security management system standard ISO/IEC 27001: A study among german organizations."*. Llevan a cabo un estudio para poder comprender los aspectos que provocan esta baja adopción, así como de explicaciones del porqué su escasa difusión, utilizando como referente el trabajo de Rogers sobre la teoría de la difusión de innovaciones y considerando a la ISO/IEC 27001 como una

innovación de carácter preventivo. Para ello, realizaron una encuesta dirigida a organizaciones alemanas, diferenciando entre aquellas que tan solo implementaron la norma y aquellas que, además, contaban con certificación oficial. A partir de los resultados lograron identificar aspectos como las motivaciones para adoptar la norma, los impactos percibidos dentro de las organizaciones, las barreras de la adopción, así como un conjunto de medidas que podrían resultar útiles para la misma. La información obtenida les resultó útil no tan solo para las organizaciones que consideran adoptar ISO/IEC 27001, sino también para las organizaciones de certificación y formuladores de políticas públicas interesados en elevar el bajo nivel general de seguridad de la información que presentan las organizaciones en general. El autor concluye que una mejor comprensión de las percepciones y obstáculos de la norma pueden facilitar la elaboración de estrategias más adecuadas para permitir la adopción de la norma, especialmente por el papel fundamental que desempeña la misma a la hora de proteger los activos informáticos y prevenir riesgos en las organizaciones actuales.

Donoso et al. (2023), en el estudio *"Aplicación del SGSI ISO 27001 en el sistema de rehabilitación social de Ecuador"*, el estudio tuvo como propósito fomentar el uso de la inteligencia artificial a partir de la implementación de la Gestión de Seguridad de la Información (SGSI) bajo el estándar ISO/IEC 27001, para mejorar el control y el monitoreo de personas que cumplen medidas sustitutivas y las personas privadas de libertad, echando mano de dispositivos electrónicos tipo tobillera, cercas electrónicas o sistemas de geolocalización. Utilizó una metodología aplicada y tecnológica, apoyada en la aplicación de un SGSI bajo la norma ISO/IEC 27001. Los resultados demostraron que el uso de inteligencia artificial y dispositivos de rastreo contribuyen a crear escenarios de prevención y mejoran la política pública en el ámbito de seguridad. El autor concluyó que la incorporación de esta tecnología fortalece el control de las personas sometidas a monitoreo y también involucra de manera importante la

mejora de la administración pública mediante decisiones sustentadas en datos y análisis prospectivo.

Yungán y Narváez (2022), en su estudio "*Aplicación de la Norma ISO 27001 para la seguridad de los Sistemas de Información".* El estudio tuvo como objetivo principal la puesta en práctica de la norma ISO 27001, con el fin de que la seguridad de los sistemas de información mejorase dentro de las organizaciones. Además de gestionar los riesgos relacionados con la información, buscaba garantizar que la confidencialidad, la integridad y la disponibilidad fueran adecuadamente protegidas. Para ello, fueron sometidas a estudio diferentes organizaciones de distintos sectores (telecomunicaciones, servicios financieros y salud) respecto a la norma ISO 27001.

Para las técnicas de recolección de datos, se siguieron entrevistas semi-estructuradas y cuestionarios, que hicieron posible conocer la percepción de la seguridad de la información y la seguridad de los procesos de los sectores elegidos. Los resultados mostraron que la puesta en práctica de un Sistema de Gestión de Seguridad de la Información (SGSI) ajustado a la norma ISO 27001 ayudó a que la identificación y la mitigación de los riesgos mejorase. Se resaltó la importancia del ciclo PDCA (Plan-Do-Check-Act) en la mejora continuada de la seguridad de la información facilitiando así a las organizaciones la adaptación de sus procesos. En conclusión, la puesta en práctica de un SGSI garantizó que los activos de información estuvieran protegidos frente a amenazas y mejoró la seguridad de la operatividad de las organizaciones, ayudó a satisfacer requisitos normativos y contractuales, contribuyó a crear confianza en el exterior y a mejorar la imagen de la organización.

De la Rosa (2021), en su estudio *"Automatización de un sistema de gestión de seguridad de la información basado en la Norma ISO/IEC 27001".* El documento ha expuesto de una manera muy sencilla cómo se debe de utilizar un sistema de gestión de seguridad de la información de acuerdo con la norma ISO/IEC 27001. Para dichos fines se utilizó una matriz

con preguntas concretas, la que fue ayuda para repasar cuestiones clave de la seguridad. Posteriormente, se realizó un análisis de cómo estaba la propia empresa comparándola con la norma, y así se pudo identificar aspectos que hace falta mejorar. Finalmente se obtuvieron tres ficheros de Excel: el primero, relacionado con los riesgos; el segundo, con las incongruencias; y, el tercero, con el control, permitiendo una mejor visualización de la situación. Al mismo tiempo, permitía evaluar el nivel que tenía la empresa y hacia dónde se deberían proponer acciones para mejorar. Por tanto, podemos decir que el trabajo sí que complementó su cometido porque logró construir herramientas simples que permiten implantar dicho sistema..

2.1.2. Antecedentes nacionales

De La Cruz (2024) en su investigación "*ISO 27001 para mejorar el sistema de gestión de seguridad de la información en una empresa de servicios, Lima 2024"*, El trabajo pretendió comprobar si la norma ISO 27001 puede mejorar la seguridad de la información en una empresa de servicios. Para ello se realizó un estudio práctico, numérico, a partir de métodos de análisis como observar, pensar y llegar a conclusiones. Se trabajó con distintos controles de la norma, pero únicamente se revisaron los correspondientes a los controles con los que se trabaja. Para la recolección de datos se utilizaron el método de la observación, mediante la utilización de una ficha de observación sencilla. Después de revisar el uso de la aplicación de la norma ISO 27001 se llega a la conclusión, de que utilizar esta norma, mejoró la forma de trabajar de la organización, ya que existen menos problemas de seguridad de información, como en un 99%, en temas tan relevantes como la protección de la información. En resumen, el uso de la norma ISO 27001 fue muy importante para mejorar el sistema de seguridad de la información.

Contador y Tapia (2024) en su estudio "*Diseño e implementación de la ISO 27001 para mejorar la seguridad de información de la Empresa Minera Colibri S.A.C. Lima – 2023*", El objetivo del estudio fue determinar si la implementación de la norma ISO 27001 contribuía a mejorar la seguridad de la información en la empresa Minera Colibrí S.A.C. en el año 2023.

Para ello participaron en su elaboración todos sus 70 trabajadores, y se consideraron diferentes formas para la recolección de la información, como la observación, la aplicación de encuestas, entrevistas y la revisión de documentos. Al inicio de la investigación se evidenció que la empresa usaba tecnología básica pero que presentaba con varios problemas en seguridad, tanto a nivel de red, como a nivel de usuarios. Los trabajadores también admitieron el uso de software sin licencia y la falta de equipos certificados, lo que podía hacer que se viesen expuestos a peligros tales como virus informáticos o a problemas legales. Tras la aplicación de la norma ISO 27001 se evidenció que la seguridad de la información había mejorado de forma considerable, con un nivel de confianza del 95%. Finalmente, cabe concluir que efectivamente la norma ISO 27001 ha sido de significativa ayuda para mejorar la calidad de la seguridad de la información en la empresa Minera Colibrí S.A.C.

Rodríguez (2023) su investigación "*Mejora de la seguridad de la información aplicando la norma ISO/IEC 27001, en una consultora de sistemas",* realizo un estudio con el propósito de establecer mejoras en la Seguridad de la Información (SI), a través de la norma ISO/IEC 27001 en una consultora de sistemas. Se utilizó la metodología experimental, cuantitativa y de investigación aplicativa. Se realizó la técnica de observación y se aplicaron cuestionarios para la recolección de datos, sobre el estado actual de la SI en la empresa. Se utilizó una muestra de 20 controles tomados de la norma ISO 27001 y se llevó a cabo el ciclo PHVA (Plan, Hacer, Verificar, Actuar) para promover la mejora continua de las políticas de seguridad. Los resultados del estudio mostraron una tendencia significativa del incremento en el nivel de madurez de la SI de 37 % a un 49 % tras la implementación de la norma. Se logró una disminución de la tasa de incidentes que afectaban la confidencialidad, integridad y disponibilidad estadística de la información considerada en un 99%. Además, se establecieron políticas y controles que permitieron a la organización gestionar eficaz y eficientemente los riesgos de seguridad que surgieron como resultado de la evaluación. En conclusión, se establece

que la investigación puso de manifiesto que la norma ISO/IEC 27001 fue importante para mejorar la Seguridad de la Información en la consultora de sistemas.

Moron (2023) su investigación "*Diseño e implementación de un sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27002 para mejorar el nivel de seguridad informática en la empresa Rash Perú S.A.C",* El siguiente ensayo tuvo por principal objetivo el diseño de un Sistema de Gestión de Seguridad de la Información para la empresa Rash Perú S.A.C. a partir de la estructura de estándares de alcance internacional aplicados a las nuevas tecnologías de la información. La investigación se realizó bajo un enfoque de campo que permitió la elaboración de una propuesta factible para la solución de los problemas en torno a la seguridad de la información en la empresa. La metodología se sustentó en el ciclo de Deming usando la norma ISO 27002 como referencia. En cuanto a los resultados en Seguridad de la Información, se tiene que el valor promedio del Re-test fue de 69.90%, mientras que el valor promedio delPost-test de 14.00%. En cuanto a los aspectos mínimos y máximos, el Re-test tuvo un valor mínimo de 50% y un valor máximo de 88%; en cuanto al Post-test la muestra tuvo un valor mínimo de 0% y un valor máximo de 27%. La significancia en el Re-test fue de 0.265 y en el Post-test de 0.108; lo que indica que los indicadores se ajustan a la distribución normal o paramétrica ($P > 0.05$). En conclusión, el diseño del Sistema de Gestión de Seguridad de la Información propuesto para la empresa Rash Perú S.A.C. fue efectivo en el proceso para identificar y mitigar riesgos relacionados a la seguridad de la información.

Huamalí (2021) en su estudio "*Diseño de un sistema de gestión de seguridad de la información bajo el enfoque de la ISO/IEC 27001 para la empresa ITS Business SAC – Lima",* el estudio tuvo su enfoque en el diseño de un Sistema de Gestión de Seguridad de la Información (SGSI) para la empresa ITS Business SAC, aplicando para ello la norma nacional NTP ISO/IEC 27001:2014, el nivel de investigación fue descriptivo, esto es, identificar y describir el diseño del SGSI; el diseño de la investigación fue no experimental, así como transaccional descriptivo;

la muestra estuvo constituida por seis trabajadores correspondientes al área de sistemas de la empresa ITS Business SAC, seleccionados con base en un muestreo no probabilístico de error o de juicio del investigador; los instrumentos que sirvieron para recolectar fueron encuestas, entrevistas y análisis documental, y los resultados hallados, manifiestan que la empresa ITS Business SAC solo llegó a cumplir el 14% de los requisitos que establece la norma NTP ISO/IEC 27001:2014, por lo que se infiere que la empresa se hallaba en la fase inicial del cumplimiento de dicha norma; se elabora una "Declaración de Aplicabilidad" que justificó los controles que debe implementar, en conclusión, la tesis alcanzó cumplir con el diseño del SGSI que permitió a la empresa ITS Business SAC mejorar su seguridad de la información, proteger sus activos críticos y cumplir con los requisitos de la norma ISO/IEC 27001:2014.

2.2. Marco conceptual

2.2.1. Identificación de la variable independiente

ISO/IEC 27001: Organización Internacional de Normalización y la Comisión Electrotécnica Internacional 27001 (ISO/IEC 27001)

2.2.2. Conceptualización de la variable independiente

La norma ISO/IEC 27001 tiene como propósito ayudar a las organizaciones a establecer un SGSI que permita identificar, gestionar y reducir los riesgos relacionados con la información, protegiendo datos corporativos, información de clientes y propiedad intelectual. Esta visión resalta el carácter organizacional e integral del estándar, orientado no solo a la prevención, sino también a la protección de la infraestructura informativa crítica (Viteri, 2022).

2.2.2.1. Definición de la variable independiente Norma ISO/IEC 27001. Es el principal referente internacional para el diseño, ejecución, mantenimiento y mejora continua de un Sistema de Gestión de Seguridad de la Información (SGSI). Su enfoque estructurado permite a las organizaciones identificar, analizar y tratar los riesgos del uso, procesamiento, almacenamiento y transmisión de información, lo cual responde a la creciente necesidad de

proteger los activos digitales en un marco global muy expuesto a las amenazas cibernéticas. Viteri (2022) considera que el propósito de la norma ISO/IEC 27001, desde el punto de vista de la estrategia, consiste en ayudar a las organizaciones a implantar un SGSI que les permita identificar, gestionar y reducir los riesgos que comporta la información con el objetivo de poder proteger datos corporativos, información sobre clientes y propiedad intelectual. Esta visión pone de relieve el enfoque organizacional e integrador del estándar, que no únicamente intenta prevenir, sino también proteger la infraestructura informativa crítica. ISOTools (2022) también pone énfasis en el carácter evolutivo y adaptativo de la norma al definirla como una solución de mejora continua, la cual permite construir un SGSI capaz de evaluar amenazas internas y externas. Esta definición aporta un enfoque operativo y dinámico al presentar la norma como un sistema que se va adaptando a la variabilidad y cambio del entorno tecnológico y organizacional.

Por último, la definición oficial normativa que brinda ISO/IEC (2022) concibe la ISO 27001 como una norma que establece exigencias concretas para estructurar un SGSI, en el contexto de cada una de las organizaciones. Este enfoque establece la necesidad de realizar un tratamiento de los riesgos de manera adaptada a las condiciones/recursos/procesos que proporciona cada entidad, garantizando la aplicabilidad en los diversos sectores y particulares.

En conjunto, estas definiciones sustentan la ISO/IEC 27001 como la base teórica y técnica fundamental para comprender la gestión moderna de la seguridad de la información. Su implementación permite no solo cumplir con estándares internacionales, sino también fortalecer la resiliencia operativa, garantizar la continuidad del negocio y proteger la confidencialidad, integridad y disponibilidad de la información organizacional.

2.2.2.2. ISO/IEC 27001 como estándar principal. En la era de la transformación digital y la globalización de los sistemas de información, garantizar la protección adecuada de los datos se ha convertido en una prioridad ineludible para toda organización que aspire a

mantener su competitividad, credibilidad y sostenibilidad. En este escenario Kamil et al. (2023) menciona que, la norma ISO/IEC 27001 ha emergido como una guía normativa de aceptación internacional para estructurar y operar un Sistema de Gestión de la Seguridad de la Información (SGSI) de forma sistemática, estratégica y proactiva.

Esta norma establece un conjunto de requisitos y prácticas que permiten identificar, controlar y minimizar los riesgos que puedan afectar la confidencialidad, integridad y disponibilidad de los activos de información, las organizaciones que implementan ISO/IEC 27001 adoptan una visión estructurada de la seguridad, basada en procesos y controles que se alinean con los objetivos del negocio, permitiéndoles anticipar amenazas y gestionar vulnerabilidades antes de que estas se conviertan en incidentes perjudiciales (Kamil et al., 2023).

La importancia de esta norma proviene no solo de su solidez técnica, sino también por ser una norma integradora, pues considera aspectos humanos, organizativos, tecnológicos y legales. La implementación de los controles conforme el Anexo A de la norma invita a una gestión integral del riesgo, que abarca desde el acceso lógico y físico a la continuidad de negocio y a la concienciación del personal. Este enfoque totalizador permite elaborar una cultura de la organización con orientación hacia la seguridad, más allá de la mera implementación de herramientas tecnológicas (Kamil et al., 2023). Culot et al. (2021) por su parte, subrayan que la ISO/IEC 27001 se halla consolidada como uno de los estándares más adoptados en el mundo de la gestión organizativa, ocupando el tercer lugar en el mundo en términos de certificaciones, por detrás de la ISO 9001 (gestión de la calidad) y de la ISO 14001 (gestión ambiental). Esta posición constata la creciente valoración de las empresas y entidades públicas hacía la seguridad de la información como uno de los ejes estratégicos para salvaguardar su reputación, cumplir con las regulaciones legales y mantener la confianza de las partes interesadas.

Una de las más importantes características de la norma ISO/IEC 27001 es su enfoque basado en el ciclo PHVA (Planificar-Hacer-Verificar-Actuar), que permite establecer un proceso dinámico de mejora continua. Gracias a este tipo de modelo, las organizaciones pueden evaluar sus controles periódicamente, actualizar sus políticas y adaptarse a los constantes cambios en tecnologías y en la normativa. De esta forma, el SGSI ya no es un núcleo de prácticas estáticas sino de un sistema vivo que va evolucionando al mismo ritmo que se producen los desafíos del entorno digital (Culot et al., 2021).

También, la ISO/IEC 27001 proporciona una buena base para hacer frente a requisitos normativos locales e internacionales, tales como el Reglamento General de Protección de Datos en Europa o leyes nacionales específicas sobre la protección de los datos personales, lo que ofrece a las organizaciones una ventaja competitiva existente, ya que les permite operar en espacios comerciales más exigentes de conformidad con un marco normativo reconocido y auditado a través de auditorías independientes (Culot et al., 2021).

No menos importante, el proceso de certificación asociado a esta norma contribuye a fortalecer la confianza entre socios comerciales, clientes y entes fiscalizadores, al demostrar que la organización no solo declara su compromiso con la seguridad de la información, sino que lo respalda con acciones concretas y verificables. Esta confianza se convierte en un activo intangible que refuerza la credibilidad institucional y facilita la expansión de relaciones estratégicas en entornos globales, además esto ha dejado de ser un simple marco técnico para convertirse en un pilar fundamental de la gobernanza organizacional moderna. Su implementación no solo contribuye a proteger la información frente a amenazas internas y externas, sino que también genera valor estratégico al promover una cultura de prevención, cumplimiento y mejora continua en todos los niveles de la organización (Culot et al., 2021).

2.2.2.3. Marcos complementarios. Para Pascoe et al. (2024) y Jevelin y Faza (2023) mencionan que a medida que la seguridad de la información se vuelve cada vez más compleja

y dinámica, las organizaciones no pueden depender exclusivamente de un único estándar o marco para garantizar una protección integral. Si bien ISO/IEC 27001 constituye un pilar sólido para la estructuración de un sistema de gestión de seguridad de la información, existen marcos complementarios que permiten reforzar y ampliar su aplicación práctica. Entre estos, destacan particularmente el Marco de Ciberseguridad del NIST versión 2.0 y los enfoques de integración entre estándares, que contribuyen a elevar la madurez y efectividad de los sistemas de seguridad implementados.

2.2.2.3.1. NIST Cybersecurity Framework 2.0. Pascoe et al. (2024) describen que el Marco de Ciberseguridad NIST 2.0 proporciona orientación a la industria, agencias gubernamentales y otras organizaciones para gestionar riesgos de ciberseguridad, incorporando ahora seis funciones principales que incluyen Gobernar como elemento central.

El National Institute of Standards and Technology (NIST) ha actualizado su marco de referencia para la ciberseguridad con el lanzamiento de la versión 2.0, la cual introduce cambios relevantes orientados a una gestión más amplia, estratégica y adaptativa del riesgo cibernético.

Conforme lo que indican Pascoe et al. (2024), la nueva versión hace extensiva su aplicación más allá de la esfera privada, abarcando también agencias públicas, organizaciones sin ánimo de lucro y otros entes que gestionan información sensible en las cuales se produce una digitalización extrema de instrucciones.

Una de las novedades más significativas de esta versión es la inclusión de la "Gobernanza" como la funcionalidad que articula el framework, que se une a las funcionalidades originales: Identifica, Protege, Detecta, Responde y Recupera. La inclusión de esta funcionalidad es muestra de un reconocimiento explícito de que la ciberseguridad debe anudarse a la gobernanza de las organizaciones incorporándose a las decisiones estratégicas, conectando con los objetivos institucionales de una forma transveral. El marco promueve una

visión global del riesgo, la cual va más allá de tratar sólo aspectos técnicos, sino que los incluye también tanto organizacionales, legales y en la cultura (Pascoe et al. 2024).

Este enfoque tiene un valor especial para aquellas organizaciones que, además de su cumplimiento con estándares como ISO/IEC 27001, buscan una herramienta práctica que sea adaptativa y orientada a la mejora continua. El NIST CSF 2.0 sugiere guías establecidas que ayudan a evaluar capacidades actuales, fijar objetivos de mejora y clasificar acciones, lo cual contribuye a dar más fuerza al proceso de toma de decisiones de seguridad digital (Pascoe et al., 2024).

2.2.2.3.2. Integración entre estándares. Jevelin y Faza (2023) Jevelin y Faza (2023) presentan una investigación empírica que provee datos de que los SGSI deben involucrar una medición de la madurez en la forma de índices cuantitativos, accediendo a confirmar que muchas de las organizaciones se encuentran efectivamente en un nivel de madurez mediado entre el I+ y el II, lo que revela déficits para poder cumplir con los requisitos de la obtención de una certificación de tipo ISO 27001.

Pasando del uso enmarcado, muchas organizaciones han realizado una apuesta por una estrategia de integración entre diferentes normas, la que les permite aunarse en algo singular que puede llegar a las necesidades que tienen y a su nivel de madurez organizacional. En esa línea la interrelación entre normas como la ISO 27001, 27005 (gestión de riesgos), COBIT (gobierno de TI), y el propio NIST CSF han demostrado su eficacia en el proceso de construir entornos que sean resilientes y adaptativos frente a unas amenazas emergentes (Pascoe et al., 2024).

Los trabajos que van más allá también evidencian que una gran parte de las organizaciones todavía no están en niveles elevados en la madurez de sus sistemas de seguridad. Usando medidas cuantitativas constataron estos autores que una porción importante de las instituciones analizadas se encuentra en niveles de madurez entre el I+ y el II, lo que revela una

falta de robustez estructural como para llegar a cumplir con los exigentes requisitos de una certificación de tipo ISO/IEC 27001 (Jevelin y Faza, 2023).

Frente a ello, la integración entre marcos y modelos de madurez no solo permite identificar con mayor precisión los puntos críticos de mejora, sino que también proporciona rutas claras y priorizadas para la progresión institucional. Esta estrategia no busca reemplazar un estándar por otro, sino más bien generar sinergias que optimicen recursos, eleven el cumplimiento normativo y fortalezcan la cultura organizacional en torno a la gestión del riesgo informático (Jevelin y Faza, 2023).

2.2.2.4. Características. Para Viteri (2022) existen varios factores que tiene esta normativa cada uno de estos es expuesto de la siguiente manera:

***2.2.2.4.1. Enfoque basado en la gestión de riesgos*.** Una de las características más características que tiene la norma ISO/IEC 27001 es que su estructura está construida a partir de un enfoque en la identificación, análisis y tratamiento del riesgo. Como consecuencia, estas organizaciones deben, previamente a la implantación de cualquier medida de seguridad, ejecutar un proceso riguroso para conocer qué amenazas pueden poner en riesgo los activos de información y en qué probabilidad y gravedad pueden ocurrir. A partir de este diagnóstico, se escogen controles proporcionales y pertinentes que permitan minimizar y/o mitigar dichos riesgos. Este enfoque no propone soluciones genéricas, sino que promueve respuestas adaptadas al contexto específico de cada entidad. Así, no se trata de implementar seguridad por cumplir, sino de asegurar aquello que realmente representa un valor estratégico para la organización, optimizando los recursos disponibles y protegiendo los intereses institucionales de forma eficaz (Culot et al., 2021).

2.2.2.4.2. Ciclo de mejora continua (PHVA). Una de las características más importantes que desarrolla la norma ISO/IEC 27001 es su conexión con el modelo de mejora continua PHVA (Planificar, Hacer, Verificar, Actuar). Esta estructura metodológica es la primera herramienta

que las organizaciones tienen para evitar que su sistema de gestión de seguridad sea un proceso fijo en el tiempo o puntual, sino que evolucione constantemente a partir de los cambios del entorno, de los aprendizajes que va adquiriendo la propia organización y de los avances tecnológicos que puedan surgir. En la etapa de planificar, se definen los objetivos, se detectan los riesgos y se determinan los controles. Después, en la etapa de hacer, se ponen en marcha las medidas que se aplican. En la siguiente etapa, en la etapa de verificar, se monitorizan o se evalúan los resultados obtenidos, para finalmente actuar, en función de la detección de los hallazgos, de mejoras o de correcciones que refuercen el sistema. Este ciclo establece por tanto un aprendizaje organizacional, brindando una cierta resiliencia a la entidad y su capacidad de cambio ante nuevos desafíos (Viteri, 2022).

2.2.2.4.3. Estructura documentada y organizada. ISO/IEC 27001 promueve una gestión sistemática y bien estructurada a través de la documentación formal de políticas, procedimientos, planes y registros. Esto no solo garantiza la trazabilidad de las acciones y decisiones adoptadas, sino que también permite establecer una base de conocimiento que facilita la continuidad operativa, incluso ante cambios de personal o situaciones de crisis. No debiera concebirse la documentación como una carga burocrática, sino como un recurso que avala la coherencia y la fortaleza del sistema de gestión que se pone en práctica. Existe un sentido práctico para la elaboración de cada uno de los documentos que la componen, desde las políticas generales que orientan la actuación que se desarrolla en las instituciones hasta la producción de los registros que dan cuenta del cumplimiento de actividades concretas. Este proceso de trazabilidad tiene un sentido práctico tanto para las auditorias internas como para auditaciones externas y se considera sustentado con el objetivo de dar cuenta de un proceso transparente y de confianza (Viteri, 2022).

2.2.2.4.4. Adaptabilidad a todo tipo de organizaciones. Una característica sumamente valorada de esta norma es su flexibilidad para ser aplicada en organizaciones de cualquier

tamaño, sector o tipo jurídico. Ya sea una entidad gubernamental, una empresa privada, una institución educativa o una ONG, todas pueden adoptar e implementar ISO/IEC 27001 de acuerdo con sus particularidades. Esta adaptabilidad se refleja en la posibilidad de definir el alcance del sistema de gestión, es decir, delimitar qué partes de la organización estarán incluidas, y qué tipo de información será protegida bajo dicho sistema. Esta versatilidad facilita la implementación gradual, permite empezar con áreas prioritarias, y posteriormente extender la cobertura en función de los recursos, capacidades y necesidades institucionales (ISOTools, 2022).

2.2.2.4.5. Reconocimiento internacional y valor estratégico. ISO/IEC 27001 es un estándar ampliamente reconocido en todo el mundo, gracias a su alta respectabilidad y a su seriedad a la hora de mostrar el compromiso con la seguridad de la información. La obtención de la certificación hace ver que se cumplen exigentes estándares, pero desde la propia organización también nos ayuda a tener la imagen de ser una entidad seria y de confianza frente a los socios en la cadena de suministro, frente a los clientes, los proveedores y frente a entes reguladores. El reconocimiento de la obtención de la certificación ISO/IEC 27001 viene a ser una ventaja competitiva en términos de mercados, puesto que, muy a menudo, en el entorno comercial o de cooperación internacional, el tener esta certificación puede ser un criterio necesario para la participación en licitaciones, para la firma de contratos o para entrar en mercados determinados. La ISO/IEC 27001 es, por tanto, una herramienta de posicionamiento estratégico que ayuda a reforzar la reputación institucional y las oportunidades de crecimiento (ISOTools, 2022).

2.2.2.4.6. Participación activa de la alta dirección. Una característica que diferencia esta norma de las demás es que exige un compromiso de la alta dirección de la organización, es decir, no es suficiente con delegar la seguridad de la información a una área técnica; la gerencia o liderazgo superior es responsable de intervenir de manera activa en la definición de políticas,

la asignación de recursos, la evaluación de resultados y las decisiones relacionadas con la seguridad. Este compromiso se traduce en un liderazgo que impulsa una cultura institucional de protección de la información, fomenta la responsabilidad compartida entre todos los miembros del equipo, y asegura que las decisiones estratégicas estén alineadas con la visión y los valores de la organización. Así, la seguridad no se percibe como una carga externa, sino como una parte esencial de la gestión organizacional (ISOTools, 2022).

***2.2.2.4.7. Integración con otros sistemas de gestión*.** El ISO/IEC 27001 está diseñada para integrarse armónicamente con otros sistemas de gestión, como los basados en ISO 9001 (calidad), ISO 14001 (medio ambiente), o ISO 22301 (continuidad del negocio). Esta compatibilidad se debe a que todas estas normas comparten una estructura común basada en el Anexo SL, lo que permite articular políticas, procesos y auditorías de manera coordinada y eficiente. La presente capacidad de integración resulta particularmente interesante para aquellas organizaciones que se encuentran en la búsqueda de la gestión integral, es decir, en la búsqueda de la gestión de la seguridad de la información de manera no aislada sino de una forma totalmente integrada al modelo de gestión institucional. Con ello, se favorece la sinergia entre diferentes áreas e incluso se optimiza la utilización de los recursos humanos, técnicos y financieros (ISOTools, 2022).

2.2.2.5. Desafíos en la adopción de estándares. La investigación de Kamil et al. (2023) revela que la efectividad de las capacidades de resolución de problemas del estándar ha generado interrogantes, llevando al desarrollo continuo de nuevos métodos de gobernanza que demandan enfoques frescos para validar operaciones y medidas de seguridad.

2.2.2.6. Enfoque basado en procesos e integración con otros sistemas de gestión. La norma ISO/IEC 27001 se basa en un enfoque por procesos, lo que implica que la organización debe gestionar sus actividades como un conjunto de procesos interrelacionados que contribuyen al logro de los resultados deseados en cuanto a seguridad de la información. Kitsios et al. (2023)

indican que a partir de este enfoque se puede comprender la seguridad no como una actividad por sí sola, sino como parte de la operación de toda la organización, donde las empresas necesitan integrar más apropiadamente estrategias de seguridad para ser más resilientes a las amenazas cibernéticas. Complementando el enfoque por procesos, Culot et al. (2021) indican que facilita el desarrollo sistemático en la identificación de riesgos y en las medidas de control dentro del entorno organizacional típico. Jevelin y Faza (2023) apuntan aún más a que la gestión por procesos es un concepto de gestión en la norma ISO/IEC 27001 que va siguiendo el ciclo PDCA (Plan-Do-Check-Act), es decir, se establece un ciclo estructurado para poder aplicar la mejora continua en el sistema de gestión la seguridad. Una de las ventajas más importantes que presenta este tipo de estructura es que permite su integración en otras normas internacionales ya que posee la estructura de alto nivel (HLS) en común con otros estándares ISO como los de ISO 9001 (calidad), ISO 14001 (medioambiente) o ISO 22301 (continuidad de negocio) (ISO/IEC, 2022). Kamil et al. (2023) confirman que esta característica de integración permite a las organizaciones elaborar sistemas de gestión que son coherentes ya que abarcan diferentes puntos de vista del riesgo empresarial. La posibilidad de emplear estos sistemas de forma conjunta e integrada permite optimizar recursos y mejorar la eficiencia en la gestión (ISO/IEC, 2022).

2.2.2.7. Ciclo de mejora continua (PDCA). De acuerdo con ISO / IEC (2022), el modelo de mejora continua que se adopta es el del ciclo PDCA (planificar - hacer - verificar - actuar) como es una metodología muy conocida en los sistemas de gestión y busca no sólo alcanzar un nivel de seguridad aceptable, sino mejorarlo de forma continua, el cual se verifica mediante los resultados de auditorías del estado de la seguridad, análisis de riesgos, incidentes o cambios en la organización. Kitsios et al. (2023) afirman que las organizaciones pueden ser más resilientes frente a amenazas de seguridad de la información y ciberataques mediante la integración de estrategias de seguridad gestionadas con éxito mediante ciclos de mejora

continua. Kamil et al. (2023) sostiene que hay un desarrollo continuo de nuevos métodos de gobernanza que demandan enfoques nuevos para validar las operaciones y las medidas de seguridad en el contexto del ciclo PDCA. En el marco de un SGSI, aplicar el ciclo PDCA significa que hay que someter a revisión continua cada etapa del sistema (desde la identificación de riesgos hasta la implementación de controles y la verificación de su efectividad) para poder adaptarse a nuevas amenazas, requisitos legales o cambios tecnológicos. Culot et al. (2021) sostienen que esta aproximación sistemática permite a las organizaciones no sólo cumplir estándares internacionales, sino también mejorar su resiliencia. El ciclo de mejora continua conocido como PDCA constituye la forma más simple de ir mejorando progresivamente el trabajo o la actividad que se está realizando. Primero se empieza por la parte de plan, es decir pensar que se quiere hacer y cómo se quiere hacer; en ocasiones no se tiene todo muy claro. En seguida se pasa a hacer, es decir poner en práctica la parte que se ha pensado aunque puede haber fallos ya que simplemente se está probando. Posteriormente se llega a verificar; es decir ver si lo que se había hecho ha ido bien o no, visto los resultados por comparación de lo que se quería hacer desde un principio. Por último se alcanza a actuar ya que se decidirán los cambios que tiene que haber para mejorar lo que se ha realizado mal o bien para seguir haciendo lo que se hacía bien. Esta es la secuencia que se va repitiendo continuamente y así se va mejorando poco a poco. Es como que cuando uno aprende algo se te puede ir de las manos al principio, pero, a través de la práctica esto va yendo mejor. Este método es importante, ya que ayuda a organizar las ideas y a no quedarse siempre estancado con el mismo error a la hora de intentar una mejora aunque a veces es un poco complicado, al empezar, el modo en que se entiende.

2.2.2.8. Compromiso de la alta dirección. Uno de los principios básicos de la norma es la participación y compromiso de la alta dirección. Kamil et al. (2023) basan su trabajo en la teoría de los grupos de interés para demostrar que el modelo implica la unión de temas empresariales y sociales, investigando cómo las presiones no empresariales pueden modificar

los motivos de los grupos de interés para utilizar estándares. ISO/IEC 27001 obliga a la dirección no solo a aprobar el SGSI sino a liderar la implementación, asignar los recursos, establecer la política de seguridad de la información y garantizar que el sistema esté alineado con los objetivos estratégicos de la organización. Culot et al. (2021) afirman que tras 15 años de investigación académica y práctica, la participación directiva debe considerarse como uno de los aspectos más relevantes a la hora de afrontar las cuestiones de eficacia y validación de los estándares de seguridad de la información. Este modelo exige ir más allá de la concepción tradicional que considera la seguridad de la información como un objeto de la parte técnica y convertirla en un eje transversal de la toma de decisiones empresariales. Kitsios et al. (2023) corroboran que las empresas necesitan dedicarse a garantizar la privacidad, accesibilidad y autenticidad de los datos, lo cual requiere liderazgo comprometido que permita generar una cultura organizacional orientada a la seguridad, involucrando a todo el personal en la protección de los activos informáticos (Viteri, 2022).

2.2.2.9. Requisitos documentales y trazabilidad. Otro aspecto relevante de ISO/IEC 27001 es su exigencia de mantener evidencia documentada de la implementación, operación, seguimiento y mejora del SGSI. Jevelin y Faza (2023) enfatizan que la evaluación de madurez de SGSI mediante enfoques de métodos mixtos requiere documentación sistemática que combine evaluaciones cuantitativas con insights cualitativos derivados de entrevistas y revisiones de literatura. Esto incluye desde la política y los objetivos, hasta los resultados de evaluaciones de riesgos, auditorías internas y acciones correctivas. Los requisitos documentales y la trazabilidad son cosas vitales si se quiere tener un trabajo en orden, aunque a veces no se comprende bien al principio. Los requisitos documentales son todos los documentos y los ficheros para tener la evidencia de que se está llevando a cabo el trabajo bien dicho, ya sea, por ejemplo, normas, registros o informes, aunque se pueden olvidar o tener una escasa cobertura. Por otro lado, trazabilidad sería ir siguiendo el camino de la job (o trabajo en español, pero se

lo ha dejado en inglés) desde el inicio hasta el final, o sea saber qué ha ocurrido, quién ha hecho lo que ha hecho y cuándo, aunque puede hacerse complicado si no hay suficiente control de información. Para mí, esto evita la pérdida de información y permite encontrar errores con mayor facilidad; sirve también para tener más confianza en lo que se hace, ya que todo queda reflejado. En general ambas cosas colaban para que el trabajo fuera más ordenado y más evidente, aunque requiere tiempo y responsabilidad para que se lleven a cabo de la mejor forma posible.

Kamil et al. (2023) señalan que existe un desarrollo continuo de nuevos métodos de gobernanza que demandan enfoques frescos para validar operaciones y medidas de seguridad, lo cual requiere documentación rigurosa. Esta trazabilidad hace posible verificar el cumplimiento que se da en la norma, facilita las auditorías externas a la hora de certificar, y nos ayuda, además, a llevar a cabo una gestión del sistema que sea realmente transparente. Culot et al. (2021), por su parte, enfatizan que la documentación sistemática es imprescindible para avanzar en la investigación que hay en este campo, ya que las sistematizaciones de información van a proporcionar las bases para los trabajos futuros en torno a este tema. A su vez, la mejora de la documentación sistemática hace que se favorezca la rendición de cuentas, la mejora continua, y la gestión del conocimiento en la organización (Viteri, 2022).

2.2.2.10. Importancia: Según Kitsios et al. (2023) hay varios aspectos los cuales son relevantes para la correcta de cualquier metodología, pero estos mismos son expuesto de la siguiente manera:

2.2.2.10.1. Protección eficaz de los activos de información. La primera gran relevancia de la norma ISO/IEC 27001 se encuentra en su capacidad para establecer un entorno seguro que preserve el valor y la integridad de los activos informacionales. Hoy en día, dado que las organizaciones trabajan en entornos provocadores, complejos y altamente conectados, se podría interpretar que la información no sólo es un input poco importante, sino que se ha convertido

en un activo estratégico, de tal forma que si se compromete podría acarrear pérdidas económicas, dañar la reputación y generar responsabilidades. Por todo esto, esta norma permite una manera estructurada de introducir políticas, controles y buenas prácticas que sirvan para impedir accesos no autorizados, evitar alteraciones maliciosas y mermar el riesgo del robo de la información y garantizar la continuidad de los servicios ante un evento que pudiera alterarlos. Su aplicación abarca desde la protección de datos digitales hasta la salvaguarda de documentos físicos, pasando por la defensa de procesos críticos y conocimientos clave que forman parte del capital intangible de la organización. En ese sentido, la ISO/IEC 27001 transforma la gestión de la seguridad de la información en una práctica transversal, preventiva y alineada con los objetivos institucionales (Kitsios, 2023).

2.2.2.10.2. Gestión estructurada del riesgo informático. Una de las mayores fortalezas de ISO/IEC 27001 consiste precisamente en su carácter sistemático a la hora de afrontar el riesgo. Esta norma requiere que las organizaciones abandonen la práctica de trabajar de forma improvisada o reactiva y, en cambio, adopten un modelo de identificar, analizar, evaluar y tratar de forma sistemática los riesgos derivados de la información. Tal forma de proceder escapa a ser simplemente técnica, ya que abarca además un enfoque multidimensional que incluye aspectos operativos, humanos, normativos y reputacionales. De esta manera, dicha metodología garantiza que la decisión que se tome en relación con la seguridad se fundamentará en un diagnóstico realista del contexto organizacional y, por tanto, se podrán asignar recursos de la forma más eficiente, jerarquizar las acciones en función de los niveles de impacto y redactar planes de contingencia específicos para cada unidad o proceso. Esta práctica de evaluación del riesgo, además de llevar necesariamente a que la toma de decisiones sea más racional y anticipativa, contribuye indudablemente a la disminución de aquellas situaciones que podrían poner en peligro la continuidad del negocio o la confianza de los stakeholders (Kitsios, 2023).

2.2.2.10.3. Fortalecimiento de la confianza institucional. ISO/IEC 27001 constituye un aval más que suficiente, con el que ampliar la imagen y la reputación internas de las organizaciones, en un contexto en que las relaciones interpersonales basadas en la confianza son muy necesarias para la operativa del ecosistema grupal. Obtener la certificación significa, en efecto, que una institución tiene medidas de seguridad para proteger la información que maneja, indicando también, en el sentido más amplio del término, que su cultura organizacional se fundamenta en el compromiso ético y responsable por parte de las organizaciones hacia sus grupos de interés: clientes, usuarios, proveedores, inversores y reguladores perciben el estándar como un símbolo y una señal de que la organización es fiable, seria y profesional. Esto se antoja un elemento especialmente importante en contextos muy delicados, como la banca, la salud, la educación o las telecomunicaciones, donde el manejo de la información privada o crítica es el día a día. De este modo, la adopción de ISO/IEC 27001 no solo tiene que ver con mejorar los sistemas internos de protección de la información, sino también con establecer relaciones más consolidadas entre instituciones, definidas por la transparencia, la previsibilidad y el cumplimiento de estándares internacionales (Culot et al., 2021).

2.2.2.10.4. Ventaja competitiva en el mercado. Dentro de un entorno globalizado en el que la competencia también tiene que ver con la capacidad para demostrar un adecuado cumplimiento y seguridad operativa, la certificación ISO/IEC 27001 ha pasado a convertirse en una herramienta diferenciadora de un cierto valor estratégico. Las organizaciones que gozan de esta acreditación multiplican sus posibilidades de crecimiento, en la medida en que pueden acceder a contratos con clientes exigentes, a licitaciones públicas, a generar alianzas a nivel internacional y a explorar nuevos nichos de mercado donde la seguridad de la información sea un prerrequisito imprescindible. Este estándar facilita, además de la mejora de la gestión interna, la presentación de una credencial ante terceros, demostrando que la empresa está preparada para proteger los datos y para gestionar los riesgos de forma profesional. Por tanto,

el decidir adoptar ISO/IEC 27001 va más allá de la mejora de los sistemas de protección, sino que también implica un acortamiento de la distancia a la que se encuentran aquellas empresas competidoras que no cuenten con dicha acreditación y la generación de nuevas oportunidades comerciales relacionadas con unas relaciones interempresariales más estables a largo plazo (Culot et al., 2021).

Progresiva y continua mejora de procesos y controles. La ISO IEC 27001 pone de manifiesto, por tanto, su auténtica filosofía de mejora continua del sistema de gestión para la seguridad de la información. De esta forma, articula el ciclo de mejora continua PHVA (Planificar, Hacer, Verificar y Actuar), a partir del cual se puede verificar que las acciones adoptadas puedan ser sometidas a evaluación, corrección, mejora a lo largo del tiempo. Por lo tanto, la seguridad no se encuentra cautiva en una única auditoría o dentro de un conjunto de procedimientos perfectamente definidos y estables en el tiempo, sino que puede evolucionar al ritmo de la organización, acompañando los cambios tecnológicos, los cambios legislativos u orientándose incluso a nuevas amenazas emergentes. Aprendiendo mediante esa dinámica, las organizaciones pueden también detectar desviaciones en los procesos definidos y aplicar los ajustes adecuados y pertinentes, manteniendo así la eficacia de sus controles y, con ello, la protección de la información, pero al mismo tiempo mejorando la calidad de los procesos organizativos que surgen de la práctica del día a día. De esta forma, la norma se convierte en una herramienta no solo defensiva de la organización, sino también garantizadora de la mejora continua mediante la búsqueda de la innovación como fuente de eficiencia (Culot et al., 2021).

2.2.2.11. Dimensiones Gestión de riesgos: La gestión de riesgos es uno de los fundamentos del Sistema de Gestión de Seguridad de la Información (SGSI), como señala la norma ISO/IEC 27001:2022. Kitsios et al. (2023) describen mediante una evaluación de riesgos, un proceso detallado de identificación de activos, análisis de amenazas y vulnerabilidades, y evaluación de impactos, el cual permite implantar medidas preventivas o

reactivas. Esta norma establece que las organizaciones deben llevar a cabo periodicamente las evaluaciones de riesgos de seguridad de la información o bien cuando se produzcan cambios significativos, de acuerdo con unos criterios previamente definidos por la organización. Jevelin y Faza (2023) añaden que la evaluación de riesgos debe llevarse a cabo mediante un método de combinación de la cuantitativa con la cualitativa, a efectos de generar una evaluación del nivel de madurez, el cual debe verse acompañado de un plan de tratamiento de riesgos documentando los resultados de ambas actividades. Se considera dentro de la gestión, no solo la identificación de amenazas y vulnerabilidades, sino la planificación de acciones preventivas y correctivas a efectos de reducir los impactos de incidentes potenciales. La gestión de riesgos consiste en las dimensiones que desde la óptica de Tang expresarían la ayuda buscada para ayudar a entender los problemas que, por algún motivo, en las organizaciones no se tienen muy claros, e incluso puede llegar a suceder que la explicabilidad de la gestión de riesgos se quiebre en favor de una visión más "intuitiva" y se olvide que la primera dimensión es la "identificación", que busca ser capaz de reconocer qué riesgos existen en la organización. Puede encontrarse que fallas, peligros, etcétera, no son los únicos riesgos sobre los que hablar o, incluso, que se olvidan por completo, ya que no se valoran en su dimensión real. La segunda dimensión de la gestión de riesgos es la "análisis", donde la finalidad es ver cuán grave puede ser ese riesgo y qué comentarios pueden relacionarse con ese riesgo, pero a veces y muchas veces no se da el enfoque en el análisis con la exactitud necesaria. La tercera dimensión es la "evaluación", donde se busca poder determinar cuáles son significativos a la hora de gestionar y, por lo tanto, sobre qué riesgos es mejor hablar. La cuarta dimensión está relacionada con el "tratamiento de los riesgos", donde se busca una posible forma para evitar o reducir dicho riesgo, ya sea haciendo cambios, implementando medidas (controles), etcétera. La quinta y última dimensión relacionada con la gestión de riesgos es el "seguimiento", donde se busca medir si las medidas implantadas tienen efecto y si no surgen nuevas problemáticas. A pesar de la descripción que

he ido dando y dando de las dimensiones que conforman la gestión de riesgos, no es sencillo explicarlas tal cual se hace aquí y luego, además, ser capaz de aplicarlas correctamente en la práctica (ISO/IEC, 2022).

Seguridad operativa. De acuerdo a la norma ISO/IEC 27001, la seguridad de las operaciones, está relacionada con la planificación, implementación y control de todos los procesos que se requieren para satisfacer los requisitos del SGSI. Kamil et al. (2023) indican que se deben aplicar medidas específicas de seguridad requeridas por el contexto operativo en el que se quieren gestionar los activos de la información. Eso implica definir criterios para los procesos, hacer que los servicios externos relevantes estén controlados y gestionar los cambios que se deban hacer (planificados o no) y que puedan afectar la seguridad. Culot et al. (2021) subrayan que la seguridad operativa debe ser capaz de integrar enfoques técnicos, organizacionales y gerenciales, y la organización debe asegurarse de que los controles técnicos y administrativos se apliquen sistemáticamente y sean coherentes con las acciones que se pueden obtener del análisis de riesgo. La seguridad operativa es como el cuidado que se tiene al realizar las actividades diarias que se desarrollan en una empresa con el fin de evitar problemas o accidente, de ahí que muchas veces no se le presupuesta gran importancia. Es el trabajar de una forma ordenada y segura, utilizando las herramientas del mejor modo posible, siguiendo las reglas básicas aunque no todos las lleven a cabo. También protege la información, los equipos, de cualquier modo que puedan dañarse o perderse datos importantes. Pueden colar errores de descuido o de no revisar antés las cosas, por esto hay que estar atentos. La seguridad operativa facilita que todas las actividades que se realizan en la empresa vayan mejor y con menos riesgos aunque requiere de la responsabilidad de las personas que en ella trabajan. En general, es algo simple de entender pero no siempre fácil de poner en práctica bien en el día a día (ISO/IEC, 2022).

Desempeño operativo. De acuerdo con la norma ISO/IEC 27001, el rendimiento del SGSI se analiza mediante el seguimiento, la medición, el análisis y la evaluación del comportamiento de los procesos. Jevelin y Faza (2023) afirman que la madurez del SGSI puede evaluarse en niveles I+ a II, mostrando déficits respecto a los objetivos de ISO 27001 y con una necesidad de seguimiento, lo que implica determinar qué hay que monitorear, qué procedimientos se emplean, con qué frecuencia y quién se va a encargar de esta tarea. Kitsios et al. (2023) subrayan que las empresas deben analizar las causas que les llevan a invertir en ISO 27001 y las motivaciones que nacen de esta evaluación. Por otro lado, las evidencias documentadas de los resultados deben de ser mantenidas. Esta labor también forma parte del ciclo de mejora continua (PDCA) que vigila la eficacia de los controles y la consecución de los objetivos que se han establecido en el marco de la seguridad de la información. El examen del rendimiento operativo sirve para evidenciar cómo está funcionando una organización o un trabajo en el día a día, aunque no siempre haya indicadores claros para ello. Consiste en revisar si se están realizando las tareas de la manera adecuada, es decir, de manera correcta, rápida y sin errores, aunque en la práctica no siempre se consigan todos los objetivos a la vez. También concierne al uso que se hace de los recursos, como el tiempo, el dinero y los materiales, tratando de que no se derrochen, aunque en la práctica, sí pudiera ser que así fuera. El rendimiento operativo a veces se ve perjudicado si hay desorganización, o mala comunicación entre el personal, o si las personas no están bien formadas. Por eso también hace falta observar de qué modo se están llevando a cabo las cosas, así como buscar modos de mejorar gradualmente. También se pueden tener algunos indicadores o fórmulas sencillas para evidenciar si se está avanzando o no; el buen rendimiento operativo ayuda a que una empresa funcione mejor, a conseguir las metas más fácilmente y a tener menos problemas. Sin embargo, no siempre es fácil mantener el rendimiento operativo, ya que pueden aparecer obstáculos inesperados. En

general lo que queda claro es que es algo importante, pero que necesita del esfuerzo constante para así poder mejorar con el tiempo (ISO/IEC, 2022).

2.2.3. Identificación de la variable dependiente

- Seguridad de los sistemas de información

2.2.4. Conceptualización de la variable dependiente

La seguridad de los sistemas de información se define como cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática, cuyos efectos puedan conllevar daños sobre la información, comprometer su confidencialidad, autenticidad o integridad, disminuir el rendimiento de los equipos o bloquear el acceso de usuarios autorizados al sistema (Samaniego y Ponce, 2021).

2.2.4.1. Definición de la variable seguridad de los sistemas de información: Conforme a la evolución que ha sufrido el concepto de seguridad en sistemas de información, se ha pasado de una mirada técnica con el foco en el estudio y la aplicación de herramientas, procedimientos y reglas de funcionamiento hacia una aproximación más holística que acoge procesos, recursos humanos y gestión de la organización. Dependiendo del foco o interés del texto de que se trate se pueden encontrar distintas aproximaciones al término.

Samaniego y Ponce (2021) muestran el enfoque funcional/operativo de la seguridad, desde el cual afirman que cualquier medida que se lleve a cabo para impedir, en un sistema, que se lleve a cabo una operación no autorizada tiene que, de tal forma, evitar causar daños en los datos e intentar ajustarse a su comportamiento que presidió el funcionamiento de un sistema; el cual sólo asegura ciertos atributos como la confidencialidad, autenticidad e integridad. Además, identifican consecuencias prácticas, como la degradación del rendimiento o el bloqueo de accesos, lo cual sitúa la seguridad como un componente crítico del funcionamiento del sistema informático.

Vega (2021) por su parte, incorpora un enfoque metodológico, al considerar que la seguridad está compuesta por procesos, buenas prácticas y metodologías que buscan evitar accesos, usos o modificaciones no autorizadas. Su definición trasciende lo técnico, y reconoce que la protección de los sistemas se logra mediante estructuras organizadas de control y monitoreo continuo

Por último, Pozo et al. 2025 presentan una mirada estratégica y del sistema, incluyendo estándares, recursos informáticos, humanos y educativos dentro de la gestión de la seguridad, entendiendo que el factor humano y la cultura organizativa son elementos imprescindibles para que cualquier estrategia de protección sea eficaz. En conjunto, las definiciones ofrecen una idea de seguridad en los sistemas de información que va más allá de los elementos tecnológicos, requiriendo una gestión entre procesos, personas y tecnología. Esto refuerza su papel como eje transversal en la gestión moderna de la información.

2.2.4.2. Características. Según Vega (2021) existen varios aspectos que se deben evaluar dentro de este proceso cada uno de estos es explicado de la siguiente manera:

***2.2.4.2.1. Confidencialidad de la información*.** Uno de los pilares esenciales de la seguridad en los sistemas de información es la confidencialidad, la cual garantiza que los datos solo sean accesibles para personas, sistemas o entidades autorizadas. Este rasgo tiene como objetivo evitar que personas ajenas puedan acceder, escuchar o dar a conocer información sensible. La confidencialidad no se refiere únicamente a información financiera o datos de carácter personal, sino que pone el acento en la información contractual, técnica o estratégica de la que una organización determinada dispone A través de métodos como el cifrado de datos, la autenticación mediante credenciales, el control de accesos o la división de redes podemos garantizar la confidencialidad, es decir, la capacidad de proteger y unos datos en cuanto a su carácter secreto o privado, evitando fugas, espionaje industrial o abusos de cualquier naturaleza que puedan ocasionar efectos en el ámbito económico o legal (Pozo et al., 2025).

***2.2.4.2.2. Integridad de los datos*.** La integridad constituye una propiedad básica de un sistema de información seguro, ya que se ocupa de que los datos permanezcan intactos, completos y sin alteraciones durante todo su vida útil. Es decir, que la información no deba ser modificada de forma no autorizada, accidental o maliciosa una vez que ha sido almacenada o transmitida. La alteración de un único dato por insignificante que pueda parecernos puede influir negativamente en los procedimientos operativos, en la toma de decisiones a nivel directivo e incluso en los informes financieros. Por este motivo, se utilizan técnicas tales como sumas de verificación (checksums) y firmas digitales, así como mecanismos de control de versiones; además se utilizan bitácoras de auditoría que detecten y corrigen cualquier intento de modificación non sanctum. La integridad, en definitiva, contempla una información confiable, exacta y consistente, tanto en origen como en destino. Esto implica que los datos tienen que ser potencialmente completos, no tener partes que falten y no llegar a ser alterados, ya sea por error, o por permisos de no autorizados. Durante el tiempo, los datos pueden ser recibidos, almacenados, manipulado, etc. y todo el tiempo es esperable que continúen igual, pero también pueden ser susceptibles de ser dañados. Por esta razón, se dice que la integridad es la propiedad primigenia de la seguridad de la información, puesto que permite confiar en que los datos son realmente de confianza. Sin integridad, la posible validez de la información puede llegar a perder toda su validez o puede llegar a generar problemas al tomar algún tipo de decisión. Como conclusión, cuidar la integridad de la información es necesario pero no siempre es sencillo lograrlo de forma adecuada (Pozo et al., 2025).

***2.2.4.2.3. Disponibilidad del sistema y los datos*.** La disponibilidad corresponde a la disponibilidad de que los sistemas, las aplicaciones, los dispositivos y la información estén disponibles en el instante que los usuarios que tienen acceso a la misma hagan uso de ellos, es decir, que exista continuidad en su uso e interacción para evitar situaciones que provoquen la interrupción o espera innecesaria para la finalización de un requerimiento. En las

organizaciones, la disponibilidad tiene especial importancia para disponer de un servicio en operación asociando que la continuidad operacional de la organización equivalente a la estabilidad de sus sistemas y a que los datos siempre estarán disponibles para su consulta, procesamiento o almacenamiento. La disponibilidad implica tener planes de operaciones, copias de seguridad, sistemas redundantes y la posibilidad de recuperación ante desastres (DRP), además de que no solo necesitan de la tecnología de la información y su infraestructura, sino también de unos procesos organizativos operativos bien establecidos. Si la disponibilidad se pierde por ataques como el ransomware o por fallos eléctricos, la organización podría perder dinero, podría ser penalizada e incluso podría perder su buena reputación organizacional. Garantizar la disponibilidad implica que la organización esté en marcha en todo momento. La disponibilidad del sistema y los datos es muy importante porque la información y los programas se puedan utilizar de forma natural cuando se necesiten, aunque de vez en cuando esta no es la situación. Esto significa que, siguiendo el principio anterior, el sistema debe funcionar en la mayor parte del tiempo posible, no debe haber caídas o fallos que eviten el acceso. La capacidad de disponibilidad también involucra que los datos estén guardados en un modo en que sean recuperables de forma rápida, aun cuando puedan existir problemas como cortes de luz, fallos preparados o errores del ser humano. La ausencia de buen seguimiento de la disponibilidad hace que la gente no puede trabajar bien y provoca paradas o pérdidas. Por este motivo, la disponibilidad debe incluir algunas medidas de ahorro de datos o revisiones, aunque muchas veces no es posible hacerlo muy bien. En términos generales, la disponibilidad es el modo en el que los sistemas están disponibles ininterrumpidamente, pero necesita mucha dedicación y labores continuas (Samaniego y Ponce, 2021).

2.2.4.2.4. Autenticación y control de acceso. Otra característica crucial dentro de la seguridad de los sistemas de información es la implementación de mecanismos de autenticación y control de accesos, los cuales permiten verificar la identidad de los usuarios y determinar qué

acciones están autorizados a realizar dentro del sistema. Estos controles aseguran que solo las personas con permisos específicos puedan acceder a determinada información o ejecutar funciones clave. Las herramientas de autenticación incluyen desde contraseñas robustas hasta métodos más avanzados como la biometría, tokens o la autenticación multifactor (MFA). Por su parte, los sistemas de control de acceso definen reglas que limitan la visualización, edición, eliminación o exportación de datos según el rol del usuario. Gracias a esta característica, se reduce el riesgo de accesos indebidos, errores humanos y brechas de seguridad derivadas del mal uso interno de los sistemas. La autenticación es el proceso que permite comprobar que una persona es quien dice ser (a través de una contraseña, un código o incluso una huella), pero muchas veces se suelen utilizar claves sencillas o se comparten, lo que puede dar lugar a un conflicto. Luego, se sitúa el control de acceso, el cual determina qué cosas se podrán hacer por dicha persona en el sistema (desde únicamente visualizar información como poder modificarla) pero hay que tener en cuenta que la asignación de permisos muchas veces no se realiza correctamente. Esto permite evitar que personas que no debieran entrar o bien realizar cambios erróneos en los datos. No obstante, pueden suceder errores por no revisar de manera habitual o bien, y de no asociar reglas a ello. En lo general, la autenticación y control de acceso es aquello que nos permite seguir las reglas y que exista la seguridad pero que requiere cuidado, responsabilidad y buena organización para que finalmente se ejecute cómo debería (Samaniego y Ponce, 2021).

2.2.4.2.5. Trazabilidad y registro de actividades. La trazabilidad, también conocida como auditoría o rastreo, es una propiedad que permite seguir el rastro de todas las actividades realizadas dentro de un sistema de información, registrando quién hizo qué, cuándo lo hizo y desde qué ubicación o dispositivo. Este seguimiento se considera un aspecto fundamental a tomar en consideración a la hora de poder detectar las irregularidades, así como, analizar los incidentes de seguridad y reconstruir los eventos ante situaciones en las que exista alguna

sospecha. Gracias a los registros de actividad (logs), a las bitácoras, a las auditorías que se pueden implementar se puede llevar un control lo más detallado posible sobre el uso que se realiza en el sistema, facilitando la identificación de los fallos, de los accesos poco habituales y de las modificaciones no autorizadas. Esta cualidad permite dejar la forma transparente de las operaciones llevadas a cabo, así como, establecer responsabilidades en caso de que les suceda algo. Por esta razón, en esta forma, la trazabilidad no solo ayuda a la prevención sino que también ayuda a investigar y responder rigurosamente cuando hay situaciones críticas (Vega, 2021).

2.2.4.3. Objetivos clave de la Seguridad de la Información. Los objetivos principales de la seguridad de la información tradicionalmente están organizados en torno a la famosa triada de la seguridad: confidencialidad, integridad y disponibilidad. La confidencialidad es una propiedad que garantiza que solo las personas con autorización accedan a la información, previniendo la fuga de la misma o el espionaje de datos confidenciales. La integridad es la propiedad que asegura que los datos se mantengan en su forma correcta, completa y no alterada por personas no autorizadas. La disponibilidad, por su parte, es la propiedad que permite el acceso a la información y los sistemas de información a los usuarios legítimos en el momento en que lo necesiten con el fin de minimizar la interrupción. Además, podríamos sumar otros como la autenticidad, que garantiza la identidad de las personas que acceden a la información, y el no repudio, que es la propiedad que impide negar la autoría de las acciones de un usuario en los sistemas. Estos principios son fundamentales para que los procesos digitales sean confiables, verificables y seguros (Pozo et al., 2025)**.**

2.2.4.4. Beneficios de Implementar un SGSI. Un Sistema de Gestión de Seguridad de la Información (SGSI) es una estructura formal basada en normas internacionales como la ISO/IEC 27001, que permite a las organizaciones identificar, gestionar y minimizar los riesgos relacionados con la información (Samaniego y Ponce, 2021). Su implementación ofrece

múltiples beneficios: fortalece la protección de datos sensibles, reduce la probabilidad de incidentes de seguridad y permite una respuesta más eficiente ante estos. Además, mejora la reputación institucional al demostrar compromiso con la seguridad, facilita el cumplimiento normativo y contractual, y optimiza procesos mediante el uso racional de los recursos tecnológicos y humanos (Pozo et al., 2025)

2.2.4.5. Fundamentos estratégicos de la Seguridad de los Sistemas de Información. La protección de los sistemas de información está basada en un conjunto de principios estratégicos que van desde la gestión de riesgos hasta la aplicación de controles técnicos y organizacionales. La gestión de riesgos implica identificar activos críticos, analizar las amenazas y vulnerabilidades, evaluar los impactos y establecer medidas preventivas y reactivas. Los controles pueden ser físicos (por ejemplo, accesos restringidos a las salas de servidores), lógicos (como firewalls o antivirus), organizativos (páginas de política y normas internas) o técnicos (ejemplo: cifrado, con herramientas y procesos: auditoría, etc.). La auditoría es otro de los pilares estratégicos que permite, de un modo explícito, revisar la efectividad de las medidas aplicadas e identificar oportunidades de mejora. Contar con políticas suficientes y procedimientos adecuados, también garantizará que el resto de los empleados de la organización tenga claro su papel en la protección de la información (Pozo et al., 2025)**.**

2.2.4.6. Áreas de aplicación y enfoques relevantes. La seguridad de los sistemas de información se extiende a diferentes aspectos, los cuales requieren de tratamientos diferentes en función del tipo de activo a proteger, por ejemplo, dentro la red se hace uso de hardware y tecnología como son cortafuegos (firewalls), sistemas de detección de intrusos (IDS), redes privadas virtuales (VPN) y protocolos seguros como SSL/TLS. La seguridad del software se centra en la evitación de vulnerabilidades comunes en las cuales han de tenerse en cuenta errores de programación, desbordamientos de búfer o configuraciones inadecuadas. La seguridad física se ocupa de proteger los espacios donde se ubica el hardware informático

mediante métodos como el control del acceso físico, la videovigilancia y la protección ambiental. La formación del personal y la sensibilización sobre ciberseguridad también son elementos clave en la prevención de ataques en los que se aplican técnicas de ingeniería social, que tienden a explotar el elemento humano como punto de fallo dentro de la cadena de seguridad (Samaniego y Ponce, 2021).

2.2.4.7. Importancia de la Seguridad de los Sistemas de Información. La seguridad de los sistemas de información es un elemento primordial para cualquier organización moderna, principalmente en virtud del papel central que juega la información a partir de la cual es posible llevar a cabo desde la toma de decisiones hasta las operaciones ordinarias pasando por la planificación estratégica. A medida que los sistemas de información continúan interconectándose y digitalizándose, también se les hace frente a motivos de riesgo permanente (como por ejemplo, ataques cibernéticos, pérdida de información, acceso no autorizado a computadoras, fallos provocados por software y tecnología, etc.) que conductan desde la posible interrupción operativa hasta consecuencias en el plano legal y económico, así como también a posibles sanciones penales, morales e, incluso, por parte de las sociedades de seguros. Por lo tanto, la seguridad de los sistemas de información no solo protege a los activos informáticos sino que, también, trata de salvaguardar o de conservar la confianza de los clientes, socios y empleados, y es una parte crucial del mantenimiento del negocio (continuidad) y de las ventajas competitivas en la economía de hoy en día (Samaniego y Ponce, 2021)**.**

2.2.4.8. Dimensiones: Confidencialidad. Según Vega (2021), la confidencialidad hace referencia a la capacidad de proteger los datos de accesos no autorizados, siendo un componente necesario de la privacidad. Esta dimensión implica que solo personas con la debida autorización puedan acceder a la información. La confidencialidad puede verse comprometida por situaciones como la pérdida de dispositivos con información, el espionaje físico o ataques cibernéticos tipo “Man in the Middle”. Por su parte, Samaniego y Ponce (2021) complementa

que esta dimensión se asegura mediante mecanismos como autenticación de usuarios, gestión de privilegios y cifrado de información, permitiendo que los datos sean accesibles únicamente por quienes tienen los derechos correspondientes.

Integridad: Vega Briceño (2021) expone que la integridad está relacionada con la capacidad de los sistemas para evitar que los datos se modifiquen de forma no autorizada o indeseada. Esto implica proteger la exactitud y consistencia de la información tanto en almacenamiento como en transmisión. La integridad se mantiene mediante sistemas de control de acceso, permisos de modificación y mecanismos de reversión de cambios no deseados. A su vez Samaniego y Ponce (2021), añade que la información íntegra es aquella completa y sin corrupción, y que para mantenerla es necesario aplicar políticas de auditoría, control de cambios y copias de seguridad, debido a amenazas como virus informáticos o errores humanos.

Disponibilidad: Vega (2021) define la disponibilidad como la capacidad de acceder a la información en el momento necesario. Esta dimensión puede verse afectada por interrupciones en la cadena de comunicaciones, fallos del sistema o ataques como los de denegación de servicio (DoS). Su objetivo es asegurar que los usuarios autorizados puedan acceder a los datos cuando lo requieran. Complementariamente Samaniego y Ponce (2021) señala que la disponibilidad se logra mediante medidas como copias de seguridad, balanceadores de tráfico, acuerdos de niveles de servicio y recursos alternativos, para garantizar que ni siquiera ante fallas críticas se pierda el acceso a la información.

2.3. Definición de términos básicos

2.3.1. Activos de información

Son todos los elementos que tienen valor para una organización y que deben ser protegidos. Incluyen datos, documentos, sistemas, bases de datos, software, hardware y hasta el conocimiento de los empleados.

2.3.2. Amenaza

Cualquier evento potencial intencionado o accidental que pueda afectar negativamente los sistemas de información. Las amenazas pueden ser naturales (como un terremoto), humanas (un ciberataque) o técnicas (una falla de hardware).

2.3.3. Incidente de seguridad

Suceso que compromete, o tiene el potencial de comprometer, la seguridad de la información. Incluye filtraciones de datos, accesos no autorizados, o interrupciones del servicio.

2.3.4. Política de seguridad

Documento formal que define las normas, objetivos y responsabilidades en relación con la protección de la información dentro de una organización. Actúa como guía para el comportamiento esperado en el uso de los sistemas.

2.3.5. Control de acceso

Conjunto de mecanismos que restringen el acceso a información o recursos, permitiendo solo el uso por parte de usuarios autorizados. Incluye contraseñas, tarjetas, biometría y sistemas de roles.

2.3.6. Gestión de incidentes

Conjunto de procesos para identificar, analizar, responder y recuperarse de eventos que afectan la seguridad de la información, con el fin de minimizar su impacto y evitar recurrencias.

CAPÍTULO III

METODOLOGÍA DE LA INVESTIGACIÓN

3.1. Tipo, nivel y diseño de investigación

3.1.1. Tipo de investigación

Este estudio adoptó el tipo de investigación aplicada. De acuerdo con Hadi et al. (2023), la investigación aplicada se fundamenta en la investigación básica o pura, utilizando teorías existentes para abordar problemas prácticos. Esta modalidad se basó en los hallazgos y soluciones previas, con el objetivo de resolver problemas concretos. Habitualmente, este tipo de investigación se aplica en campos como la medicina o la ingeniería, donde la teoría se utiliza para generar soluciones prácticas y aplicables.

3.1.2. Nivel de investigación

El nivel de investigación fue explicativo. Según Hinojosa et al. (2024), la investigación explicativa tiene como objetivo identificar y esclarecer las causas y consecuencias de un fenómeno específico. En este tipo de investigación, se manipula una variable independiente para analizar cómo influye sobre una variable dependiente, con el fin de entender mejor el impacto de la intervención sobre el fenómeno estudiado.

3.1.3. Diseño de investigación

El diseño fue no experimental, de corte longitudinal con alcance panel. Este diseño consiste en observar y medir las variables en su contexto natural, sin manipulación por parte del investigador, recolectando datos de manera repetida en múltiples momentos del tiempo (90 observaciones diarias por cada sistema). Según Supo y Zacarías (2024) este diseño es apropiado para estudios explicativos observacionales donde se busca analizar la relación e influencia entre variables sin intervención, pero con seguimiento temporal de las mismas.

La investigación se representa en el siguiente esquema:

Control Net = $M_1 \rightarrow O_{1\ 1}\ O_{1\ 1} \rightarrow O_{1\ 2}\ O_{1\ 2} \ldots\ldots\ldots\ldots\ldots\ O_{1\ 90}\ O_{1\ 90}$

NubeFact = $M_2 \rightarrow O_{2\,1}\ O_{1\,1} \rightarrow O_{2\,2}\ O_{2\,2}$……. $O_{2\,90}\ O_{2\,90}$

Cognos = $M_3 \rightarrow O_{3\,1}\ O_{3\,1} \rightarrow O_{3\,2}\ O_{3\,2}$……. $O_{3\,90}\ O_{3\,90}$

Citrix = $M_4 \rightarrow O_{4\,1}\ O_{4\,1} \rightarrow O_{4\,2}\ O_{4\,2}$……. $O_{4\,90}\ O_{4\,90}$

Siam = $M_5 \rightarrow O_{5\,1}\ O_{5\,1} \rightarrow O_{5\,2}\ O_{5\,2}$……. $O_{5\,90}\ O_{5\,90}$

M_1, M_2, M_3, M_4, M_5: Los cinco sistemas de información de Inversiones RMK

O_{iy}: Observación diaria del cumplimiento de criterios ISO/IEC 27001 en el sistema i durante el día j y de la seguridad del sistema de información i durante el día j

i: Sistema evaluado (1 = Control Net, 2 = NubeFact, 3 = Cognos, 4 = Citrix, 5 = Siam)

j: Día de observación (1 al 90)

→: Observación longitudinal sin manipulación

3.2. Población, muestra y muestreo

3.2.1. Descripción de la población

La población de este estudio estuvo constituida por los cinco (5) sistemas de información operativos de la empresa Inversiones RMK, los cuales fueron evaluados en el contexto de la implementación de los controles de seguridad establecidos por la norma ISO/IEC 27001. La investigación llevó a cabo una revisión a estos sistemas de información, estudiando algunos aspectos como las políticas de seguridad, los procedimientos de operación, los registros de incidentes y los planes de respuesta a los incidentes, que son claves para evaluar la eficacia de los controles establecidos por la norma ISO/IEC 27001. En el caso de Hadi et al. (2023), la población de estudio es el conjunto de elementos o unidades de análisis de las que se pretende obtener información y datos relevantes.

3.2.2. Selección de la muestra

La muestra del estudio consistió en los cinco (5) sistemas de información operativos de la empresa, los cuales están directamente involucrados en la implementación y aplicación de los controles de seguridad según la norma ISO/IEC 27001. No se realizó el proceso de muestreo

de individuos, sino que se trabajó con los sistemas como unidades de análisis. Los sistemas seleccionados son los más representativos en cuanto a la seguridad de la información y la gestión de riesgos.

3.2.3. Tipo de muestreo

El muestreo utilizado fue censal, seleccionando los cinco (5) sistemas de información operativos de la empresa que están directamente involucrados en la aplicación de la norma ISO/IEC 27001. Esto permitió una evaluación completa y detallada de los sistemas clave y sus respectivos controles de seguridad, sin realizar un proceso de selección de muestra.

3.3. Técnicas e instrumentos de recolección de datos

3.3.1. Técnica

Esta investigación utilizó dos técnicas de recolección de datos: la observación y el análisis documental. La observación se empleó con la finalidad de conocer de forma directa cómo se ejecutan las políticas de seguridad recogidas bajo la norma ISO/IEC 27001 dentro de la organización en la cotidianidad, observando comportamientos y procesos asociados con la seguridad de los sistemas de información. El análisis documental, por otra parte, habilitó el estudio de los documentos relevantes generados durante un período de tiempo que es de 90 días, los cuales eran, entre otros, las políticas, los procedimientos, los informes de auditoría y los registros de los incidentes. Esta técnica proporcionó una visión clara sobre cómo se ha implementado la norma ISO/IEC 27001 y su efectividad en la mejora de la seguridad de la información en la empresa.

3.3.2. Instrumento

En cuanto a los instrumentos la Ficha de Observación se usó para registrar las observaciones directas durante el proceso de observación. Incluyó detalles como la fecha, hora, y contexto de la observación, además de los comportamientos observados relacionados con los tres pilares de la seguridad (confidencialidad, integridad y disponibilidad). Se hicieron

observaciones complementarias para el cumplimiento de las políticas de seguridad y cualquier aspecto que deba ser mejorado.

La Ficha de Análisis Documental se aplicó a los documentos generados durante los 90 días y apuntó la siguiente información: título, fecha de emisión, responsable del documento, se verificó la conformidad con la norma ISO/IEC 27001 y se realizó un resumen, se identificaron las áreas de mejora para cumplir con los controles de la seguridad que se determinan para esta norma.

3.4. Aplicación de instrumentos de evaluación, tabulación y procesamiento

El proceso de recolección de datos se llevó a cabo durante 90 días consecutivos, del [fecha inicio] al [fecha fin], mediante observación diaria estructurada. Se utilizaron dos técnicas de manera simultánea:

a) Observación directa: Se aplicó diariamente una ficha de observación (Anexo C) para registrar el comportamiento de cada sistema de información en relación con los controles establecidos por la norma ISO/IEC 27001 y los indicadores de seguridad. Cada ficha fue diligenciada por el investigador al final de la jornada laboral, consolidando las incidencias y el desempeño observado durante las últimas 24 horas.

b) Análisis documental: Paralelamente, se revisaron los registros generados por cada sistema (logs, reportes de incidentes, bitácoras de acceso, respaldos) para contrastar y complementar la información obtenida mediante observación directa. Esta técnica permitió validar la ocurrencia de eventos y el cumplimiento de procedimientos operativos.

Procedimiento de registro:

Cada día, para cada uno de los cinco sistemas operativos (S1 al S5), se aplicó una ficha de observación que contenía 30 ítems distribuidos en tres dimensiones de la variable independiente (gestión de riesgos, seguridad operativa, desempeño operativo) y tres dimensiones de la variable dependiente (confidencialidad, integridad, disponibilidad).

Los ítems fueron de naturaleza dicotómica (1 = Sí/Cumple/Seguro; 0 = No/No cumple/Inseguro), registrando la condición observada durante el día.

Se completaron un total de 450 fichas de observación (5 sistemas × 90 días), generando una base de datos con 450 registros y 30 variables cada uno.

Tabulación y procesamiento:

Los datos fueron organizados en una hoja de cálculo (Anexo F) y posteriormente exportados al software estadístico R Studio para su procesamiento. Se realizó un análisis descriptivo de frecuencias y porcentajes por cada ítem y por cada sistema. Para la contrastación de hipótesis, se aplicó un modelo de regresión lineal simple, dado que se buscaba determinar la influencia de la variable independiente (cumplimiento de ISO/IEC 27001) sobre la variable dependiente (seguridad de los sistemas de información) y sus dimensiones.

Previamente al análisis inferencial, se evaluó la confiabilidad del instrumento mediante el coeficiente Kuder-Richardson 20 (KR-20), obteniendo valores de 0.878 para la variable independiente y 0.83 para la variable dependiente, lo que indica una consistencia interna buena. Asimismo, se verificaron los supuestos de normalidad mediante la prueba de Kolmogorov-Smirnov y los supuestos de regresión a través del paquete gvlma en R.

3.5. Ética investigativa

El estudio se llevó a cabo respetando los principios éticos establecidos en el Código de Ética en la Investigación de la Universidad para el Desarrollo Andino (UDEA). Se garantizo que todos los participantes proporcionen su consentimiento libre, previo e informado antes de participar en el estudio, tal como se establece en el Artículo 9 del código. Además, se aseguró la confidencialidad de la información y el anonimato de los participantes, protegiendo sus derechos en todo momento.

El estudio también se regio por principios de honestidad intelectual y responsabilidad. Se garantizo la veracidad y transparencia en la recolección y análisis de los datos, reconociendo

adecuadamente las contribuciones de todos los involucrados. Además, se tomó en cuenta el principio precautorio, minimizando cualquier riesgo para los participantes y maximizando los beneficios del estudio.

Todo el proceso fue supervisado por el Comité de Ética en la Investigación de la UDEA, que garantizará que se cumplan todas las normativas éticas necesarias. Cualquier conflicto de interés fue declarado de manera transparente para asegurar la imparcialidad y la integridad del estudio.

CAPÍTULO IV

RESULTADOS Y DISCUSIONES

4.1. Resultados

4.1.1. Confiabilidad del instrumento

Se empleó el coeficiente Kuder-Richardson 20 (KR-20) para evaluar la consistencia interna del cuestionario aplicado, dado que los ítems fueron de naturaleza dicotómica. Este coeficiente permite determinar qué tan homogéneas son las preguntas dentro de un mismo constructo. Un valor de KR-20 superior a 0.70 se considera indicativo de una confiabilidad aceptable.

ISO/IEC 27001

Tabla 1

Tabla de interpretación del coeficiente de Kuder-Richardson 20

Coeficiente KR-20	Intensidad de la Consistencia Interna
$\alpha \geq 0.90$	Excelente
$0.80 \leq \alpha < 0.90$	Buena
$0.70 \leq \alpha < 0.80$	Aceptable
$0.60 \leq \alpha < 0.70$	Cuestionable
$\alpha < 0.60$	Inaceptable

Fuente. Kuder y Richardson (1937). The theory of the estimation of test reliability. Psychometrika.

Tabla 2

Estadísticas de fiabilidad de la variable ISO/IEC 27001

Coeficiente KR-20	N de elementos
0.878	15

Fuente. Elaboración Propia (2025)

Interpretación: El coeficiente KR-20 representa la consistencia interna del cuestionario considerando todas las preguntas en conjunto. En este caso, el valor es 0.878, lo cual indica una consistencia interna buena en el instrumento para la variable ISO/IEC 27001.

Seguridad de los sistemas de información

Tabla 3

Estadísticas de fiabilidad de la variable seguridad de los sistemas de información

Coeficiente KR-20	N de elementos
0.83	15

Fuente. Elaboración Propia (2025)

Interpretación: El coeficiente KR-20 representa la consistencia interna del cuestionario considerando todas las preguntas en conjunto. En este caso, el valor es 0.83, lo cual indica una consistencia interna buena en el instrumento para la variable Seguridad de los sistemas de información.

4.1.2. Análisis de datos cuantitativos

A) Variable ISO/IEC 27001

Tabla 4

¿Se ejecutaron las evaluaciones de riesgo programadas para hoy?

	Sistemas				
	S1 N = 90 (20%)	S2 N = 90 (20%)	S3 N = 90 (20%)	S4 N = 90 (20%)	S5 N = 90 (20%)
Respuesta					
No	34 (38%)	30 (33%)	26 (29%)	38 (42%)	28 (31%)
Si	56 (62%)	60 (67%)	64 (71%)	52 (58%)	62 (69%)

Fuente. Elaboración Propia (2025)

Figura 1

¿Se ejecutaron las evaluaciones de riesgo programadas para hoy?

Fuente. Elaboración Propia (2025)

Interpretación: Para la variable ISO/IEC 27001, figura 1, la tabla muestra que, según el sistema evaluado, entre 58 y 71 de las encuestas se respondió con “Sí/Cumple”, mientras que aproximadamente entre 29 y 42 se indicó “No/No cumple”. En conjunto, estos resultados evidencian que la mayoría de los participantes percibe que el requisito de la pregunta 1 se cumple en los sistemas evaluados, aunque permanece un porcentaje no desdeñable de respuestas de no cumplimiento. Esto sugiere que, si bien existe un nivel de alineación importante con la norma ISO/IEC 27001 en este aspecto específico, aún hay brechas de implementación que deberían ser atendidas para lograr un cumplimiento más homogéneo y robusto en todos los sistemas.

Tabla 5

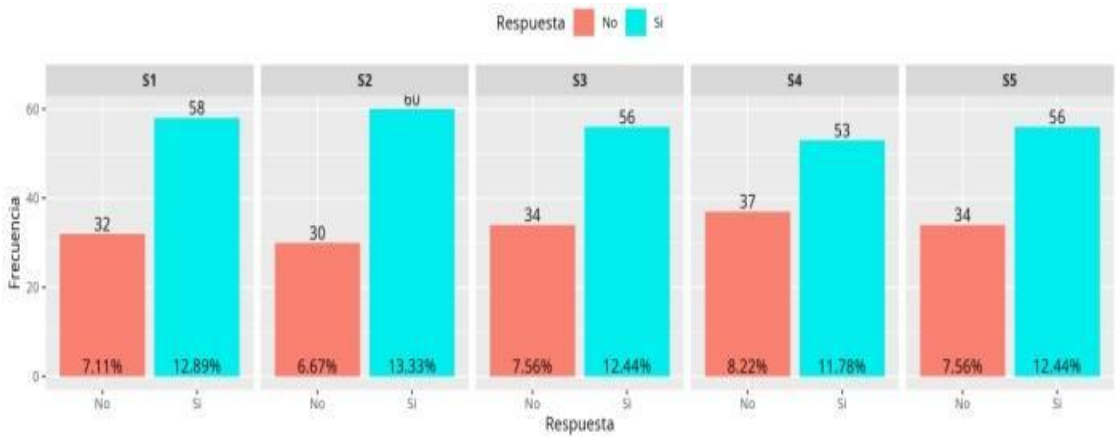
¿Los controles de riesgo funcionaron sin incidencias?

	Sistemas				
	S1 N = 90 (20%)	S2 N = 90 (20%)	S3 N = 90 (20%)	S4 N = 90 (20%)	S5 N = 90 (20%)
Respuesta					
No	32 (36%)	30 (33%)	34 (38%)	37 (41%)	34 (38%)
Si	58 (64%)	60 (67%)	56 (62%)	53 (59%)	56 (62%)

Fuente. Elaboración Propia (2025)

Figura 2

¿Los controles de riesgo funcionaron sin incidencias?



Fuente. Elaboración Propia (2025)

Interpretación: En la figura 2 de la variable ISO/IEC 27001, los resultados muestran que, en todos los sistemas evaluados, la opción “Sí/Cumple” se mantiene por encima del 59,

alcanzando valores entre 59 y 67, mientras que las respuestas “No/No cumple” fluctúan entre aproximadamente 33 y 41. Esto indica que la mayoría de los encuestados percibe que el requisito evaluado en la pregunta 2 se cumple, aunque cerca de un tercio a poco más de dos quintas partes aún reporta no cumplimiento. En consecuencia, se observa un nivel de cumplimiento globalmente favorable, pero con espacios de mejora importantes para fortalecer la implementación del control correspondiente en todos los sistemas y reducir la proporción de respuestas negativas.

Tabla 6

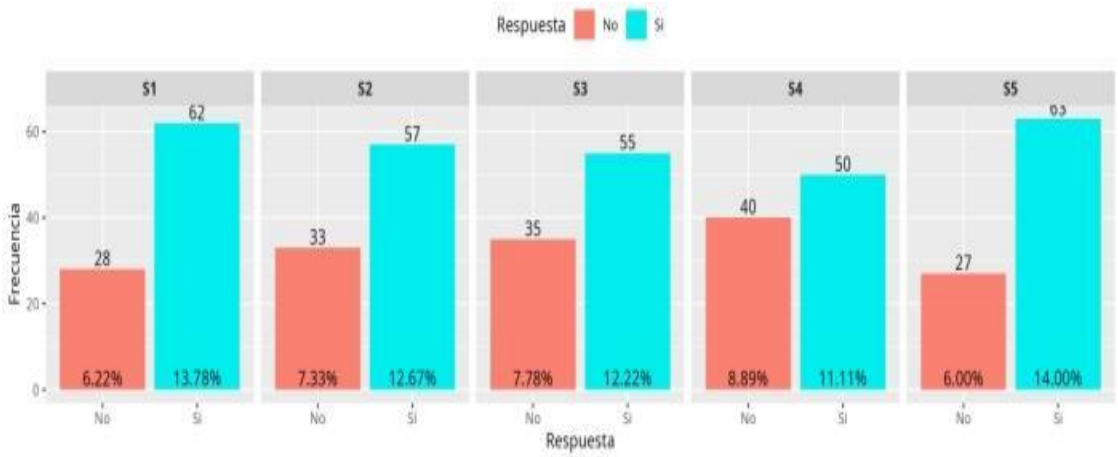
¿Se registraron y trataron adecuadamente los nuevos riesgos identificados?

	Sistemas				
	S1 N = 90 (20%)	S2 N = 90 (20%)	S3 N = 90 (20%)	S4 N = 90 (20%)	S5 N = 90 (20%)
Respuesta					
No	28 (31%)	33 (37%)	35 (39%)	40 (44%)	27 (30%)
Si	62 (69%)	57 (63%)	55 (61%)	50 (56%)	63 (70%)

Fuente. Elaboración Propia (2025)

Figura 3

¿Se registraron y trataron adecuadamente los nuevos riesgos identificados?



Fuente. Elaboración Propia (2025)

Interpretación: En la figura 3 de la variable ISO/IEC 27001, los resultados muestran que la alternativa “Sí/Cumple” oscila aproximadamente entre 56 y 70 en los distintos sistemas (S1–S5), mientras que la opción “No/No cumple” se sitúa entre 30 y 44. En términos generales, esto

evidencia que la mayoría de los encuestados considera que el requisito de la pregunta 3 se cumple, manteniéndose proporciones de cumplimiento relativamente altas en todos los sistemas. No obstante, el porcentaje de respuestas de no cumplimiento, que llega a superar el 40 en uno de los sistemas, refleja la existencia de brechas relevantes en la aplicación homogénea del control, por lo que aún se requiere fortalecer las prácticas asociadas a este aspecto de la norma ISO/IEC 27001.

Tabla 7

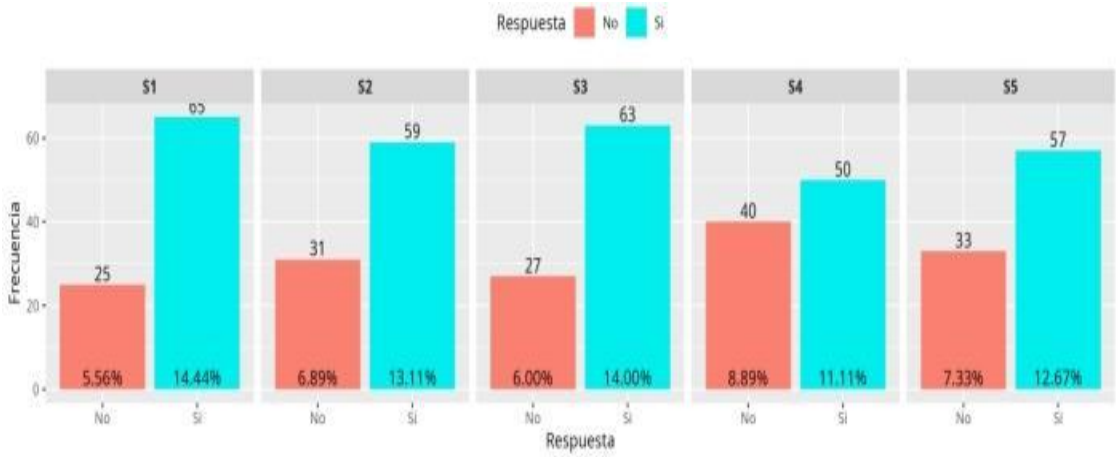
¿Las políticas de seguridad estuvieron disponibles y accesibles?

	Sistemas				
	S1 N = 90 (20%)	S2 N = 90 (20%)	S3 N = 90 (20%)	S4 N = 90 (20%)	S5 N = 90 (20%)
Respuesta					
No	25 (28%)	31 (34%)	27 (30%)	40 (44%)	33 (37%)
Si	65 (72%)	59 (66%)	63 (70%)	50 (56%)	57 (63%)

Fuente. Elaboración Propia (2025)

Figura 4

¿Las políticas de seguridad estuvieron disponibles y accesibles?



Fuente. Elaboración Propia (2025)

Interpretación: En la figura 4 de la variable ISO/IEC 27001, se observa que la opción "Sí/Cumple" presenta proporciones que varían aproximadamente entre 56 y 72 en los distintos sistemas, mientras que la alternativa "No/No cumple" se sitúa entre 28 y 44. En conjunto, estos resultados indican un nivel de cumplimiento mayoritario respecto del requisito evaluado en la

pregunta 4, ya que en todos los sistemas más de la mitad de los encuestados declara que dicho control se cumple. Sin embargo, la presencia de hasta alrededor de cuatro de cada diez respuestas de no cumplimiento en algunos sistemas pone de manifiesto desigualdades en la implementación del control, lo que sugiere la necesidad de reforzar las acciones de mejora para lograr una aplicación más consistente de lo establecido por la norma ISO/IEC 27001.

Tabla 8

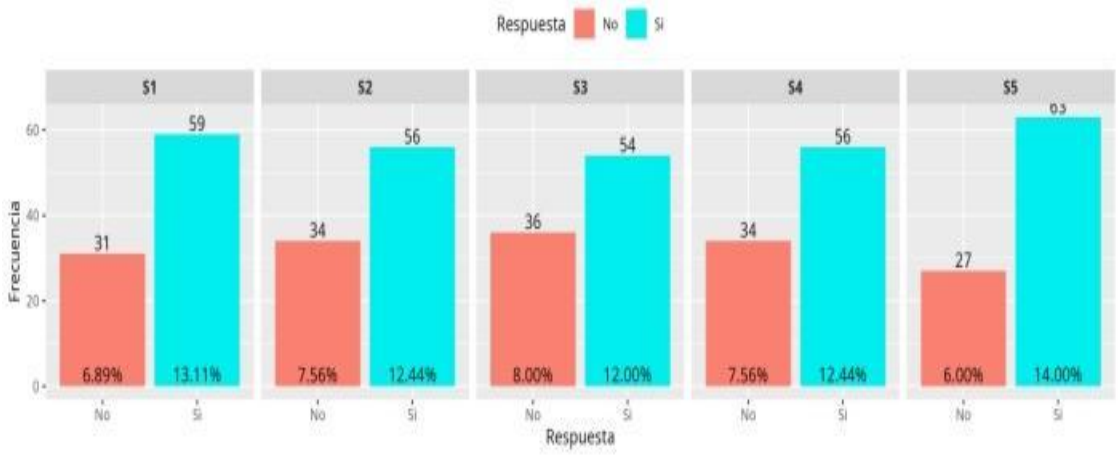
¿Se cumplieron los procedimientos operativos de seguridad establecidos?

	Sistemas				
	S1 N = 90 (20%)	S2 N = 90 (20%)	S3 N = 90 (20%)	S4 N = 90 (20%)	S5 N = 90 (20%)
Respuesta					
No	31 (34%)	34 (38%)	36 (40%)	34 (38%)	27 (30%)
Si	59 (66%)	56 (62%)	54 (60%)	56 (62%)	63 (70%)

Fuente. Elaboración Propia (2025)

Figura 5

¿Se cumplieron los procedimientos operativos de seguridad establecidos?



Fuente. Elaboración Propia (2025)

Interpretación: En la figura 5 de la variable ISO/IEC 27001, la alternativa “Sí/Cumple” alcanza proporciones que oscilan aproximadamente entre 60 y 70 en los distintos sistemas, mientras que las respuestas “No/No cumple” se sitúan entre 30 y 40. Estos resultados muestran que la mayoría de los encuestados percibe que el requisito evaluado en la pregunta 5 se cumple en los sistemas analizados, lo que evidencia un nivel de cumplimiento globalmente favorable.

Sin embargo, el hecho de que alrededor de tres a cuatro de cada diez participantes señalen no cumplimiento revela que aún persisten brechas importantes en la aplicación uniforme del control, por lo que se recomienda fortalecer las acciones orientadas a consolidar el cumplimiento de este aspecto específico de la norma ISO/IEC 27001.

Tabla 9

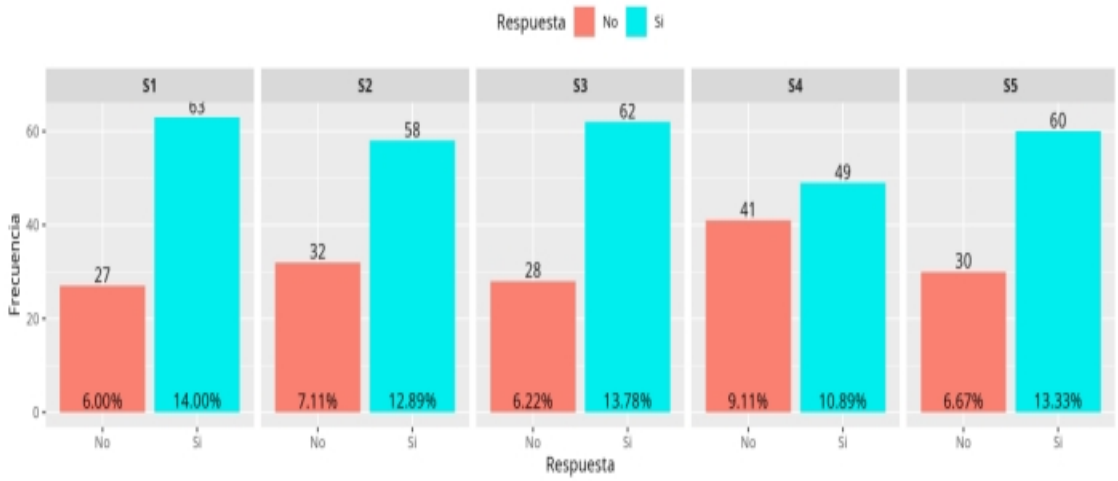
¿Los procedimientos de acceso funcionaron correctamente?

	Sistemas				
	S1 N = 90 (20%)	S2 N = 90 (20%)	S3 N = 90 (20%)	S4 N = 90 (20%)	S5 N = 90 (20%)
Respuesta					
No	27 (30%)	32 (36%)	28 (31%)	41 (46%)	30 (33%)
Si	63 (70%)	58 (64%)	62 (69%)	49 (54%)	60 (67%)

Fuente. Elaboración Propia (2025)

Figura 6

¿Los procedimientos de acceso funcionaron correctamente?



Fuente. Elaboración Propia (2025)

Interpretación: En la figura 6 de la variable ISO/IEC 27001, la opción “Sí/Cumple” presenta proporciones que fluctúan aproximadamente entre 54 y 70 en los distintos sistemas, mientras que la alternativa “No/No cumple” se ubica entre 30 y 46. En términos generales, esto evidencia que la mayoría de los encuestados considera que el requisito evaluado en la pregunta 6 se cumple, lo que refleja un nivel de cumplimiento predominantemente favorable. No obstante, el hecho de que en algunos sistemas cerca de la mitad o más de un tercio de los

participantes señale no cumplimiento pone de manifiesto brechas significativas en la implementación homogénea del control, por lo que resulta necesario reforzar las medidas orientadas a consolidar este aspecto específico de la norma ISO/IEC 27001 en todos los sistemas.

Tabla 10

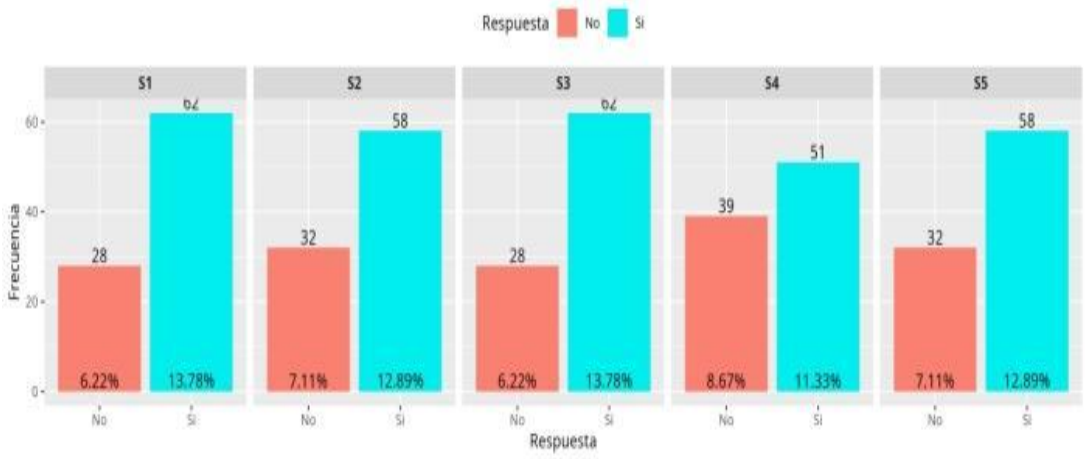
¿El cifrado de datos críticos estuvo operativo?

	Sistemas				
	S1 N = 90 (20%)	S2 N = 90 (20%)	S3 N = 90 (20%)	S4 N = 90 (20%)	S5 N = 90 (20%)
Respuesta					
No	28 (31%)	32 (36%)	28 (31%)	39 (43%)	32 (36%)
Si	62 (69%)	58 (64%)	62 (69%)	51 (57%)	58 (64%)

Fuente. Elaboración Propia (2025)

Figura 7

¿El cifrado de datos críticos estuvo operativo?



Fuente. Elaboración Propia (2025)

Interpretación: En la figura 7 de la variable ISO/IEC 27001, se observa que la alternativa "Sí/Cumple" alcanza proporciones que oscilan aproximadamente entre 57 y 69 en los distintos sistemas, mientras que las respuestas "No/No cumple" se sitúan entre 31 y 43. En conjunto, estos resultados indican un nivel de cumplimiento mayoritario respecto del requisito evaluado en la pregunta 7, ya que en todos los sistemas más de la mitad de los encuestados señala que dicho control se cumple. Sin embargo, la presencia de hasta alrededor de cuatro de cada diez

respuestas de no cumplimiento revela brechas relevantes en la aplicación uniforme del control, lo que sugiere la necesidad de fortalecer las acciones orientadas a estandarizar y consolidar este aspecto específico de la norma ISO/IEC 27001 en todos los sistemas.

Tabla 11

¿Los sistemas antimalware estuvieron actualizados y funcionando?

	Sistemas				
	S1 N = 90 (20%)	S2 N = 90 (20%)	S3 N = 90 (20%)	S4 N = 90 (20%)	S5 N = 90 (20%)
Respuesta					
No	25 (28%)	38 (42%)	29 (32%)	33 (37%)	31 (34%)
Si	65 (72%)	52 (58%)	61 (68%)	57 (63%)	59 (66%)

Fuente. Elaboración Propia (2025)

Figura 8

¿Los sistemas antimalware estuvieron actualizados y funcionando?

Fuente. Elaboración Propia (2025)

Interpretación: En la figura 8 de la variable ISO/IEC 27001, la alternativa “Sí/Cumple” alcanza proporciones que fluctúan aproximadamente entre 58 y 72 en los distintos sistemas, mientras que la opción “No/No cumple” se sitúa entre 28 y 42. Estos resultados muestran que la mayoría de los encuestados percibe que el requisito evaluado en la pregunta 8 se cumple en los sistemas analizados, lo que refleja un nivel de cumplimiento globalmente favorable. No obstante, la presencia de hasta algo más de cuatro de cada diez respuestas de no cumplimiento en uno de los sistemas evidencia desigualdades en la implementación del control, por lo que se

recomienda reforzar las acciones orientadas a lograr una aplicación más homogénea y consistente de este aspecto específico de la norma ISO/IEC 27001.

Tabla 12

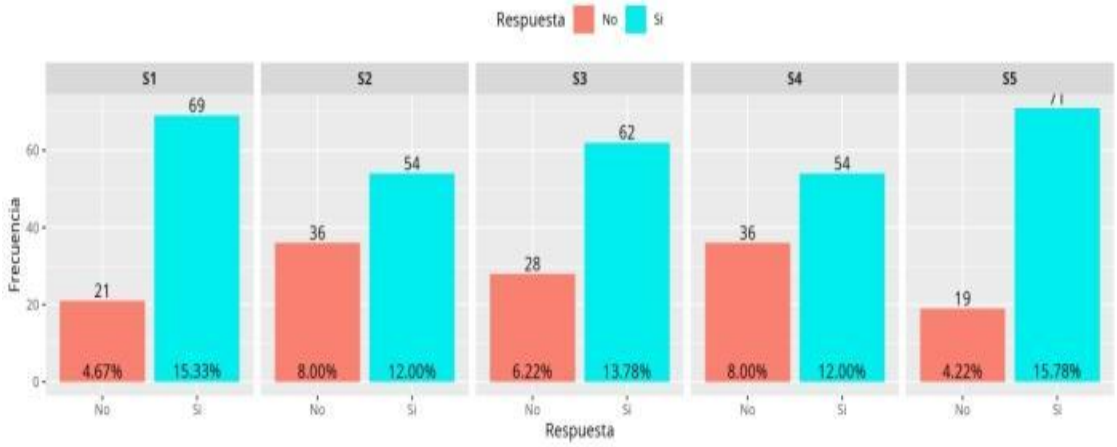
¿Se gestionaron adecuadamente los incidentes ocurridos?

	Sistemas				
	S1 N = 90 (20%)[1]	S2 N = 90 (20%)[1]	S3 N = 90 (20%)[1]	S4 N = 90 (20%)[1]	S5 N = 90 (20%)[1]
Respuesta					
No	21 (23%)	36 (40%)	28 (31%)	36 (40%)	19 (21%)
Si	69 (77%)	54 (60%)	62 (69%)	54 (60%)	71 (79%)

Fuente. Elaboración Propia (2025)

Figura 9

¿Se gestionaron adecuadamente los incidentes ocurridos?



Fuente. Elaboración Propia (2025)

Interpretación: En la figura 9 de la variable ISO/IEC 27001, la opción “Sí/Cumple” alcanza proporciones que oscilan aproximadamente entre 60 y 79 en los distintos sistemas, mientras que las respuestas “No/No cumple” se sitúan entre 21 y 40. En términos generales, esto refleja un nivel de cumplimiento elevado del requisito evaluado en la pregunta 9, dado que en todos los sistemas la mayoría de los encuestados indica que el control se cumple. Sin embargo, la presencia de hasta cuatro de cada diez respuestas de no cumplimiento en algunos sistemas evidencia que aún existen brechas en la aplicación uniforme del control, por lo que

resulta pertinente implementar acciones de mejora orientadas a reducir estas discrepancias y consolidar el cumplimiento del lineamiento correspondiente de la norma ISO/IEC 27001.

Tabla 13

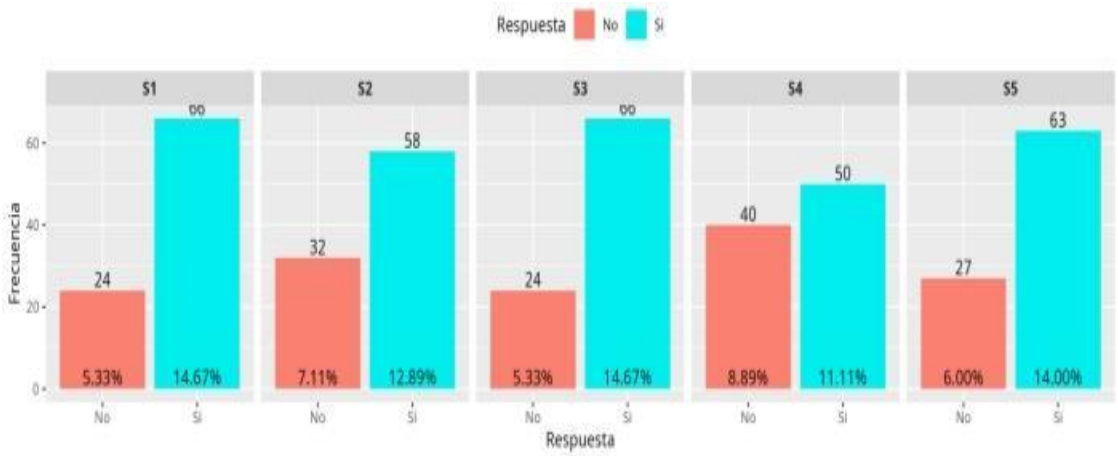
¿Los controles de acceso físico y lógico funcionaron sin fallas?

	Sistemas				
	S1 N = 90 (20%)[1]	S2 N = 90 (20%)[1]	S3 N = 90 (20%)[1]	S4 N = 90 (20%)[1]	S5 N = 90 (20%)[1]
Respuesta					
No	24 (27%)	32 (36%)	24 (27%)	40 (44%)	27 (30%)
Si	66 (73%)	58 (64%)	66 (73%)	50 (56%)	63 (70%)

Fuente. Elaboración Propia (2025)

Figura 10

¿Los controles de acceso físico y lógico funcionaron sin fallas?



Fuente. Elaboración Propia (2025)

Interpretación: En la figura 10 de la variable ISO/IEC 27001, la alternativa “Sí/Cumple” presenta proporciones que fluctúan aproximadamente entre 56 y 73 en los distintos sistemas, mientras que las respuestas “No/No cumple” se sitúan entre 27 y 44. En conjunto, estos resultados evidencian un nivel de cumplimiento mayoritariamente favorable respecto del requisito evaluado en la pregunta 10, ya que en todos los sistemas más de la mitad de los encuestados declara que el control se cumple. No obstante, la presencia de hasta casi la mitad de respuestas de no cumplimiento en uno de los sistemas muestra brechas importantes en la aplicación homogénea del control, lo que sugiere la necesidad de reforzar las acciones de

mejora para asegurar una implementación más consistente de este lineamiento de la norma ISO/IEC 27001 en todos los sistemas.

Tabla 14

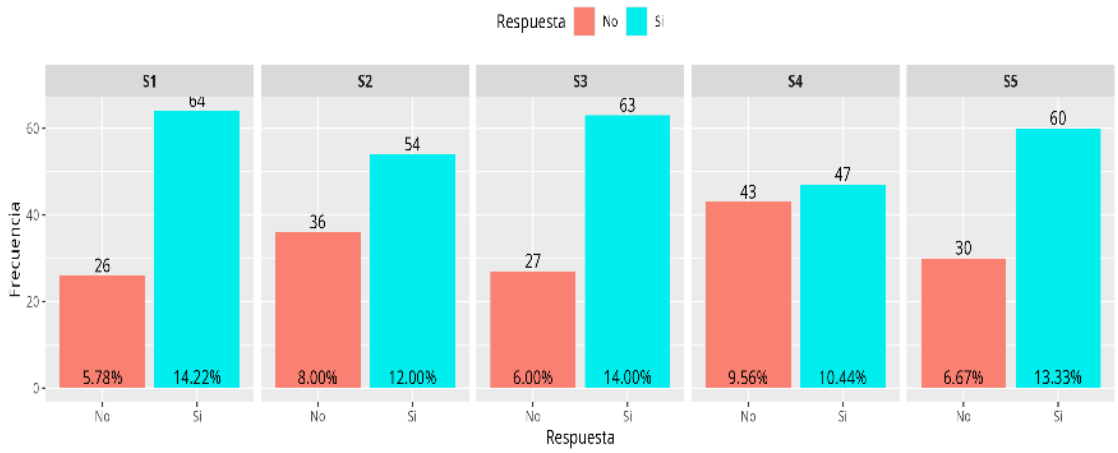
¿Se ejecutaron las actividades de monitoreo programadas?

	Sistemas				
	S1 N = 90 (20%)[1]	S2 N = 90 (20%)[1]	S3 N = 90 (20%)[1]	S4 N = 90 (20%)[1]	S5 N = 90 (20%)[1]
Respuesta					
No	26 (29%)	36 (40%)	27 (30%)	43 (48%)	30 (33%)
Si	64 (71%)	54 (60%)	63 (70%)	47 (52%)	60 (67%)

Fuente. Elaboración Propia (2025)

Figura 11

¿Se ejecutaron las actividades de monitoreo programadas?



Fuente. Elaboración Propia (2025)

Interpretación: En la figura 11 de la variable ISO/IEC 27001, la alternativa “Sí/Cumple” alcanza proporciones que oscilan aproximadamente entre 52% y 71% en los distintos sistemas, mientras que las respuestas “No/No cumple” se sitúan entre 29% y 48%. En términos generales, estos resultados evidencian que la mayoría de los encuestados considera que el requisito evaluado en la pregunta 11 se cumple, aunque en algunos sistemas el cumplimiento apenas supera la mitad de las respuestas. La presencia de hasta casi la mitad de participantes que reportan no cumplimiento revela brechas significativas en la implementación uniforme del control, lo que sugiere la necesidad de fortalecer las acciones correctivas y de seguimiento para

asegurar una aplicación más consistente de este aspecto específico de la norma ISO/IEC 27001 en todos los sistemas.

Tabla 15

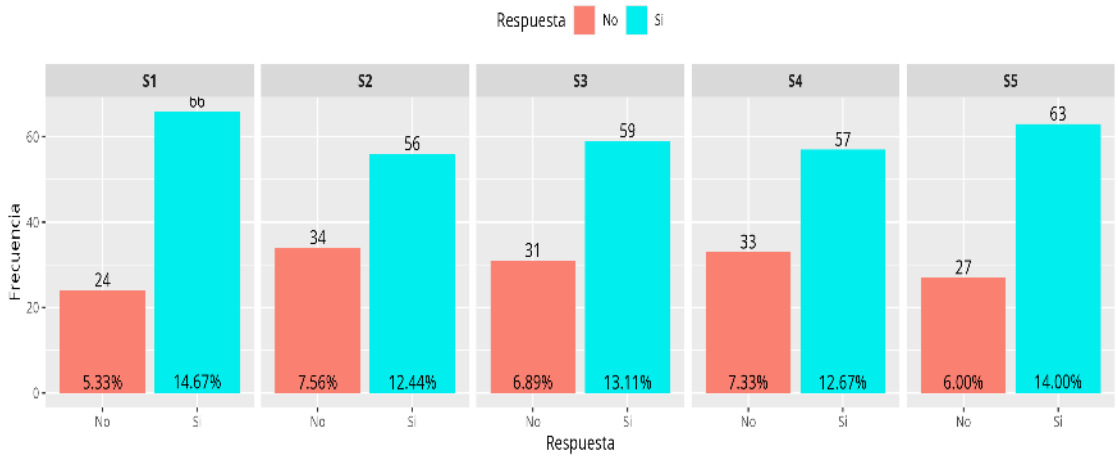
¿Los indicadores de desempeño se midieron según cronograma?

	Sistemas				
	S1 N = 90 (20%)[1]	S2 N = 90 (20%)[1]	S3 N = 90 (20%)[1]	S4 N = 90 (20%)[1]	S5 N = 90 (20%)[1]
Respuesta					
No	24 (27%)	34 (38%)	31 (34%)	33 (37%)	27 (30%)
Si	66 (73%)	56 (62%)	59 (66%)	57 (63%)	63 (70%)

Fuente. Elaboración Propia (2025)

Figura 12

¿Los indicadores de desempeño se midieron según cronograma?



Fuente. Elaboración Propia (2025)

Interpretación: En la figura 12 de la variable ISO/IEC 27001, la alternativa “Sí/Cumple” presenta proporciones que fluctúan aproximadamente entre 62% y 73% en los distintos sistemas, mientras que las respuestas “No/No cumple” se sitúan entre 27% y 38%. En conjunto, estos resultados evidencian un nivel de cumplimiento mayoritariamente favorable del requisito evaluado en la pregunta 12, dado que en todos los sistemas más de la mitad de los encuestados indica que el control se cumple. Sin embargo, la presencia de cerca de un tercio de respuestas de no cumplimiento en varios sistemas muestra que aún existen brechas en la implementación homogénea del control, por lo que se recomienda reforzar las acciones orientadas a consolidar este aspecto específico de la norma ISO/IEC 27001 en todos los sistemas.

Tabla 16

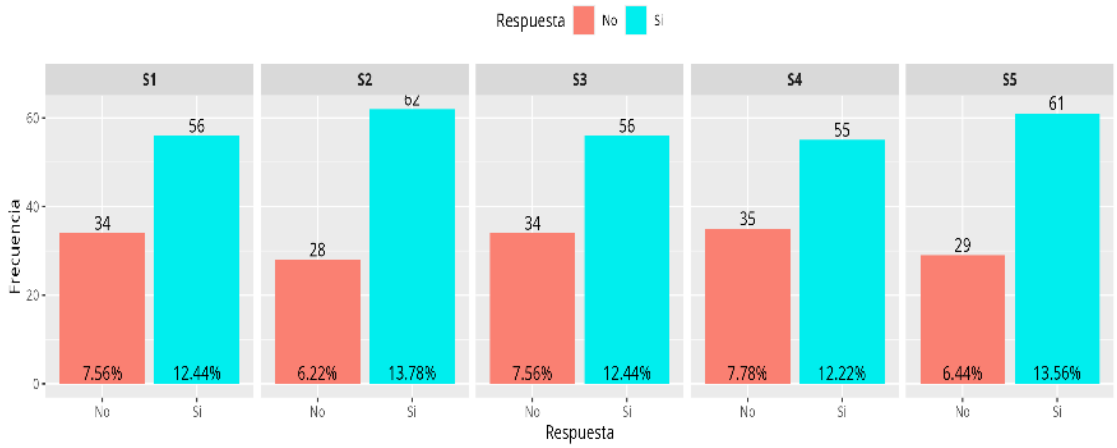
¿Se documentaron las no conformidades identificadas?

	Sistemas				
	S1 N = 90 (20%)[1]	S2 N = 90 (20%)[1]	S3 N = 90 (20%)[1]	S4 N = 90 (20%)[1]	S5 N = 90 (20%)[1]
Respuesta					
No	34 (38%)	28 (31%)	34 (38%)	35 (39%)	29 (32%)
Si	56 (62%)	62 (69%)	56 (62%)	55 (61%)	61 (68%)

Fuente. Elaboración Propia (2025)

Figura 13

¿Se documentaron las no conformidades identificadas?



Fuente. Elaboración Propia (2025)

Interpretación: En la figura 13 de la variable ISO/IEC 27001, la alternativa “Sí/Cumple” alcanza proporciones que oscilan aproximadamente entre 61% y 69% en los distintos sistemas, mientras que las respuestas “No/No cumple” se sitúan entre 31% y 39%. En términos generales, estos resultados muestran un nivel de cumplimiento predominantemente favorable del requisito evaluado en la pregunta 13, dado que en todos los sistemas la mayoría de los encuestados declara que el control se cumple. No obstante, el hecho de que alrededor de tres a casi cuatro de cada diez participantes reporten no cumplimiento indica la existencia de brechas relevantes en la aplicación uniforme del control, lo que sugiere la necesidad de fortalecer las medidas de mejora continua para asegurar una implementación más consistente de este aspecto de la norma ISO/IEC 27001.

Tabla 17

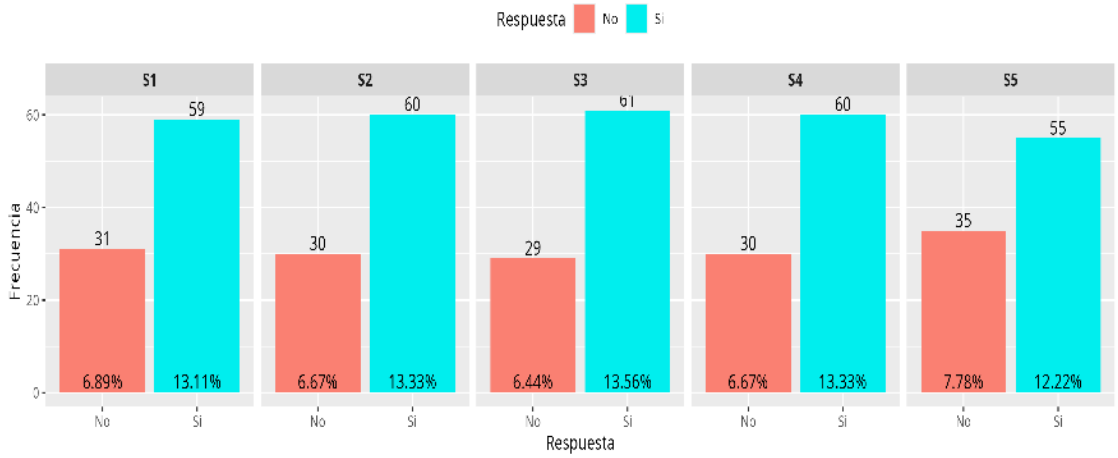
¿Se implementaron las acciones correctivas planificadas?

	Sistemas				
	S1 N = 90 (20%)[1]	S2 N = 90 (20%)[1]	S3 N = 90 (20%)[1]	S4 N = 90 (20%)[1]	S5 N = 90 (20%)[1]
Respuesta					
No	31 (34%)	30 (33%)	29 (32%)	30 (33%)	35 (39%)
Si	59 (66%)	60 (67%)	61 (68%)	60 (67%)	55 (61%)

Fuente. Elaboración Propia (2025)

Figura 14

¿Se implementaron las acciones correctivas planificadas?



Fuente. Elaboración Propia (2025)

Interpretación: En la figura 14 de la variable ISO/IEC 27001, la alternativa “Sí/Cumple” presenta proporciones que fluctúan aproximadamente entre 61% y 68% en los distintos sistemas, mientras que las respuestas “No/No cumple” se ubican entre 32% y 39%. En conjunto, estos resultados evidencian un nivel de cumplimiento mayoritariamente favorable del requisito evaluado en la pregunta 14, dado que en todos los sistemas más de la mitad de los encuestados señala que el control se cumple. Sin embargo, el hecho de que cerca de un tercio a casi cuatro de cada diez participantes manifieste no cumplimiento indica la presencia de brechas importantes en la aplicación homogénea del control, por lo que se recomienda reforzar las acciones de mejora para consolidar este aspecto específico de la norma ISO/IEC 27001 en todos los sistemas.

Tabla 18

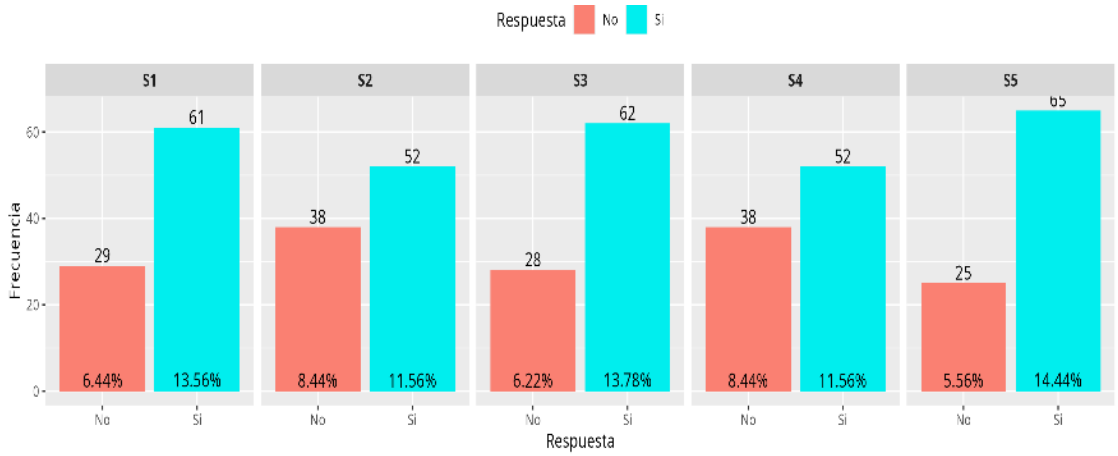
¿Los procesos de mejora continua estuvieron activos?

	Sistemas				
	S1 N = 90 (20%)[1]	S2 N = 90 (20%)[1]	S3 N = 90 (20%)[1]	S4 N = 90 (20%)[1]	S5 N = 90 (20%)[1]
Respuesta					
No	29 (32%)	38 (42%)	28 (31%)	38 (42%)	25 (28%)
Si	61 (68%)	52 (58%)	62 (69%)	52 (58%)	65 (72%)

Fuente. Elaboración Propia (2025)

Figura 15

¿Los procesos de mejora continua estuvieron activos?



Fuente. Elaboración Propia (2025)

Interpretación: En la figura 15 de la variable ISO/IEC 27001, la alternativa “Sí/Cumple” alcanza proporciones que oscilan aproximadamente entre 58% y 72% en los distintos sistemas, mientras que las respuestas “No/No cumple” se sitúan entre 28% y 42%. En términos generales, estos resultados evidencian un nivel de cumplimiento mayoritariamente favorable del requisito evaluado en la pregunta 15, ya que en todos los sistemas más de la mitad de los encuestados indica que el control se cumple. No obstante, la presencia de hasta algo más de cuatro de cada diez respuestas de no cumplimiento en algunos sistemas revela brechas relevantes en la aplicación uniforme del control, por lo que se recomienda fortalecer las acciones de mejora orientadas a consolidar este aspecto específico de la norma ISO/IEC 27001 en todos los sistemas evaluados.

B) Variable Seguridad de los sistemas de información

Tabla 19

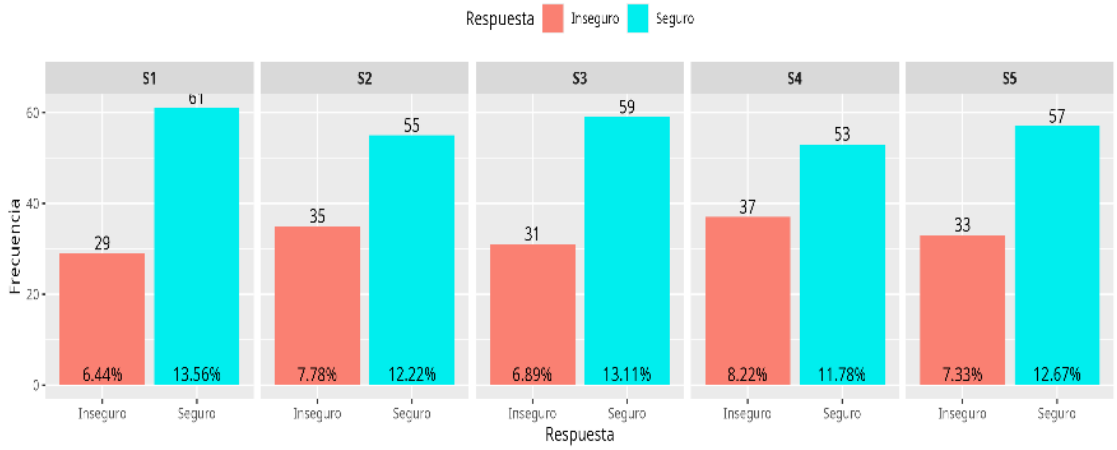
¿Cero (0) accesos no autorizados detectados en el día?

	Sistemas				
	S1 N = 90 (20%)	S2 N = 90 (20%)	S3 N = 90 (20%)	S4 N = 90 (20%)	S5 N = 90 (20%)
Respuesta					
Inseguro	29 (32%)	35 (39%)	31 (34%)	37 (41%)	33 (37%)
Seguro	61 (68%)	55 (61%)	59 (66%)	53 (59%)	57 (63%)

Fuente. Elaboración Propia (2025)

Figura 16

¿Cero (0) accesos no autorizados detectados en el día?



Fuente. Elaboración Propia (2025)

Interpretación: En la figura 1 de la variable “Seguridad de los sistemas de información”, la opción “Seguro” alcanza proporciones que oscilan aproximadamente entre 59% y 68% en los distintos sistemas, mientras que las respuestas “Inseguro” se sitúan entre 32% y 41%. En términos generales, estos resultados indican que la mayoría de los usuarios percibe los sistemas como seguros, lo que refleja un nivel de seguridad percibida globalmente favorable. Sin embargo, el hecho de que alrededor de un tercio a algo más de cuatro de cada diez participantes considere los sistemas inseguros evidencia la existencia de preocupaciones y vulnerabilidades percibidas que aún deben ser atendidas. Esto sugiere la necesidad de reforzar los controles de seguridad y la comunicación sobre las medidas implementadas, a fin de incrementar la confianza de los usuarios en todos los sistemas evaluados.

Tabla 20

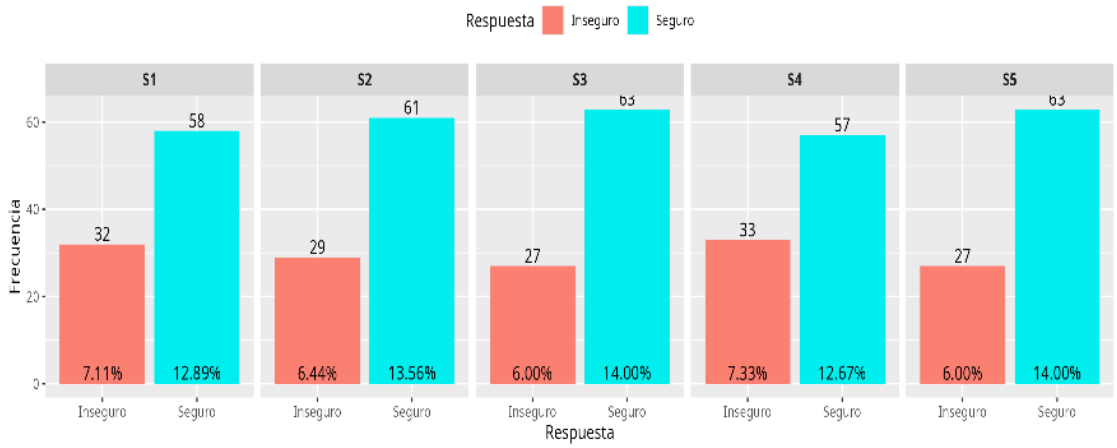
¿Todos los usuarios ingresaron con credenciales válidas?

	Sistemas				
	S1 N = 90 (20%)	S2 N = 90 (20%)	S3 N = 90 (20%)	S4 N = 90 (20%)	S5 N = 90 (20%)
Respuesta					
Inseguro	32 (36%)	29 (32%)	27 (30%)	33 (37%)	27 (30%)
Seguro	58 (64%)	61 (68%)	63 (70%)	57 (63%)	63 (70%)

Fuente. Elaboración Propia (2025)

Figura 17

¿Todos los usuarios ingresaron con credenciales válidas?



Fuente. Elaboración Propia (2025)

Interpretación: En la figura 17 de la variable "Seguridad de los sistemas de información", la alternativa "Seguro" presenta proporciones que fluctúan aproximadamente entre 63% y 70% en los distintos sistemas, mientras que las respuestas "Inseguro" se sitúan entre 30% y 37%. En conjunto, estos resultados evidencian que la mayoría de los usuarios percibe los sistemas como seguros respecto del aspecto evaluado en la pregunta 2, lo que refleja un nivel de seguridad percibida globalmente favorable. No obstante, el hecho de que alrededor de tres a casi cuatro de cada diez participantes considere los sistemas inseguros pone de manifiesto la existencia de riesgos o debilidades percibidas que aún deben ser abordadas, por lo que se recomienda reforzar los controles asociados y las estrategias de mitigación a fin de incrementar la confianza de los usuarios en todos los sistemas analizados.

Tabla 21

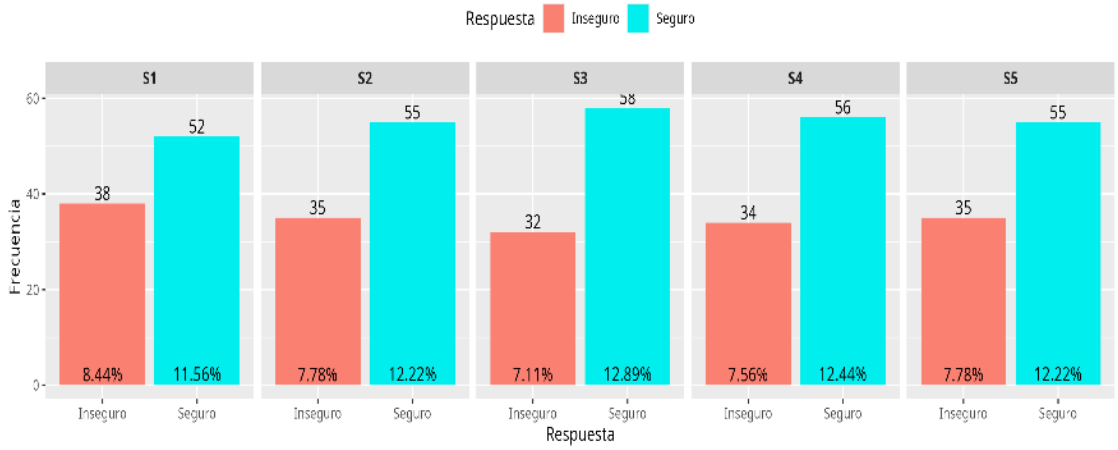
¿El sistema de cifrado funcionó sin interrupciones?

	Sistemas				
	S1 N = 90 (20%)	S2 N = 90 (20%)	S3 N = 90 (20%)	S4 N = 90 (20%)	S5 N = 90 (20%)
Respuesta					
Inseguro	38 (42%)	35 (39%)	32 (36%)	34 (38%)	35 (39%)
Seguro	52 (58%)	55 (61%)	58 (64%)	56 (62%)	55 (61%)

Fuente. Elaboración Propia (2025)

Figura 18

¿El sistema de cifrado funcionó sin interrupciones?



Fuente. Elaboración Propia (2025)

Interpretación: En la figura 18 de la variable "Seguridad de los sistemas de información", la opción "Seguro" alcanza proporciones que oscilan aproximadamente entre 58% y 64% en los distintos sistemas, mientras que las respuestas "Inseguro" se sitúan entre 36% y 42%. En términos generales, los resultados muestran que la mayoría de los usuarios percibe los sistemas como seguros en relación con el aspecto evaluado en esta pregunta, aunque con márgenes relativamente estrechos respecto de la opción "Inseguro" en algunos sistemas. Esto indica un nivel de seguridad percibida moderadamente favorable, pero también revela que más de un tercio de los participantes manifiesta percepciones de inseguridad, lo que pone de relieve la necesidad de reforzar los controles y las acciones de mejora para disminuir estas percepciones de riesgo y fortalecer la confianza de los usuarios.

Tabla 22

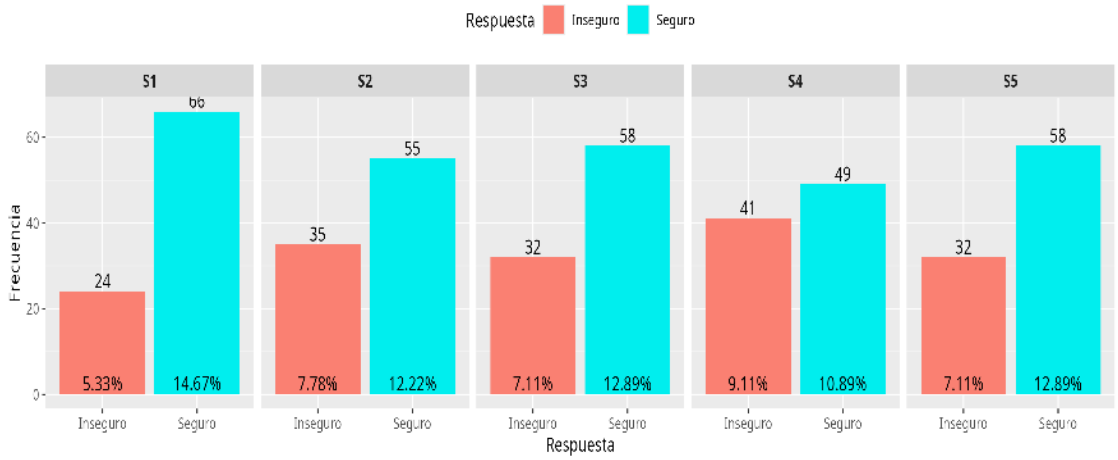
¿Cero (0) accesos a áreas restringidas sin autorización?

	Sistemas				
	S1 N = 90 (20%)	S2 N = 90 (20%)	S3 N = 90 (20%)	S4 N = 90 (20%)	S5 N = 90 (20%)
Respuesta					
Inseguro	24 (27%)	35 (39%)	32 (36%)	41 (46%)	32 (36%)
Seguro	66 (73%)	55 (61%)	58 (64%)	49 (54%)	58 (64%)

Fuente. Elaboración Propia (2025)

Figura 19

¿Cero (0) accesos a áreas restringidas sin autorización?



Fuente. Elaboración Propia (2025)

Interpretación: En la figura 19 de la variable "Seguridad de los sistemas de información", la alternativa "Seguro" presenta proporciones que fluctúan aproximadamente entre 54% y 73% en los distintos sistemas, mientras que las respuestas "Inseguro" se sitúan entre 27% y 46%. En conjunto, estos resultados indican que la mayoría de los usuarios percibe los sistemas como seguros respecto del aspecto evaluado en esta pregunta, lo que refleja un nivel de seguridad percibida globalmente favorable. Sin embargo, el hecho de que en algunos sistemas casi la mitad de los encuestados los considere inseguros evidencia la existencia de brechas importantes en la protección y en la percepción de seguridad, por lo que se recomienda reforzar los controles y las prácticas de gestión de riesgos asociadas para reducir dichas percepciones de inseguridad y lograr una mayor homogeneidad entre los sistemas evaluados.

Tabla 23

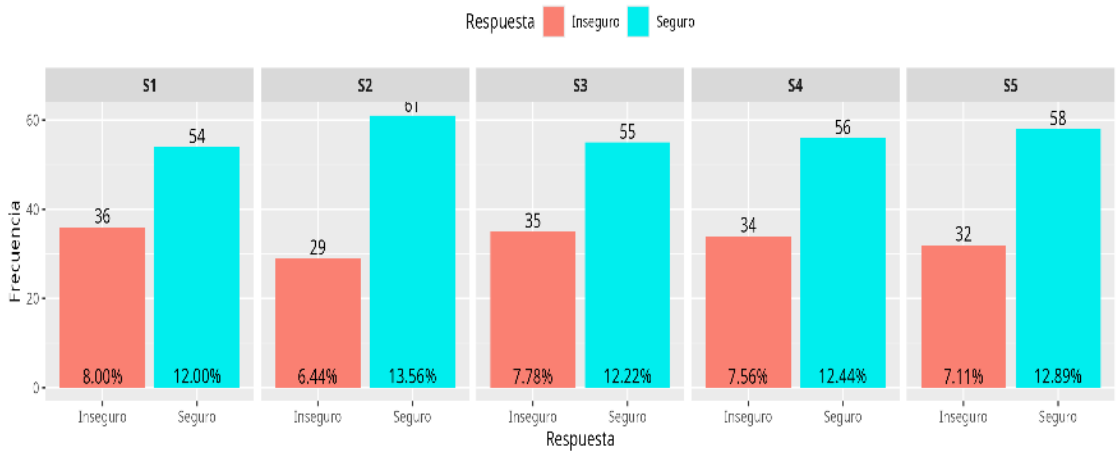
¿La autenticación multifactor estuvo disponible todo el día?

	Sistemas				
	S1 N = 90 (20%)	S2 N = 90 (20%)	S3 N = 90 (20%)	S4 N = 90 (20%)	S5 N = 90 (20%)
Respuesta					
Inseguro	36 (40%)	29 (32%)	35 (39%)	34 (38%)	32 (36%)
Seguro	54 (60%)	61 (68%)	55 (61%)	56 (62%)	58 (64%)

Fuente. Elaboración Propia (2025)

Figura 20

¿La autenticación multifactor estuvo disponible todo el día?



Fuente. Elaboración Propia (2025)

Interpretación: En la figura 20 de la variable "Seguridad de los sistemas de información", la opción "Seguro" alcanza proporciones que oscilan aproximadamente entre 60% y 68% en los distintos sistemas, mientras que las respuestas "Inseguro" se sitúan entre 32% y 40%. En términos generales, estos resultados muestran un nivel de seguridad percibida mayoritariamente favorable respecto del aspecto evaluado en esta pregunta, dado que en todos los sistemas más de la mitad de los usuarios considera que los sistemas son seguros. No obstante, el hecho de que alrededor de un tercio a cuatro de cada diez participantes los perciba como inseguros evidencia la existencia de riesgos o debilidades percibidas que aún deben ser atendidas, por lo que se recomienda fortalecer los controles asociados y las acciones de mejora orientadas a aumentar la confianza de los usuarios en todos los sistemas analizados.

Tabla 24

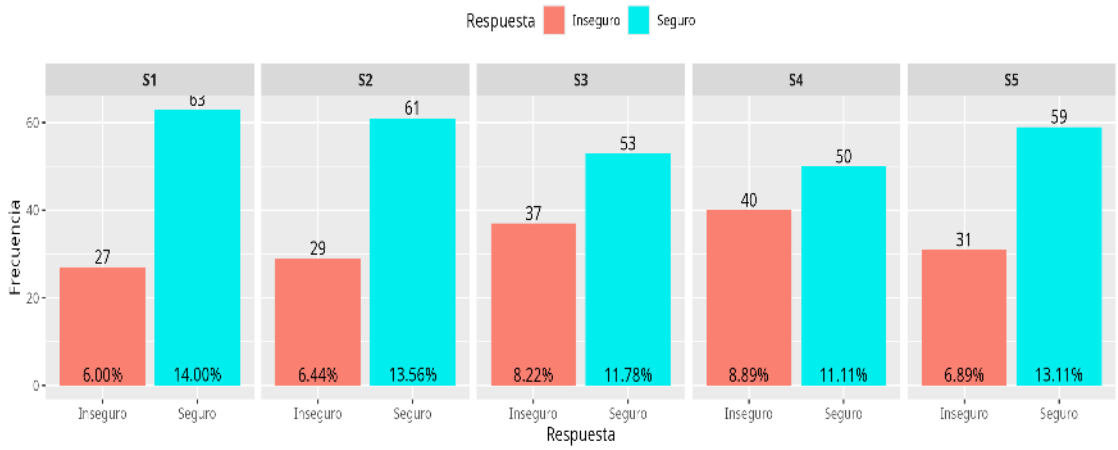
¿Cero (0) modificaciones no autorizadas detectadas?

	Sistemas				
	S1 N = 90 (20%)	S2 N = 90 (20%)	S3 N = 90 (20%)	S4 N = 90 (20%)	S5 N = 90 (20%)
Respuesta					
Inseguro	27 (30%)	29 (32%)	37 (41%)	40 (44%)	31 (34%)
Seguro	63 (70%)	61 (68%)	53 (59%)	50 (56%)	59 (66%)

Fuente. Elaboración Propia (2025)

Figura 21

¿Cero (0) modificaciones no autorizadas detectadas?



Fuente. Elaboración Propia (2025)

Interpretación: En la figura 21 de la variable "Seguridad de los sistemas de información", la alternativa "Seguro" presenta proporciones que fluctúan aproximadamente entre 56% y 70% en los distintos sistemas, mientras que las respuestas "Inseguro" se sitúan entre 30% y 44%. En conjunto, estos resultados indican un nivel de seguridad percibida mayoritariamente favorable respecto del aspecto evaluado en esta pregunta, ya que en todos los sistemas más de la mitad de los usuarios los considera seguros. Sin embargo, la presencia de hasta casi la mitad de participantes que los perciben como inseguros en algunos sistemas revela brechas relevantes en la protección y en la percepción de seguridad, por lo que se hace necesario reforzar los controles y las acciones de mitigación de riesgos para reducir dichas percepciones de inseguridad y lograr una mayor homogeneidad entre los sistemas evaluados.

Tabla 25

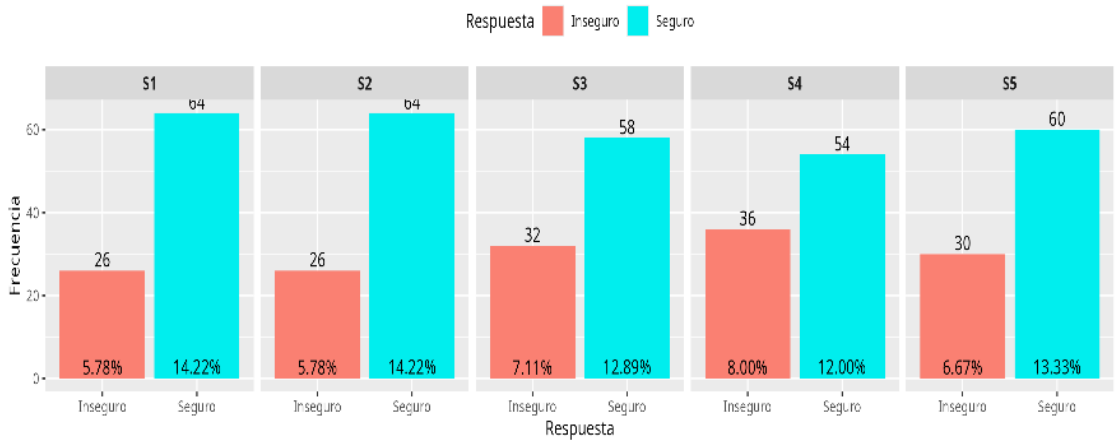
¿Las verificaciones de integridad se completaron sin errores?

	Sistemas				
	S1 N = 90 (20%)[1]	S2 N = 90 (20%)[1]	S3 N = 90 (20%)[1]	S4 N = 90 (20%)[1]	S5 N = 90 (20%)[1]
Respuesta					
Inseguro	26 (29%)	26 (29%)	32 (36%)	36 (40%)	30 (33%)
Seguro	64 (71%)	64 (71%)	58 (64%)	54 (60%)	60 (67%)

Fuente. Elaboración Propia (2025)

Figura 22

¿Las verificaciones de integridad se completaron sin errores?



Fuente. Elaboración Propia (2025)

Interpretación: En la figura 22 de la variable "Seguridad de los sistemas de información", la alternativa "Seguro" alcanza proporciones que oscilan aproximadamente entre 60% y 71% en los distintos sistemas, mientras que las respuestas "Inseguro" se sitúan entre 29% y 40%. En términos generales, estos resultados evidencian un nivel de seguridad percibida mayoritariamente favorable respecto del aspecto evaluado en esta pregunta, dado que en todos los sistemas más de la mitad de los usuarios considera que los sistemas son seguros. No obstante, el hecho de que cerca de un tercio a cuatro de cada diez participantes los perciba como inseguros indica la presencia de riesgos o debilidades percibidas que aún deben ser abordadas, por lo que se recomienda fortalecer los controles asociados y las acciones de mejora continua para incrementar la confianza de los usuarios en todos los sistemas analizados.

Tabla 26

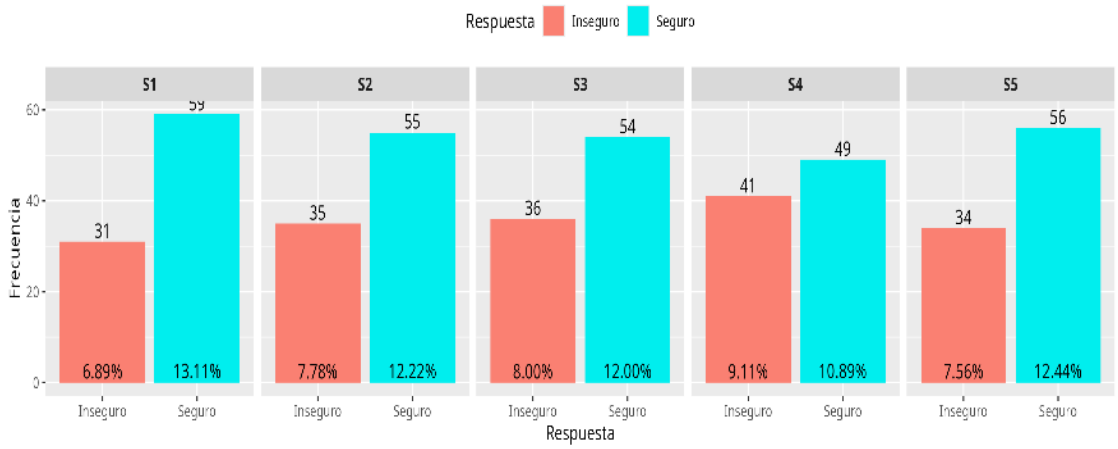
¿Las bases de datos funcionaron sin errores de consistencia?

	Sistemas				
	S1 N = 90 (20%)	S2 N = 90 (20%)	S3 N = 90 (20%)	S4 N = 90 (20%)	S5 N = 90 (20%)
Respuesta					
Inseguro	31 (34%)	35 (39%)	36 (40%)	41 (46%)	34 (38%)
Seguro	59 (66%)	55 (61%)	54 (60%)	49 (54%)	56 (62%)

Fuente. Elaboración Propia (2025)

Figura 23

¿Las bases de datos funcionaron sin errores de consistencia?



Fuente. Elaboración Propia (2025)

Interpretación: En la figura 23 de la variable "Seguridad de los sistemas de información", la opción "Seguro" presenta proporciones que fluctúan aproximadamente entre 54% y 66% en los distintos sistemas, mientras que las respuestas "Inseguro" se sitúan entre 34% y 46%. En conjunto, los resultados muestran un nivel de seguridad percibida solo moderadamente favorable, ya que, aunque en todos los sistemas la mayoría de los usuarios considera que son seguros, en algunos casos casi la mitad de los participantes los percibe como inseguros. Esto evidencia brechas importantes en la protección y en la percepción de seguridad, por lo que se hace necesario reforzar los controles técnicos y procedimentales asociados al aspecto evaluado en esta pregunta, así como las acciones de sensibilización y comunicación, con el fin de disminuir las percepciones de inseguridad y fortalecer la confianza de los usuarios en todos los sistemas.

Tabla 27

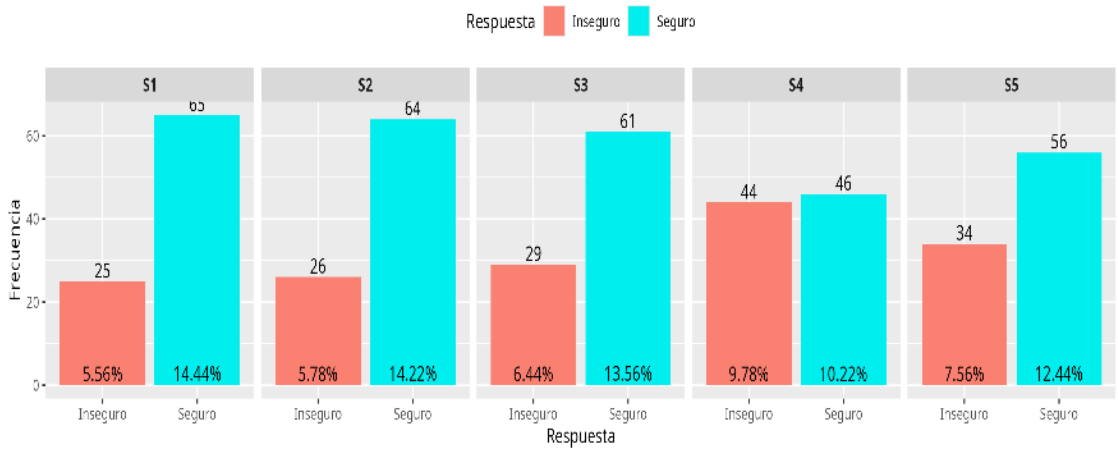
¿El control de versiones registró todos los cambios correctamente?

	Sistemas				
	S1 N = 90 (20%)[1]	S2 N = 90 (20%)[1]	S3 N = 90 (20%)[1]	S4 N = 90 (20%)[1]	S5 N = 90 (20%)[1]
Respuesta					
Inseguro	25 (28%)	26 (29%)	29 (32%)	44 (49%)	34 (38%)
Seguro	65 (72%)	64 (71%)	61 (68%)	46 (51%)	56 (62%)

Fuente. Elaboración Propia (2025)

Figura 24

¿El control de versiones registró todos los cambios correctamente?



Fuente. Elaboración Propia (2025)

Interpretación: En la figura 24 de la variable "Seguridad de los sistemas de información", la alternativa "Seguro" alcanza proporciones que oscilan aproximadamente entre 51% y 72% en los distintos sistemas, mientras que las respuestas "Inseguro" se sitúan entre 28% y 49%. En términos generales, estos resultados muestran un nivel de seguridad percibida mayoritariamente favorable, dado que en todos los sistemas la proporción de usuarios que los considera seguros es superior a la de quienes los perciben como inseguros. Sin embargo, el hecho de que en algunos sistemas casi la mitad de los participantes los califique como inseguros evidencia brechas significativas en la protección y en la percepción de seguridad, lo que sugiere la necesidad de reforzar los controles y las medidas de mitigación de riesgos vinculadas al aspecto evaluado en esta pregunta, con el fin de reducir dichas percepciones de inseguridad y mejorar la confianza de los usuarios.

Tabla 28

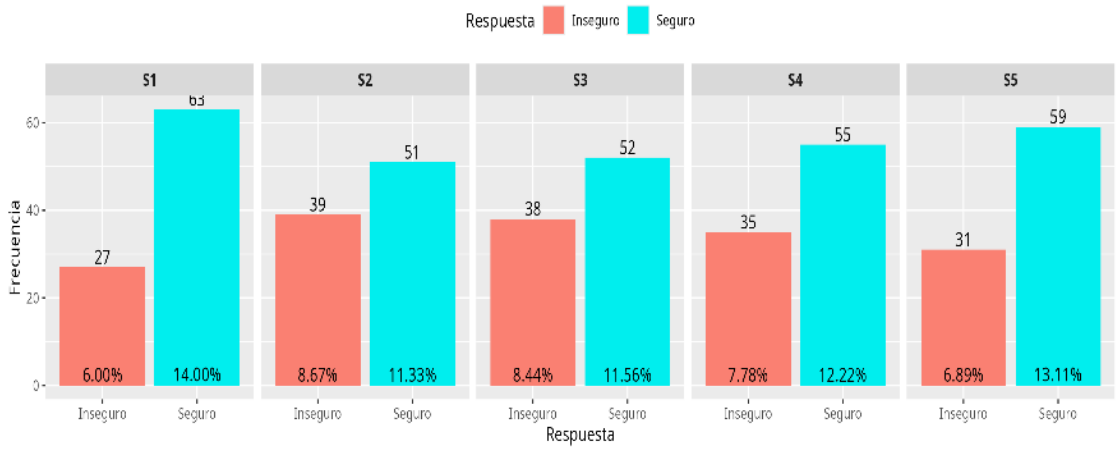
¿Las validaciones automáticas detectaron anomalías?

	Sistemas				
	S1 N = 90 (20%)[1]	S2 N = 90 (20%)[1]	S3 N = 90 (20%)[1]	S4 N = 90 (20%)[1]	S5 N = 90 (20%)[1]
Respuesta					
Inseguro	27 (30%)	39 (43%)	38 (42%)	35 (39%)	31 (34%)
Seguro	63 (70%)	51 (57%)	52 (58%)	55 (61%)	59 (66%)

Fuente. Elaboración Propia (2025)

Figura 25

¿Las validaciones automáticas detectaron anomalías?



Fuente. Elaboración Propia (2025)

Interpretación: En la figura 25 de la variable "Seguridad de los sistemas de información", la alternativa "Seguro" alcanza proporciones que oscilan aproximadamente entre 57% y 70% en los distintos sistemas, mientras que las respuestas "Inseguro" se sitúan entre 30% y 43%. En términos generales, estos resultados evidencian un nivel de seguridad percibida mayoritariamente favorable respecto del aspecto evaluado en esta pregunta, ya que en todos los sistemas la proporción de usuarios que los considera seguros supera a la de quienes los perciben como inseguros. No obstante, el hecho de que en algunos sistemas cerca de cuatro de cada diez participantes los califique como inseguros revela la existencia de riesgos o debilidades percibidas que aún deben ser atendidas, por lo que se recomienda reforzar los controles y las acciones de mejora orientadas a incrementar la confianza de los usuarios en todos los sistemas analizados.

Tabla 29

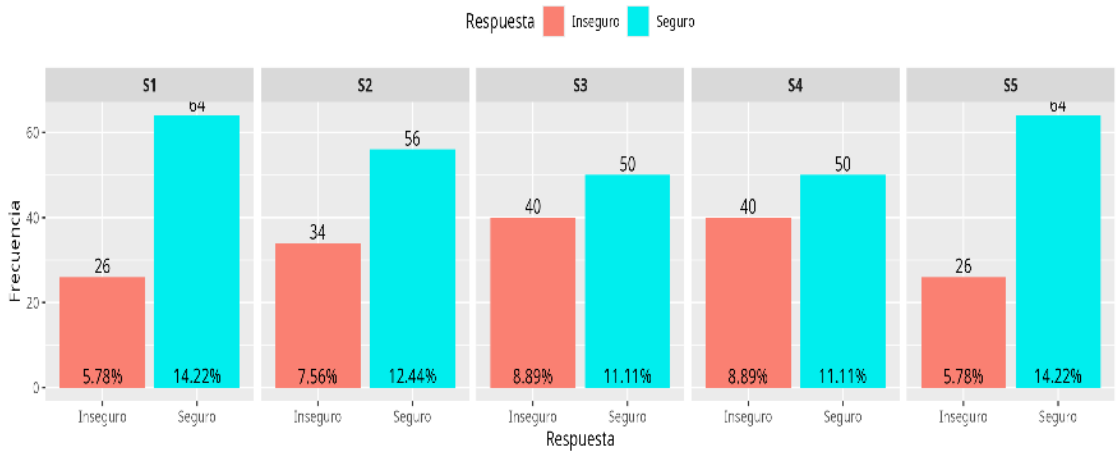
¿El sistema estuvo disponible durante todo el horario laboral?

	Sistemas				
	S1 N = 90 (20%)[1]	S2 N = 90 (20%)[1]	S3 N = 90 (20%)[1]	S4 N = 90 (20%)[1]	S5 N = 90 (20%)[1]
Respuesta					
Inseguro	26 (29%)	34 (38%)	40 (44%)	40 (44%)	26 (29%)
Seguro	64 (71%)	56 (62%)	50 (56%)	50 (56%)	64 (71%)

Fuente. Elaboración Propia (2025)

Figura 26

¿El sistema estuvo disponible durante todo el horario laboral?



Fuente. Elaboración Propia (2025)

Interpretación: En la figura 26 de la variable "Seguridad de los sistemas de información", la alternativa "Seguro" presenta proporciones que fluctúan aproximadamente entre 56% y 71% en los distintos sistemas, mientras que las respuestas "Inseguro" se sitúan entre 29% y 44%. En conjunto, estos resultados evidencian un nivel de seguridad percibida mayoritariamente favorable respecto del aspecto evaluado en esta pregunta, dado que en todos los sistemas la proporción de usuarios que los considera seguros es superior a la de quienes los perciben como inseguros. Sin embargo, el hecho de que en algunos sistemas cerca de cuatro de cada diez participantes los califique como inseguros revela brechas importantes en la protección y en la percepción de seguridad, por lo que se recomienda reforzar los controles y las medidas

de mitigación de riesgos asociadas, con el fin de reducir dichas percepciones de inseguridad y fortalecer la confianza de los usuarios en todos los sistemas.

Tabla 30

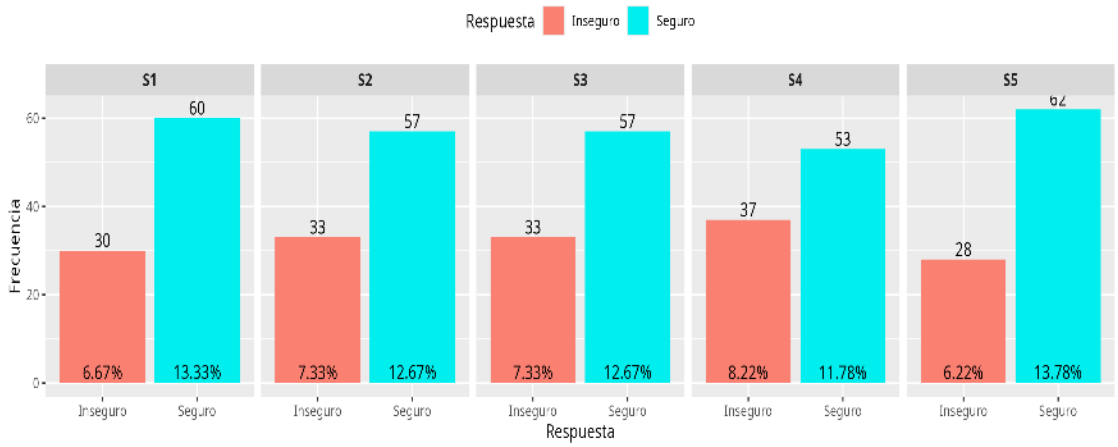
¿Cero (0) caídas del sistema reportadas en el día?

	Sistemas				
	S1 N = 90 (20%)	S2 N = 90 (20%)	S3 N = 90 (20%)	S4 N = 90 (20%)	S5 N = 90 (20%)
Respuesta					
Inseguro	30 (33%)	33 (37%)	33 (37%)	37 (41%)	28 (31%)
Seguro	60 (67%)	57 (63%)	57 (63%)	53 (59%)	62 (69%)

Fuente. Elaboración Propia (2025)

Figura 27

¿Cero (0) caídas del sistema reportadas en el día?



Fuente. Elaboración Propia (2025)

Interpretación: En la figura 27 de la variable "Seguridad de los sistemas de información", la alternativa "Seguro" alcanza proporciones que oscilan aproximadamente entre 59% y 69% en los distintos sistemas, mientras que las respuestas "Inseguro" se sitúan entre 31% y 41%. En términos generales, estos resultados muestran un nivel de seguridad percibida mayoritariamente favorable respecto del aspecto evaluado en esta pregunta, ya que en todos los sistemas más de la mitad de los usuarios considera que los sistemas son seguros. No obstante, el hecho de que alrededor de un tercio a algo más de cuatro de cada diez participantes los perciba como inseguros evidencia riesgos o debilidades percibidas que aún deben ser abordadas, por lo

que se recomienda fortalecer los controles correspondientes y las acciones de mejora continua para incrementar la confianza de los usuarios en todos los sistemas analizados.

Tabla 31

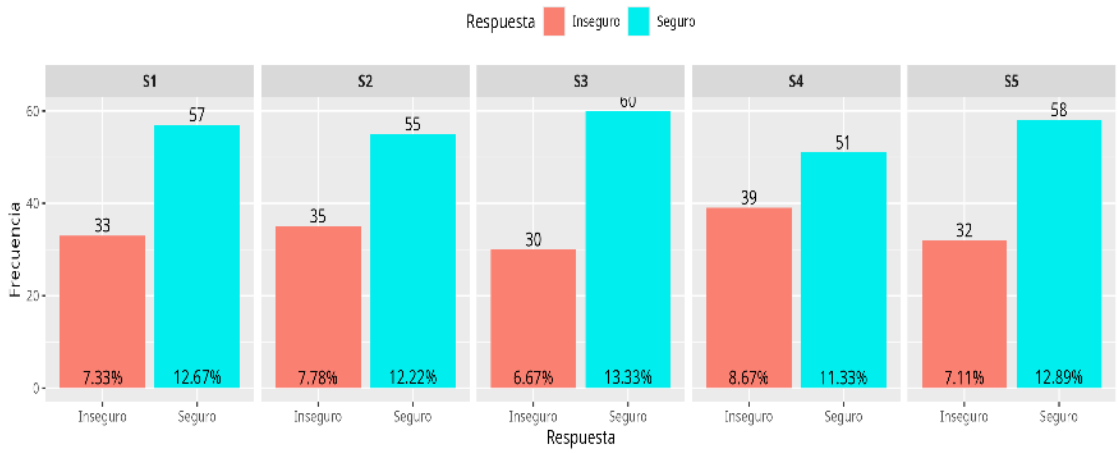
¿El respaldo diario programado se ejecutó exitosamente?

	Sistemas				
	S1 N = 90 (20%)[1]	S2 N = 90 (20%)[1]	S3 N = 90 (20%)[1]	S4 N = 90 (20%)[1]	S5 N = 90 (20%)[1]
Respuesta					
Inseguro	33 (37%)	35 (39%)	30 (33%)	39 (43%)	32 (36%)
Seguro	57 (63%)	55 (61%)	60 (67%)	51 (57%)	58 (64%)

Fuente. Elaboración Propia (2025)

Figura 28

¿El respaldo diario programado se ejecutó exitosamente?



Fuente. Elaboración Propia (2025)

Interpretación: En la figura 28 de la variable “Seguridad de los sistemas de información”, la alternativa “Seguro” presenta proporciones que fluctúan aproximadamente entre 57% y 67% en los distintos sistemas, mientras que las respuestas “Inseguro” se sitúan entre 33% y 43%. En conjunto, estos resultados evidencian un nivel de seguridad percibida mayoritariamente favorable respecto del aspecto evaluado en esta pregunta, ya que en todos los sistemas más de la mitad de los usuarios considera que los sistemas son seguros. Sin embargo, el hecho de que alrededor de un tercio a más de cuatro de cada diez participantes los perciba como inseguros revela brechas significativas en la protección y en la percepción de seguridad, por lo que se recomienda reforzar los controles y las acciones de mejora orientadas a reducir

dichas percepciones de inseguridad y fortalecer la confianza de los usuarios en todos los sistemas analizados.

Tabla 32

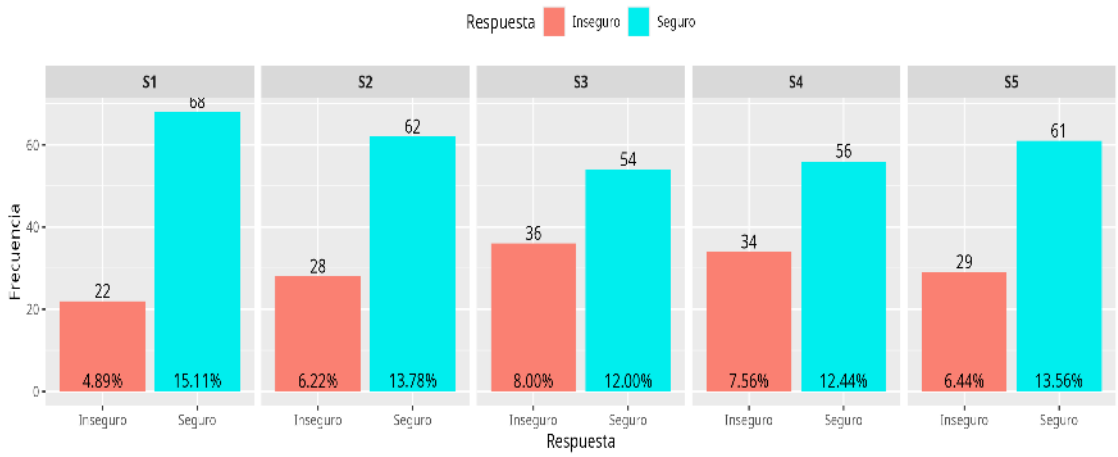
¿El sistema respondió con velocidad normal durante el día?

	Sistemas				
	S1 N = 90 (20%)	S2 N = 90 (20%)	S3 N = 90 (20%)	S4 N = 90 (20%)	S5 N = 90 (20%)
Respuesta					
Inseguro	22 (24%)	28 (31%)	36 (40%)	34 (38%)	29 (32%)
Seguro	68 (76%)	62 (69%)	54 (60%)	56 (62%)	61 (68%)

Fuente. Elaboración Propia (2025)

Figura 29

¿El sistema respondió con velocidad normal durante el día?



Fuente. Elaboración Propia (2025)

Interpretación: En la figura 29 de la variable "Seguridad de los sistemas de información", la alternativa "Seguro" alcanza proporciones que oscilan aproximadamente entre 60% y 76% en los distintos sistemas, mientras que las respuestas "Inseguro" se sitúan entre 24% y 40%. En términos generales, estos resultados muestran un nivel de seguridad percibida claramente favorable respecto del aspecto evaluado en esta pregunta, dado que en todos los sistemas la mayoría de los usuarios considera que los sistemas son seguros. No obstante, el hecho de que hasta cuatro de cada diez participantes los perciba como inseguros en algunos casos evidencia brechas aún presentes en la protección y en la percepción de seguridad, por lo que se recomienda continuar reforzando los controles técnicos y procedimentales, así como las

acciones de sensibilización, con el fin de disminuir estas percepciones de inseguridad y fortalecer la confianza de los usuarios.

Tabla 33

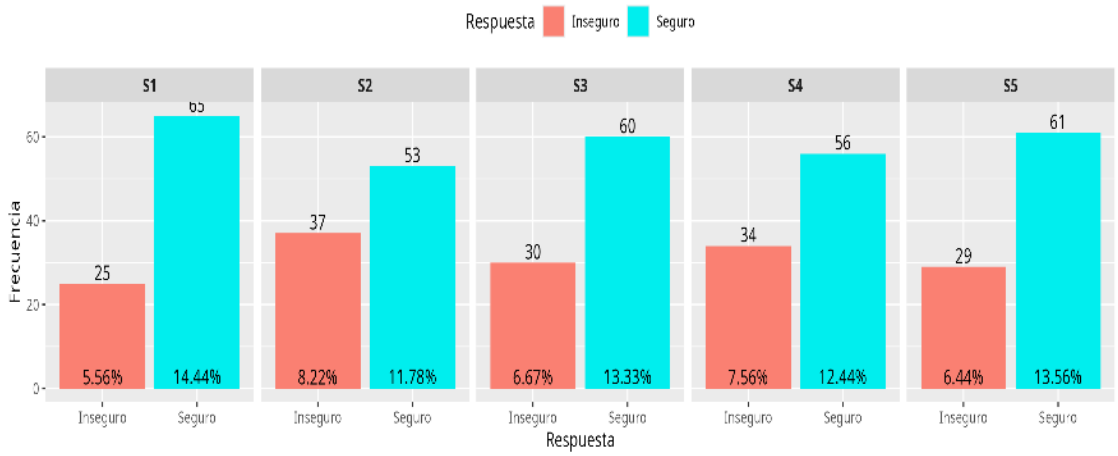
¿Los planes de continuidad estuvieron accesibles y actualizados?

	Sistemas				
	S1 N = 90 (20%)	S2 N = 90 (20%)	S3 N = 90 (20%)	S4 N = 90 (20%)	S5 N = 90 (20%)
Respuesta					
Inseguro	25 (28%)	37 (41%)	30 (33%)	34 (38%)	29 (32%)
Seguro	65 (72%)	53 (59%)	60 (67%)	56 (62%)	61 (68%)

Fuente. Elaboración Propia (2025)

Figura 30

¿Los planes de continuidad estuvieron accesibles y actualizados?



Fuente. Elaboración Propia (2025)

Interpretación: En la figura 30 de la variable "Seguridad de los sistemas de información", la alternativa "Seguro" alcanza proporciones que oscilan aproximadamente entre 59% y 72% en los distintos sistemas, mientras que las respuestas "Inseguro" se sitúan entre 28% y 41%. En términos generales, estos resultados evidencian un nivel de seguridad percibida mayoritariamente favorable respecto del aspecto evaluado en esta pregunta, ya que en todos los sistemas la mayoría de los usuarios considera que los sistemas son seguros. Sin embargo, el hecho de que entre casi un tercio y algo más de cuatro de cada diez participantes los perciba como inseguros revela la existencia de riesgos o debilidades percibidas que aún deben ser abordadas, por lo que se recomienda fortalecer los controles y las acciones de mejora orientadas

a reducir dichas percepciones de inseguridad y consolidar la confianza de los usuarios en todos los sistemas analizados.

Análisis descriptivo

Los resultados del análisis fueron presentados en tablas y gráficos, como se detalla:

ISO/IEC 27001

Tabla 34

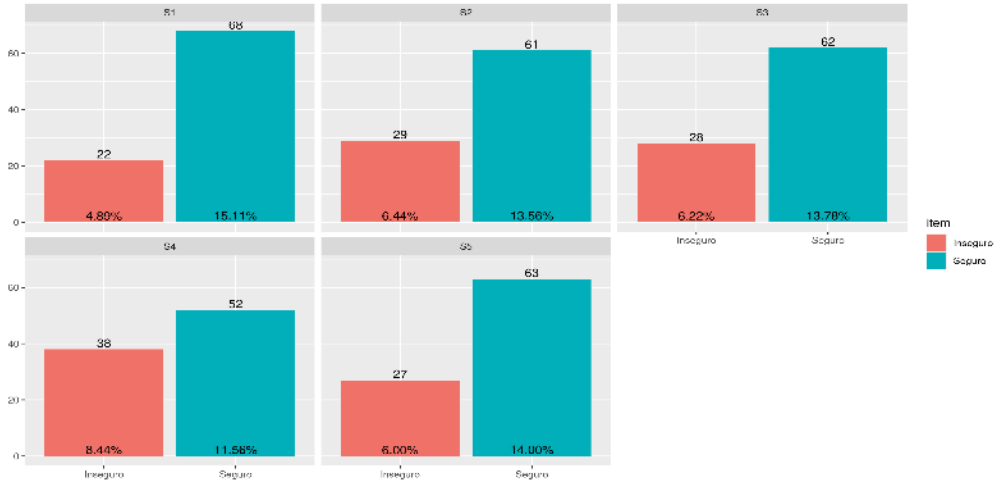
Observaciones sobre la seguridad de los sistemas de información por sistema evaluado según la norma ISO/IEC 27001

	ISO/IEC 27001	
Características	Inseguro N = 144 (32%)	Seguro N = 306 (68%)
Sistema		
S1	22 (15%)	68 (22%)
S2	29 (20%)	61 (20%)
S3	28 (19%)	62 (20%)
S4	38 (26%)	52 (17%)
S5	27 (19%)	63 (21%)

Fuente. Elaboración Propia (2025)

Figura 31

Gráfico sobre las observaciones sobre la seguridad de los sistemas de información por sistema evaluado según la norma ISO/IEC 27001



Fuente. Elaboración Propia (2025)

Interpretación: En conjunto, 306 registros equivalentes al 68 % se clasificaron como seguros, mientras que 144 registros que representan el 32 % quedaron en condición insegura. El sistema S1 alcanzó 68 registros seguros (22 %) y solo 22 inseguros (15 %), lo que indica

predominio del cumplimiento de criterios de la norma. En S2 y S3 la distribución resultó equilibrada, con 20 % de registros seguros y porcentajes de inseguridad cercanos al 19–20 %, lo que sugiere estabilidad, aunque con márgenes sensibles. S4 fue la categoría que arrojó el porcentaje más elevado de inseguridad con 38 registros inseguros que suponen el 26 % y solamente 52 seguros correspondientes al 17 %. Este comportamiento sugiere la presencia de un punto crítico. S5, por su parte, exhibió 63 registros seguros (21 %) mientras que el número de los inseguros sólo ascendió a 27, es decir, el 19 %, por lo que la conformidad a esta categoría fue la preferencia. Por último, el funcionamiento global respalda a este panorama ya que la gran mayoría de registros estaría en estado seguro, pero que no se distribuyen homogéneamente: el peso de S4 sobre la categoría insegura hace crecer la proporción global de inseguridad en el total de los registros analizados, tal como la polivalencia de S1 y S5 pone de manifiesto y señala las diferentes prácticas de gestión de la norma ISO/IEC 27001, lo que da lugar a prácticas de gestión diferenciadas para los distintos sistemas evaluados.

Gestión de riesgos

Tabla 35

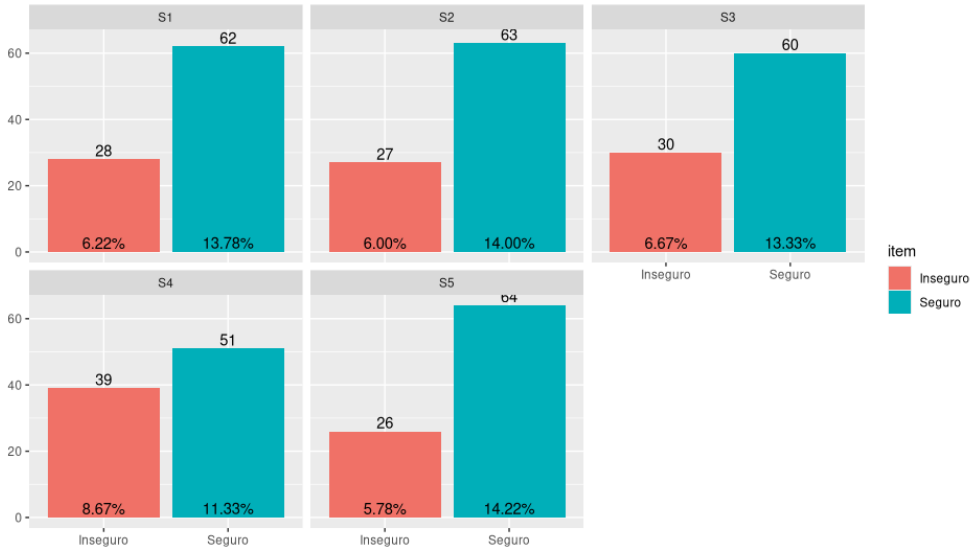
Observaciones sobre la gestión de riesgos por sistema de información según la norma ISO/IEC 27001

	Gestión de riesgos	
Características	Inseguro N = 150 (33%)	Seguro N = 300 (67%)
Sistema		
S1	28 (19%)	62 (21%)
S2	27 (18%)	63 (21%)
S3	30 (20%)	60 (20%)
S4	39 (26%)	51 (17%)
S5	26 (17%)	64 (21%)

Fuente. Elaboración Propia (2025)

Figura 32

Gráfico sobre las observaciones sobre la gestión de riesgos por sistema de información según la norma ISO/IEC 27001



Fuente. Elaboración Propia (2025)

Interpretación: En el conjunto global se evidenció que 300 registros equivalentes al 67 % fueron clasificados como seguros, mientras que 150 registros que representan el 33 % se ubicaron en condición insegura. En S1 la relación fue favorable con 62 seguros (21 %) frente a 28 inseguros (19 %); S2 mostró un comportamiento semejante con 61 seguros (21 %) y 27 inseguros (18 %); S3 se mantuvo equilibrado al registrar 60 seguros (20 %) y 30 inseguros (20 %); S4 presentó la mayor concentración de inseguridad con 39 registros inseguros (26 %) y solo 51 seguros (17 %); y S5 alcanzó el mejor desempeño relativo con 64 seguros (21 %) y apenas 26 inseguros (17 %). La adecuada prevalencia de la condición segura en los cuatro de los cinco sistemas da cuenta del grado de cumplimiento general aceptable de la norma en gestión de riesgos, si bien el resultado de S4 constituye un indicador de alerta dado que llega a concentrarse más de una cuarta parte de los registros inseguros y está reduciendo la proporción de seguridad total; en el caso de S4 y S5, el contraste resulta especialmente revelador, dado que operan dentro de un mismo entorno institucional, pero exhiben trayectorias diferentes cuando se pone en juego la capacidad para identificar y tratar riesgos.

Seguridad operativa

Tabla 36

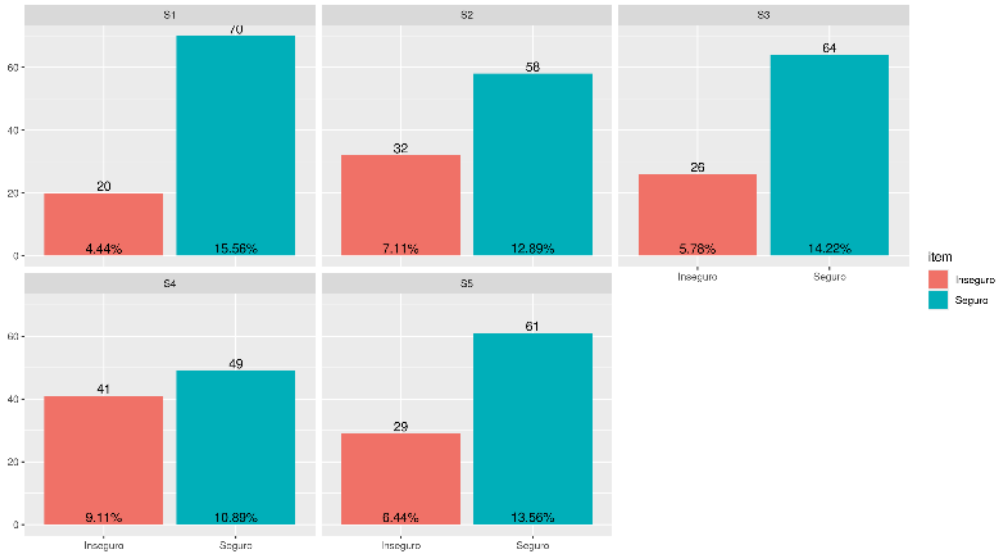
Observaciones sobre la seguridad operativa por sistema de información según la norma ISO/IEC 27001

	Seguridad operativa	
Características	Inseguro 148 (33%)	Seguro N = 302 (67%)
Sistema		
S1	20 (14%)	70 (23%)
S2	32 (22%)	58 (19%)
S3	26 (18%)	64 (21%)
S4	41 (28%)	49 (16%)
S5	29 (20%)	61 (20%)

Fuente. Elaboración Propia (2025)

Figura 33

Gráfico sobre las observaciones sobre la seguridad operativa por sistema de información según la norma ISO/IEC 27001



Fuente. Elaboración Propia (2025)

Interpretación: S1 destacó con 70 registros seguros (23 %) y únicamente 20 inseguros (14 %), lo que marca una proporción claramente favorable; S2 mostró un comportamiento más equilibrado aunque con cierta inclinación a la vulnerabilidad con 58 seguros (19 %) frente a 32 inseguros (22 %); S3 registró 64 seguros (21 %) y 26 inseguros (18 %), confirmando un balance positivo; S4 se convirtió en el punto más crítico al contabilizar 41 inseguros (28 %) frente a solo 49 seguros (16 %); y S5 mantuvo una distribución estable con 61 seguros (20 %) y 29

inseguros (20 %). La posición predominante de la condición segura es evidente en S1 y S3, lo que parece indicar que los controles operativos de seguridad como accesos, monitoreo de incidencias y actualización de sistemas operativos se han ejecutado de forma habitual; mientras que S2 y S5 muestran proporciones más ajustadas, lo que parece sugerir, que una nueva posible pérdida podría decantar la balanza hacia la condición insegura. S4 muestra nuevamente la mayor proporción de registros inseguros, con lo que parece corroborarse un patrón repetido de vulnerabilidad ya identificado en la dimensión de gestión de riesgos. La vulnerabilidad sistemática de S4 plantea el desafío de implementar medidas específicas que garanticen una cobertura homogénea de seguridad operativa para todo el entorno organizacional durante el 2025.

Desempeño operativo

Tabla 37

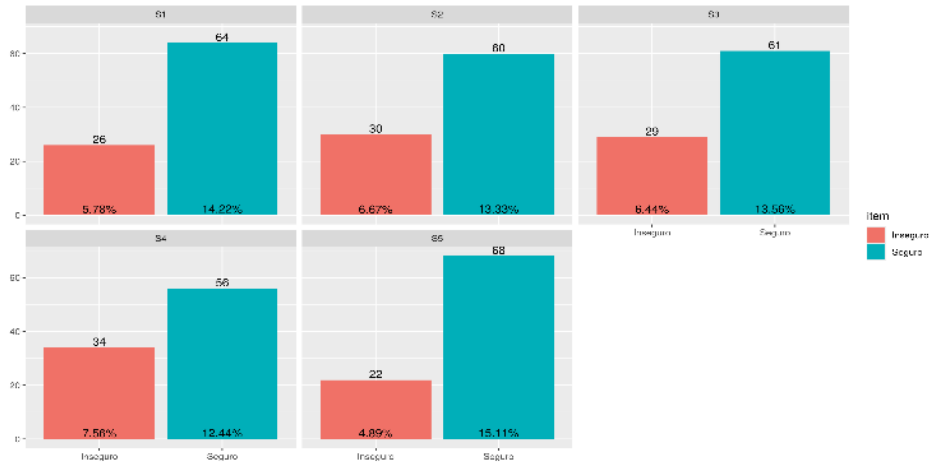
Observaciones sobre el desempeño operativo por sistema de información según la norma ISO/IEC 27001

Desempeño operativo		
Características	Inseguro 141 (31%)	Seguro N = 309 (69%)
Sistema		
S1	26 (18%)	64 (21%)
S2	30 (21%)	60 (19%)
S3	29 (21%)	61 (20%)
S4	34 (24%)	56 (18%)
S5	22 (16%)	68 (22%)

Fuente. Elaboración Propia (2025)

Figura 34

Gráfico sobre las observaciones sobre el desempeño operativo por sistema de información según la norma ISO/IEC 27001



Fuente. Elaboración Propia (2025)

Interpretación: S1 alcanzó 64 seguros (21 %) y 26 inseguros (18 %), reflejando un predominio favorable; S2 presentó 60 seguros (19 %) frente a 30 inseguros (21 %), dando lugar a un balance más ajustado; S3 registró 61 seguros (20 %) y 29 inseguros (21 %), manteniendo un perfil similar al de S2; S4 concentró 56 seguros (18 %) y 34 inseguros (24 %), configurando nuevamente el nivel más alto de vulnerabilidad relativa; y S5 se consolidó como el sistema con mejor desempeño al obtener 68 seguros (22 %) y solo 22 inseguros (16 %). La tendencia general confirma que los sistemas tienden a dar cumplimento de adecuado a los indicadores de desempeño operativo, desde las evaluaciones de gestión y los procedimientos de mejora continua; no obstante, S2 y S3 muestran proporciones equilibradas hasta el punto de reducir el margen de seguridad, mientras que S4 se apuesta por la mayor proporción de registros inseguros, con lo que parece repetirse un patrón crítico ya mencionado a través de las otras dimensiones. Sin embargo S5 se presenta como el sistema más robusto, con una ventaja clara en la condición segura. Esta heterogeneidad sugiere que Inversiones RMK debe priorizar la estandarización de procesos de mejora continua y fortalecer la rendición de cuentas a nivel de todos los sistemas de información si desea consolidar una cultura homogénea de seguridad durante el año 2025.

Seguridad de los sistemas de información

Tabla 38

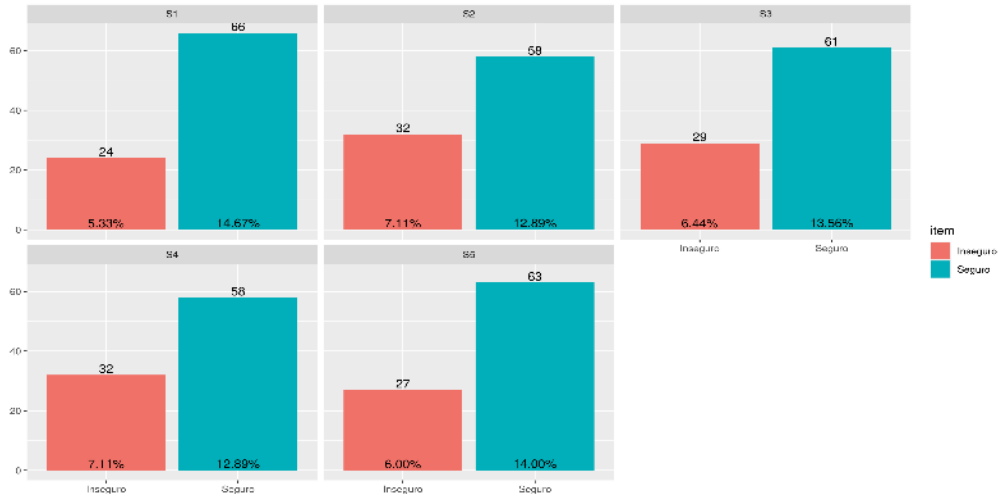
Observaciones sobre la seguridad global de los sistemas de información por sistema según la norma ISO/IEC 27001

	Seguridad de los sistemas de información	
Características	Inseguro N = 144 (32%)	Inseguro N = 144 (32%)
Sistema		
S1	24 (17%)	24 (17%)
S2	32 (22%)	32 (22%)
S3	29 (20%)	29 (20%)
S4	32 (22%)	32 (22%)
S5	27 (19%)	27 (19%)

Fuente. Elaboración Propia (2025)

Figura 35

Gráfico sobre las observaciones sobre el desempeño operativo por sistema de información según la norma ISO/IEC 27001



Fuente. Elaboración Propia (2025)

Interpretación: El total para el panorama global es de 306 registros seguros, entendidos como el 68 %; mientras que de registros inseguros alcanzamos los 144, el 32 %. S1 llegó a 66 seguros (22 %) frente a 24 inseguros (17 %), resultando un predominio favorable; S2 fue de 58 seguros (19 %) frente a 32 inseguros (22 %), resultado de un balance inclinado hacia la inseguridad; S3 fue de 61 seguros (20 %) frente a 29 inseguros (20 %) que genera un equilibrio con una pequeña ventaja hacia la condición segura; S4 tuvo el mismo perfil que S2, llegando a

58 seguros (19 %) frente a 32 inseguros (22 %), lo que refuerza la vulnerabilidad relativa; y S5 correspondió a 63 seguros (21 %) frente a 27 inseguros (19 %), con un resultado más favorable. En términos generales, el resultado del panorama indica que la mayoría de los sistemas logra llegar a la condición segura, aunque dos de ellos (S2, S4) tienen un porcentaje más elevado de inseguridad. La diferencia entre S1 y S5 frente a S2 y S4 permite deducir que la seguridad de la información no sólo depende de tener controles, sino de cómo son, y cómo se les da seguimiento en el día a día. La evidencia señala que Inversiones RMK en Lircay presenta un nivel de seguridad que va a tender a ser estable en términos generales, pero que va a estar desarticulado entre sistemas; la vulnerabilidad persistente de S2 y S4 presenta la oportunidad para abordar las particularidades operativas de cada uno de ellos mediante políticas específicas.

Confidencialidad

Tabla 39

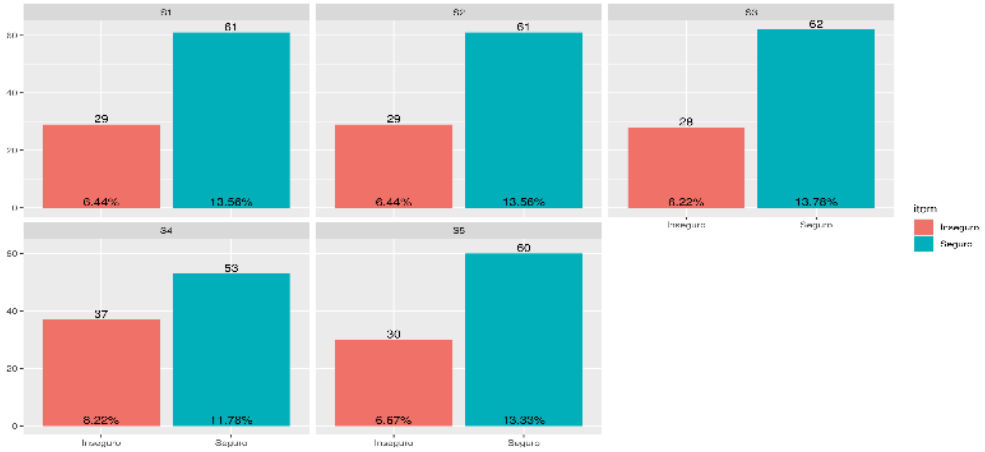
Observaciones sobre la confidencialidad por sistema de información según la norma ISO/IEC 27001

	Confidencialidad	
Características	Inseguro N = 153 (34%)[1]	Inseguro N = 153 (34%)[1]
Sistema		
S1	29 (19%)	29 (19%)
S2	29 (19%)	29 (19%)
S3	28 (18%)	28 (18%)
S4	37 (24%)	37 (24%)
S5	30 (20%)	30 (20%)

Fuente. Elaboración Propia (2025)

Figura 36

Gráfico sobre las observaciones sobre la confidencialidad por sistema de información según la norma ISO/IEC 27001



Fuente. Elaboración Propia (2025)

Interpretación: S1 y S2 presentan la misma distribución con 61 seguros (21 %) y 29 inseguros (19 %) cada uno, lo que sugiere una condición relativamente equilibrada aunque con ligera ventaja hacia la seguridad; S3 obtuvo 62 seguros (21 %) frente a 28 inseguros (18 %), consolidando un balance favorable; S4 se ubicó como el sistema más vulnerable al registrar 53 seguros (18 %) y 37 inseguros (24 %), constituyendo la mayor proporción de inseguridad en esta dimensión; y S5 alcanzó 60 seguros (20 %) frente a 30 inseguros (20 %), configurando una distribución simétrica. El predominio de la condición segura es claro en la mayoría de sistemas, sin embargo, la vulnerabilidad de S4 introduce un punto crítico. La confidencialidad depende de factores como el control de accesos, el cifrado y la asignación adecuada de permisos, por lo que la diferencia entre sistemas refleja desigualdades en la implementación de estos mecanismos; en términos relativos, S3 se posiciona como el sistema con mejor protección mientras que S4 queda rezagado en la protección de datos sensibles. Por tanto, el reto para el año 2025 no será únicamente sostener los porcentajes de seguridad en los sistemas que ya se desempeñan de forma adecuada, sino sobre todo elevar el estándar en S4 para que la protección de la información confidencial sea uniforme en toda la organización.

Integridad

Tabla 40

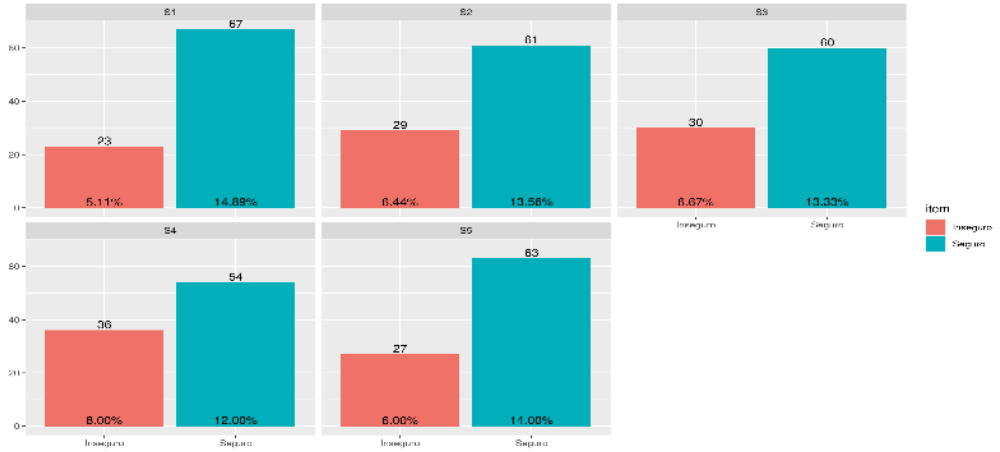
Observaciones sobre la integridad por sistema de información según la norma ISO/IEC 27001

	Integridad	
Características	Inseguro N = 145 (32%)	Inseguro N = 145 (32%)
Sistema		
S1	23 (16%)	23 (16%)
S2	29 (20%)	29 (20%)
S3	30 (21%)	30 (21%)
S4	36 (25%)	36 (25%)
S5	27 (19%)	27 (19%)

Fuente. Elaboración Propia (2025)

Figura 37

Gráfico sobre las observaciones sobre la integridad por sistema de información según la norma ISO/IEC 27001



Fuente. Elaboración Propia (2025)

Interpretación: S1 registró 67 seguros (22 %) y 23 inseguros (16 %), marcando el perfil más favorable en esta dimensión; S2 alcanzó 61 seguros (20 %) frente a 29 inseguros (20 %), reflejando una proporción equilibrada; S3 obtuvo 60 seguros (20 %) y 30 inseguros (21 %), evidenciando un balance muy similar al de S2; S4 destacó por su vulnerabilidad relativa con 54 seguros (18 %) y 36 inseguros (25 %), configurando la mayor proporción de inseguridad; y S5 alcanzó 63 seguros (21 %) y 27 inseguros (19 %), con predominio seguro aunque no tan marcado como en S1. El comportamiento de los sistemas indica que la integridad de los datos se respeta en la mayoría de los casos, aunque con diferencias relevantes entre ellos: S1 y S5

muestran mejores estados en los mecanismos de control de cambios y de validaciones de la información, mientras que S2 y S3 se sitúan en un intermedio que sugiere la estabilidad pero con latentes peligros, y S4 nuevamente concentra la mayor proporción de inseguridad, repitiendo el patrón crítico ya observado en dimensiones anteriores. La recurrencia de S4 como sistema vulnerable señala la necesidad de intervenciones focalizadas que refuercen los controles de validación, trazabilidad y auditoría para garantizar un nivel uniforme de seguridad en todos los sistemas durante el año 2025.

Disponibilidad

Tabla 41

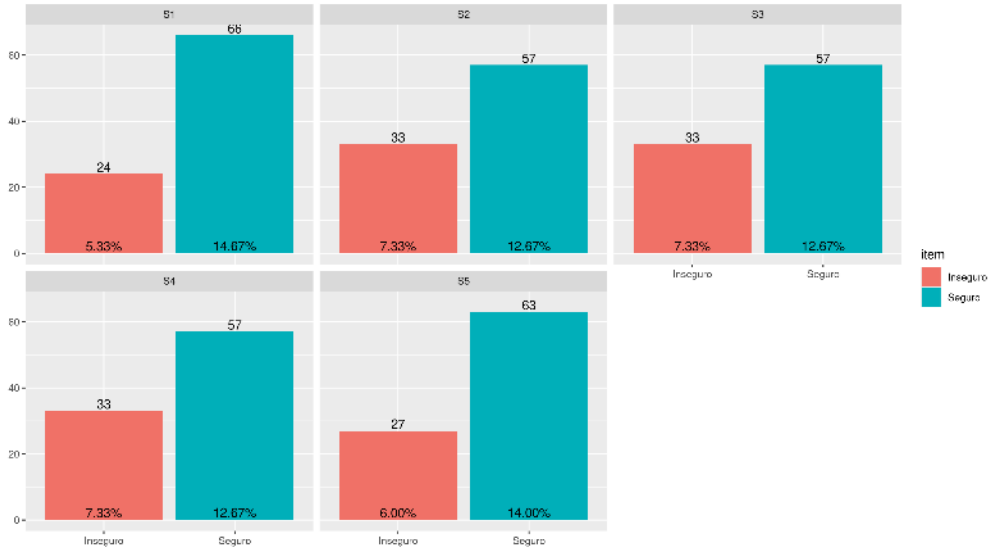
Observaciones sobre la disponibilidad por sistema de información según la norma ISO/IEC 27001

	Disponibilidad	
Características	Inseguro N = 150 (33%)	Inseguro N = 150 (33%)
Sistema		
S1	24 (16%)	24 (16%)
S2	33 (22%)	33 (22%)
S3	33 (22%)	33 (22%)
S4	33 (22%)	33 (22%)
S5	27 (18%)	27 (18%)

Fuente. Elaboración Propia (2025)

Figura 38

Gráfico sobre las observaciones sobre la disponibilidad por sistema de información según la norma ISO/IEC 27001



Fuente. Elaboración Propia (2025)

Interpretación: S1 alcanzó 66 seguros (22 %) y 24 inseguros (16 %), mostrando un balance favorable; S2 reportó 57 seguros (19 %) y 33 inseguros (22 %), reflejando una proporción inclinada hacia la inseguridad; S3 presentó la misma distribución que S2 con 57 seguros (19 %) y 33 inseguros (22 %); S4 también repitió el patrón con 57 seguros (19 %) y 33 inseguros (22 %), confirmando una condición de vulnerabilidad sostenida; y S5 registró 63 seguros (21 %) frente a 27 inseguros (18 %), consolidándose como el segundo sistema con mejor desempeño junto a S1. La contraposición de los sistemas es indiscutible: S1 y S5 exponen prácticas sólidas en la gestión de backups y de recuperación de fallos, mientras que S2, S3 y S4 acumulan la mayor proporción de registros inseguros, lo que indica problemáticas recurrentes en la disponibilidad de los servicios críticos. La concentración de estos tres sistemas en la misma proporción de inseguridad advierte un patrón estructural que puede deberse a insuficiencias comunes en la gestión de la infraestructura o de los protocolos de contingencia.

4.2. Discusiones

4.2.1. En relación al objetivo general

La presente investigación tuvo como objetivo general evaluar la influencia de los criterios de la norma ISO/IEC 27001 en la seguridad de los sistemas de información en Inversiones RMK, Lircay – 2025. Los resultados obtenidos a través del modelo de regresión

lineal evidenciaron que el cumplimiento de la norma influyó de manera significativa en la seguridad de los sistemas de información, con un coeficiente $\beta_1 = 0.778$, un $R^2 = 0.636$ y un valor $p = 0.000$. Estos valores muestran que más del 63% de la variabilidad en la seguridad fue explicada por la aplicación de la norma, lo que confirma que las prácticas normativas tienen un efecto directo y positivo sobre la protección de la información. Este hallazgo evidencia que, incluso en un contexto regional con limitaciones tecnológicas, la implementación de estándares internacionales puede generar mejoras medibles en la gestión de la seguridad. En el ámbito local, los antecedentes en Huancavelica son escasos y se centran principalmente en la gestión administrativa o procesos organizacionales, lo que refuerza el vacío de literatura en torno a la seguridad informática en este espacio geográfico. Esto resalta que los resultados alcanzados en Inversiones RMK representan un aporte novedoso, pues trasladan un estándar internacional a un entorno con condiciones socioeconómicas particulares. A nivel nacional, estudios como el de De la Cruz (2024) evidencian que, en el caso de la ciudad de Lima, la norma ISO/IEC 27001 terminó beneficiando a la primera, con una disminución de los incidentes de seguridad del 99%. Complementariamente, Rodríguez (2023) encuentra que la aplicación del ciclo PHVA se traduce en un incremento de la madurez de la seguridad, en una consultora de sistemas, con reducción de las vulnerabilidades de confidencialidad, integridad y disponibilidad. Ambos estudios, ambos realizados en la capital, son concordantes con los resultados de Lircay respecto a los efectos positivos de la norma, pero muestran magnitudes que son superiores y que son explicadas por las diferencias en la infraestructura tecnológica y la disponibilidad de los recursos. A nivel internacional, Mirtsch (2023), en Alemania, identificó que la adopción de la norma ISO/IEC 27001 se llevó a cabo en función de factores como la cultura organizacional y de motivaciones estratégicas, mientras que Salas et al. (2024), en Quito, mostraron que las micro y pequeñas empresas tienen que enfrentarse a dificultades asociadas a recursos y resistencia al cambio. Estos hallazgos internacionales muestran que la norma ISO/IEC 27001

sólo es efectiva si se da en un determinado contexto. En Alemania, el nivel limitante es la percepción de los costes frente a beneficios, mientras que en Quito las limitaciones son económicas y humanas. La situación de Lircay se asemeja más a la ecuatoriana, lo que explica la magnitud intermedia del efecto identificado en Inversiones RMK. Desde el marco teórico, el estándar ISO/IEC 27001 establece que un-Sistema de Gestión de Seguridad de la Información permite proteger la confidencialidad, integridad y disponibilidad de los datos mediante un enfoque estructurado de gestión del riesgo y mejora continua (ISO/IEC, 2022; Viteri, 2022). Culot et al. (2021) sostienen que la norma se ha consolidado como uno de los marcos más adoptados a nivel mundial gracias a su alineación con el ciclo PHVA. En este sentido, los resultados obtenidos en Inversiones RMK se alinean plenamente con lo planteado en la teoría, confirmando que la aplicación disciplinada de la norma permite generar un efecto positivo y verificable en la seguridad de la información.

4.2.2. En relación a los objetivos específicos

- La investigación presentada tuvo como objetivo específico valorar cómo afectan los criterios de normativa ISO/IEC 27001 a la confidencialidad de los sistemas de información de la organización Inversiones RMK, Lircay – 2025. El análisis inferencial permitió observar que la norma ISO/IEC 27001 influyó de forma significativa en la confidencialidad según se desprende de un coeficiente $\beta_1 = 1.907$, un $R^2 = 0.491$ y un $p = 0.000$. El resultado hace pensar que cerca del 49% del valor de la confidencialidad es influido por la aplicación de la norma. El resultado mostrado corrobora la relación positiva y fuerte que existe: a mayor grado de cumplimiento de norma mayor capacidad para proteger la confidencialidad de los datos frente a accesos no autorizados, espionaje y revelaciones indebidas. En el ámbito local, la literatura de Huancavelica se ha ceñido a la gestión educativa o administrativa, dejando al margen el entorno de la seguridad digital, razón por la cual se considera que el hallazgo es relevante, pues muestra que la

norma ISO/IEC 27001 puede ser aplicada debidamente en un contexto donde las limitaciones tecnológicas y la alta vulnerabilidad frente a ciber amenazas puedan existir. A nivel nacional Rodríguez (2023) documentó que tras una aplicación de la norma ISO/IEC 27001 en una consultora de sistemas, la madurez en seguridad había mejorado y los incidentes en confidencialidad se habían visto reducidos casi por completo. Este patrón fue respaldado por De la Cruz (2024) en una empresa de servicios de Lima, donde encontró una mejora del 99% en la protección de datos. Los resultados para Inversiones RMK eran convergentes respecto a la dirección del impacto pero con un R^2 menor, lo cual puede explicarse por las brechas tecnológicas y de recursos humanos que diferencian a la empresa de Huancavelica respecto a la capital. En otro contexto, el de Quito, Salas et al. (2024) encontraron que las micro y pequeñas empresas enfrentaban serias dificultades para asegurar la confidencialidad debido a la falta de personal capacitado y a la resistencia al cambio, a su vez que Yungán y Narváez (2022) concluyeron que la norma no solo facilita la mitigación de riesgos y la protección de los activos para diversos sectores. En este sentido, todos ellos llegan a la misma conclusión: la norma ISO/IEC 27001 tiene un efecto claro en la confidencialidad, dando cuenta de un efecto que depende del tamaño de la empresa y de su capacidad de invertir. El caso de Lircay, con un efecto positivo, pero menos robusto, se asemeja más al contexto ecuatoriano que a los de mayor desarrollo tecnológico. Desde el marco teórico, la ISO/IEC 27001 establece la confidencialidad como uno de los pilares de la seguridad de la información, junto con la integridad y la disponibilidad (ISO/IEC, 2022). Viteri (2022) indica que la norma permite proteger datos corporativos y de clientes mediante un Sistema de Gestión de Seguridad de la Información, mientras que Pozo et al. (2025) destacan mecanismos como cifrado, autenticación y segmentación de accesos como claves para garantizar la confidencialidad. Los resultados de Inversiones RMK engrosan

estas bases conceptuales, apoyando la afirmación de que el cumplimiento normativo da como resultado un incremento real en la capacidad de proteger la privacidad de los datos.

- La presente investigación tuvo como propósito específico comprobar el cumplimiento de los criterios de la norma ISO/IEC 27001 en la integridad de los sistemas de información en Inversiones RMK, Lircay – 2025. El modelo de regresión nos sugiere que el cumplimiento de la norma efectivamente incide en la integridad, alcanzando un coeficiente $\beta_1 = 0.251$, un $R^2 = 0.490$ y un valor $p = 0.000$, indicando que el 49% de la variabilidad de la variable integridad es explicada gracias al cumplimiento de la norma. Este hallazgo confirma que las prácticas de ISO/IEC 27001 fortalecen la capacidad de los sistemas para garantizar la exactitud y consistencia de la información frente a errores o modificaciones no autorizadas. A nivel local, no se han desarrollado trabajos empíricos en Huancavelica que midan la influencia de la ISO/IEC 27001 en la integridad de los sistemas. Esta limitación en las evidencias nos hace notar que los resultados que han sido obtenidos en Inversiones RMK son innovadores en el ámbito regional en tanto demuestran la posibilidad de aplicar la norma hasta en ambientes con infraestructuras precarias. A nivel nacional, Morón (2023), en Rash Perú S.A.C., adoptó un sistema de gestión basado en la norma ISO/IEC 27002 que reportó mejoras en la seguridad informática, especialmente en cuanto a integridad de los datos, que pasó de estadísticas mínimas del 0% al 27% en posteriores pruebas. De la Cruz (2024) mostró que la implementación de la norma ISO/IEC 27001 logró reducir en un 99% el número de incidentes relacionados con la alteración de datos en una empresa prestadora de servicios en Lima. Los resultados de Inversiones RMK son acordes con este tipo de evidencias: sin embargo, el efecto hallado (49%) es más modesto que en los contextos limeños. Esta diferencia puede explicarse atendiendo a las condiciones de recursos

técnicos y humanos en la capital con respecto a una provincia como Lircay. Por último, a nivel internacional, Yungán y Narváez (2022) observaron que la norma ISO/IEC 27001 permite identificar riesgos que afectan la integridad de los activos informáticos, mientras que Salas et al. (2024) en Quito mostraron que muchas microempresas eran vulnerables, fundamentalmente por la falta de formación y resistencia organizacional. Los resultados de Inversiones RMK se sitúan en un punto medio: se aprecia un efecto positivo de la norma, pero también indican que la integridad no llega a niveles óptimos, probablemente por razones parecidas a las descritas de Quito. En cuanto al marco teórico, la integridad se encuentra entre los tres pilares de la seguridad de la información. ISO/IEC (2022) justifica esto al exponer que los controles normativos persiguen evitar la alteración no autorizada de los datos y su exactitud en el ciclo de vida. En cambio, Vega (2021) dice que la integridad se tiene que alcanzar mediante políticas de control de cambios, así como auditorías sistemáticas, y Pozo et al. (2025) alude a que los mecanismos describe como checksums y firmas digitales son elementos clave para garantizar la confiabilidad. Los resultados de Inversiones RMK se alinean con esto al poder asegurar que implementar ISO/IEC 27001 se traduce en mejoras directas en la protección de la integridad de la información.

El presente proyecto de investigación tuvo como objetivo específico el evaluar el cumplimiento de los criterios establecidos en la norma ISO/IEC 27001 en la disponibilidad de los sistemas de información de Inversiones RMK, Lircay – 2025. El análisis de regresión nos permitió comprobar que la norma tenía un efecto significativo sobre la disponibilidad, pues se obtuvo $\beta_1 = 0.270$ desde $R^2 = 0.545$ y $p = 0.000$, en tanto que el 54.5% de la variación de la disponibilidad era explicada por la norma.

La conclusión es que la ejecución de los controles normativos puede incrementar de manera clara la disponibilidad de los sistemas de información.

En el contexto local, no se encontraron investigaciones previas en Huancavelica vinculadas con la norma ISO/IEC 27001 y la disponibilidad, lo que aumenta la singularidad de los resultados obtenidos en el caso de Inversiones RMK, donde se puede evidenciar que la norma fue capaz de traducir el limitado estado de la infraestructura en un incremento de la continuidad operativa de los sistemas de información y en la disponibilidad oportuna de los datos. A nivel nacional, Contador y Tapia (2024) informan que en el caso de una empresa minera de Lima la implementación de la norma ISO/IEC 27001 generó mejoras de tipo estadístico en la disponibilidad de los sistemas, mientras que De la Cruz (2024) registró reducciones en el número de acontecimientos que ponían en peligro la continuidad del servicio en una empresa de servicios. A pesar de que en la ciudad de Lima los efectos expuestos alcanzaron casi los niveles absolutos, los resultados de Inversiones RMK alcanzaron una explicación del 54.5%, valor que denota una brecha que debe ser atribuida a la infraestructura tecnológica y a la disponibilidad de recursos que permite la capital frente a Lircay. A nivel internacional, Donoso et al. (2023) evidencian en Ecuador que el uso de un SGSI basado en la ISO/IEC 27001 en el sistema de rehabilitación social deriva en mejoras en la capacidad de disponibilidad de los sistemas merced la inclusión de tecnología avanzada, pero también Mirtsch (2023) en Alemania argumenta que la disponibilidad no solo deriva del cumplimento de las normas, sino que requiere de financiar la infraestructura de la empresa en términos de inversión sostenida. Los resultados de Inversiones RMK confirman la línea argumentativa planteada: la norma genera un efecto positivo, pero la fuerza que alcanza está determinando por el nivel de recursos que se dispone y por el grado madurez tecnológica de cada contexto. Desde el marco teórico, para la norma ISO/IEC 27001, la disponibilidad es uno de los tres principios de la tríada de la seguridad de la información junto con la confidencialidad y la integridad (ISO/IEC,

2022). Según Samaniego y Ponce (2021), esta dimensión requiere planes de respaldo en caso de errores, mecanismos redundantes y protocolos específicos de recuperación ante desastres, mientras que Pozo et al. (2025) sostienen la comunicación en procesos organizativos aceptables en términos de disponibilidad y no solo dependerá de controles técnicos. Los resultados que ofrece Inversiones RMK responden a estos planteamientos y muestran que la aplicación de la norma contribuye para mantener la continuidad de servicios, pero también evidencian que la norma debe complementarse con inversiones en infraestructura y con el entrenamiento del personal para que su aplicación sea efectiva.

4.3. Contrastación de hipótesis

4.3.1. Pruebas de normalidad y supuestos para la elección de la prueba estadística

Para la selección de la prueba estadística adecuada en el análisis de los datos del estudio, fue indispensable evaluar previamente el cumplimiento de los criterios de normalidad y los supuestos propios del modelo de regresión.

4.3.1.1. Prueba de normalidad - Variable ISO/IEC 27001

Se aplicó el test de normalidad de Kolmogorov-Smirnov y el test de Lilliefors

1. Planteamiento de la hipótesis nula y alternativa

- H_0: La variable ISO/IEC 27001 sigue una distribución normal
- H_1: La variable ISO/IEC 27001 no sigue una distribución normal.

2. Elección del nivel de significancia α

El grado de significancia elegido para evaluar la hipótesis es $\alpha = 5\% = 0.05$.

3. Cálculo del estadístico de prueba

Tabla 42

Prueba de normalidad de la variable ISO/IEC 27001

	Kolmogorov-Smirnov	Lilliefors

	Estadístico	gl	Sig.	Estadístico	gl	Sig.
ISO/IEC 27001	.155	n	.000	.155	n	.000

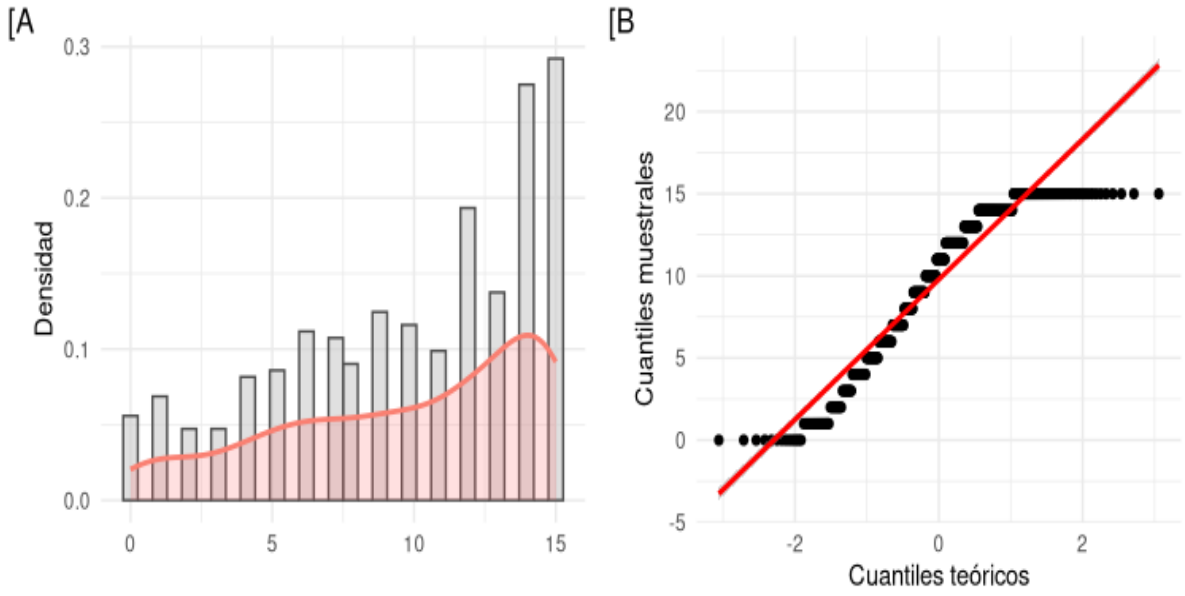
Fuente. Elaboración Propia (2025)

4. Toma de decisión

Resultado	Decisión
Si el valor p ≤ α	Se rechaza H_0 en favor de H_1
Si el valor p > α	No se rechaza H_0

Figura 39

Gráfico de la normalidad de la variable ISO/IEC 27001



Fuente. Elaboración Propia (2025)

Decisión: Como p-valor = .000 ≤ .05 se rechaza H_0 y se acepta H_1, entonces la variable ISO/IEC 27001 no sigue una distribución normal.

Interpretación: La evidencia empírica indica que la variable ISO/IEC 27001 no se ajusta a un modelo de distribución normal. Este hallazgo tiene implicancias directas en la elección de los estadísticos de prueba para la contrastación de hipótesis ya que obliga a privilegiar métodos no paramétricos que no dependen de supuestos de normalidad. En el contexto de Inversiones RMK en Lircay esto refleja que la implementación de controles de seguridad se distribuye de manera heterogénea entre sistemas lo que genera asimetrías en los datos. Por ello el análisis inferencial deberá apoyarse en técnicas robustas capaces de capturar estas irregularidades y ofrecer

conclusiones fiables sobre la relación entre la norma ISO/IEC 27001 y la seguridad de los sistemas de información.

4.3.1.2. Prueba de normalidad - Variable Seguridad de los sistemas de información

Se aplicó el test de normalidad de Kolmogorov-Smirnov y el test de Lilliefors

1. Planteamiento de la hipótesis nula y alternativa

- H_0: La variable Seguridad de los sistemas de información sigue una distribución normal.
- H_1: La variable Seguridad de los sistemas de información no sigue una distribución normal.

2. Elección del nivel de significancia α

El grado de significancia elegido para evaluar la hipótesis es $\alpha = 5\% = 0.05$.

3. Cálculo del estadístico de prueba

Tabla 43

Prueba de normalidad de la variable Seguridad de los sistemas de información

	Kolmogorov-Smirnov			Lilliefors		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
Seguridad de los sistemas de información	.122	n	.000	.132	n	.000

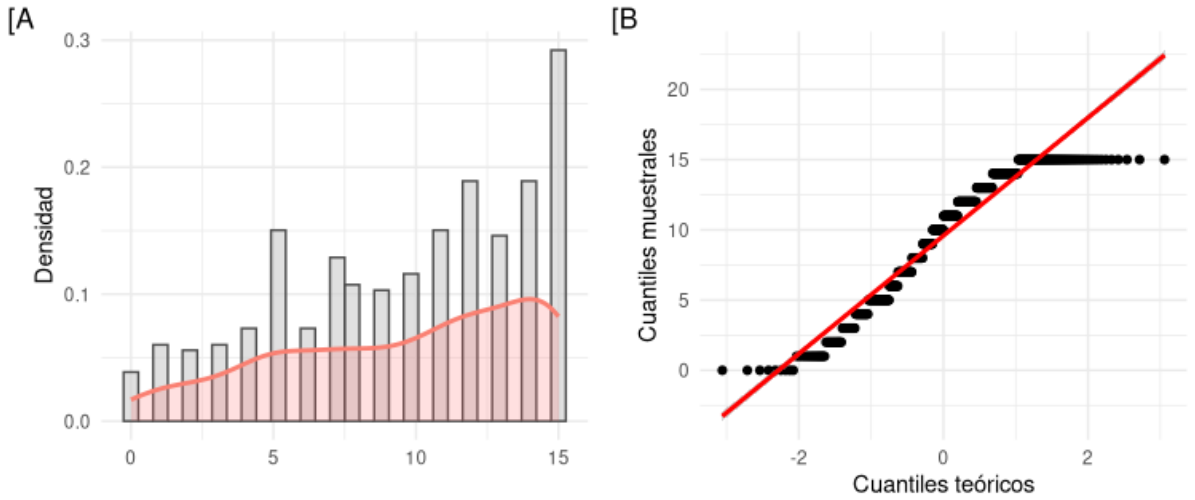
Fuente. Elaboración Propia (2025)

4. Toma de decisión

Resultado	Decisión
Si el valor $p \leq \alpha$	Se rechaza H_0 en favor de H_1
Si el valor $p > \alpha$	No se rechaza H_0

Figura 40

Gráfico de la normalidad de la variable Seguridad de los sistemas de información



Fuente. Elaboración Propia (2025)

Decisión: Como p-value = .000 ≤ .05 se rechaza H_0 y se acepta H_1, entonces la variable Seguridad de los sistemas de información no sigue una distribución normal.

Interpretación: Los resultados estadísticos confirman que la variable Seguridad de los sistemas de información no presenta un ajuste normal. Esto implica que la distribución de registros seguros e inseguros entre los diferentes sistemas de Inversiones RMK es heterogénea y que los datos no se concentran en torno a un valor promedio estable. En términos metodológicos el hallazgo orienta a trabajar con pruebas no paramétricas para el contraste de hipótesis ya que éstas no exigen el supuesto de normalidad. Desde la perspectiva contextual el patrón irregular refleja la realidad organizacional de Lircay donde la madurez de los sistemas de información es desigual y donde la vulnerabilidad cibernética tiende a concentrarse en determinados nodos. Por tanto, los análisis posteriores deberán considerar esta dispersión para ofrecer conclusiones sólidas sobre la relación entre la norma ISO/IEC 27001 y la seguridad alcanzada en la empresa.

4.3.1.3. Evaluación de los supuestos de regresión

Se aplicó la función para examinar los supuestos clásicos de la regresión lineal en el modelo ajustado.

1. Planteamiento de la hipótesis nula y alternativa

- H_0: El modelo de regresión lineal cumple con los supuestos de normalidad de los residuos, ausencia de sesgo, homocedasticidad y adecuación funcional.
- H_1: El modelo de regresión lineal no cumple con al menos uno de los supuestos anteriores.

2. Nivel de significancia α

Se estableció un nivel de significancia de α = 5% = 0.05.

3. Resumen de los resultados del test global y de cada componente

Tabla 44

Supuestos de la regresión

Supuesto evaluado	Estadístico	p-value	Decisión
Global	19.825	.001	Supuestos NO cumplidos
Skewness	13.147	.000	Supuestos NO cumplidos
Kurtosis	6.478	.011	Supuestos NO cumplidos
Link Function	0.021	.886	Supuestos aceptables
Heteroscedasticidad	0.180	.672	Supuestos aceptables

Fuente. Elaboración Propia (2025)

4. Toma de decisión

Resultado	Decisión
Si el valor $p \leq \alpha$	Se rechaza H_0 en favor de H_1
Si el valor $p > \alpha$	No se rechaza H_0

Decisión: Como el p-value del estadístico global = .001 ≤ .05, se rechaza H_0 y se acepta H_1, por lo que el modelo de regresión lineal no satisface plenamente los supuestos requeridos.

Interpretación: El test global sugiere que el modelo no cumple los principios de la regresión lineal. En especial se da sesgo en la distribución de los residuos (skewness) y el hecho de ser diferente a la normal respecto a la curtosis implica colas más pesadas o más extremos que en una distribución normal. Sin embargo, los supuestos de homocedasticidad y de adecuada especificación del vínculo lineal sí se cumplen, lo que

implica que la relación entre la variable independiente y la dependiente es lineal y no se produce varianza desigual en la residual. El incumplimiento de normalidad y simetría en los residuos es esperable porque los datos provienen de sumatorias de variables dicotómicas, lo que genera distribuciones inherentemente sesgadas.

4.3.1.4. Test para la prueba estadística

Con base en los resultados obtenidos en la evaluación de los criterios de normalidad y de los supuestos del modelo, se procedió a seleccionar la prueba correspondiente para el análisis de la relación entre las variables del estudio. En este sentido, se aplicó un modelo de regresión lineal en el que el cumplimiento de la norma ISO/IEC 27001 se estableció como variable independiente y las variables dependientes correspondientes a cada hipótesis, con el propósito de estimar la influencia que ejerce la norma sobre cada dimensión de la seguridad de los sistemas de información.

4.3.2. Contrastación de hipótesis general

4.3.2.1. Planteamiento de la hipótesis

- **Hipótesis Nula (H_0):** El cumplimiento de los criterios de la norma ISO/IEC 27001 no influye en la seguridad de los sistemas de información en Inversiones RMK, Lircay – 2025.
- **Hipótesis Alterna (H_1):** El cumplimiento de los criterios de la norma ISO/IEC 27001 influye en la seguridad de los sistemas de información en Inversiones RMK, Lircay – 2025.

4.3.2.2. Determinación del nivel de significancia

Se adoptó un nivel de significancia de $\alpha = 0.05$ (5%), lo que implica un nivel de confianza del 95% para la toma de decisiones.

4.3.2.3. Elección de la prueba estadística

Para evaluar la influencia del cumplimiento de los criterios de la norma ISO/IEC 27001 sobre la seguridad de los sistemas de información, se seleccionó el modelo de regresión lineal simple. Esta prueba permite estimar la magnitud y dirección de la relación entre la variable independiente (cumplimiento normativo) y la variable dependiente (seguridad de los sistemas), así como determinar si dicha relación es estadísticamente significativa.

- **Variable independiente (X):** Cumplimiento de criterios ISO/IEC 27001
- **Variable dependiente (Y):** Seguridad de los sistemas de información.

4.3.2.4. Cálculo del valor tabular

Tabla 45

Estadísticos e interpretación de la regresión – Hipótesis general

Estadístico	Valor
β_1	0.778
Valor p	< .001
R^2	0.636
Prueba F	781.3

Fuente. Elaboración Propia (2025)

Tabla 46

Resumen del modelo de regresión lineal – Hipótesis general

Modelo	R	R cuadrado	R cuadrado ajustado	Error estándar de la estimación	Cambio en R cuadrado	Cambio en F	gl1	gl2	Sig. cambio en F
1	0.797	0.636	0.635	2.637	0.636	781.3	1	448	.000

Fuente. Elaboración Propia (2025)

Tabla 47

ANOVA de la regresión lineal – Hipótesis general

Modelo	Suma de cuadrados	gl	Media cuadrática	F	Sig.
Regresión	5433.2	1	5433.2	781.3	.000
Residual	3116.0	448	6.9		

Total	**8549.2**	**449**

Fuente. Elaboración Propia (2025)

Tabla 48

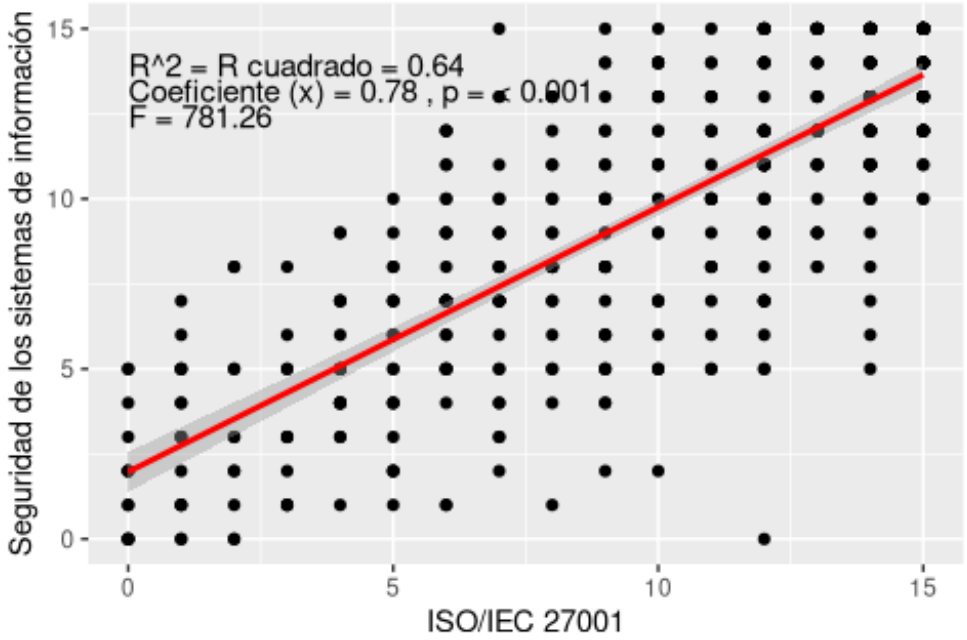
Coeficientes de la regresión lineal – Hipótesis general

Modelo	Variable	Coef. no estandarizados B	Error estándar	Coef. estandarizados Beta	t	Sig.
1	(Constante)	1.974	0.299		6.592	.000
	ISO/IEC 27001	0.778	0.028	0.797	27.951	.000

Fuente. Elaboración Propia (2025)

Figura 41

Influencia de ISO/IEC 27001 en Seguridad de los sistemas de información



Fuente. Elaboración Propia (2025)

4.3.2.5. Decisión estadística

Regla de decisión:

- Si el valor $p \leq \alpha$ (0.05) → Se rechaza la hipótesis nula (H_0)
- Si el valor $p > \alpha$ (0.05) → No se rechaza la hipótesis nula (H_0)

Decisión: Dado que el valor p = 0.000 es menor que el nivel de significancia α = 0.05, se rechaza la hipótesis nula (H_0) y se acepta la hipótesis alterna (H_1).

4.3.2.6. Interpretación

El modelo de regresión confirma que el cumplimiento de los criterios de la norma ISO/IEC 27001 influye de manera significativa sobre la seguridad de los sistemas de información en Inversiones RMK. El coeficiente $\beta_1 = 0.778$ indica que por cada incremento en el cumplimiento de la norma se produce un aumento proporcional en la seguridad, lo que refleja una relación fuerte y positiva. El valor de $R^2 = 0.636$ muestra que más del 60% de la variabilidad en la seguridad puede ser explicada directamente por el nivel de cumplimiento de la norma, lo cual respalda su validez como marco regulador. La significancia de la prueba F y la magnitud del coeficiente Beta (.797) consolidan la robustez del modelo. Aunque los supuestos de normalidad de los residuos no se cumplieron plenamente, la linealidad y homocedasticidad permanecen estables, lo que otorga confiabilidad al análisis.

4.3.3. Contrastación de hipótesis específica 1

4.3.3.1. Planteamiento de hipótesis

- **Hipótesis Nula (H_0):** El cumplimiento de los criterios de la norma ISO/IEC 27001 no influye en la confidencialidad de los sistemas de información en Inversiones RMK, Lircay – 2025.
- **Hipótesis Alterna (H_1):** El cumplimiento de los criterios de la norma ISO/IEC 27001 influye en la confidencialidad de los sistemas de información en Inversiones RMK, Lircay – 2025.

4.3.3.2. Determinación del nivel de significancia

Se mantiene el nivel de significancia de α = 0.05 (5%)

4.3.3.3. Elección de la prueba estadística

Para evaluar la influencia del cumplimiento de los criterios de la norma ISO/IEC 27001 sobre la confidencialidad de los sistemas de información, se aplicó un modelo de regresión lineal simple.

- **Variable independiente (X):** Cumplimiento de criterios ISO/IEC 27001
- **Variable dependiente (Y):** Confidencialidad de los sistemas de información

4.3.3.4. Cálculo del valor tabular

Tabla 49

Estadísticos e interpretación de la regresión – Hipótesis específica 1

Estadístico	Valor
β_1	1.907
Valor p	< .001
R^2	0.491
Prueba F	432.8

Fuente. Elaboración Propia (2025)

Tabla 50

Resumen del modelo de regresión lineal – Hipótesis específica 1

Modelo	R	R cuadrado	R cuadrado ajustado	Error estándar de la estimación	Cambio en R cuadrado	Cambio en F	gl1	gl2	Sig. cambio en F
1	0.701	0.491	0.490	3.191	0.491	432.8	1	448	.000

Fuente. Elaboración Propia (2025)

Tabla 51

ANOVA de la regresión lineal – Hipótesis específica 1

Modelo	Suma de cuadrados	gl	Media cuadrática	F	Sig.

Regresión	4395.3	1	4395.3	432.8	.000
Residual	4550.0	448	10.2		
Total	**8945.3**	**449**			

Fuente. Elaboración Propia (2025)

Tabla 52

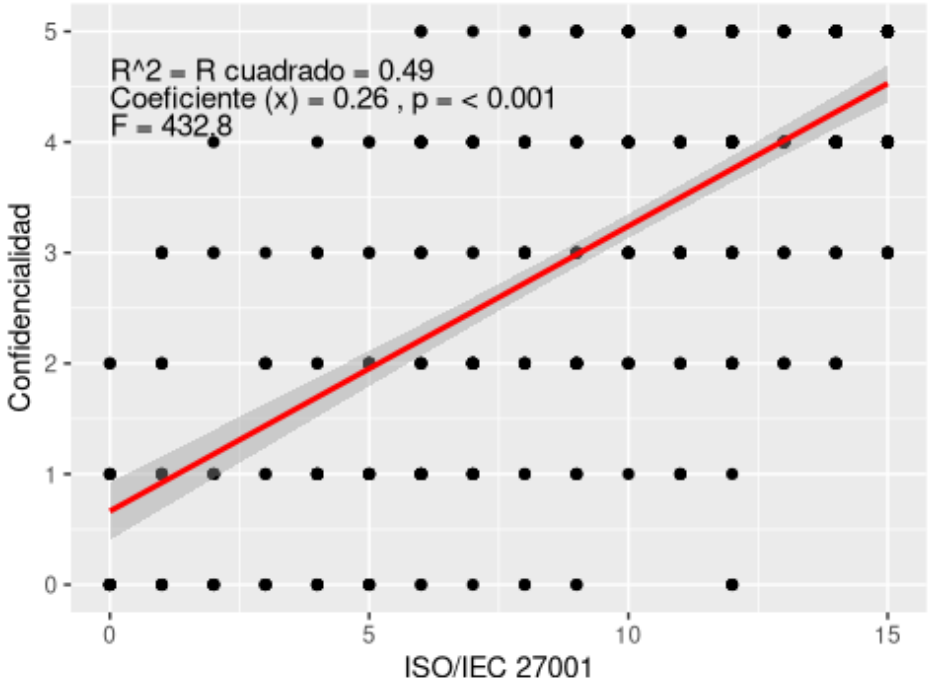
Coeficientes de la regresión lineal – Hipótesis específica 1

Modelo	Variable	Coef. no estandarizados B	Error estándar	Coef. estandarizados Beta	t	Sig.
1	(Constante)	3.708	0.328		11.290	.000
	ISO/IEC 27001	1.907	0.092	0.701	20.800	.000

Fuente. Elaboración Propia (2025)

Figura 42

Influencia de ISO/IEC 27001 en Confidencialidad



Fuente. Elaboración Propia (2025)

4.3.3.5. Decisión estadística

Regla de decisión:

- Si el valor $p \leq \alpha$ (0.05) → Se rechaza la hipótesis nula (H_0)

- Si el valor $p > \alpha$ (0.05) → No se rechaza la hipótesis nula (H_0)

Decisión: Dado que $p < 0.001 \leq 0.05$, se rechaza la hipótesis nula (H_0) y se acepta la hipótesis alterna (H_1).

4.3.3.6. Interpretación

El análisis confirma que el cumplimiento de ISO/IEC 27001 tiene una influencia estadísticamente significativa en la confidencialidad. El valor $\beta_1 = 1.907$ refiere un efecto benéfico y fuerte en; esto es, la norma cuanto más se aplique va proporcionando mayor protección frente a accesos no regulados también con respecto al cifrado de datos y del control del acceso. Un $R^2 = 0.491$ refiere que casi la mitad de la variabilidad que presenta la confidencialidad puede ser explicada por la norma, pero existe un 50% que puede ser explicado por factores técnicos y organizacionales ajenos. Esto lleva a que la norma sea un factor determinante pero no exclusivo. En el entorno de Lircay, este resultado revela que el avance en la aplicación de la norma se traduce en mejoras directas sobre la protección de información sensible. La evidencia empírica respalda que la implementación sistemática de controles normativos no solo fortalece las barreras de seguridad, sino que también construye confianza institucional frente a riesgos crecientes en 2025.

4.3.4. Contrastación de hipótesis específica 2

4.3.4.1. Planteamiento de la hipótesis

- **Hipótesis Nula (H_0):** El cumplimiento de los criterios de la norma ISO/IEC 27001 no influye en la integridad de los sistemas de información en Inversiones RMK, Lircay – 2025.
- **Hipótesis Alterna (H_1):** El cumplimiento de los criterios de la norma ISO/IEC 27001 influye en la integridad de los sistemas de información en Inversiones RMK, Lircay – 2025.

4.3.4.2. Determinación del nivel de significancia

Se mantiene el nivel de significancia de $\alpha = 0.05$ (5%)

4.3.4.3. Elección de la prueba estadística

Para evaluar la influencia del cumplimiento de los criterios de la norma ISO/IEC 27001 sobre la integridad de los sistemas de información, se aplicó un modelo de regresión lineal simple.

- **Variable independiente (X):** Cumplimiento de criterios ISO/IEC 27001
- **Variable dependiente (Y):** Integridad de los sistemas de información

4.3.4.4. Cálculo del valor tabular

Tabla 53

Estadísticos e interpretación de la regresión – Hipótesis específica 2

Estadístico	Valor
β_1	0.251
Valor p	< .001
R^2	0.490
Prueba F	430.4

Fuente. Elaboración Propia (2025)

Tabla 54

Resumen del modelo de regresión lineal – Hipótesis específica 2

Modelo	R	R cuadrado	R cuadrado ajustado	Error estándar de la estimación	Cambio en R cuadrado	Cambio en F	gl1	gl2	Sig. cambio en F
1	0.700	0.490	0.489	1.146	0.490	430.4	1	448	.000

Fuente. Elaboración Propia (2025)

Tabla 55

ANOVA de la regresión lineal – Hipótesis específica 2

Modelo	Suma de cuadrados	gl	Media cuadrática	F	Sig.
Regresión	565.6	1	565.6	430.4	.000
Residual	589.8	448	1.3		
Total	**1155.4**	**449**			

Fuente. Elaboración Propia (2025)

Tabla 56

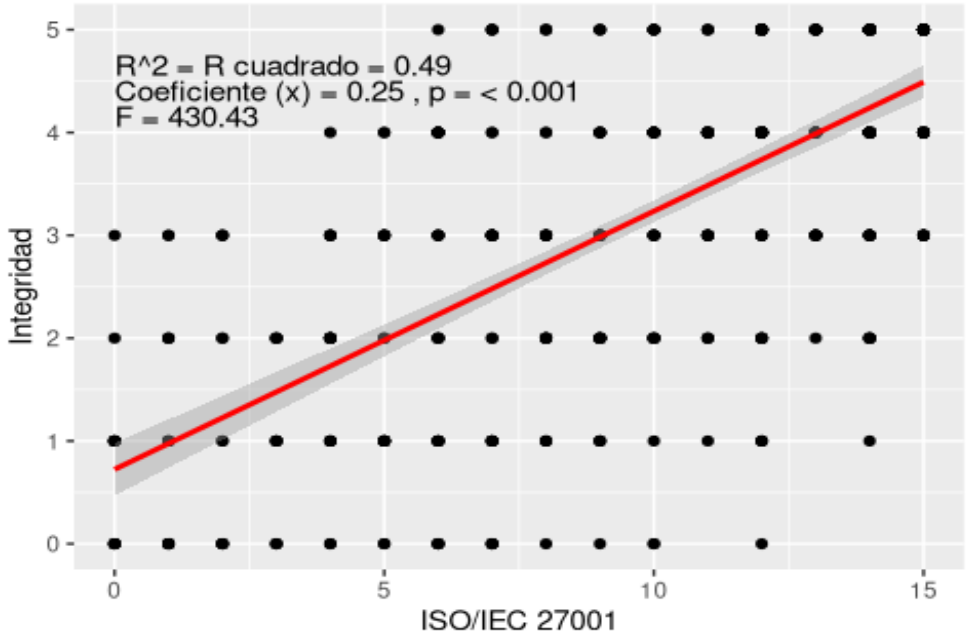
Coeficientes de la regresión lineal – Hipótesis específica 2

Modelo	Variable	Coef. no estandarizados B	Error estándar	Coef. estandarizados Beta	t	Sig.
1	(Constante)	0.724	0.130		5.559	.000
	ISO/IEC 27001	0.251	0.012	0.700	20.747	.000

Fuente. Elaboración Propia (2025)

Figura 43

Influencia de ISO/IEC 27001 en Integridad



Fuente. Elaboración Propia (2025)

4.3.4.5. Decisión estadística

Regla de decisión:

- Si el valor $p \leq \alpha$ (0.05) → Se rechaza la hipótesis nula (H_0)
- Si el valor $p > \alpha$ (0.05) → No se rechaza la hipótesis nula (H_0)

Decisión: Dado que $p < 0.001 \leq 0.05$, se rechaza la hipótesis nula (H_0) y se acepta la hipótesis alterna (H_1).

4.3.4.6. Interpretación

El modelo de regresión muestra que ISO/IEC 27001 influye de manera significativa en la integridad de los sistemas de información. El coeficiente $\beta_1 = 0.251$ refleja que cada incremento en el cumplimiento de la norma refuerza la capacidad de los sistemas para evitar modificaciones no autorizadas, detectar errores y mantener registros de control. El valor de $R^2 = 0.490$ evidencia que aproximadamente la mitad de la variabilidad de la integridad se explica por la aplicación de la norma, mientras el resto corresponde a factores adicionales como la gestión de personal, el soporte tecnológico y la cultura organizacional.

4.3.5. Contrastación de hipótesis específica 3

4.3.5.1. Planteamiento de la hipótesis

- **Hipótesis Nula (H_0):** El cumplimiento de los criterios de la norma ISO/IEC 27001 no influye en la disponibilidad de los sistemas de información en Inversiones RMK, Lircay – 2025.
- **Hipótesis Alterna (H_1):** El cumplimiento de los criterios de la norma ISO/IEC 27001 influye en la disponibilidad de los sistemas de información en Inversiones RMK, Lircay – 2025.

4.3.5.2. Determinación del nivel de significancia

Se mantiene el nivel de significancia de $\alpha = 0.05$ (5%).

4.3.5.3. Elección de la prueba estadística

Para evaluar la influencia del cumplimiento de los criterios de la norma ISO/IEC 27001 sobre la disponibilidad de los sistemas de información, se aplicó un modelo de regresión lineal simple.

- **Variable independiente (X):** Cumplimiento de criterios ISO/IEC 27001
- **Variable dependiente (Y):** Disponibilidad de los sistemas de información

4.3.5.4. Cálculo del valor tabular

Tabla 57

Estadísticos e interpretación de la regresión – Hipótesis específica 3

Estadístico	Valor
β_1	0.270
Valor p	< .001
R^2	0.545
Prueba F	536.5

Fuente. Elaboración Propia (2025)

Tabla 58

Resumen del modelo de regresión lineal – Hipótesis específica 3

Modelo	R	R cuadrado	R cuadrado ajustado	Error estándar de la estimación	Cambio en R cuadrado	Cambio en F	gl1	gl2	Sig. cambio en F
1	0.739	0.545	0.544	1.102	0.545	536.5	1	448	.000

Fuente. Elaboración Propia (2025)

Tabla 59

ANOVA de la regresión lineal – Hipótesis específica 3

Modelo	Suma de cuadrados	gl	Media cuadrática	F	Sig.
Regresión	651.2	1	651.2	536.5	.000
Residual	543.9	448	1.2		
Total	**1195.1**	**449**			

Fuente. Elaboración Propia (2025)

Tabla 60

Coeficientes de la regresión lineal – Hipótesis específica 3

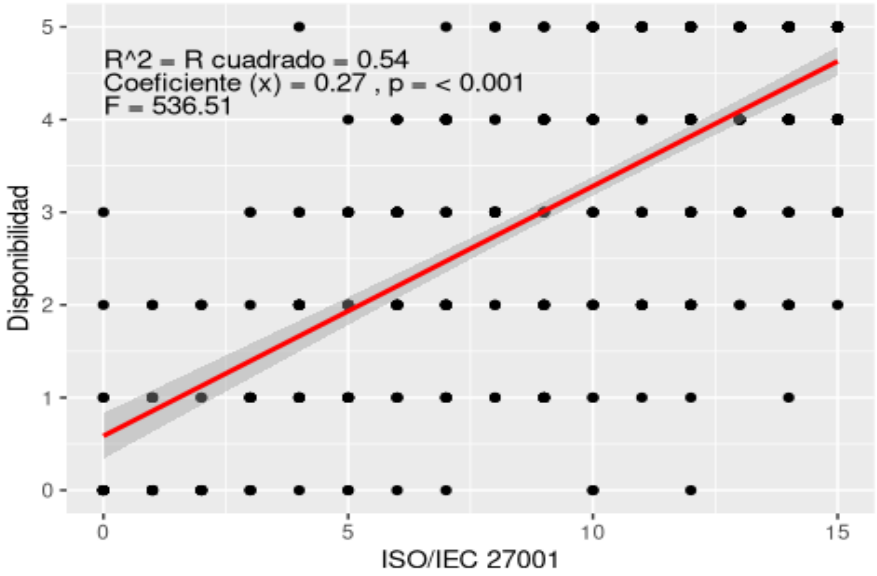
Modelo	Variable	Coef. no estandarizados B	Error estándar	Coef. estandarizados Beta	t	Sig.

1	(Constante)	0.586	0.125		4.681	.000
	ISO/IEC 27001	0.270	0.012	0.739	23.163	.000

Fuente. Elaboración Propia (2025)

Figura 44

Influencia de ISO/IEC 27001 en Disponibilidad



Fuente. Elaboración Propia (2025)

4.3.5.5. Decisión estadística

Regla de decisión:

- Si el valor $p \leq \alpha$ (0.05) → Se rechaza la hipótesis nula (H_0)
- Si el valor $p > \alpha$ (0.05) → No se rechaza la hipótesis nula (H_0)

Decisión: Dado que $p < 0.001 \leq 0.05$, se rechaza la hipótesis nula (H_0) y se acepta la hipótesis alterna (H_1).

4.3.5.6. Interpretación

El análisis estadístico confirma que ISO/IEC 27001 influye significativamente en la disponibilidad de los sistemas de información. El coeficiente $\beta_1 = 0.270$ indica que a mayor cumplimiento de la norma se incrementa la capacidad de los sistemas para permanecer accesibles y funcionales frente a incidentes. El valor de $R^2 = 0.545$ muestra

que más de la mitad de la variabilidad en disponibilidad se explica por la norma, lo que convierte a ISO/IEC 27001 en un factor clave para garantizar la continuidad operativa.

CAPÍTULO V
CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

1. Se confirma una relación lineal y positiva entre ISO/IEC 27001 y la seguridad de los sistemas de información. El modelo reportó β_1 = 0.778 con R^2 = .636 y F = 781.3 con p = .000. La función de enlace y la varianza resultaron estables según gvlma mientras que asimetría y curtosis no cumplieron normalidad como era esperable por el origen dicotómico de los datos. Aun así, la relación estimada se mantuvo consistente y útil para decisión directiva. En este entorno se deduce que elevar el cumplimiento normativo incrementó de forma clara la protección global de los sistemas durante 2025 en Lircay donde la heterogeneidad tecnológica exige priorizar controles que escalen con recursos limitados.
2. El CM de la ISO/IEC 27001 tuvo un efecto estadístico sobre la confidencialidad. Se obtuvo β_1 = 1.907 con R^2 = .491 y F = 432.8 con p = .000. Este efecto resultó en mejoras significativas en control de accesos cifrado y permisos. La fuerza que tiene este coeficiente dice que pequeñas aumentaciones en el CM se traducen en grandes aumentaciones en el resguardo de datos sensibles. Por el hecho que en el contexto operativo de Inversiones RMK esto quería decir blindar información crítica frente ciclos operativos que consideran las brechas de infraestructura a las que está expuesta esta plaza regional que requiere mucho de la disciplina procedimental en su carácter diario.
3. La influencia de la norma sobre la integridad fue consistente. Los resultados del modelo arrojan β_1 = 0.251 con R^2 = .490 y F = 430.4 con p = .000. Los efectos prácticos apoyan la mejora en control de cambios trazabilidad y validación de registros. La fuerza del efecto es moderada pero estable lo que sugiere que la estandarización de procesos llegó a acompañar a auditoría y la auditoría operó el mantenimiento de la exactitud de la información. En el año 2025 y en una lógica organizacional con recursos cortos esto

se traduce en decisiones más seguras y en menos probabilidades de alteraciones no autorizadas.

4. Se observó una relación importante entre el cumplimiento de la ISO/IEC 27001 y la disponibilidad. Se calculó $\beta_1 = 0.270$, con $R^2 = .545$ y $F = 536.5$, $p = .000$. La relación mostraba un efecto de mayor continuidad operativa como resultado de los planes de respaldo de continuidad operativa y los controles para operación diaria. La explicación de más de la mitad de la variabilidad indica que los controles demandados por la norma ayudaron a mantener un acceso oportuno a servicios y a datos. Para Lircay en el 2025 esto significó que se redujeran las interrupciones y se limitaran los riesgos de operación incluso con sus limitaciones de conectividad y de equipamiento.

5.2. Recomendaciones

1. Cada propuesta respondió a la necesidad de trasladar la norma ISO/IEC 27001 a un entorno regional con limitaciones de infraestructura. Se fundamentó en el ciclo de mejora continua (Planificar, Hacer, Verificar, Actuar) descrito en ISO/IEC (2022) (ISO/IEC, 2022), en la gestión de riesgos como pilar estratégico de la seguridad de la información (Culot et al., 2021), y en el principio de la tríada de seguridad de la información (confidencialidad, integridad, disponibilidad) (Pozo et al., 2025). Las técnicas diseñadas para la organización integraron controles automáticos con controles humanos, lo que permitió a la organización obtener resultados sin depender de invertir una alta cifra según el contexto operativo y social de Inversiones RMK en Lircay.
2. Se recomendó implantar un proceso esperado de auditoría de cumplimiento normativo que considere las revisiones periódicas de todos los controles exigidos por la norma ISO/IEC 27001. Consistió en integrar el control en un proceso esporádico de muchas revisiones de auditoría a partir de fichas estándar elaboradas por responsables internos, así como la auditoría trimestral externa, simplificando su proceso.

3. Se recomendó implantar una técnica de segmentación de accesos y trazabilidad doble. Consistía en el almacenamiento paralelo de accesos físicos y accesos digitales, de forma que cada intento de conexión quede evidenciado tanto en un control de usuarios como en una control alterno cifrado. El uso de este doble canal permitía una detección de accesos no autorizados más inmediata y validable.
4. Se acordó implementar un procedimiento de validación de la redundancia lógica. Se trataba de complementar las comprobaciones automáticas de la integridad mediante sumas de verificación y firmas digitales contrastadas, además de mantener auditorías manuales semanales. La confluencia entre el mecanismo automático y la revisión manual garantizaba que no se produjera una alteración de la información sin una detección oportuna.
5. Se diseñó un procedimiento de recuperación ante fallos en escalones. Esto incluyó tres niveles: respaldos automáticos diarios en servidores internos, copias semanales en la nube y un procedimiento de contingencia operativo, asignando roles en caso de fallos en el servicio. La recuperación se aplicó por escalones, priorizando en primer lugar los servicios críticos y, después, los secundarios.

REFERENCIAS BIBLIOGRÁFICAS

Arrieta, F. (30 de diciembre de 2024). *La importancia de las normas ISO en el desarrollo de sistemas de inteligencia artificial confiables*. Infobae. https://www.infobae.com/opinion/2024/12/30/la-importancia-de-las-normas-iso-en-el-desarrollo-de-sistemas-de-inteligencia-artificial-confiables/

Chavarria, A. (21 de marzo de 2025). *Ciberseguridad empresarial en el Perú: ¿Cómo la ISO 27001 ayuda a prevenir los ciberataques?* Órbita. https://agenciaorbita.org/ciberseguridad-empresarial-en-el-peru-como-la-iso-27001-ayuda-a-prevenir-los-ciberataques/

Contador, J., & Tapia, C. (2024). *Diseño e implementación de la ISO 27001 para mejorar la seguridad de información de la Empresa Minera Colibri S.A.C. Lima - 2023.* Universidad Nacional José Faustino Sánchez Carrión. Recuperado el 15 de abril de 2025, de http://hdl.handle.net/20.500.14067/8975

Culot, G., Nassimbeni, G., Podrecca, M., & Sartor, M. (2021). The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda. *The TQM Journal, 33*(7), 76-105. https://doi.org/10.1108/TQM-09-2020-0202

De La Cruz, C. (2024). *ISO 27001 para mejorar el sistema de gestión de seguridad de la información en una empresa de servicios, Lima 2024.* Universidad Norbert Wiener. Recuperado el 15 de abril de 2025, de https://hdl.handle.net/20.500.13053/11487

De la Rosa, M. T. (2021). Automatización de un sistema de gestión de seguridad de la información basado en la Norma ISO/IEC 27001. *Revista Universidad y Sociedad, 13*(5), 495-506. Recuperado el 15 de abril de 2025, de http://scielo.sld.cu/pdf/rus/v13n5/2218-3620-rus-13-05-495.pdf

Donoso, V. D., Calahorrano, R. C., & Donoso, V. S. (2023). Aplicación del SGSI ISO 27001 en el sistema de rehabilitación social de Ecuador. *Universidad Y Sociedad, 15*(2), 274–284. https://doi.org/https://rus.ucf.edu.cu/index.php/rus/article/view/3628

Hadi, M., Martel, C., Huayta, F., Rojas, C., & Arias, J. (2023). *Metodología de la investigación: Guía para el proyecto de tesis* (Primera ed.). Puno, Peru: Instituto Universitario de Innovación Ciencia y Tecnología Inudi Perú S.A.C. https://doi.org/https://doi.org/10.35622/inudi.b.073

Hernández-Sampieri, R., & Mendoza, C. (2018). *Metodología de la investigación: Las rutas cuantitativa, cualitativa y mixta.* McGraw-Hill Education.

Hinojosa, M. J., Mamani, G. J., & Catacora, L. E. (2024). *Proyecto de Tesis: Guía práctica para investigación cuantitativa* (1ra ed.). científica digital.

Huamalí, M. (2021). *Diseño de un sistema de gestión de seguridad de la información bajo el enfoque de la ISO/IEC 27001 para la empresa ITS Business SAC - Lima.* Universidad Nacional José María Arguedas. Recuperado el 15 de abril de 2025, de https://hdl.handle.net/20.500.14168/826

ISO/IEC. (2022). *ISO/IEC 27001:2022 Seguridad de la información, ciberseguridad y protección de la privacidad – Sistemas de gestión de la seguridad de la información – Requisitos* .

ISOTools. (2022). *La norma ISO 27001: Aspectos clave de su diseño e implantación.* ISOTools.

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

Kamil, Y., Lund , S., & Islam, M. (2023). Information security objectives and the output legitimacy of ISO/IEC 27001: stakeholders' perspective on expectations in private

organizations in Sweden. *Information Systems and e-business Management, 21*, 699–722. https://doi.org/10.1007/s10257-023-00646-y

Kitsios, F. (2023). The ISO/IEC 27001 Information Security Management Standard: How to Extract Value from Data in the IT Sector. *Sustainability, 15*(7), 5828. https://doi.org/10.3390/su15075828

Kuder, G., & Richardson, M. (1937). The theory of the estimation of test reliability. Psychometrika.

Mirtsch, M. (2023). Adoption of the information security management system standard ISO/IEC 27001: A study among german organizations. *International Journal for Quality Research, 17*(3), 747–768. https://doi.org/10.24874/IJQR17.03-08

Moron, K. (2023). *Diseño e implementación de un sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27002 para mejorar el nivel de seguridad informática en la empresa Rash Perú S.A.C.* Universidad Señor de Sipán. Recuperado el 15 de abril de 2025, de https://hdl.handle.net/20.500.12802/10629

Pascoe, C., Quinn, S., & Scarfone, K. (2024). The NIST Cybersecurity Framework (CSF) 2.0. *National Institute of Standards and Technology, Gaithersburg, MD.* https://doi.org/10.6028/NIST.CSWP.29

Pozo, H. C., Reascos, P. R., & Minaya, M. R. (2025). *Fundamentos de seguridad informática y ciberseguridad.* Ediciones GESICAP.

Rodriguez, M. (2023). *Mejora de la seguridad de la información aplicando la norma ISO/IEC 27001, en una consultora de sistemas.* Universidad San Ignacio de Loyola. Recuperado el 15 de abril de 2025, de https://hdl.handle.net/20.500.14005/14008

Ruiz, V. (09 de marzo de 2025). *El incremento en la adquisición de herramientas tecnológicas no ha resuelto el problema de la ciberseguridad*. Infobae.

https://www.infobae.com/mexico/2025/03/10/el-incremento-en-la-adquisicion-de-herramientas-tecnologicas-no-ha-resuelto-el-problema-de-la-ciberseguridad/

Salas, M. D., Honores, C. L., Naranjo, P. G., & Guailla, C. A. (2024). Evaluación de la aplicación de la norma ISO 27001 en micro y pequeñas empresas del sur Quito. *Revista De Producción, Ciencias E Investigación, 8*(53), 166–176. https://doi.org/https://doi.org/10.29018/issn.2588-1000vol8iss53.2024pp166-176

Samaniego, M. E., & Ponce, O. J. (2021). *Fundamentos de seguridad informática.* Grupo Compás.

Solar, D. (04 de enero de 2025). *En 2025 aumentarán ciberataques en Perú: ¿cómo impactará en las empresas?* Infobae. https://www.infobae.com/peru/2025/01/04/en-2025-aumentaran-ciberataques-en-peru-como-impactara-en-las-empresas/

Supo, J., & Zacarías, H. (2024). *Metodología de la investigacion científica* (Cuarta ed.). (B. E. EIRL, Ed.) Lima: Bioestadistico EEDU EIRL.

Torres, M. (24 de enero de 2025). *Actualización de la ISO 27001: más preparadas para las nuevas amenazas*. NTT DATA. https://pe.nttdata.com/insights/blog/actualizacion-de-la-iso-27001

Vega, B. E. (2021). *Seguridad de la información.* Área de Innovación y Desarrollo, S.L.

Viteri, C. (2022). *ISO/IEC 27001:2022 La Guía definitiva.*

Yungán, J., & Narváez, C. (2022). Aplicación de la Norma ISO 27001 para la seguridad de los Sistemas de Información. *Revista cientifica Dominio de las Ciencias, 8*(3), 1025-1041. https://doi.org/http://dx.doi.org/10.23857/dc.v8i3

ANEXOS

Anexo A: Matriz de consistencia

ISO/IEC 27001 para evaluar la seguridad de los sistemas de información en Inversiones RMK, Lircay – 2025

Problema general	Objetivo general	Hipótesis general	Variables	Metodología
¿De qué manera los criterios de la norma ISO/IEC 27001 influyen en la seguridad de los sistemas de información en Inversiones RMK, Lircay – 2025? Problemas específicos **a)** ¿De qué manera los criterios de la norma ISO/IEC 27001 permiten influyen en la confidencialidad de los sistemas de información en Inversiones RMK, Lircay – 2025? **b)** ¿De qué manera los criterios de la norma ISO/IEC 27001 permiten influyen en la integridad de los sistemas de información en Inversiones RMK, Lircay – 2025? **c)** ¿De qué manera los criterios de la norma ISO/IEC 27001 permiten influyen en la disponibilidad de los sistemas de información en Inversiones RMK, Lircay – 2025?	Evaluar la influencia de los criterios de la norma ISO/IEC 27001 en la seguridad de los sistemas de información en Inversiones RMK, Lircay – 2025. Objetivos específicos **a)** Evaluar la influencia de los criterios de la norma ISO/IEC 27001 en la confidencialidad de los sistemas de información en Inversiones RMK, Lircay – 2025. **b)** Evaluar la influencia de los criterios de la norma ISO/IEC 27001 en la integridad de los sistemas de información en Inversiones RMK, Lircay – 2025. **c)** Evaluar la influencia de los criterios de la norma ISO/IEC 27001 en la disponibilidad de los sistemas de información en Inversiones RMK, Lircay – 2025.	El cumplimiento de los criterios de la norma ISO/IEC 27001 influye en la seguridad de los sistemas de información en Inversiones RMK, Lircay – 2025. Hipótesis específicas **a)** El cumplimiento de los criterios de la norma ISO/IEC 27001 influye en la confidencialidad de los sistemas de información en Inversiones RMK, Lircay – 2025. **b)** El cumplimiento de los criterios de la norma ISO/IEC 27001 influye en la integridad de los sistemas de información en Inversiones RMK, Lircay – 2025. **c)** El cumplimiento de los criterios de la norma ISO/IEC 27001 influye en la disponibilidad de los sistemas de información en Inversiones RMK, Lircay – 2025.	X: ISO/IEC 27001 1. Gestión de riesgos 2. Seguridad operativa 3. Desempeño operativo Y: Seguridad de los sistemas de información 1. Confidencialidad 2. Integridad 3. Disponibilidad	1. Tipo: Aplicada 2. Nivel: Explicativo 3. Diseño: No experimental, longitudinal M_1, M_2, M_3, M_4, M_5: Los cinco sistemas de información de Inversiones RMK Oiy: Observación diaria del cumplimiento de criterios ISO/IEC 27001 en el sistema i durante el día j y de la seguridad del sistema de información i durante el día j i: Sistema evaluado (1 = Control Net, 2 = NubeFact, 3 = Cognos, 4 = Citrix, 5 = Siam) j: Día de observación (1 al 90) 4. Población: Cinco (5) sistemas de información operativos 5. Muestra: Los cinco (5) sistemas de información operativos. 6. Tipo de muestreo: Se empleó un muestreo de tipo censal, debido a que la unidad de análisis es accesible, se trabajarán con todos los sistemas de información operativos disponible al momento de realizar la investigación. 7.Técnicas: Observación y Análisis documental 8. Instrumento: Ficha de Observación y Ficha de Análisis documental

Nota: Elaboración propia

Anexo B: Matriz de operacionalización de variable

Variable	Dimensión	Indicador	Ítem	Escala de medición
V.I. (X) ISO/IEC 27001	X.1. Gestión de riesgos	Identificación y evaluación de riesgos	1	Escala dicotómica 1 = Sí/Cumple 0 = No/No cumple Criterio por dimensión: Cumple (1): ≥ 3 de 5 = Sí No cumple (0): < 3 de 5 = No
			2	
		Tratamiento de riesgos	3	
			4	
			5	
	X.2. Seguridad operativa	Implementación de medidas operativas de seguridad	6	
			7	
		Gestión de incidentes de seguridad	8	
		Monitoreo y mejora continua de los controles de seguridad	9	
			10	
	X.3. Desempeño operativo	Evaluación directiva basada en evidencias	11	
			12	
			13	
			14	
			15	
V.D. Y: Seguridad de los sistemas de información	Y.1. Confidencialidad	Número de accesos no autorizados detectados	16	Escala dicotómica 1 = Seguro 0 = Inseguro Criterio por dimensión: Seguro (1): ≥ 3 de 5 = Sí Inseguro (0): < 3 de 5 = No
		Existencia de políticas de control de acceso	17	
		Nivel de uso de cifrado en datos sensibles	18	
		Porcentaje de personal con acceso restringido correctamente asignado	19	
			20	
	Y.2. Integridad	Número de modificaciones no autorizadas detectadas	21	
		Frecuencia de uso de mecanismos de verificación (hash, checksum)	22	
		Cantidad de errores detectados en bases de datos	23	
		Existencia de controles de cambios y trazabilidad	24	
			25	
	Y.3. Disponibilidad	Tiempo en línea del sistema	26	
		Número de incidentes por caída del sistema	27	
		Frecuencia de respaldos (backup)	28	
		Tiempo promedio de recuperación ante fallos (MTTR)	29	
			30	

Nota: Elaboración propia

Anexo C: Instrumentos de recolección de datos

REGISTRO DIARIO DE CUMPLIMIENTO ISO/IEC 27001

Objetivo: Registrar diariamente el cumplimiento de criterios ISO/IEC 27001 en los 5 sistemas de información durante 90 días consecutivos.

DATOS GENERALES DEL REGISTRO

Fecha: ____//____// 2025 (Día _____de 30)

Hora de inicio: hh:_____mm:_____ Hora de finalización: hh:_____mm:_____

Sistema Evaluado: S1☐ S2 ☐ S3 ☐ S4 ☐ S5 ☐

Escala de medición

- 1 = SÍ/CUMPLE: Criterio implementado y funcionando correctamente en las últimas 24h
- 0 = NO/NO CUMPLE: Criterio no implementado o con fallas en las últimas 24h

DIMENSIÓN 1: GESTIÓN DE RIESGOS

Indicador Diario	Sí	No	Observación
1. ¿Se ejecutaron las evaluaciones de riesgo programadas para hoy?	☐	☐	
2. ¿Los controles de riesgo funcionaron sin incidencias?	☐	☐	
3. ¿Se registraron y trataron adecuadamente los nuevos riesgos identificados?	☐	☐	
4. ¿Las políticas de seguridad estuvieron disponibles y accesibles?	☐	☐	
5. ¿Se cumplieron los procedimientos operativos de seguridad establecidos?	☐	☐	

DIMENSIÓN 2: SEGURIDAD OPERATIVA

Indicador Diario	Sí	No	Observación
6. ¿Los procedimientos de acceso funcionaron correctamente?	☐	☐	
7. ¿El cifrado de datos críticos estuvo operativo?	☐	☐	
8. ¿Los sistemas antimalware estuvieron actualizados y funcionando?	☐	☐	
9. ¿Se gestionaron adecuadamente los incidentes ocurridos?	☐	☐	
10. ¿Los controles de acceso físico y lógico funcionaron sin fallas?	☐	☐	

DIMENSIÓN 3: DESEMPEÑO OPERATIVO

Indicador Diario	Sí	No	Observación
11. ¿Se ejecutaron las actividades de monitoreo programadas?	☐	☐	
12. ¿Los indicadores de desempeño se midieron según cronograma?	☐	☐	
13. ¿Se documentaron las no conformidades identificadas?	☐	☐	
14. ¿Se implementaron las acciones correctivas planificadas?	☐	☐	
15. ¿Los procesos de mejora continua estuvieron activos?	☐	☐	

Ficha de observación

REGISTRO DIARIO DE SEGURIDAD DE SISTEMAS

Objetivo: Registrar diariamente el nivel de seguridad de los sistemas de información mediante indicadores observables durante 90 días consecutivos.

DATOS GENERALES DEL REGISTRO

Fecha: //2025 (Día ____ de 30)

Hora de inicio: hh:_____mm:_____ Hora de finalización: hh:_____mm:_____

Sistema Observado: ☐ S1 ☐ S2 ☐ S3 ☐ S4 ☐ S5

Escala de medición

- 1 = SEGURO: Indicador dentro de parámetros aceptables en las últimas 24h
- 0 = INSEGURO: Indicador fuera de parámetros aceptables en las últimas 24h

DIMENSIÓN 1: CONFIDENCIALIDAD

Indicador Diario	Seguro	Inseguro	Observación
16. ¿Cero (0) accesos no autorizados detectados en el día?	☐	☐	___ accesos detectados
17. ¿Todos los usuarios ingresaron con credenciales válidas?	☐	☐	☐ Sí ☐ No
18. ¿El sistema de cifrado funcionó sin interrupciones?	☐	☐	☐ Sí ☐ No
19. ¿Cero (0) accesos a áreas restringidas sin autorización?	☐	☐	___ accesos indebidos
20. ¿La autenticación multifactor estuvo disponible todo el día?	☐	☐	☐ Sí ☐ No

Total Confidencialidad: _____ / 5

DIMENSIÓN 2: INTEGRIDAD

Indicador Diario	Seguro	Inseguro	Observación
21. ¿Cero (0) modificaciones no autorizadas detectadas?	☐	☐	___ modificaciones
22. ¿Las verificaciones de integridad se completaron sin errores?	☐	☐	☐ Sí ☐ No
23. ¿Las bases de datos funcionaron sin errores de consistencia?	☐	☐	☐ Sí ☐ No
24. ¿El control de versiones registró todos los cambios correctamente?	☐	☐	☐ Sí ☐ No
25. ¿Las validaciones automáticas detectaron anomalías?	☐	☐	☐ No detectó ☐ Detectó

Total Integridad: _____ / 5

DIMENSIÓN 3: DISPONIBILIDAD

Indicador Diario	Seguro	Inseguro	Observación
26. ¿El sistema estuvo disponible durante todo el horario laboral?	☐	☐	☐ Sí ☐ No
27. ¿Cero (0) caídas del sistema reportadas en el día?	☐	☐	___ caídas reportadas
28. ¿El respaldo diario programado se ejecutó exitosamente?	☐	☐	☐ Sí ☐ No
29. ¿El sistema respondió con velocidad normal durante el día?	☐	☐	☐ Sí ☐ No
30. ¿Los planes de continuidad estuvieron accesibles y actualizados?	☐	☐	☐ Sí ☐ No

Total Disponibilidad: _____

EVALUACIÓN GENERAL DIARIA DE SEGURIDAD

Dimensión	Puntaje	Estado Diario		Seguridad general del sistema del día:
		Seguro	Inseguro	
Confidencialidad	___/5			☐ Seguro (1): Al menos 2 de 3 dimensiones seguras ☐ Inseguro (0): 2 o más dimensiones inseguras
Integridad	/5			
Disponibilidad	___/5			

Anexo D: Permiso para autorización para uso de información de la empresa

"Año de la recuperación y consolidación de la economía peruana"

SOLICITUD DE PERMISO PARA USO DE INFORMACIÓN DE LA EMPRESA

Lircay, 12 de marzo del 2025

SEÑOR:

GERENTE DE EMPRESA INERSIONES RMK S.A.C

PRESENTE. –

Yo, Samuel Huincho Taype, identificado con DNI N° 72275714, bachiller de la **Escuela Profesional de Ingeniería Informática** de la Universidad para el Desarrollo Andino, me dirijo a usted para expresarle un cordial saludo y, a la vez, solicitar su autorización para llevar a cabo actividades vinculadas al trabajo de investigación titulado: **"ISO/IEC 27001 para evaluar la seguridad de los sistemas de información en Inversiones RMK, Lircay – 2025"**, como parte del proceso académico para optar por el título profesional de Ingeniero Informático.

Solicito su gentil autorización para acceder a información relevante y realizar actividades como documentación, revisión de manuales y evaluación de sistemas, garantizando en todo momento la confidencialidad de los datos y el normal desarrollo de las operaciones internas de la empresa.

Cabe resaltar que esta investigación no generará ningún gasto para su institución y que se tomarán todas las medidas necesarias para no interferir con sus actividades cotidianas. Los datos obtenidos serán utilizados exclusivamente para fines académicos.

Sin otro particular, reitero mi agradecimiento por su atención y disposición.

Atentamente;

HUINCHO TAYPE, Samuel

DNI N° 72275714

Anexo E: Permiso de autorización de la empresa

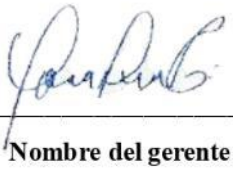
"Año de la recuperación y consolidación de la economía peruana"

PERMISO DE AUTORIZACIÓN DE LA EMPRESA

Lircay, 15 de marzo del 2025

La empresa ***"Inversiones RMK S.A.C."*** con R.U.C N° 10409360161; autoriza y se compromete a brindar información la información solicitada para el desarrollo del trabajo mencionado, la misma que solo puede ser usada para fines estrictamente académico vinculados al trabajo de investigación, Declaramos conocer que el trabajo de investigación titulado **"ISO/IEC 27001 para evaluar la seguridad de los sistemas de información en Inversiones RMK, Lircay – 2025"**, que será de público conocimiento a través del repositorio de la universidad,

Cordialmente;



Nombre del gerente

RONALD CARLOS CAUCHOS RIVEROS

DNI N° 40936016

GERENTE

Anexo F: Base de datos

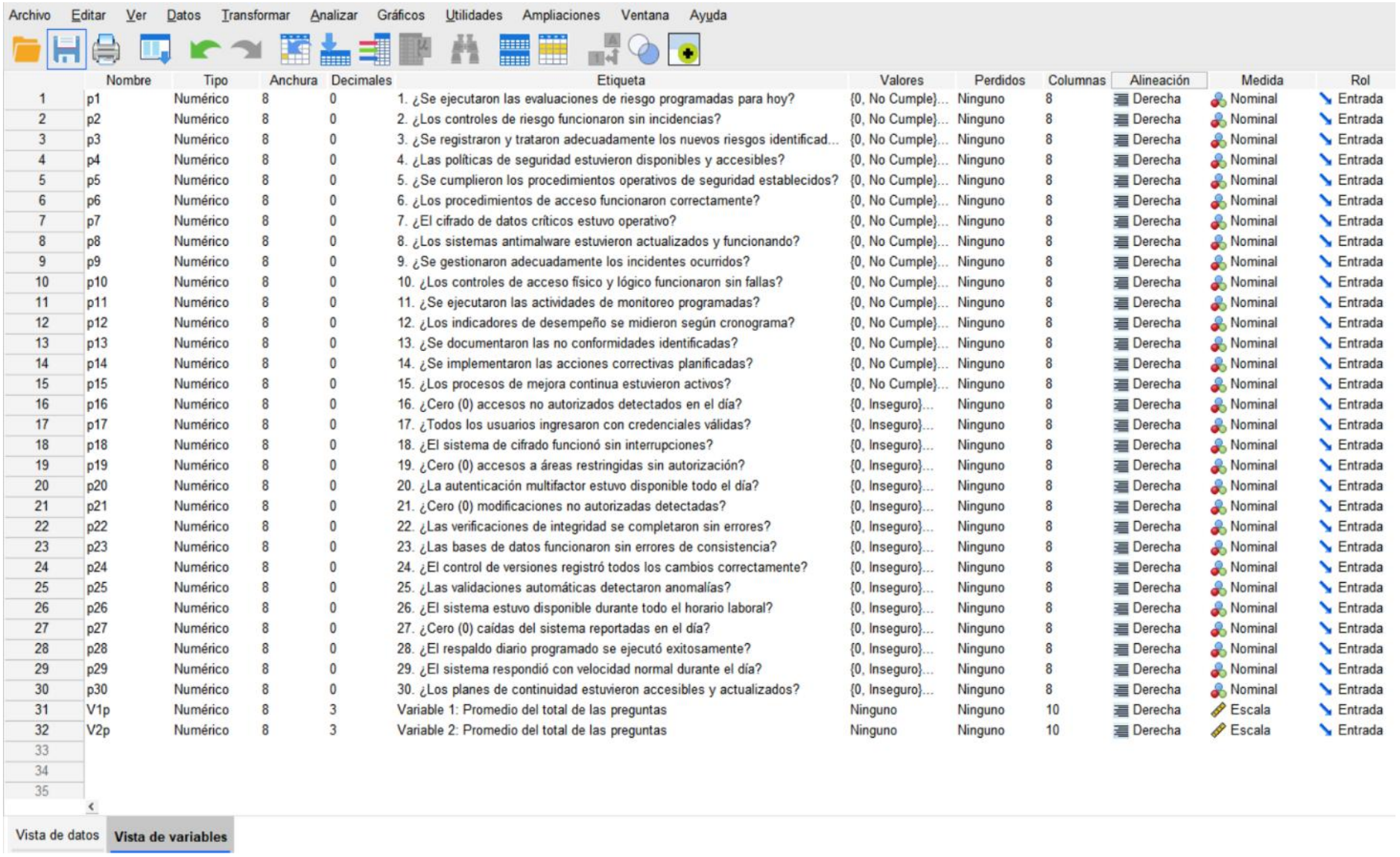
Variable ISO/IEC 27001

Sistema	promedio_p1	promedio_p2	promedio_p3	promedio_p4	promedio_p5	promedio_p6	promedio_p7	promedio_p8	promedio_p9	promedio_p10	promedio_p11	promedio_p12	promedio_p13	promedio_p14	promedio_p15
S1	0.622	0.644	0.689	0.722	0.656	0.700	0.689	0.722	0.767	0.733	0.711	0.733	0.622	0.656	0.678
S2	0.667	0.667	0.633	0.656	0.622	0.644	0.644	0.578	0.600	0.644	0.600	0.622	0.689	0.667	0.578
S3	0.711	0.622	0.611	0.700	0.600	0.689	0.689	0.678	0.689	0.733	0.700	0.656	0.622	0.678	0.689
S4	0.578	0.589	0.556	0.556	0.622	0.544	0.567	0.633	0.600	0.556	0.522	0.633	0.611	0.667	0.578
S5	0.689	0.622	0.700	0.633	0.700	0.667	0.644	0.656	0.789	0.700	0.667	0.700	0.678	0.611	0.722

Variable seguridad de los sistemas

Sistema	promedio_p1	promedio_p2	promedio_p3	promedio_p4	promedio_p5	promedio_p6	promedio_p7	promedio_p8	promedio_p9	promedio_p10	promedio_p11	promedio_p12	promedio_p13	promedio_p14	promedio_p15
S1	0.678	0.644	0.578	0.733	0.600	0.700	0.711	0.656	0.722	0.700	0.711	0.667	0.633	0.756	0.722
S2	0.611	0.678	0.611	0.611	0.678	0.678	0.711	0.611	0.711	0.567	0.622	0.633	0.611	0.689	0.589
S3	0.656	0.700	0.644	0.644	0.611	0.589	0.644	0.600	0.678	0.578	0.556	0.633	0.667	0.600	0.667
S4	0.589	0.633	0.622	0.544	0.622	0.556	0.600	0.544	0.511	0.611	0.556	0.589	0.567	0.622	0.622
S5	0.633	0.700	0.611	0.644	0.644	0.656	0.667	0.622	0.622	0.656	0.711	0.689	0.644	0.678	0.678

Anexo G: Medida de datos

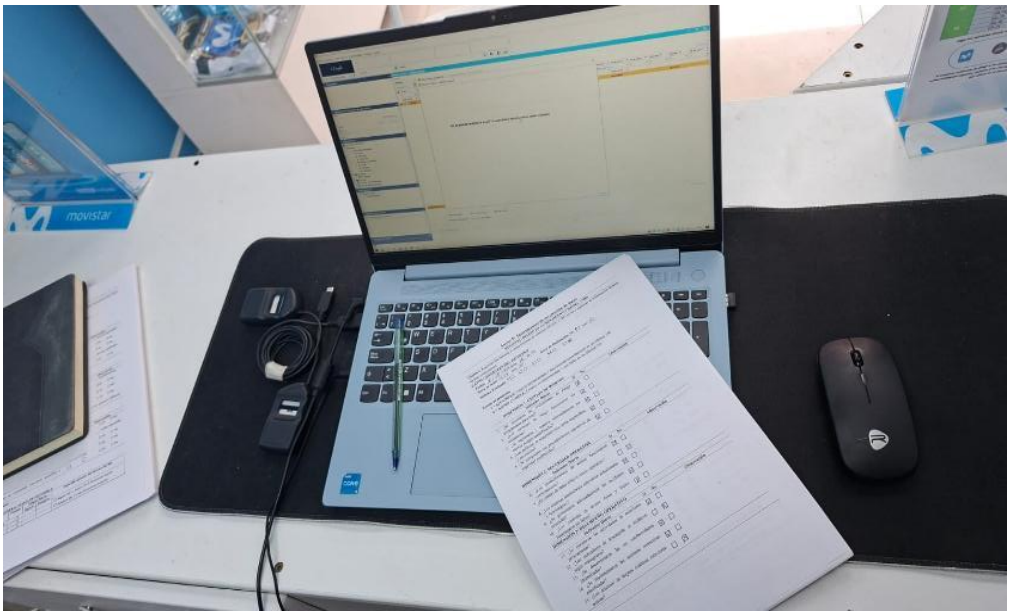


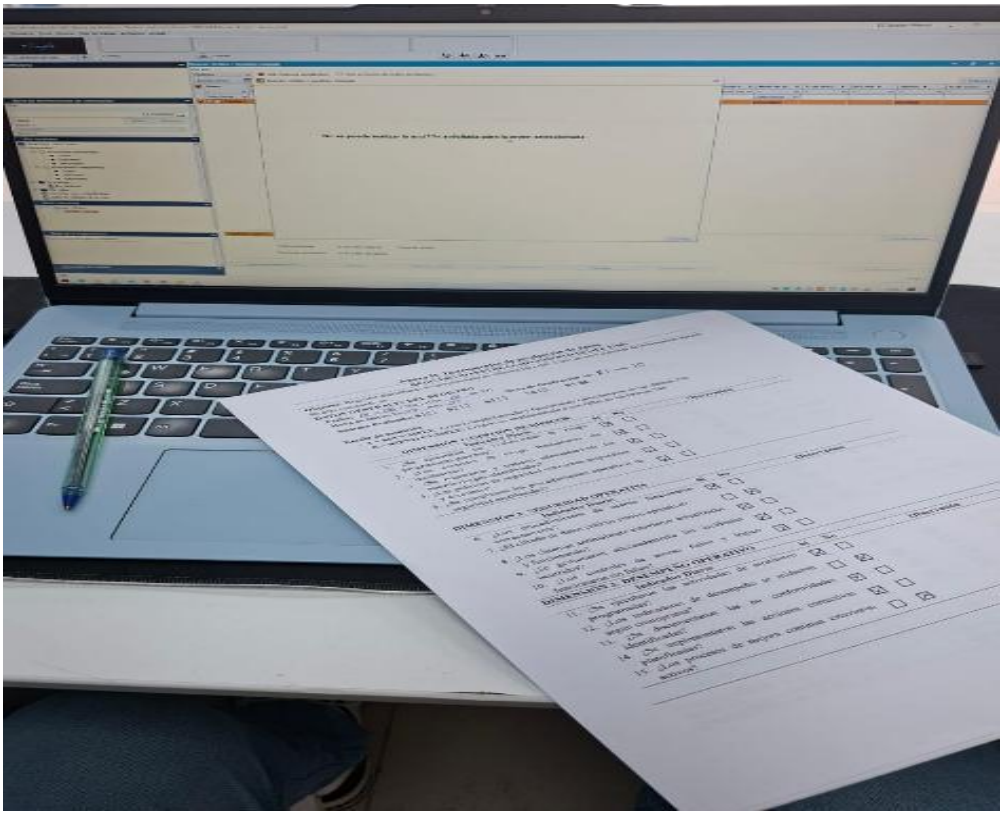
Archivo Editar Ver Datos Transformar Analizar Gráficos Utilidades Ampliaciones Ventana Ayuda

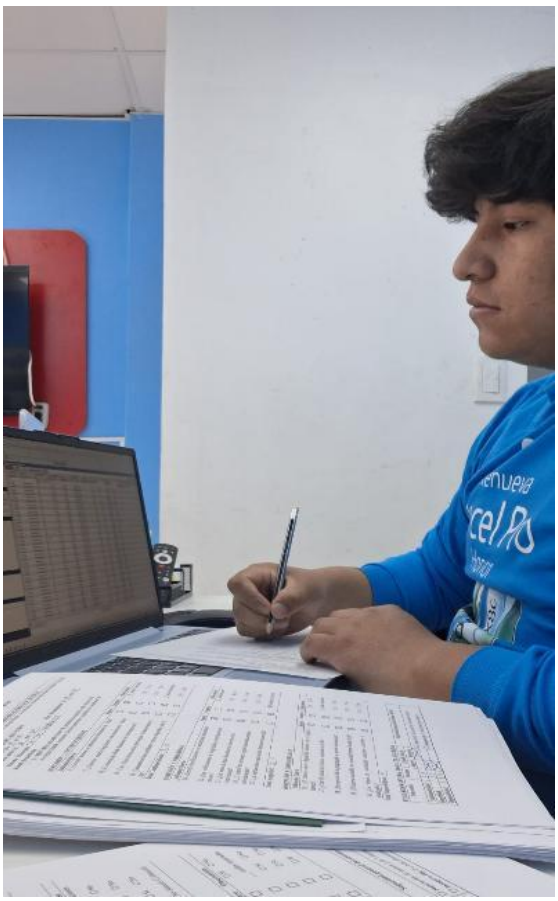
	Nombre	Tipo	Anchura	Decimales	Etiqueta	Valores	Perdidos	Columnas	Alineación	Medida	Rol
1	p1	Numérico	8	0	1. ¿Se ejecutaron las evaluaciones de riesgo programadas para hoy?	{0, No Cumple}...	Ninguno	8	Derecha	Nominal	Entrada
2	p2	Numérico	8	0	2. ¿Los controles de riesgo funcionaron sin incidencias?	{0, No Cumple}...	Ninguno	8	Derecha	Nominal	Entrada
3	p3	Numérico	8	0	3. ¿Se registraron y trataron adecuadamente los nuevos riesgos identificad...	{0, No Cumple}...	Ninguno	8	Derecha	Nominal	Entrada
4	p4	Numérico	8	0	4. ¿Las políticas de seguridad estuvieron disponibles y accesibles?	{0, No Cumple}...	Ninguno	8	Derecha	Nominal	Entrada
5	p5	Numérico	8	0	5. ¿Se cumplieron los procedimientos operativos de seguridad establecidos?	{0, No Cumple}...	Ninguno	8	Derecha	Nominal	Entrada
6	p6	Numérico	8	0	6. ¿Los procedimientos de acceso funcionaron correctamente?	{0, No Cumple}...	Ninguno	8	Derecha	Nominal	Entrada
7	p7	Numérico	8	0	7. ¿El cifrado de datos críticos estuvo operativo?	{0, No Cumple}...	Ninguno	8	Derecha	Nominal	Entrada
8	p8	Numérico	8	0	8. ¿Los sistemas antimalware estuvieron actualizados y funcionando?	{0, No Cumple}...	Ninguno	8	Derecha	Nominal	Entrada
9	p9	Numérico	8	0	9. ¿Se gestionaron adecuadamente los incidentes ocurridos?	{0, No Cumple}...	Ninguno	8	Derecha	Nominal	Entrada
10	p10	Numérico	8	0	10. ¿Los controles de acceso físico y lógico funcionaron sin fallas?	{0, No Cumple}...	Ninguno	8	Derecha	Nominal	Entrada
11	p11	Numérico	8	0	11. ¿Se ejecutaron las actividades de monitoreo programadas?	{0, No Cumple}...	Ninguno	8	Derecha	Nominal	Entrada
12	p12	Numérico	8	0	12. ¿Los indicadores de desempeño se midieron según cronograma?	{0, No Cumple}...	Ninguno	8	Derecha	Nominal	Entrada
13	p13	Numérico	8	0	13. ¿Se documentaron las no conformidades identificadas?	{0, No Cumple}...	Ninguno	8	Derecha	Nominal	Entrada
14	p14	Numérico	8	0	14. ¿Se implementaron las acciones correctivas planificadas?	{0, No Cumple}...	Ninguno	8	Derecha	Nominal	Entrada
15	p15	Numérico	8	0	15. ¿Los procesos de mejora continua estuvieron activos?	{0, No Cumple}...	Ninguno	8	Derecha	Nominal	Entrada
16	p16	Numérico	8	0	16. ¿Cero (0) accesos no autorizados detectados en el día?	{0, Inseguro}...	Ninguno	8	Derecha	Nominal	Entrada
17	p17	Numérico	8	0	17. ¿Todos los usuarios ingresaron con credenciales válidas?	{0, Inseguro}...	Ninguno	8	Derecha	Nominal	Entrada
18	p18	Numérico	8	0	18. ¿El sistema de cifrado funcionó sin interrupciones?	{0, Inseguro}...	Ninguno	8	Derecha	Nominal	Entrada
19	p19	Numérico	8	0	19. ¿Cero (0) accesos a áreas restringidas sin autorización?	{0, Inseguro}...	Ninguno	8	Derecha	Nominal	Entrada
20	p20	Numérico	8	0	20. ¿La autenticación multifactor estuvo disponible todo el día?	{0, Inseguro}...	Ninguno	8	Derecha	Nominal	Entrada
21	p21	Numérico	8	0	21. ¿Cero (0) modificaciones no autorizadas detectadas?	{0, Inseguro}...	Ninguno	8	Derecha	Nominal	Entrada
22	p22	Numérico	8	0	22. ¿Las verificaciones de integridad se completaron sin errores?	{0, Inseguro}...	Ninguno	8	Derecha	Nominal	Entrada
23	p23	Numérico	8	0	23. ¿Las bases de datos funcionaron sin errores de consistencia?	{0, Inseguro}...	Ninguno	8	Derecha	Nominal	Entrada
24	p24	Numérico	8	0	24. ¿El control de versiones registró todos los cambios correctamente?	{0, Inseguro}...	Ninguno	8	Derecha	Nominal	Entrada
25	p25	Numérico	8	0	25. ¿Las validaciones automáticas detectaron anomalías?	{0, Inseguro}...	Ninguno	8	Derecha	Nominal	Entrada
26	p26	Numérico	8	0	26. ¿El sistema estuvo disponible durante todo el horario laboral?	{0, Inseguro}...	Ninguno	8	Derecha	Nominal	Entrada
27	p27	Numérico	8	0	27. ¿Cero (0) caídas del sistema reportadas en el día?	{0, Inseguro}...	Ninguno	8	Derecha	Nominal	Entrada
28	p28	Numérico	8	0	28. ¿El respaldo diario programado se ejecutó exitosamente?	{0, Inseguro}...	Ninguno	8	Derecha	Nominal	Entrada
29	p29	Numérico	8	0	29. ¿El sistema respondió con velocidad normal durante el día?	{0, Inseguro}...	Ninguno	8	Derecha	Nominal	Entrada
30	p30	Numérico	8	0	30. ¿Los planes de continuidad estuvieron accesibles y actualizados?	{0, Inseguro}...	Ninguno	8	Derecha	Nominal	Entrada
31	V1p	Numérico	8	3	Variable 1: Promedio del total de las preguntas	Ninguno	Ninguno	10	Derecha	Escala	Entrada
32	V2p	Numérico	8	3	Variable 2: Promedio del total de las preguntas	Ninguno	Ninguno	10	Derecha	Escala	Entrada
33											
34											
35											

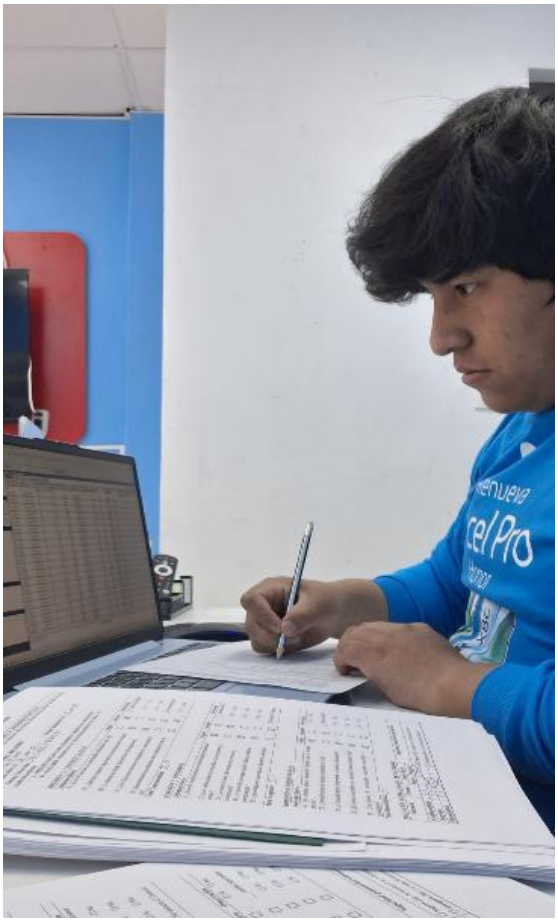
Vista de datos | Vista de variables

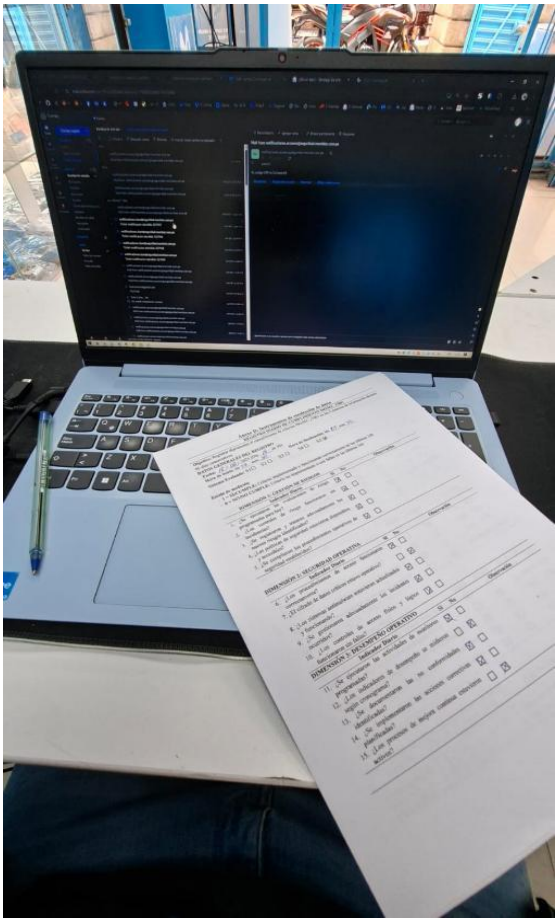
Anexo H: Fotografías











REGISTRO DIARIO DE CUMPLIMIENTO ISO/IEC 27001

Objetivo: Registrar diariamente el cumplimiento de criterios ISO/IEC 27001 en los 5 sistemas de información durante 90 días consecutivos.

DATOS GENERALES DEL REGISTRO

Fecha: 03 // 08 // 2025 (Día 03 de 30)

Hora de inicio: hh: 08 mm: 31 **Hora de finalización:** hh: 10 mm: 34

Sistema Evaluado: S1 ☒ S2 ☐ S3 ☐ S4 ☐ S5 ☐

Escala de medición

- **1 = SÍ/CUMPLE:** Criterio implementado y funcionando correctamente en las últimas 24h
- **0 = NO/NO CUMPLE:** Criterio no implementado o con fallas en las últimas 24h

DIMENSIÓN 1: GESTIÓN DE RIESGOS

Indicador Diario	Sí	No	Observación
1. ¿Se ejecutaron las evaluaciones de riesgo programadas para hoy?	☒	☐	
2. ¿Los controles de riesgo funcionaron sin incidencias?	☒	☐	
3. ¿Se registraron y trataron adecuadamente los nuevos riesgos identificados?	☒	☐	
4. ¿Las políticas de seguridad estuvieron disponibles y accesibles?	☐	☒	
5. ¿Se cumplieron los procedimientos operativos de seguridad establecidos?	☒	☐	

DIMENSIÓN 2: SEGURIDAD OPERATIVA

Indicador Diario	Sí	No	Observación
6. ¿Los procedimientos de acceso funcionaron correctamente?	☒	☐	
7. ¿El cifrado de datos críticos estuvo operativo?	☐	☒	
8. ¿Los sistemas antimalware estuvieron actualizados y funcionando?	☒	☐	
9. ¿Se gestionaron adecuadamente los incidentes ocurridos?	☒	☐	
10. ¿Los controles de acceso físico y lógico funcionaron sin fallas?	☐	☒	

DIMENSIÓN 3: DESEMPEÑO OPERATIVO

Indicador Diario	Sí	No	Observación
11. ¿Se ejecutaron las actividades de monitoreo programadas?	☒	☐	
12. ¿Los indicadores de desempeño se midieron según cronograma?	☒	☐	
13. ¿Se documentaron las no conformidades identificadas?	☒	☐	
14. ¿Se implementaron las acciones correctivas planificadas?	☒	☐	
15. ¿Los procesos de mejora continua estuvieron activos?	☒	☐	

Ficha de observación

REGISTRO DIARIO DE SEGURIDAD DE SISTEMAS

Objetivo: Registrar diariamente el nivel de seguridad de los sistemas de información mediante indicadores observables durante 90 días consecutivos.

DATOS GENERALES DEL REGISTRO

Fecha: //2025 (Día 3 de 30)

Hora de inicio: hh: 08 mm: 34 **Hora de finalización:** hh: 10 mm: 34

Sistema Observado: ☒ S1 ☐ S2 ☐ S3 ☐ S4 ☐ S5

Escala de medición

- **1 = SEGURO:** Indicador dentro de parámetros aceptables en las últimas 24h
- **0 = INSEGURO:** Indicador fuera de parámetros aceptables en las últimas 24h

DIMENSIÓN 1: CONFIDENCIALIDAD

Indicador Diario	Seguro	Inseguro	Observación
16. ¿Cero (0) accesos no autorizados detectados en el día?	☐	☒	2 accesos detectados
17. ¿Todos los usuarios ingresaron con credenciales válidas?	☒	☐	☒ Sí ☐ No
18. ¿El sistema de cifrado funcionó sin interrupciones?	☒	☐	☐ Sí ☐ No
19. ¿Cero (0) accesos a áreas restringidas sin autorización?	☒	☐	___ accesos indebidos
20. ¿La autenticación multifactor estuvo disponible todo el día?	☐	☒	☒ Sí ☐ No

Total Confidencialidad: 3 / 5

DIMENSIÓN 2: INTEGRIDAD

Indicador Diario	Seguro	Inseguro	Observación
21. ¿Cero (0) modificaciones no autorizadas detectadas?	☒	☐	___ modificaciones
22. ¿Las verificaciones de integridad se completaron sin errores?	☒	☐	☐ Sí ☐ No
23. ¿Las bases de datos funcionaron sin errores de consistencia?	☐	☒	☐ Sí ☐ No
24. ¿El control de versiones registró todos los cambios correctamente?	☒	☐	☐ Sí ☐ No
25. ¿Las validaciones automáticas detectaron anomalías?	☐	☒	☐ No detectó ☒ Detectó

Total Integridad: 3 / 5

DIMENSIÓN 3: DISPONIBILIDAD

Indicador Diario	Seguro	Inseguro	Observación
26. ¿El sistema estuvo disponible durante todo el horario laboral?	☐	☒	☐ Sí ☒ No
27. ¿Cero (0) caídas del sistema reportadas en el día?	☐	☒	2 caídas reportadas
28. ¿El respaldo diario programado se ejecutó exitosamente?	☒	☐	☐ Sí ☐ No
29. ¿El sistema respondió con velocidad normal durante el día?	☐	☒	☒ Sí ☐ No
30. ¿Los planes de continuidad estuvieron accesibles y actualizados?	☒	☐	☐ Sí ☐ No

Total Disponibilidad: 2

EVALUACIÓN GENERAL DIARIA DE SEGURIDAD

Dimensión	Puntaje	Estado Diario		Seguridad general del sistema del día:
		Seguro	Inseguro	
Confidencialidad	3 /5	X		☐ **Seguro (1):** Al menos 2 de 3 dimensiones seguras
Integridad	3 /5	X		☐ **Inseguro (0):** 2 o más dimensiones inseguras
Disponibilidad	2 /5		X	

Anexo D: Instrumentos de recolección de datos

REGISTRO DIARIO DE CUMPLIMIENTO ISO/IEC 27001

Objetivo: Registrar diariamente el cumplimiento de criterios ISO/IEC 27001 en los 5 sistemas de información durante 90 días consecutivos.

DATOS GENERALES DEL REGISTRO

Fecha: 10 // 08 // 2025 (Día 8 de 30)

Hora de inicio: hh: 09 mm: 00 **Hora de finalización**: hh: 10 mm: 55

Sistema Evaluado: S1☐ S2☒ S3☐ S4☐ S5☐

Escala de medición

- **1 = SÍ/CUMPLE:** Criterio implementado y funcionando correctamente en las últimas 24h
- **0 = NO/NO CUMPLE:** Criterio no implementado o con fallas en las últimas 24h

DIMENSIÓN 1: GESTIÓN DE RIESGOS

Indicador Diario	Sí	No	Observación
1. ¿Se ejecutaron las evaluaciones de riesgo programadas para hoy?	☒	☐	
2. ¿Los controles de riesgo funcionaron sin incidencias?	☐	☒	
3. ¿Se registraron y trataron adecuadamente los nuevos riesgos identificados?	☒	☐	
4. ¿Las políticas de seguridad estuvieron disponibles y accesibles?	☒	☐	
5. ¿Se cumplieron los procedimientos operativos de seguridad establecidos?	☒	☐	

DIMENSIÓN 2: SEGURIDAD OPERATIVA

Indicador Diario	Sí	No	Observación
6. ¿Los procedimientos de acceso funcionaron correctamente?	☐	☒	
7. ¿El cifrado de datos críticos estuvo operativo?	☒	☐	
8. ¿Los sistemas antimalware estuvieron actualizados y funcionando?	☐	☒	
9. ¿Se gestionaron adecuadamente los incidentes ocurridos?	☒	☐	
10. ¿Los controles de acceso físico y lógico funcionaron sin fallas?	☒	☐	

DIMENSIÓN 3: DESEMPEÑO OPERATIVO

Indicador Diario	Sí	No	Observación
11. ¿Se ejecutaron las actividades de monitoreo programadas?	☐	☒	
12. ¿Los indicadores de desempeño se midieron según cronograma?	☐	☒	
13. ¿Se documentaron las no conformidades identificadas?	☒	☐	
14. ¿Se implementaron las acciones correctivas planificadas?	☒	☐	
15. ¿Los procesos de mejora continua estuvieron activos?	☒	☐	

Ficha de observación

REGISTRO DIARIO DE SEGURIDAD DE SISTEMAS

Objetivo: Registrar diariamente el nivel de seguridad de los sistemas de información mediante indicadores observables durante 90 días consecutivos.

DATOS GENERALES DEL REGISTRO

Fecha: //2025 (Día 6 de 30)

Hora de inicio: hh: 09 mm: 00 **Hora de finalización:** hh: 10 mm: 55

Sistema Observado: ☐ S1 ☒ S2 ☐ S3 ☐ S4 ☐ S5

Escala de medición

- **1 = SEGURO:** Indicador dentro de parámetros aceptables en las últimas 24h
- **0 = INSEGURO:** Indicador fuera de parámetros aceptables en las últimas 24h

DIMENSIÓN 1: CONFIDENCIALIDAD

Indicador Diario	Seguro	Inseguro	Observación
16. ¿Cero (0) accesos no autorizados detectados en el día?	☒	☐	___ accesos detectados
17. ¿Todos los usuarios ingresaron con credenciales válidas?	☐	☒	☒ Sí ☐ No
18. ¿El sistema de cifrado funcionó sin interrupciones?	☐	☒	☒ Sí ☐ No
19. ¿Cero (0) accesos a áreas restringidas sin autorización?	☒	☐	___ accesos indebidos
20. ¿La autenticación multifactor estuvo disponible todo el día?	☒	☐	☐ Sí ☐ No

Total Confidencialidad: 3 / 5

DIMENSIÓN 2: INTEGRIDAD

Indicador Diario	Seguro	Inseguro	Observación
21. ¿Cero (0) modificaciones no autorizadas detectadas?	☐	☒	1 modificaciones
22. ¿Las verificaciones de integridad se completaron sin errores?	☒	☐	☐ Sí ☐ No
23. ¿Las bases de datos funcionaron sin errores de consistencia?	☒	☐	☐ Sí ☐ No
24. ¿El control de versiones registró todos los cambios correctamente?	☒	☐	☐ Sí ☐ No
25. ¿Las validaciones automáticas detectaron anomalías?	☐	☒	☐ No detectó ☒ Detectó

Total Integridad: 3 / 5

DIMENSIÓN 3: DISPONIBILIDAD

Indicador Diario	Seguro	Inseguro	Observación
26. ¿El sistema estuvo disponible durante todo el horario laboral?	☒	☐	☐ Sí ☐ No
27. ¿Cero (0) caídas del sistema reportadas en el día?	☒	☐	___ caídas reportadas
28. ¿El respaldo diario programado se ejecutó exitosamente?	☒	☐	☐ Sí ☐ No
29. ¿El sistema respondió con velocidad normal durante el día?	☒	☐	☐ Sí ☐ No
30. ¿Los planes de continuidad estuvieron accesibles y actualizados?	☐	☒	☒ Sí ☐ No

Total Disponibilidad: 4

EVALUACIÓN GENERAL DIARIA DE SEGURIDAD

Dimensión	Puntaje	Estado Diario		Seguridad general del sistema del día:
		Seguro	Inseguro	
Confidencialidad	3 /5	X		☐ **Seguro (1):** Al menos 2 de 3 dimensiones seguras
Integridad	3 /5	X		☐ **Inseguro (0):** 2 o más dimensiones inseguras
Disponibilidad	4 /5		X	

Anexo D: Instrumentos de recolección de datos

REGISTRO DIARIO DE CUMPLIMIENTO ISO/IEC 27001

Objetivo: Registrar diariamente el cumplimiento de criterios ISO/IEC 27001 en los 5 sistemas de información durante 90 días consecutivos.

DATOS GENERALES DEL REGISTRO

Fecha: 15 // 08 // 2025 (Día 15 de 30)

Hora de inicio: hh: 08 mm: 00 **Hora de finalización:** hh: 10 mm: 10

Sistema Evaluado: S1☐ S2☐ S3☒ S4☐ S5☐

Escala de medición

- **1 = SÍ/CUMPLE:** Criterio implementado y funcionando correctamente en las últimas 24h
- **0 = NO/NO CUMPLE:** Criterio no implementado o con fallas en las últimas 24h

DIMENSIÓN 1: GESTIÓN DE RIESGOS

Indicador Diario	Sí	No	Observación
1. ¿Se ejecutaron las evaluaciones de riesgo programadas para hoy?	☒	☐	
2. ¿Los controles de riesgo funcionaron sin incidencias?	☐	☒	
3. ¿Se registraron y trataron adecuadamente los nuevos riesgos identificados?	☐	☒	
4. ¿Las políticas de seguridad estuvieron disponibles y accesibles?	☐	☒	
5. ¿Se cumplieron los procedimientos operativos de seguridad establecidos?	☒	☐	

DIMENSIÓN 2: SEGURIDAD OPERATIVA

Indicador Diario	Sí	No	Observación
6. ¿Los procedimientos de acceso funcionaron correctamente?	☒	☐	
7. ¿El cifrado de datos críticos estuvo operativo?	☒	☐	
8. ¿Los sistemas antimalware estuvieron actualizados y funcionando?	☒	☐	
9. ¿Se gestionaron adecuadamente los incidentes ocurridos?	☒	☐	
10. ¿Los controles de acceso físico y lógico funcionaron sin fallas?	☒	☐	

DIMENSIÓN 3: DESEMPEÑO OPERATIVO

Indicador Diario	Sí	No	Observación
11. ¿Se ejecutaron las actividades de monitoreo programadas?	☒	☐	
12. ¿Los indicadores de desempeño se midieron según cronograma?	☒	☐	
13. ¿Se documentaron las no conformidades identificadas?	☒	☐	
14. ¿Se implementaron las acciones correctivas planificadas?	☒	☐	
15. ¿Los procesos de mejora continua estuvieron activos?	☐	☒	

Ficha de observación

REGISTRO DIARIO DE SEGURIDAD DE SISTEMAS

Objetivo: Registrar diariamente el nivel de seguridad de los sistemas de información mediante indicadores observables durante 90 días consecutivos.

DATOS GENERALES DEL REGISTRO

Fecha: //2025 (Día 15 de 30)

Hora de inicio: hh: 08 mm: 00 **Hora de finalización**: hh: 10 mm: 10

Sistema Observado: ☐ S1 ☐ S2 ☒ S3 ☐ S4 ☐ S5

Escala de medición

- **1 = SEGURO:** Indicador dentro de parámetros aceptables en las últimas 24h
- **0 = INSEGURO:** Indicador fuera de parámetros aceptables en las últimas 24h

DIMENSIÓN 1: CONFIDENCIALIDAD

Indicador Diario	Seguro	Inseguro	Observación
16. ¿Cero (0) accesos no autorizados detectados en el día?	☒	☐	___ accesos detectados
17. ¿Todos los usuarios ingresaron con credenciales válidas?	☒	☐	☐ Sí ☐ No
18. ¿El sistema de cifrado funcionó sin interrupciones?	☒	☐	☐ Sí ☐ No
19. ¿Cero (0) accesos a áreas restringidas sin autorización?	☒	☐	___ accesos indebidos
20. ¿La autenticación multifactor estuvo disponible todo el día?	☒	☐	☐ Sí ☐ No

Total Confidencialidad: 5 / 5

DIMENSIÓN 2: INTEGRIDAD

Indicador Diario	Seguro	Inseguro	Observación
21. ¿Cero (0) modificaciones no autorizadas detectadas?	☐	☒	3 modificaciones
22. ¿Las verificaciones de integridad se completaron sin errores?	☒	☐	☐ Sí ☐ No
23. ¿Las bases de datos funcionaron sin errores de consistencia?	☒	☐	☐ Sí ☐ No
24. ¿El control de versiones registró todos los cambios correctamente?	☒	☐	☐ Sí ☐ No
25. ¿Las validaciones automáticas detectaron anomalías?	☒	☐	☐ No detectó ☐ Detectó

Total Integridad: 4 / 5

DIMENSIÓN 3: DISPONIBILIDAD

Indicador Diario	Seguro	Inseguro	Observación
26. ¿El sistema estuvo disponible durante todo el horario laboral?	☒	☐	☐ Sí ☐ No
27. ¿Cero (0) caídas del sistema reportadas en el día?	☒	☐	___ caídas reportadas
28. ¿El respaldo diario programado se ejecutó exitosamente?	☒	☐	☐ Sí ☐ No
29. ¿El sistema respondió con velocidad normal durante el día?	☒	☐	☐ Sí ☐ No
30. ¿Los planes de continuidad estuvieron accesibles y actualizados?	☒	☐	☐ Sí ☐ No

Total Disponibilidad: 5

EVALUACIÓN GENERAL DIARIA DE SEGURIDAD

Dimensión	Puntaje	Estado Diario		Seguridad general del sistema del día:
		Seguro	Inseguro	
Confidencialidad	5 /5	X		☐ **Seguro (1):** Al menos 2 de 3 dimensiones seguras
Integridad	4 /5	X		☐ **Inseguro (0):** 2 o más dimensiones inseguras
Disponibilidad	5 /5	X		

Anexo D: Instrumentos de recolección de datos

REGISTRO DIARIO DE CUMPLIMIENTO ISO/IEC 27001

Objetivo: Registrar diariamente el cumplimiento de criterios ISO/IEC 27001 en los 5 sistemas de información durante 90 días consecutivos.

DATOS GENERALES DEL REGISTRO

Fecha: 04 // 08 // 2025 (Dia 4 de 30)

Hora de inicio: hh: 08 mm: 00 **Hora de finalización**: hh: 09 mm: 30

Sistema Evaluado: S1☐ S2☐ S3☐ S4☒ S5☐

Escala de medición

- **1 = SÍ/CUMPLE:** Criterio implementado y funcionando correctamente en las últimas 24h
- **0 = NO/NO CUMPLE:** Criterio no implementado o con fallas en las últimas 24h

DIMENSIÓN 1: GESTIÓN DE RIESGOS

Indicador Diario	Sí	No	Observación
1. ¿Se ejecutaron las evaluaciones de riesgo programadas para hoy?	☒	☐	
2. ¿Los controles de riesgo funcionaron sin incidencias?	☒	☐	
3. ¿Se registraron y trataron adecuadamente los nuevos riesgos identificados?	☒	☐	
4. ¿Las políticas de seguridad estuvieron disponibles y accesibles?	☒	☐	
5. ¿Se cumplieron los procedimientos operativos de seguridad establecidos?	☐	☒	

DIMENSIÓN 2: SEGURIDAD OPERATIVA

Indicador Diario	Sí	No	Observación
6. ¿Los procedimientos de acceso funcionaron correctamente?	☐	☒	
7. ¿El cifrado de datos críticos estuvo operativo?	☒	☐	
8. ¿Los sistemas antimalware estuvieron actualizados y funcionando?	☐	☒	
9. ¿Se gestionaron adecuadamente los incidentes ocurridos?	☐	☒	
10. ¿Los controles de acceso físico y lógico funcionaron sin fallas?	☐	☒	

DIMENSIÓN 3: DESEMPEÑO OPERATIVO

Indicador Diario	Sí	No	Observación
11. ¿Se ejecutaron las actividades de monitoreo programadas?	☐	☒	
12. ¿Los indicadores de desempeño se midieron según cronograma?	☒	☐	
13. ¿Se documentaron las no conformidades identificadas?	☐	☒	
14. ¿Se implementaron las acciones correctivas planificadas?	☒	☐	
15. ¿Los procesos de mejora continua estuvieron activos?	☒	☐	

Ficha de observación

REGISTRO DIARIO DE SEGURIDAD DE SISTEMAS

Objetivo: Registrar diariamente el nivel de seguridad de los sistemas de información mediante indicadores observables durante 90 días consecutivos.

DATOS GENERALES DEL REGISTRO

Fecha: //2025 (Día 09 de 30)

Hora de inicio: hh: 08 mm: 00 **Hora de finalización**: hh: 09 mm: 30

Sistema Observado: ☐ S1 ☐ S2 ☐ S3 ☒ S4 ☐ S5

Escala de medición

- **1 = SEGURO:** Indicador dentro de parámetros aceptables en las últimas 24h
- **0 = INSEGURO:** Indicador fuera de parámetros aceptables en las últimas 24h

DIMENSIÓN 1: CONFIDENCIALIDAD

Indicador Diario	Seguro	Inseguro	Observación
16. ¿Cero (0) accesos no autorizados detectados en el día?	☐	☒	6 accesos detectados
17. ¿Todos los usuarios ingresaron con credenciales válidas?	☒	☐	☐ Sí ☐ No
18. ¿El sistema de cifrado funcionó sin interrupciones?	☒	☐	☐ Sí ☐ No
19. ¿Cero (0) accesos a áreas restringidas sin autorización?	☐	☒	6 accesos indebidos
20. ¿La autenticación multifactor estuvo disponible todo el día?	☐	☒	☐ Sí ☒ No

Total Confidencialidad: 2 / 5

DIMENSIÓN 2: INTEGRIDAD

Indicador Diario	Seguro	Inseguro	Observación
21. ¿Cero (0) modificaciones no autorizadas detectadas?	☒	☐	6 modificaciones
22. ¿Las verificaciones de integridad se completaron sin errores?	☐	☒	☐ Sí ☒ No
23. ¿Las bases de datos funcionaron sin errores de consistencia?	☒	☐	☐ Sí ☐ No
24. ¿El control de versiones registró todos los cambios correctamente?	☒	☐	☐ Sí ☐ No
25. ¿Las validaciones automáticas detectaron anomalías?	☐	☒	☒ No detectó ☐ Detectó

Total Integridad: 3 / 5

DIMENSIÓN 3: DISPONIBILIDAD

Indicador Diario	Seguro	Inseguro	Observación
26. ¿El sistema estuvo disponible durante todo el horario laboral?	☒	☐	☐ Sí ☐ No
27. ¿Cero (0) caídas del sistema reportadas en el día?	☐	☒	3 caídas reportadas
28. ¿El respaldo diario programado se ejecutó exitosamente?	☒	☐	☐ Sí ☐ No
29. ¿El sistema respondió con velocidad normal durante el día?	☒	☐	☐ Sí ☐ No
30. ¿Los planes de continuidad estuvieron accesibles y actualizados?	☒	☐	☐ Sí ☐ No

Total Disponibilidad: 4

EVALUACIÓN GENERAL DIARIA DE SEGURIDAD

Dimensión	Puntaje	Estado Diario		Seguridad general del sistema del día:
		Seguro	Inseguro	
Confidencialidad	2 /5		X	☐ **Seguro (1):** Al menos 2 de 3 dimensiones seguras
Integridad	3 /5	X		☐ **Inseguro (0):** 2 o más dimensiones inseguras
Disponibilidad	4 /5	X		

Anexo D: Instrumentos de recolección de datos

REGISTRO DIARIO DE CUMPLIMIENTO ISO/IEC 27001

Objetivo: Registrar diariamente el cumplimiento de criterios ISO/IEC 27001 en los 5 sistemas de información durante 90 días consecutivos.

DATOS GENERALES DEL REGISTRO

Fecha: 18 // 08 // 2025 (Día 18 de 30)

Hora de inicio: hh: 07 mm: 30 **Hora de finalización**: hh: 09 mm: 30

Sistema Evaluado: S1☐ S2☐ S3☐ S4☐ S5☒

Escala de medición

- **1 = SÍ/CUMPLE:** Criterio implementado y funcionando correctamente en las últimas 24h
- **0 = NO/NO CUMPLE:** Criterio no implementado o con fallas en las últimas 24h

DIMENSIÓN 1: GESTIÓN DE RIESGOS

Indicador Diario	Sí	No	Observación
1. ¿Se ejecutaron las evaluaciones de riesgo programadas para hoy?	☒	☐	
2. ¿Los controles de riesgo funcionaron sin incidencias?	☒	☐	
3. ¿Se registraron y trataron adecuadamente los nuevos riesgos identificados?	☒	☐	
4. ¿Las políticas de seguridad estuvieron disponibles y accesibles?	☒	☐	
5. ¿Se cumplieron los procedimientos operativos de seguridad establecidos?	☒	☐	

DIMENSIÓN 2: SEGURIDAD OPERATIVA

Indicador Diario	Sí	No	Observación
6. ¿Los procedimientos de acceso funcionaron correctamente?	☒	☐	
7. ¿El cifrado de datos críticos estuvo operativo?	☐	☒	
8. ¿Los sistemas antimalware estuvieron actualizados y funcionando?	☒	☐	
9. ¿Se gestionaron adecuadamente los incidentes ocurridos?	☒	☐	
10. ¿Los controles de acceso físico y lógico funcionaron sin fallas?	☒	☐	

DIMENSIÓN 3: DESEMPEÑO OPERATIVO

Indicador Diario	Sí	No	Observación
11. ¿Se ejecutaron las actividades de monitoreo programadas?	☒	☐	
12. ¿Los indicadores de desempeño se midieron según cronograma?	☐	☒	
13. ¿Se documentaron las no conformidades identificadas?	☒	☐	
14. ¿Se implementaron las acciones correctivas planificadas?	☒	☐	
15. ¿Los procesos de mejora continua estuvieron activos?	☐	☒	

Ficha de observación

REGISTRO DIARIO DE SEGURIDAD DE SISTEMAS

Objetivo: Registrar diariamente el nivel de seguridad de los sistemas de información mediante indicadores observables durante 90 días consecutivos.

DATOS GENERALES DEL REGISTRO

Fecha: //2025 (Día 18 de 30)

Hora de inicio: hh: 07 mm: 30 **Hora de finalización:** hh: 08 mm: 30

Sistema Observado: ☐ S1 ☐ S2 ☐ S3 ☐ S4 ☒ S5

Escala de medición

- **1 = SEGURO:** Indicador dentro de parámetros aceptables en las últimas 24h
- **0 = INSEGURO:** Indicador fuera de parámetros aceptables en las últimas 24h

DIMENSIÓN 1: CONFIDENCIALIDAD

Indicador Diario	Seguro	Inseguro	Observación
16. ¿Cero (0) accesos no autorizados detectados en el día?	☒	☐	___ accesos detectados
17. ¿Todos los usuarios ingresaron con credenciales válidas?	☒	☐	☐ Sí ☐ No
18. ¿El sistema de cifrado funcionó sin interrupciones?	☒	☐	☐ Sí ☐ No
19. ¿Cero (0) accesos a áreas restringidas sin autorización?	☐	☒	1 accesos indebidos
20. ¿La autenticación multifactor estuvo disponible todo el día?	☒	☐	☐ Sí ☐ No

Total Confidencialidad: 4 / 5

DIMENSIÓN 2: INTEGRIDAD

Indicador Diario	Seguro	Inseguro	Observación
21. ¿Cero (0) modificaciones no autorizadas detectadas?	☒	☐	___ modificaciones
22. ¿Las verificaciones de integridad se completaron sin errores?	☒	☐	☐ Sí ☐ No
23. ¿Las bases de datos funcionaron sin errores de consistencia?	☒	☐	☐ Sí ☐ No
24. ¿El control de versiones registró todos los cambios correctamente?	☒	☐	☐ Sí ☐ No
25. ¿Las validaciones automáticas detectaron anomalías?	☐	☒	☐ No detectó ☒ Detectó

Total Integridad: 4 / 5

DIMENSIÓN 3: DISPONIBILIDAD

Indicador Diario	Seguro	Inseguro	Observación
26. ¿El sistema estuvo disponible durante todo el horario laboral?	☒	☐	☐ Sí ☐ No
27. ¿Cero (0) caídas del sistema reportadas en el día?	☒	☐	___ caídas reportadas
28. ¿El respaldo diario programado se ejecutó exitosamente?	☒	☐	☐ Sí ☐ No
29. ¿El sistema respondió con velocidad normal durante el día?	☐	☒	☐ Sí ☒ No
30. ¿Los planes de continuidad estuvieron accesibles y actualizados?	☒	☐	☐ Sí ☐ No

Total Disponibilidad: 4

EVALUACIÓN GENERAL DIARIA DE SEGURIDAD

Dimensión	Puntaje	Estado Diario		Seguridad general del sistema del día:
		Seguro	Inseguro	
Confidencialidad	4 /5	X		☐ **Seguro (1):** Al menos 2 de 3 dimensiones seguras
Integridad	4 /5	X		☐ **Inseguro (0):** 2 o más dimensiones inseguras
Disponibilidad	4 /5	X		