UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

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

Norma ISO 27001 e ISO 31000 en gestión de riesgos de activos de información de empresa de telecomunicaciones, Lima 2023

TESIS PARA OBTENER EL GRADO ACADÉMICO DE:

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

AUTORA:

Bernardo Infancion, Fiorella Denisse (orcid.org/0000-0003-0742-6322)

ASESORES:

Mg. Poletti Gaitan, Eduardo Humberto (orcid.org/0000-0002-2143-4444)

Dr. Pereyra Acosta, Manuel Antonio (orcid.org/0000-0002-2593-5772)

LÍNEA DE INVESTIGACIÓN:

Auditoría de Sistemas y Seguridad de la Información

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:

Desarrollo económico, empleo y emprendimiento

LIMA – PERÚ

2024

Dedicatoria

A Dios por darme la fuerza necesaria para culminar esta meta, a mi familia por su apoyo incondicional y por ser quienes me motivan a ser mejor cada día.

Agradecimiento

Quisiera expresar mi agradecimiento a mi familia por su comprensión y apoyo, a mis asesores por su dedicación, paciencia y guía y a mis compañeros que estuvieron conmigo en los momentos de estrés y alegría durante este largo y retador camino.

UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

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

Declaratoria de Autenticidad del Asesor

Yo, POLETTI GAITAN EDUARDO HUMBERTO, docente de la ESCUELA DE POSGRADO MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA NORTE, asesor de Tesis titulada: "Norma ISO 27001 e ISO 31000 en gestión de riesgos de activos de información de empresa de telecomunicaciones, Lima 2023", cuyo autor es BERNARDO INFANCION FIORELLA DENISSE, constato que la investigación tiene un índice de similitud de 16.00%, verificable en el reporte de originalidad del programa Turnitin, el cual ha sido realizado sin filtros, ni exclusiones.

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

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

LIMA, 04 de Enero del 2024

Apellidos y Nombres del Asesor:	**Firma**
POLETTI GAITAN EDUARDO HUMBERTO **DNI:** 18073124 **ORCID:** 0000-0002-2143-4444	Firmado electrónicamente por: EPOLETTIG el 07-01-2024 17:23:44

Código documento Trilce: TRI - 0719704

INVESTIGA UCV

UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

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

Declaratoria de Originalidad del Autor

Yo, BERNARDO INFANCION FIORELLA DENISSE estudiante de la ESCUELA DE POSGRADO del programa de MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA NORTE, declaro bajo juramento que todos los datos e información que acompañan la Tesis titulada: "Norma ISO 27001 e ISO 31000 en gestión de riesgos de activos de información de empresa de telecomunicaciones, Lima 2023", es de mi autorí a, por lo tanto, declaro que la Tesis:

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

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

Nombres y Apellidos	Firma
BERNARDO INFANCION FIORELLA DENISSE **DNI:** 43187871 **ORCID:** 0000-0003-0742-6322	Firmado electrónicamente por: FBERNARDOI el 08-01-2024 10:25:50

Código documento Trilce: INV - 1465594

INVESTIGA UCV

Índice de contenidos

Índice de tablas

Resumen

La finalidad de la investigación fue determinar la relación de la norma ISO 27001 y la norma ISO 31000 en la gestión de riesgo de una empresa del sector de telecomunicaciones, Lima. El tipo de investigación es aplicada, y de diseño no experimental transversal descriptivo correlacional. La población es 162 activos de información, tipo de muestreo es probabilístico tipo aleatoria simple quedando como muestra 115 activos de información. Se empleó la técnica de análisis documental teniendo como instrumento la ficha de datos que permitió conocer la información y obtener indicadores, se realizó la validación de contenido mediante la validez de juicios de expertos. Los resultados de la prueba de la normalidad con el Kolmogorov-Smirnov se rechaza la hipótesis nula de que los datos tienen una distribución normal y se acepta la Hipótesis alternativa que los datos no tienen una distribución normal y para la contratación de hipótesis se utilizó el coeficiente de correlación de Pearson según correspondan, donde se obtuvo los valores que se ubican en la zona de rechazo de la hipótesis nula, en consecuencia, se concluye que existe una asociación significativa y positiva la norma ISO 27001 y la norma ISO 31000 con la gestión de riesgos.

Palabras clave: Norma ISO 27001, Norma ISO 31000 y gestión de riesgos.

Abstract

The purpose of the research was to determine the relationship between the ISO 27001 standard and the ISO 31000 standard in the risk management of a company in the telecommunications sector, Lima. The type of research is applied, with a cross-sectional descriptive correlational non-experimental design. The population is 162 information assets, the type of sampling is probabilistic simple random type, leaving 115 information assets as a sample. The documentary analysis technique was used with the data sheet as an instrument that allowed the information to be known and indicators obtained, content validation was carried out through the validity of expert judgments. The results of the normality test with the Kolmogorov-Smirnov reject the null hypothesis that the data have a normal distribution and accept the alternative hypothesis that the data do not have a normal distribution and to contract the hypothesis the coefficient was used of Pearson correlation as appropriate, where the values that are located in the rejection zone of the null hypothesis were obtained, consequently, it is concluded that there is a significant and positive association between the ISO 27001 standard and the ISO 31000 standard with the management of risks.

Keywords: ISO 27001 Standard, ISO 31000 Standard and risk management.

I. INTRODUCCIÓN

En ámbito internacional, Valencia y Orozco (2017) señalan que actualmente, las incidencias tecnológicas forman parte esencial de nuestras vidas diarias y también son inherentes al entorno empresarial. Estas amenazas engloban una variedad de virus, así como incidentes de ransomware recientes y ataques más avanzados, como los de día cero, los cuales requieren una gestión adaptada garantizando una seguridad adecuada. Las TIC son elementos cruciales para la efectividad y capacidad empresarial. Sin embargo, al igual que cualquier recurso, están expuestas a diversas amenazas que pueden generar incidentes con múltiples implicaciones. El estudio presente resalta la relevancia de desarrollar un marco de referencia en el desarrollo del SGSI fundamentado en normatividad ISO-27001 y otras normas e incluir las fases de desarrollo de administración de incidentes de Información respecto a la seguridad, con la finalidad de salvaguardar los activos de información frente a diferentes amenazas tecnológicas que aumentan día a día.

Asimismo, Kitsios et al. (2023) señalan que existe un alza en acciones maliciosas cibernéticas en los últimos años. El crecimiento de una organización puede hacerla más atractiva como objetivo de estos ataques, la divulgación accidental de información confidencial puede provocar daños a la reputación, los ingresos y credibilidad en la organización. La normatividad ISO-27001 incorpora circunstancias necesarias y personalizadas para cumplir con proyecciones de la organización en evaluación y administración de amenazas referente a la seguridad. Estos requisitos previos son esenciales en garantizar que los recursos de información respecto al resguardo se mitiguen de manera eficiente. Recientemente, el marco de administración en riesgos ISO-31000 en su versión 2018 se ha propuesto la meta de realizar una investigación en profundidad sobre la administración de riesgos. Se pretende ejecutar la investigación para comprender mejor la administración de riesgos y estar preparados para los actuales ataques cibernéticos.

Tobi et al. (2019) señalan, que, para la permanencia de una organización, se necesita una estrategia enfocada en administración de riesgo respecto a los activos y que proporcione sencillez ante el riesgo. Por ello la priorización de críticos activos y el desarrollo de fundamentos de criticidad es necesaria para proteger la operación de los activos y seguridad.

Kamil et al. (2023) indican, al no adoptar un SGSI adecuado para las operaciones y los sistemas puede comprometer la capacidad de garantizar la permanencia del negocio. Estas referencias como la ISO-27001 se consideran herramientas necesarias e influyentes en la actualidad, dadas las crecientes amenazas del cibercrimen, el hacktivismo y los gobiernos extranjeros que atacan valiosos activos organizacionales. En otras palabras, resguardar la información de recursos de las empresas es crucial, particularmente en entornos comerciales interconectados, para mitigar el impacto de las incidencias de seguridad y garantizar la permanencia del negocio.

Razikin y Soewito (2022) nos dicen que amenazas y ataques a las aplicaciones tecnológicas en la seguridad han aumentado de manera muy significativa. Las organizaciones deben llevar a cabo una administración de riesgos y evaluar la preparación de los sistemas de tecnología en la seguridad para disminuir el nivel de riesgo en seguridad y brindar garantías para la continuidad del negocio. Con analizar riesgos y revisión de cumplimiento de ciberseguridad se puede ver el nivel de riesgo de cada amenaza y brecha de seguridad existente en la empresa.

A nivel nacional, Rodriguez et al. (2020) indican que tanto la información física como la digital desempeñan un papel crucial como activos fundamentales para cualquier entidad. Si una empresa no gestiona sus datos respecto al riesgo de manera adecuada, se vuelve susceptible a poner en peligro la continuidad de sus operaciones. Señala que insuficientes medidas de control y seguridad pueden generar vulnerabilidades legales, por lo tanto, es imperativo que las compañías establezcan políticas o mecanismos para resguardar no solo su información, también sus clientes, asociados comerciales y socios claves. La carencia de estos mecanismos de seguridad expone a las organizaciones a ataques que pueden

resultar en riesgos graves, daños relevantes y la pérdida de datos confidenciales. La importancia del estudio diagnostica la influencia de la ISO-27001 referente a la información en la empresa.

Huaura (2019) señala que las empresas del ámbito de las telco experimentan pérdidas económicas, ya sea por factores externos o internos, como el extravío de datos, debido a que los riesgos no son administrados adecuadamente, podrían tener un origen desconocido o conocido. El resguardo de la información y administración de riesgos es elemental para las organizaciones logren alcanzar sus metas. Por esta razón, este estudio busca entender la administración de riesgos sustentada: NTP-ISO/IEC-31000 impacta en monitoreo de riesgos.

Huayllani (2020) señala que, en épocas anteriores, los sistemas informáticos de administración de información en temas de seguridad no eran considerados como un componente crucial en las organizaciones. Sin embargo, en la actualidad, tanto los líderes empresariales como los de tecnología en instituciones privadas y públicas muestran un creciente interés en estos sistemas, resultado del avance tecnológico actual. La exposición de información valiosa a cualquier usuario puede acarrear incidencias como eliminación o divulgación de contenidos privados. Aunque es válido que la información de una organización esté accesible para todos, esto no implica que deba estar completamente disponible para cualquier persona. En nuestro ámbito el MINSA ha completado el desarrollo de su SGSI y una gestión de riesgos basada en la ISO-27001-Normatividad.

A nivel local, el 29% de los recursos de información catalogados como críticos en la organización del ámbito de telco, se encontraban expuestos ante cualquier amenaza. Se pudo identificar que los activos críticos tenían implementados controles de seguridad parcialmente, las cuales los hacían vulnerables y por ello también a la organización en cuanto a confidencialidad, integridad y disponibilidad. Donde la ISO 27001 nos brinda las directrices para salvaguardar datos y la ISO-31000 nos ayuda una gestión de riesgos. Por ello se tiene que analizar la relación de ambos para que nos ayuden a reducir los riesgos en los activos de información catalogados como críticos o no en la empresa, ya que

en la actualidad debido al creciente desarrollo tecnológico se encuentran expuestos ante cualquier amenaza.

El impacto en el ámbito social de esta investigación se puede tomar como referencia y estar preparados con los lineamientos a utilizar como son la normatividad ISO- 27001 e ISO-31000 para hacer frente ante las diferentes amenazas y ante la ciberdelincuencia aumentándose anualmente por la transformación digital. Asimismo, el impacto de ámbito profesional esta investigación puede ser consultada para abordar los riesgos de información en temas de seguridad.

Ante lo expuesto se identifica el siguiente problema general: ¿Existe una relación de la norma ISO 27001 y la norma ISO 31000 en la gestión de riesgo de los activos de información de una empresa del sector de telecomunicaciones, Lima 2023?; así también, los problemas específicos: ¿Existe una relación de la norma ISO 27001 y la norma ISO 31000 en el nivel de activos para la gestión de riesgos de los activos de información de una empresa del sector de telecomunicaciones, Lima 2023? y ¿Existe una relación de la norma ISO 27001 y la norma ISO 31000 en el nivel de riesgos para la gestión de riesgos de los activos de información de una empresa del sector de telecomunicaciones, Lima 2023?.

Esta investigación tiene una justificación práctica, ya que aborda los problemas identificados sobre la conexión de la norma ISO-27001 e ISO-31000 con la administración de riesgos de recursos de información de la organización del sector de comunicaciones. Donde se demuestra que hay una positiva conexión entre ellas para la administración de riesgos de la empresa.

Teniendo ante ello los siguientes objetivos: como general; Determinar la relación de la norma ISO 27001 y la norma ISO 31000 en la gestión de riesgos de los activos de información de una empresa de telecomunicaciones, Lima 2023; objetivos específicos: Determinar la relación de la norma ISO 27001 y la norma ISO 31000 en el nivel de activos para la gestión de riesgos de los activos de información de una empresa del sector de telecomunicaciones, Lima 2023 y Determinar la relación de la norma ISO 27001 y la norma ISO 31000 el nivel de riesgos para la gestión del riesgos de los activos de información de una empresa

de telecomunicaciones, Lima 2023.

Derivando del problema de investigación las siguientes hipótesis: Existe una asociación significativa de la norma ISO 27001 y la norma ISO 31000 en la gestión de riesgos de los activos de información de una empresa de telecomunicaciones, Lima 2023 y las hipótesis específicas; Existe una relación significativa de la norma ISO 27001 y la norma ISO 31000 en el nivel de activos para la gestión del riesgo de los activos de información de una empresa de telecomunicaciones, Lima 2023 y Existe una relación significativa de la norma ISO 27001 y la norma ISO 31000 impacta el nivel de riesgos para la gestión del riesgo de los activos de información de una empresa de telecomunicaciones, Lima 2023.

II. MARCO TEÓRICO

Este apartado considero los precedentes nacionales y mundiales relevantes para la indagación, los cuales se detallan a continuación:

Según Valencia y Orozco (2017) dicen que la información respecto a la seguridad es una disciplina tradicionalmente asociada a la administración de las TIC, teniendo como objetivo conservar un grado aceptable de riesgo para los datos de la organización y los dispositivos técnicos que permiten recolectar, procesar, acceder, intercambiar, almacenar, transformar y presentar adecuadamente mediante un diseño de un marco metodológico. Por lo que se generó como resultado una etapa metodológica que brinda respuestas sobre cómo abordar un proyecto tan importante en el contexto organizacional actual y con base en estándares internacionales.

Kitsios et al. (2023) indican que, al integrar eficazmente estrategias de seguridad, las empresas pueden mejorar su capacidad para defenderse contra amenazas al resguardo de la información y ataques cibernéticos. El propósito es describir el desarrollo de estrategias por una empresa del sector de tecnologías para garantizar la realización de los requisitos de la ISO-27001. Con un diseño descriptivo enfocándose en las buenas prácticas, y teniendo como resultado la empresa gana la confianza y la ventaja competitiva que necesita para ampliar su base de clientes.

Tobi et al. (2019) indican que en base al riesgo potencial se define un proceso de evaluación de trascendencia en la gestión de riesgos para los activos del centro de datos. La meta de la investigación es el modelado del desarrollo de un proceso de criticidad basado en riesgos para la gestión de activos. El diseño utilizado es exploratorio ya que busca entender y proponer un nuevo enfoque o modelo en la gestión de activos a partir de la relación entre criticidad y riesgo. Como resultado proporciona contribución a la gestión de riesgos, aumenta la confianza en una guía de apoyo basado en condiciones.

Kamil et al. (2023) nos dice que, para garantizar el resguardo de la información dentro de empresas, se recomienda establecer un SGSI que permita el monitoreo y administración de la información segura. Teniendo como objetivo

buscar la legitimidad de resultados de ISO-IEC 27001 a partir del enfoque de las expectativas de los interesados. Para esto, se hizo el estudio basado en entrevistas, en el que participaron partes interesadas relevantes involucradas en el manejo de la información respecto a temas de seguridad en organizaciones privadas en Suecia. Los detalles del estudio indican que la legitimidad de los hallazgos de ISO/IEC 27001 varía dependiendo de las metas específicas que las partes interesadas pretenden alcanzar. El estándar demuestra un alto nivel de legitimidad de resultados en relación con la implementación, establecimiento, operación y monitoreo de un SGSI.

Razikin y Soewito (2022) comentan en su propuesta de diseño de soporte a decisiones de ciberseguridad, para el despliegue del sistema de tecnologías de información respecto a la seguridad apoyado en la inspección de riesgo y marco de ISO/IEC 27001- Ciberseguridad. Teniendo como meta obtener el mejor sistema referente a la seguridad para reducir las amenazas. La propuesta construida mapea la urgencia de la rebaja de amenazas tomando la calificación relativa de la amenaza frente a la calificación relativa de la implementación del cumplimiento de ISO/IEC-27001. Dando como resultado del estudio bajas en el nivel de criticidad de las amenazas a las condiciones anteriores y después del desarrollo de las recomendaciones del sistema. Previo a la implementación de las recomendaciones de seguridad se encontraron amenazas con niveles de criticidad extrema y mayor, mientras que después del desarrollo de las recomendaciones del sistema de seguridad no se volvieron a encontrar.

Asimismo, Rodríguez et al. (2020) dicen que el desarrollo tecnológico ha permitido tratar información esencial para los intereses estratégicos de la empresa. Teniendo como objeto de estudio desarrollar el impacto de utilización de la normatividad ISO-27001 aplicada al resguardo de la información en una compañía privada de Lima (Perú). El diseño utilizado fue un pre-experimento; se consideraron y evaluaron 30 contribuyentes antes y después de la implementación de la intervención. Como resultado, se obtuvo una muestra que refleja el impacto de implementar la normatividad ISO-27001 de acuerdo con la información de seguridad interna de la organización. Además, se identificaron consecuencias notables en términos de disponibilidad, privacidad e integridad.

Huaura (2019) en su estudio indica que al realizar la administración de riesgos es asegurar que los probables riesgos de seguridad sean ubicados, estimados y desarrollados oportunamente. Su principal objetivo es definir que la administración de riesgos fundamentada en la NTP-ISO/IEC-31000 afecta en controlar riesgos en empresas del ámbito de telecomunicaciones. Su diseño del estudio es de tipo descriptivo formulando una hipótesis para predecir un suceso, donde examina la conexión existente para determinar si la hipótesis es válida. Como resultados encuentra una positiva media asociación de la seguridad de información y administración de riesgos.

Huayllani (2020) señala que el MINSA ha desarrollado un sistema de administración de seguridad junto con una gestión de riesgos. El propósito es evaluar cómo el sistema de administración de información respecto a la seguridad influye en la gestión del riesgo. La argumentación metodológica se halla en la necesidad de emplear un estudio de tipo correlacional para alcanzar los objetivos establecidos. Los hallazgos presentados indican de manera concluyente la existencia de conexión positiva y significativa de las variables de sistemas de administración de seguridad y administración del riesgo.

A continuación, se expone las variables de la investigación, con respecto a la variable independiente, según la normatividad ISO-27001 quien establece los lineamientos para poner en práctica y llevar a cabo el SGSI, que abarca un grupo de medidas de control destinadas a supervisar y disminuir riesgos vinculados a recursos de información donde las empresas intentan resguardar durante su funcionamiento. Asimismo, las organizaciones que implementan un SGSI pueden auditar y certificar su cumplimiento.

Según International Organization for Standardization - ISO 27001-2013 (2013), las aplicaciones encargadas del manejo de la seguridad de la información garantizan las tres bases de los SGSI, aplicando procesos para la administración de riesgos. Asimismo, ofrecen seguridad a las partes pertinentes, asegurando una administración adecuada de los riesgos.

Igualmente, con la segunda variable independiente, la International Organization for Standardization - ISO 31000:2018 (2018), está diseñada para personas que crean y protegen a la organización mediante la administración de los

riesgos, establecimiento, logro de objetivos, toma de decisiones, y mejora del desempeño.

Según International Organization for Standardization-ISO 31000:2018 (2018), indica que este archivo brinda instrucciones acerca del manejo de riesgos que enfrentan las organizaciones, donde ofrece un método estándar para manejar riesgos de cualquier índole, sin estar dirigido a una industria o sector en particular.

Según la International Organization for Standardization - ISO 31000:2018 (2018), dice que entidades de diversas índoles y dimensiones se ven confrontadas por elementos e influencias externas e internas generando dudas respecto a su habilidad para alcanzar sus metas. La administración de riesgos es iterativa y facilita a las entidades el desarrollo de estrategias, logro de metas y toma de informadas decisiones.

De acuerdo con la gestión de riesgos, según la normatividad - ISO 27000:2018 (2018), la gestión de riesgos se refiere a acciones sincronizadas destinadas a liderar y supervisar una organización en relación con los riesgos, en lo relativo al riesgo, en lo relativo al riesgo. Asimismo, señala que el procedimiento de administración de riesgos involucra la aplicación organizada de prácticas, políticas y procedimientos para gestionar actividades. Esto incluye la comunicación, consulta, contextualización, monitoreo, revisión, identificación, análisis, tratamiento del riesgo y su evaluación.

Según la International Organization for Standardization - ISO 27000:2018 (2018) indica que los controles son las medidas que modifican un riesgo. Asimismo, los controles se pueden incluir en cualquier parte del proceso. También es posible que no necesariamente los controles proporcionen el efecto modificador esperado.

Según la International Organization for Standardization - ISO 27000:2018 (2018) la media de un riesgo es resultado o descrito en función de la integración de su probabilidad y consecuencias. Siendo la probabilidad de que cualquier evento se produzca. Y la consecuencia, el desenlace de un evento que impacta en los objetivos de la entidad u organización.

Según la International Organization for Standardization - ISO 27000:2018 (2018), se presentan dos ámbitos: el ámbito externo, donde la organización

persigue sus metas. Este entorno abarca aspectos como lo cultural, social, político, legal, regulatorio, tecnológico, económico, nacional, internacional, regional o local, además de tendencias y factores que inciden en las metas, también la relación con las partes interesadas. Por otro lado, se encuentra el ambiente interno, donde la organización busca cumplir sus objetivos. Este entorno involucra aspectos como el gobierno, la estructura, funciones, políticas, metas, capacidades, recursos, procesos, información, relaciones, cultura y acuerdos contractuales.

Según la International Organization for Standardization - ISO 27000:2018 (2018), la familia SGSI desarrolla e implementa una estructura para administrar la protección de su marco para administrar la seguridad de sus recursos de información. Un activo de información es todo aquel activo que da valor a su empresa.

Según la International Organization for Standardization - ISO 27002:2013 (2013), indica que la norma contiene 14 capítulos de monitoreo de información respecto a la seguridad y que cada sección establece acciones de seguridad que incluyen una o varias categorías fundamentales de protección. Que se utilizan en la categoría 6.1.3 atención de riesgos de la norma ISO 27001.

Según la International Organization for Standardization - ISO 31000:2018 (2018), establece que el contexto es poder definir parámetros interna y externamente para tener en cuenta en qué tiempo se administra el riesgo.

Según la International Organization for Standardization - ISO 27005:2018 (2018), indica que la evaluación de activos es un fragmento de las actividades del manejo de seguridad de la información respecto a riesgos.

Según la International Organization for Standardization - ISO 27000:2018 (2018), define al análisis del riesgo como el proceso que va a facilitar la comprensión de la esencia y establecer el grado de riesgo.

Araujo (2017) mencionó que, al evaluar los riesgos, la organización puede analizar de qué manera los potenciales riesgos afectan la capacidad para alcanzar sus metas establecidas y, en consecuencia, sus objetivos.

Guerra et al. (2021) señalan que, en ocasiones, tanto el gobierno corporativo como la gestión empresarial pasan por alto el activo más significativo: la

información.

Toro et al. (2019) indican que las bases del resguardo de la información se describen como: confidencialidad, que implica resguardar los datos contra divulgaciones no permitidas; disponibilidad, que garantiza la continuidad de las operaciones, vital para la productividad; e integridad, que asegura la inalterabilidad de los datos.

Chavez (2016) comenta que el resguardo de la información se focaliza en preservar confidencialidad y la integridad de datos alojados en entornos digitales. Este campo implica una diversidad de componentes, estándares, protocolos de control y procesos reconocidos internacionalmente, cuyo propósito es mitigar riesgos, evitar entradas sin autorización y garantizar en el momento requerido la accesibilidad de información. Sus pilares fundamentales incluyen la gestión de riesgos, la privacidad de datos, prevención de intrusiones, protección contra amenazas y la continuidad del negocio.

Rodríguez et al. (2020) nos dicen que la norma ISO 27001 proporciona un marco detallado que orienta en la salvaguardia de privacidad en la administración de la información. En lo que respecta a la integridad, su enfoque principal radica en proteger la información para prevenir cualquier tipo de cambios no autorizados por la entidad responsable. Esta norma constituye un conjunto de directrices exhaustivas que buscan respaldar la integridad y privacidad de la información en los entornos de administración de la información. Esta norma simplifica el establecimiento de procesos particulares para preservar la incorruptibilidad de la información, garantizando su precisión y coherencia a lo largo del tiempo.

Rantao y Njenga (2020) indican que las directrices de seguridad informática tienen como propósito garantizar que los usuarios de los recursos informáticos de una empresa sigan pautas específicas orientadas a proteger dichos recursos de probables riesgos. Estas recomendaciones abarcan acciones como el empleo de contraseñas robustas, restricciones en el acceso, encriptado de información y aplicación de estándares de seguridad. Asimismo, buscan concienciar sobre los riesgos en entornos digitales y fomentar conductas responsables en el manejo de datos confidenciales. Esta práctica fortalece la capacidad de las empresas ante vulnerabilidades potenciales y posibles ciberataques.

Zuña et al. (2019) comentan que de acuerdo con Instituto Nacional de Ciberseguridad de España - INCIBE, estos sucesos representan amenazas considerables en el ámbito de la seguridad digital como el espionaje cibernético, las intrusiones en redes corporativas, denegación de servicio distribuido (DDoS), el phishing, los fallos en programas, la presencia de malware y las filtraciones de información son incidentes persistentes que requieren una gestión activa y estrategias de protección robustas. Para conservar la incorruptibilidad de información y sistemas, es crucial implementar enfoques proactivos y estrategias de seguridad de alto nivel. Estas amenazas continuas destacan la urgencia de mantener una respuesta constante e incorporación de medidas sólidas para garantizar el resguardo y confidencialidad.

Kovalenko et al. (2019) mencionan que los peligros respecto a seguridad de datos se clasifican en dos categorías principales: amenazas naturales y artificiales. Prestemos especial atención a las amenazas provenientes de eventos naturales y busquemos reconocer las más significativas. Los riesgos naturales engloban situaciones como incendios, inundaciones, huracanes, descargas eléctricas y otros sucesos catastróficos o fenómenos naturales no causados por acciones humanas. Dentro de estas amenazas, los incendios suelen destacarse como los más comunes. Es esencial comprender y prepararse adecuadamente para afrontar estos posibles peligros naturales. Para asegurar la información en su seguridad, es fundamental equipar las instalaciones que albergan los elementos del sistema, como los medios digitales, servidores y archivos, con sistemas de detección de incendios, designar responsables encargados de la seguridad contra incendios y contar con dispositivos de extinción de incendios. La observancia de estas normativas contribuirá a reducir la posibilidad de pérdida de información debido a un incendio. Además, entre los riesgos deliberados externos se cuentan posibles ataques perpetrados por hackers. En caso de que la aplicación de información esté en línea a la red global de Internet, resulta esencial instalar un firewall (o cortafuegos) para evitar este tipo de ataques. Este mecanismo de protección puede ser parte integrante del hardware o ser implementado mediante programas específicos.

Diéguez y Cares (2019) explican que la supervisión del resguardo de la

información se logra mediante el establecimiento y funcionamiento de un SGSI. Estos sistemas tienen como objetivo identificar y aplicar acciones de seguridad para reducir el riesgo vinculado con el manejo de la información.

Pretorius y Ngejane (2019) argumentan que solamente administrar y responder a incidentes no asegurará una seguridad total de la información o al nivel absoluto del 100%. Un sistema de información respecto a la seguridad demanda una evolución constante y un proceso continuo de aprendizaje. Esta mejora se alcanza a través de evaluaciones periódicas que deben abordar tres elementos esenciales: protección, detección y respuesta. Este enfoque iterativo es crucial para mantener la efectividad y la adaptabilidad del sistema de información respecto a la seguridad ante las cambiantes amenazas y desafíos.

Tonysé de la Rosa (2021) señalan que, conforme a la mejora constante, un sistema de administración de información de seguridad se compone de 4 etapas esenciales que demandan una ejecución ininterrumpida para reducir los riesgos asociados a la información. Estas etapas, que abarcan la planificación, implementación, evaluación y acción, deben ser aplicadas de manera continua y rigurosa asegurando la efectividad y cuidado adecuado de la información.

Portugal (2017) indica que varias empresas eligen utilizar la normativa de Gestión de Riesgos (ISO 31000) debido a su mayor practicidad y facilidad en su aplicación. Esta norma resulta más accesible y amigable para su integración en el entorno empresarial.

Lizarzaburu et al. (2018) señalan que las empresas están otorgando mayor importancia a la gestión de riesgos, como resultado de una serie de eventos tanto internos como externos que están ocurriendo. Esta creciente atención hacia la administración de riesgos se debe a diversos sucesos que afectan tanto el ámbito interno como el externo de las organizaciones.

Gerson et al. (2023) explican que una estrategia efectiva para proteger los comercios electrónicos sería adoptar la norma ISO 27001, la cual ofrece una serie de directrices y requerimientos necesarios para alcanzar un elevado nivel de seguridad, tanto para la organización como para sus clientes. Esta norma proporciona un marco sólido para fortalecer la seguridad de las operaciones y

salvaguardar la información sensible. Esto se logra mediante la creación y desarrollo de un SGSI, lo que permite que la organización tenga el control y la confianza de que sus activos críticos, como servidores, información y recursos humanos, estén resguardados ante cualquier posible amenaza o riesgo latente. Este sistema proporciona un marco sólido para resguardar los activos más valiosos de la empresa.

Ramos et al. (2023) indican que, de acuerdo con la norma ISO-27001, es necesario realizar revisiones periódicas para asegurar la información de acuerdo a la seguridad. Estas evaluaciones se llevan a cabo mediante la implementación de normativas de seguridad y requieren auditorías para verificar las normativas establecidas de seguridad, como de los monitoreos de seguridad documentados aplicables, asegurando la conformidad continua con las especificaciones de seguridad y garantizando la protección de información.

Bustamante et al. (2021) plantean que para que el usuario comprenda mejor y se transforme en un elemento esencial de la administración de seguridad, es esencial realizar una sensibilización por áreas específicas. Esta estrategia busca aumentar la conciencia y comprensión de la seguridad en diferentes sectores o departamentos de la organización.

Ferreira et al. (2018) sostienen que la información respecto a la seguridad se alcanza mediante la ejecución del grupo de medidas apropiadas, que abarcan estructuras organizativas, procesos, políticas, software, hardware y procedimientos. Este monitoreo debe ser establecido, implementado, supervisado, evaluado críticamente y mejorado continuamente teniendo el fin del logro de las metas comerciales y la protección de la información en la organización.

Satizábal y Acevedo (2018) señalan que la prevención de riesgos es un proceso continuo implicando: analizar los riesgos presentes en un sistema de información; diseñar e implementar acciones a inmediato y largo plazo con el objetivo de prevenir o mitigar los riesgos identificados; evaluar la efectividad de estas acciones y ajustarlas según los cambios internos y externos en el ámbito de la institución.

Lykhova et al. (2022) apuntan en su exploración sobre estándares

internacionales que, dada la naturaleza dinámica más que estática del resguardo de la información, los estándares adoptados tienden a volverse obsoletos con el tiempo. Los principales estándares internacionales y nacionales de seguridad de la información abordados en este estudio indican que su aprobación suele depender del progreso tecnológico de la información, la emergencia de nuevas amenazas a la información y el creciente riesgo asociado a la misma. Presentemente, la seguridad de información a nivel mundial se asegura mediante el cumplimiento de diversas normas ISO internacionales, que delinean los procedimientos para analizar y evaluar los riesgos de la información y los métodos para combatirlos.

Sabillon (2018) señalan en su investigación sobre el modelo integral de auditoría de ciberseguridad la relevancia de auditorías para asegurar la presencia de controles de seguridad de la información e identificar posibles debilidades inexistentes o controles de ciberseguridad obsoletos. Esto se debe a la constante amenaza que enfrentan las organizaciones de ser el foco de ciber ataques y ciber amenazas. La complejidad y sofisticación de los ciber criminales actuales, así como las tácticas y procedimientos de los criminales informáticos, incluyendo las tácticas, técnicas y procedimientos (TTP), Están progresando a una velocidad nunca vista. Los ciberdelincuentes están perpetuamente adaptando nuevas tácticas para la planificación y llevar a cabo ciberataques, aprovechando las debilidades de ciber seguridad vigentes y explotando mediante técnicas de ingeniería social.

Cruz et al. (2018) aseguran que las empresas adoptan de manera continua estándares técnicos en sistemas de administración, como ISO-9001, ISO-14001, OHSAS-18001, ISO/IEC-27001 e ISO-22000, con la finalidad de incrementar su habilidad para competir y alcanzar la excelencia. Resaltan los sistemas de administración certificados, como el de administración de calidad ISO-9001, sistema de administración del ambiente ISO-14001 y el sistema de administración de salud ocupacional OHSAS-18001, han obtenido aceptación en distintas naciones. Además, sugieren que una estrategia para mejorar la eficacia del sistema integrado de administración consiste en abordar estos estándares de manera conjunta.

Mayayise (2021) señala que la ISO/IEC-27001 es una norma para prácticas de resguardo de la información, asimismo muchos criterios ISO, suele ser revisado para estar alineado con los avances en la industria de las TIC. Según los requisitos de este estándar de seguridad, es necesario que una organización establezca una política que regule el resguardo de la información. Además de este requisito, es crucial que los empleados estén familiarizados con el contenido de dicha política.

III. METODOLOGÍA

3.1 Tipo y diseño de investigación

Tipo de investigación

Fue de tipo aplicada, de conformidad con Sánchez et al. (2018), describen que este enfoque de investigación tiene como objetivo comprender con detalle la ejecución de acciones específicas destinadas a implementar medidas, realizar las transformaciones necesarias y asegurar la continuidad frente a situaciones o eventos reales que puedan surgir.

Hinojosa (2017) destaca que tiene como objetivo este tipo de investigación abordar un desafío al integrar el conocimiento mediante su aplicación y contribuir al ámbito científico.

Según Baena (2017) nos dice que se enfoca la investigación aplicada en las ventajas específicas de poner en práctica las teorías generales, centrándose en abordar las planteadas necesidades por las personas y la sociedad.

Diseño de investigación

Fue no experimental transversal descriptivo correlacional, según Hernández et al. (2018) explican que el diseño no experimental se distingue por no intervenir deliberadamente en las variables; en este enfoque, se observan los eventos de la realidad sin provocar cambios o alteraciones en ellos.

Otzen y Manterola (2017) definen la investigación no experimental como centrada en la evaluación y descripción de fenómenos cuantitativos, evitando métodos invasivos que puedan afectar el comportamiento natural de las personas. Este enfoque metodológico tiene como objetivo comprender los fenómenos observados sin ejercer una influencia directa sobre ellos.

3.2 Variables y operacionalización

Hernández y Mendoza (2018) sostienen lo esencial de realizar la medición, observación e inferencia de las variables de acuerdo con un análisis teórico, ya que mediante estas variables se recopilan datos que reflejan la realidad que se está investigando.

Se contaron con las variables siguientes:

Variable independiente 1: Norma ISO 27001

Variable independiente 2: Norma ISO 31000

Variable dependiente: Gestión de Riesgos

En Anexo 01 encontramos la matriz operacionalización de variables, donde está lo correspondiente a dimensiones, indicadores y variables que se utilizó para esta investigación.

Arias (2022), afirma que el propósito fundamental de esta investigación científica es elaborar una guía destinada a docentes, académicos, estudiantes y doctorandos interesados en la exploración del enfoque cuantitativo. Este manual pretende ofrecer dirección en la gestión y desarrollo de variables.

3.3 Población, muestra, muestreo y unidad de análisis

Población

Según Robles (2019), comunica que el grupo poblacional muestra el conjunto completo de componentes que comparten una característica común y que serán objeto de análisis e investigación. Este término alude al conjunto global de elementos sobre los cuales se lleva a cabo un estudio o investigación particular.

Argerich y Cruz (2017) delimitan los grupos de investigación como un conjunto de elementos u objetos que se estudian para obtener conclusiones generales. Esta población se caracteriza por su homogeneidad, lo que implica que sus miembros comparten características similares. Además, se consideran

aspectos temporales, espaciales, ubicación geográfica y tamaño de población como factores relevantes en el estudio.

Criterios de cálculo de la población:

(a) Inclusión
    1. Se están considerando aquellos activos que forman parte del proceso del alcance del SGSI

(b) Exclusión
    1. No se están considerando aquellos activos de información que no son transversales a la organización o no forman parte del proceso del SGSI.

El resultado del cálculo es el siguiente:

N=162 activos de información

Muestra

Para Carballo y Guelmés (2016) los sujetos seleccionados mediante métodos de muestreo para los cuales se recopilaron datos se denominan muestras. A menudo no es posible lograr la medición utilizando toda la población. Para toda la población, el subconjunto se representa como un conjunto confiable. Cualquier método de muestreo cuantitativo debe ser representativo de la población total.

La ecuación es la siguiente:

$$n = \frac{N Z^2 S^2}{(N-1) e^2 + Z^2 S^2}$$

Donde:
n: tamaño muestral
N: tamaño poblacional (162)
S: desviación estándar

e: error o precisión (5%)
Z: nivel de confianza (95%)

El cálculo es el siguiente:

n=115 activos de información.

Muestreo

Se utilizó la evaluación probabilística aleatoria simple, según Gaviria y Márquez (2019) indican que este tipo de muestreo se utiliza con frecuencia debido a que representa una técnica más confiable y representativa del grupo.

Unidad de análisis

Activos de información.

3.4 Técnicas e instrumentos de recolección de datos

Se aplicó el análisis documental permitiendo recopilar y ordenar las fuentes de los activos de información.

El instrumento es: Ficha de Datos, se encuentra la estructura de datos en el anexo 2.

3.5 Procedimientos

Se realizó los siguientes pasos.

- Coordinación con las partes interesadas del proyecto que pertenecen al proceso de estudio.
- Se solicitó la entrega de indicadores.
- Se validó la información de indicadores.
- Se tabuló la información de indicadores.
- Se procesaron los datos e información

3.6 Método de análisis de datos

Se empleo el análisis estadístico descriptivo en las gráficas de las tablas, validación y contrastación de hipótesis, en cuanto a la inferencia estadística, se aplicará la técnica de coeficiente alfa de Cronbach en la confiabilidad de los datos; cuyos resultados se encuentran en la tabla siguiente:

Las pruebas de confiabilidad se describen en el Anexo 5.

Pruebas de Normalidad

Según Flores y Flores (2021) en una evaluación se busca identificar la normalidad o anormalidad de la distribución de datos, utilizando pruebas como Anderson-Darling, Shapiro-Wilk y Kolmogórov-Smirnov, se busca determinar si la muestra extraída proviene de un grupo poblacional que sigue una normal distribución. Por otro lado, las pruebas no paramétricas se centran en analizar datos el cual no exhiben una normal distribución, caracterizándose por tener un valor de p inferior a 0.05, según las pruebas paramétricas se apoyan en la normalidad de la distribución para analizar los elementos de una muestra, con un valor de p superior a 0. 05.

Para la normalidad en casos de muestras superiores a 50, se emplea el método de Kolmogorov-Smirnov, según Flores et al. (2019), indican que, durante la prueba de datos, se lleva a cabo una verificación preliminar de la distribución normal utilizando pruebas estadísticas como las de Kolmogorov-Smirnov, las cuales proporcionan evidencia significativa sobre su importancia estadística.

Las pruebas de normalidad se describen en el Anexo 6.

3.7 Aspectos éticos

La honestidad, la privacidad y la protección de la confidencialidad se aplicaron. Conforme a APA en su edición séptima, la redacción de la investigación revela una autonomía inherente y respeta en la citación a los autores y referencias en trabajos de investigación, artículos y revistas. El contenido total del estudio es genuino y original, y los textos han sido parafraseados.

Igualmente, se incluirá una prueba a través de Turnitin para asegurar su integridad de que la información se entregue con la aprobación de la entidad educativa correspondiente

Según Luna et al. (2010) identifican que los atributos más destacados se encuentran: la honestidad y responsabilidad, ocupando los dos primeros lugares, seguidos por preparación, formación y conocimiento, se considera la ética individual y principios profesionales. Estos aspectos fueron señalados como particularmente apreciados en la investigación.

Todos los datos recopilados han sido autorizados por la entidad que se aplica en la investigación.

IV. RESULTADOS

Análisis descriptivo

Según Guevara, et al. (2020), sostienen que simplemente mostrar las características del fenómeno recolectadas mediante los métodos de recopilación de datos no es suficiente. Además, se requiere que estas características sean estructuradas y analizadas en el contexto de un marco teórico adecuado, que sirva como fundamento para la investigación.

Tabla 1

Cuadro de estadística descriptiva de la variable independiente: Norma ISO 27001

	Descriptivos		**Estadístico**	**Error estándar**
ISO 27001	Media		45.8609	0.28432
	95% de intervalo de confianza para la media	Límite inferior	45.2976	
		Límite superior	46.4241	
	Media recortada al 5%		45.9010	
	Mediana		45.0000	
	Varianza		9.296	
	Desviación estándar		3.04898	
	Mínimo		42.00	
	Máximo		49.00	
	Rango		7.00	
	Rango intercuartil		6.00	
	Asimetría		-0.21	0.226
	Curtosis		-1.888	0.447

La explicación de los resultados de la tabla 1, fueron:

1) Media (Promedio): La media es 45.8609, lo cual señala el valor característico de la variable. En este contexto, refleja un nivel moderado

de la variable.

2) Error Estándar: El error estándar es de 0.28432. Este resultado refleja la variabilidad esperada en la media de las muestras. A menor error estándar, mayor precisión, lo que implica una evaluación más exacta de la media. En este contexto, un error típico relativamente bajo sugiere una estimación precisa de la media poblacional.
3) Intervalo de confianza al 95% ofrece un rango en el cual es probable que resida la media real del grupo poblacional. En esta situación, el intervalo abarca desde 45.2976 hasta 46.4241.
4) Media Recortada al 5%: La media recortada al 5% (45.9010) se determina al excluir el 5% de los valores extremos. Este procedimiento resulta beneficioso para mitigar el efecto de valores atípicos en la estimación de la media.
5) Mediana: La mediana es 45.0000, y se asemeja a la media. Esto sugiere que la disposición de los datos no presenta un sesgo significativo.
6) La variabilidad se registra en 9.296, y desviación estándar es de 3.04898. Ambas medidas proporcionan información acerca de la dispersión de los datos con respecto a la media. En este contexto, la desviación estándar señala que existe una dispersión moderada alrededor de la media.
7) El valor más bajo es 42.00 y el más alto es 49.00. Esto brinda detalles sobre el rango completo de la variable, que equivale a 7.00.
8) El rango representa la disparidad entre el valor máximo y mínimo (10.00 - 5.00 = 5.00), evidenciando la amplitud completa de los datos.
9) Rango intercuartil (IQR): Consiste en la discrepancia entre el primer cuartil (Q1) y tercer cuartil (Q3). En esta situación, este valor es 6.00, señalando la dispersión central de los datos y excluyendo los valores extremos.
10) Asimetría: La medida de asimetría es -0.21, indicando una leve asimetría positiva. Esto implica que los datos presentan una inclinación leve hacia la derecha, aunque no de manera notable.
11) La medida de curtosis es -1.888, señalando una leve curva en la distribución. La curtosis negativa sugiere colas menos pronunciadas y una distribución más aplanada en comparación con una distribución normal.

Tabla 2

Cuadro de estadística descriptiva de la variable independiente: Norma ISO 31000

	Descriptivos		Estadístico	Error estándar
ISO 31000	Media		32.2174	0.15267
	95% de intervalo de confianza para la media	Límite inferior	31.9150	
		Límite superior	32.5198	
	Media recortada al 5%		32.1860	
	Mediana		32.0000	
	Varianza		2.680	
	Desviación estándar		1.63719	
	Mínimo		30.00	
	Máximo		35.00	
	Rango		5.00	
	Rango intercuartil		3.00	
	Asimetría		0.424	0.226
	Curtosis		-1.296	0.447

La explicación de los resultados de la tabla 2, fueron:

1) Media (Promedio): La media es 32.2174, señalando el valor característico de la variable. En este contexto, refleja un nivel moderado de la variable
2) Error Estándar: El error estándar es de 0.15267. Este resultado refleja la variabilidad anticipada en la media de las muestras. A medida que disminuye, la estimación de la media se vuelve más precisa. En este escenario, un error estándar relativamente bajo indica una estimación precisa de la media poblacional.
3) Intervalo de Confianza al 95%: El intervalo de confianza ofrece un rango en el cual es probable que resida la media real de la población. En esta

situación, el intervalo abarca desde 31.9150 hasta 32.5198.

4) Media Recortada al 5%: La media recortada al 5% (32.1860) se obtiene excluyendo el 5% de los valores extremos. Este procedimiento resulta beneficioso para mitigar el efecto de valores atípicos en la estimación de la media.
5) Mediana: La mediana es 32.0000, y se asemeja a la media. Esto sugiere que la distribución de los datos no presenta un sesgo significativo.
6) La varianza es 2.680 y la desviación estándar es 1.63719. Ambas métricas ofrecen detalles sobre la dispersión de los datos respecto a la media. En este escenario, la desviación estándar indica una dispersión moderada alrededor de la media.
7) El valor más bajo es 30.00 y el más alto es 35.00. Esto ofrece detalles sobre el rango completo de la variable, que equivale a 5.00.
8) Rango: El rango representa la discrepancia entre el valor máximo y mínimo (10.00 - 5.00 = 5.00), evidenciando la amplitud completa de los datos.
9) Rango intercuartil (IQR): Consiste en la discrepancia entre el tercer cuartil (Q3) y el primer cuartil (Q1). En esta situación, este valor es 3.00, señalando la dispersión central de los datos y excluyendo los valores extremos.
10) Asimetría: La medida de asimetría es 0.424, indicando una leve asimetría positiva. Esto implica que los datos presentan una inclinación leve hacia la derecha, aunque no de manera notable.
11) Curtosis: La medida de curtosis es -1.296, señalando una leve curva en la distribución. La curtosis negativa sugiere colas menos pronunciadas y una distribución más aplanada en comparación con una distribución normal.

Tabla 3

Cuadro de estadística descriptiva de la variable dependiente: Gestión de Riesgos

	Descriptivos		Estadístico	Error estándar
Gestión de Riesgos	Media		7.0957	0.10032
	95% de intervalo de confianza para la media	Límite inferior	6.8969	
		Límite superior	7.2944	
	Media recortada al 5%		7.0507	
	Mediana		8.0000	
	Varianza		1.157	
	Desviación estándar		1.07584	
	Mínimo		6.00	
	Máximo		9.00	
	Rango		3.00	
	Rango intercuartil		2.00	
	Asimetría		0.065	0.226
	Curtosis		-1.740	.447

La explicación de los resultados de la tabla 3, fueron:

1) Media (Promedio): La media es 7.0957, lo que indica el valor típico de la variable. En este caso, representa un nivel moderado de la variable.
2) Error Estándar: El error estándar es 0.10032. Este valor indica la variabilidad esperada en la media de las muestras. Cuanto menor sea el estándar error, será la estimación de la media más precisa. En este caso, un error estándar relativamente bajo sugiere una estimación precisa de la poblacional media.
3) El intervalo de confianza al 95% ofrece un rango donde es probable que se ubique la media real de la población. En este escenario, el intervalo abarca desde 6.8969 hasta 7.2944.
4) Media Recortada al 5%: La media recortada al 5% (7.0507) se calcula

eliminando el 5% de los valores extremos. Esto es útil para reducir el impacto de valores atípicos en la estimación de la media.

5) Mediana: La mediana es 8.0000, que es similar a la media. Indica que la distribución de los datos no está sesgada de manera significativa.
6) La varianza es 1.157 y la desviación estándar es 1.07584. Ambas medidas proporcionan información sobre la dispersión de los datos alrededor de la media. En esta situación, la desviación típica muestra que hay una moderada dispersión alrededor de la media.
7) Mínimo y Máximo: El valor mínimo es 6.00 y el máximo es 9.00. Esto proporciona información sobre el rango total de la variable, que es 3.00.
8) El rango representa la diferencia entre el valor máximo y mínimo (9.00 - 6.00 = 3.00), indicando la amplitud total de los datos.
9) Rango intercuartil (IQR): Consiste en la discrepancia entre el tercer cuartil (Q3) y el primer cuartil (Q1). En esta situación, este valor es 2.00, señalando la dispersión central de los datos y excluyendo los valores extremos.
10) Asimetría: La asimetría es 0.065, lo que indica ligera asimetría positiva. Los datos están ligeramente sesgados hacia la derecha, pero no de manera significativa.
11) Curtosis: La curtosis es -1.740, lo que indica una ligera curva en la distribución. La curtosis negativa sugiere colas más ligeras y una distribución más aplanada en comparación con una distribución normal.

Análisis Inferencial de Resultados de Correlación

Según Martínez et al. (2020), mencionan que tanto los métodos de correlación de Pearson como Spearman son enfoques bivariados que se utilizan en situaciones multivariadas para analizar diversas variables de forma no paramétrica, especialmente cuando no se cumple el criterio de normalidad en las variables.

Tabla 4

Cuadro de formulación del objetivo e hipótesis general y criterios de evaluación de la prueba de correlación

Objetivo general	
Determinar la relación de la norma ISO 27001 y la norma ISO 31000 en la gestión de riesgos de los activos de información de una empresa de telecomunicaciones, Lima 2023	
Hipótesis general	
Existe una relación significativa de la norma ISO 27001 y la norma ISO 31000 en la gestión de riesgos de los activos de información de una empresa de telecomunicaciones, Lima 2023.	
Formulación de hipótesis	
Hipótesis nula:	Ho: No existe una relación significativa de la norma ISO 27001 y la norma ISO 31000 en la gestión de riesgos de los activos de información de una empresa de telecomunicaciones, Lima 2023.
Hipótesis alternativa:	Ha: Existe una relación significativa de la norma ISO 27001 y la norma ISO 31000 en la gestión de riesgos de los activos de información de una empresa de telecomunicaciones, Lima 2023.

Nivel de significancia: NC	0.95
Error: α	0.05
Prueba de correlación	Distribución normal: Prueba paramétrica Pearson
	Distribución no normal: Prueba no paramétrica Rho de Spearman
Criterio de decisión	p-valor < 0.05 Rechazar Ho Aceptar Ha
	p-valor >= 0.05 Aceptar Ho Rechazar Ha
Interpretación de coeficiente de correlación	-1.0 entre -0.8: Inversa: Correlación negativa muy fuerte -0.79 entre -0.6: Inversa: Correlación negativa fuerte -0.59 entre -0.4: Inversa: Correlación negativa moderada -0.39 entre -0.2: Inversa: Correlación negativa débil -0.19 entre -0.01 Inversa: Correlación negativa muy débil 0: Correlación neutra 0.01 entre 0.19: Directa: Correlación positiva muy débil 0.2 entre 0.39: Directa: Correlación positiva débil 0.4 entre 0.59: Directa: Correlación positiva moderada 0.6 entre 0.79: Directa: Correlación positiva fuerte 0.8 entre 1.0: Directa: Correlación positiva muy fuerte

Se observaron los hallazgos en la asociación entre: Norma ISO 27001 y Norma ISO 31000 con la Gestión de Riesgos en la tabla 5:

Tabla 5

Resultados de la correlación

Correlaciones			ISO27001	ISO31000
Rho Spearman	Gestión de Riesgos	Coeficiente de correlación	0.325	0.352
		Sig. (bilateral)	0.001	0.001
		N	115	115

Interpretación de resultados:

Respecto a la variable independiente ISO-27001 con la variable dependiente gestión de riesgos son las siguientes:

1. El índice de correlación de Spearman entre la ISO 27001 y Gestión de Riesgos es 0.325. Este valor indica la fuerza y orientación de la asociación entre las dos variables.
2. Significancia Estadística: Muestra significancia la correlación a un nivel de confianza del 0.001 (bilateral).
3. El p-valor es menor a 0.05, y de acuerdo con la Tabla 8, se descarta la hipótesis nula a beneficio de la hipótesis alternativa, indicando existencia de correlación entre la norma ISO 27001 y la gestión de riesgos en una empresa del sector de telecomunicaciones en Lima en 2023.
4. La correlación de 0.325 sugiere una conexión positiva leve entre la ISO 27001 en la muestra estudiada. La relevancia estadística respalda la asociación entre las variables. Por lo tanto, se observa una asociación significativa y positiva entre ISO 27001 y la administración de riesgos en la muestra examinada.

Respecto a la variable independiente ISO 31000 con la variable dependiente gestión de riesgos fueron:

1. Índice de correlación de Spearman (Rho) entre la ISO 31000 y la Gestión de Riesgos es de 0.352. Este indicador refleja la intensidad y orientación de la conexión entre las variables.

2. Significancia Estadística: La correlación es estadísticamente significativa con un nivel significativo del 0.001 (bilateral).
3. El p-valor es inferior a 0.05, según la Tabla 8, lo cual conduce a descartar la hipótesis nula a beneficio de la hipótesis alternativa, señalando una relación significativa entre la norma 31000 y la gestión de riesgo en una empresa del sector de telecomunicaciones en Lima en 2023.
4. La correlación de 0.352 sugiere una relación positiva débil entre la ISO 31000 en la muestra analizada. La significancia estadística respalda la relación entre las variables. Por lo tanto, hay una asociación significativa y positiva entre ISO 31000 y la gestión de riesgos en la muestra examinada.

Tabla 6

Cuadro de formulación del objetivo e hipótesis específicos 1 y criterios de evaluación de la prueba de correlación

Objetivo específico 1	
Determinar la relación de la norma ISO 27001 y la norma ISO 31000 en el nivel de activos para la gestión de riesgos de los activos de información de una empresa del sector de telecomunicaciones, Lima 2023	
Hipótesis específica 1	
Existe una relación significativa de la norma ISO 27001 y la norma ISO 31000 en el nivel de activos para la gestión de riesgos de los activos de información de una empresa de telecomunicaciones, Lima 2023.	
Formulación de hipótesis estadística	
Hipótesis nula:	Ho: No existe una relación significativa de la norma ISO 27001 y la norma ISO 31000 en el nivel de activos para la gestión del riesgo de una empresa de telecomunicaciones, Lima 2023.
Hipótesis alternativa:	Ha: Existe una relación significativa de

	la norma ISO 27001 y la norma ISO 31000 en el nivel de activos para la gestión del riesgo de una empresa de telecomunicaciones, Lima 2023.
Nivel de significancia: NC	0.95
Error: α	0.05
Prueba de correlación	Distribución normal: Prueba paramétrica Pearson
	Distribución no normal: Prueba no paramétrica Rho de Spearman
Criterio de decisión	p-valor < 0.05 Rechazar Ho Aceptar Ha
	p-valor >= 0.05 Aceptar Ho Rechazar Ha
Interpretación de coeficiente de correlación	-1.0 entre -0.8: Inversa: Correlación negativa muy fuerte -0.79 entre -0.6: Inversa: Correlación negativa fuerte -0.59 entre -0.4: Inversa: Correlación negativa moderada -0.39 entre -0.2: Inversa: Correlación negativa débil -0.19 entre -0.01 Inversa: Correlación negativa muy débil 0: Correlación neutra 0.01 entre 0.19: Directa: Correlación positiva muy débil 0.2 entre 0.39: Directa: Correlación positiva débil 0.4 entre 0.59: Directa: Correlación positiva moderada 0.6 entre 0.79: Directa: Correlación positiva fuerte 0.8 entre 1.0: Directa: Correlación positiva muy fuerte

Se observaron los hallazgos en la tabla 7 de la correlación de la norma ISO 27001 y la norma ISO 31000 con dimensión valor del activo de la variable gestión de riesgos dependiente:

Tabla 7

Resultados de la correlación

Correlaciones			**ISO27001**	**ISO31000**
Rho Spearman	Evaluación del Activo	Coeficiente de correlación	0.340	0.376
		Sig. (bilateral)	0.001	0.001
		N	115	115
** Es significativa en el nivel 0,01 (bilateral).				

Interpretación de resultados:

Los resultados entre la variable ISO 27001 independiente y la dimensión evaluación del Activo de la variable gestión de riesgos dependiente fueron:

1. El índice de correlación de Spearman entre ISO 27001 es de 0.340. Este valor representa la fuerza y orientación de la asociación entre la norma ISO 27001 y la evaluación de la dimensión del activo.
2. Significancia Estadística: La correlación es significativa a un nivel de significancia del **0.001** (bilateral).
3. El p-valor es inferior a 0.05, y según la Tabla 10, se descarta la hipótesis nula a beneficio de la hipótesis alternativa, indicando una correlación existente de la normatividad ISO 27001 en los activos para la gestión de riesgos en una empresa del sector de telecomunicaciones en Lima en 2023.
4. La correlación de 0.340 sugiere una asociación positiva débil entre la ISO 27001 en la muestra analizada. La significancia estadística respalda que las variables están relacionadas. Por lo tanto, existe una asociación significativa y positiva entre ISO 27001 y la dimensión evaluación del activo en la Gestión de Riesgos en la muestra analizada.

La explicación de resultados respecto a la variable independiente ISO 31000 con la dimensión evaluación de activo de la variable dependiente Gestión de

Riesgos:

1. índice de correlación de spearman (Rho) entre la ISO 31000 es de 0.376. Este coeficiente indica la fuerza y orientación de la relación entre la variable independiente ISO 31000 y la dimensión de evaluación del activo.
2. Significancia Estadística: La correlación es significativa a un nivel de significancia del **0.001** (bilateral).
3. El p-valor es inferior a 0.05, según la Tabla 10, lo que descarta la hipótesis nula a beneficio de la hipótesis alternativa, de que existe correlación de la norma ISO 31000 en los activos para la gestión de riesgo de una empresa del sector de telecomunicaciones, Lima 2023.
4. La correlación de 0.376 sugiere una relación positiva débil entre la ISO 31000 en la muestra analizada. La significancia estadística respalda que las variables están relacionadas. Por lo tanto, existe una asociación significativa y positiva entre ISO 31000 y la dimensión evaluación del activo de la Gestión de Riesgos en la muestra analizada.

Tabla 8

Cuadro de formulación del objetivo e hipótesis específica 2 y criterios de evaluación de la prueba de correlación

Objetivo específico 2
Determinar la relación de la norma ISO 27001 y la norma ISO 31000 en el nivel de riesgos para la gestión de riesgos de los activos de información de una empresa de telecomunicaciones, Lima 2023.
Hipótesis especifica 2
Existe una relación significativa de la norma ISO 27001 y la norma ISO 31000 impacta en el nivel de riesgos para la gestión del riesgo de los activos de información de una empresa de telecomunicaciones, Lima 2023.
Formulación de hipótesis estadística

Hipótesis nula:	Ho: No existe una relación significativa de la norma ISO 27001 y la norma ISO 31000 impacta en el nivel de riesgos para la gestión del riesgo de los activos de información de una empresa de telecomunicaciones, Lima 2023.
Hipótesis alternativa:	Ha: Existe una relación significativa de la norma ISO 27001 y la norma ISO 31000 impacta en el nivel de riesgos para la gestión del riesgo de los activos de información de una empresa de telecomunicaciones, Lima 2023.
Nivel de significancia: NC	0.95
Error: α	0.05
Prueba de correlación	Distribución normal: Prueba paramétrica Pearson
	Distribución no normal: Prueba no paramétrica Rho de Spearman
Criterio de decisión	p-valor < 0.05 Rechazar Ho Aceptar Ha
	p-valor >= 0.05 Aceptar Ho Rechazar Ha
Interpretación de coeficiente de correlación	-1.0 entre -0.8: Inversa: Correlación negativa muy fuerte -0.79 entre -0.6: Inversa: Correlación negativa fuerte -0.59 entre -0.4: Inversa: Correlación negativa moderada -0.39 entre -0.2: Inversa: Correlación negativa débil -0.19 entre -0.01 Inversa: Correlación negativa muy débil 0: Correlación neutra 0.01 entre 0.19: Directa: Correlación positiva muy débil

	0.2 entre 0.39: Directa: Correlación positiva débil 0.4 entre 0.59: Directa: Correlación positiva moderada 0.6 entre 0.79: Directa: Correlación positiva fuerte 0.8 entre 1.0: Directa: Correlación positiva muy fuerte

Se visualiza los hallazgos de la correlación en la tabla 9:

Tabla 9

Resultados de la correlación

Correlaciones			**ISO27001**	**ISO31000**
Rho Spearman	Análisis de Riesgos	Coeficiente de correlación	0.294	0.309
		Sig. (bilateral)	0.001	0.001
		N	115	115
**. La correlación es significativa en el nivel 0,01 (bilateral).				

Interpretación de resultados:

Los hallazgos con respecto a la Norma ISO 27001 variable independiente con la dimensión análisis de Riesgos de la variable Gestión de Riesgos dependiente fueron:

1. Coeficiente de Correlación de Spearman (Rho) entre la ISO 27001 es de 0.294. Este coeficiente proporciona información sobre la intensidad y dirección de la relación entre las variables norma ISO 27001 y la dimensión análisis de riesgos de variable gestión de Riesgos.
2. Significancia Estadística: La correlación es significativa a un nivel de significancia del **0.001** (bilateral).
3. El p-valor es inferior a 0.05, y según la Tabla 12, se descarta la hipótesis nula en favor de la hipótesis alternativa, sugiriendo que existe una relación entre la norma ISO 27001 y el nivel de riesgos para la gestión de riesgos en una empresa del sector de telecomunicaciones en Lima en 2023.
4. La correlación de 0.294 indica una relación positiva muy débil entre ISO

27001 en la muestra analizada. La significancia estadística respalda la relación entre las variables. Por lo tanto, se observa una asociación significativa y positiva entre ISO 27001 y la dimensión de análisis de riesgos de la variable Gestión de Riesgos en la muestra examinada.

La interpretación con respecto a la variable independiente Norma ISO 31000 con la dimensión análisis de Riesgos de la variable dependiente Gestión de Riesgos fueron:

1. Coeficiente de Correlación de Spearman (Rho) entre la ISO 31000 es de 0.309. Este coeficiente sugiere la fuerza y dirección de la relación entre la variable ISO 31000 con la dimensión análisis de riesgos de la variable gestión de riesgos.
2. Significancia Estadística: La correlación es significativa a un nivel de significancia del 0.001 (bilateral).
3. El p-valor es menor a 0.05, y conforme la Tabla 12, se descarta la hipótesis nula a beneficio de la hipótesis alternativa, de que existe correlación de la norma ISO 27001 impacta en el nivel de riesgos para la gestión de riesgo de una empresa del sector de telecomunicaciones, Lima 2023.
4. La correlación de 0.309 sugiere una relación positiva débil entre la ISO 31000 en la muestra analizada. La significancia estadística respalda que las variables están relacionadas. Por lo tanto, existe una asociación significativa y positiva entre ISO 31000 y la dimensión análisis de riesgos de la variable de Gestión de Riesgos en la muestra analizada.

Análisis de Resultados de Regresión lineal

Tabla 10

Regresión lineal: ANOVA

ANOVA[a]						
Modelo		**Suma de cuadrados**	**gl**	**Media cuadrática**	**F**	**Sig.**
1	Regresión	17.070	2	8.535	8.321	<.001[b]
	Residuo	114.878	112	1.026		
	Total	131.948	114			

a. Var. dependiente: Gestión de Riesgos

b. Predictores: Norma ISO 27001 y Norma ISO 31000

La interpretación de los hallazgos de la tabla 10, fue el siguiente:

1) **ANOVA General:**
   a) El ANOVA general evalúa si el modelo en su conjunto es estadísticamente significativo en la predicción de la variable dependiente Gestión de Riesgos.

2) **Componentes de la Suma de Cuadrados:**
   a) Regresión: La suma de cuadrados para la regresión es 17.070. Indica la variabilidad explicada por el modelo.
   b) Residuo: La suma de cuadrados para el residuo es 114.878. Indica la variabilidad no explicada por el modelo.
   c) Total: La suma de cuadrados total es 131.948, que es la suma de la regresión y el residuo.

3) **Grados de Libertad (gl):**
   a) Para la regresión, hay 2 grados de libertad (uno para cada predictor).
   b) Para el residuo, hay 112 grados de libertad.
   c) En total, hay 114 grados de libertad.

4) **Media Cuadrática (Mean Square):**

a) Para la regresión, la media cuadrática es 8.535 (suma de cuadrados dividida por grados de libertad).
b) Para el residuo, la media cuadrática es 1.026.

5) Estadística F y Significancia:

a) La estadística F es 8.321.
b) La significancia (p-valor) es <.001(menos de 0.05).

6) Conclusiones:

a) La estadística F significativa (p-valor < 0.05) indica que el modelo en su conjunto es estadísticamente significativo en la predicción de la Gestión de Riesgos.
b) La regresión explica significativamente más variabilidad de la que se esperaría por azar.

7) Consecuentemente, el ANOVA indica que el modelo, que incluye las variables predictoras mencionadas, es estadísticamente significativo para predecir la variable dependiente Gestión de Riesgos. La regresión es significativamente mejor que un modelo nulo, lo que sugiere que al menos una de las variables predictoras tiene un efecto significativo en la variable dependiente.

Tabla 11

Regresión lineal: Modelo

Resumen del modelo[b]				
Modelo	**R**	**R cuadrado**	**R cuadrado ajustado**	**Error estándar de la estimación**
1	0.360[a]	0.129	0.114	1.01277

a. Predictores: (Constante), Norma ISO 27001 y Norma ISO 31000

b. Variable dependiente: Gestión de Riesgos

La interpretación de los hallazgos de la tabla 11, fue el siguiente:

1) **Modelo y Variables:**
   a) Se ha ajustado un modelo con la gestión de riesgos como variable dependiente y varias variables predictoras: Norma ISO 27001 y Norma ISO 31000
2) **Estadísticas del Modelo:**
   a) R: El coeficiente de correlación múltiple (R) es 0.360. Indica la fuerza y dirección de la relación global entre las variables predictoras y la variable dependiente.
   b) R cuadrado (R^2): Es 0.129, lo que significa que aproximadamente el 12.9% de la variabilidad en la variable dependiente puede explicarse por las variables predictoras en el modelo.
   c) R cuadrado ajustado: Es 0.114, ajusta el R cuadrado por el número de predictores en el modelo y proporciona una medida más precisa del ajuste.
3) **Evaluación de la Calidad del Ajuste:**
   a) Un R cuadrado alto (en este caso, 0.129) indica que el modelo tiene una buena capacidad para explicar la variabilidad en la variable dependiente
   b) El Error estándar de la estimación (1.01277) proporciona una medida de la dispersión de los residuos del modelo.
4) **Significancia del Modelo:**
   a) La letra "a" junto a las estadísticas indica que la significancia del modelo se ha evaluado, y se ha encontrado que el modelo en su conjunto es estadísticamente significativo.
5) **Variables Predictoras:**
   a) Las variables predictoras incluidas en el modelo son: Norma ISO 27001 y Norma ISO 31000.
6) Consecuentemente, el modelo tiene un buen ajuste, explicando alrededor del 12.9% de la variabilidad en la gestión de riesgos. Las variables predictoras incluidas en el modelo son todas estadísticamente significativas.

V. DISCUSIÓN

Se detalló determinar el objetivo de la relación de las normas ISO 27001 e ISO 31000 en la gestión de riesgos de los activos de información de una empresa del sector de telecomunicaciones. Por lo cual se dará exposición a diversas investigaciones a nivel internacional y nacional.

Al examinar los hallazgos, se notó que el índice de correlación de Spearman de la variable independiente ISO 27001 y variable gestión de riesgos dependiente es 0.325. Este coeficiente señala la dirección y fuerza de la asociación entre ambas variables. Además, es significativa la correlación estadísticamente a un alcance de significancia del 0.001.

Internacionalmente, el resultado encontrado se encuentra alineado con lo señalado por Valencia y Orozco (2017) mostrando la relevancia de la administración de riesgos al desarrollar un sistema de administración de resguardo de información fundamentado en la normatividad ISO-27001 y la familia 27000, considerando entre una de sus principales fases para el desarrollo del sistema de administración de resguardo de la información es identificar los activos de información, realizar la valoración de riesgos, establecimiento del contexto, y planificar el tratamiento de riesgos. Fases que pertenecen a la ISO 27001 en el acápite generalidades, estimación de riesgo de seguridad de información y manejo de riesgos. Concluyen que utilizar las normas ISO-27000 entre ellas la norma 27001 y la 27005, contribuyen a la administración de riesgos facilitando la iniciación de proyectos de este tipo y respondiendo así a una necesidad percibida en la comunidad profesional de desarrollar metodologías alineadas con los estándares internacionales.

Sin embargo, a diferencia de lo mencionado por Valencia y Orozco se tomó también en contemplar la norma ISO 31000 indicando las bases a cumplirse para hacer eficaz la gestión del riesgo y nos permite estar en sintonía con el logro de los metas de la empresa.

Asimismo, sería interesante poder incluir lineamientos de la norma ISO-27005 de administración de riesgos incluida en la investigación de Valencia y Orozco, para poder enriquecer y minimizar la seguridad respecto a los riesgos, ya que la ISO 27005 nos da los lineamientos sobre la aplicación de un enfoque de administración de riesgos orientado a procesos.

Lo encontrado coincide con Kitsios et al., (2023) donde indica que lo primero al gestionar la norma ISO 27001 en la organización, es efectuar una estrategia de resguardo de la información según la normatividad ISO-27001, abordando mejor a amenazas de la seguridad y riesgos, considerando la información como uno de los recursos más preciados de la organización. También indica que los riesgos son únicos para cada empresa, pero el objetivo final es el mismo: salvaguardar los datos y encontrar la mejor solución posible que cumpla con todos los requisitos del negocio. Además, dice que realizar una estimación de riesgos es crucial y consume más tiempo en desarrollo de estrategias de seguridad de información para una empresa. También se reconoce que el flujo del examen de riesgos no es estático y será necesario realizarlo varias veces.

A diferencia de lo mencionado por Kitsios et al., (2023), se tomó en análisis los resultados de los indicadores basados en la metodología de riesgos implementada en la empresa del sector de telecomunicaciones.

También, podría ser interesante poder incluir una periodicidad para la revisión de metodología de administración de riesgos, para poder actualizar e implementar mejoras en la gestión de riesgos.

Kamil et al. (2023) mencionan la legitimidad de los resultados de ISO/IEC 27001 desde la perspectiva de las expectativas de las partes interesadas, donde para cumplir esto, se llevó el estudio basado en entrevistas, en el que participaron partes interesadas relevantes involucradas en la administración de la seguridad dentro de organizaciones privadas en Suecia. Los hallazgos revelan ocho objetivos clave de seguridad de la información. Donde el objetivo número 2 y 7 es alcanzar un nivel de seguridad aceptable, donde enfatizan en alcanzar un nivel aceptable de seguridad que estuviera alineado con los riesgos comerciales. Donde todas las

partes interesadas reconocieron la reconocieron unánimemente la importancia de identificar, gestionar y monitorear continuamente las amenazas, riesgos e inseguridades. Además, se enfatizó que las organizaciones tenían la responsabilidad, como se describe en ISO/IEC 27001, de abordar proactivamente los riesgos Los hallazgos sugieren que el nivel de legitimidad del estándar varía según estos objetivos, desde alto a medio y bajo. Los hallazgos del estudio indican que la legitimidad de los resultados de ISO/IEC 27001 varía dependiendo de los objetivos específicos que las partes interesadas pretenden alcanzar. El estudio demuestra un alto nivel de legitimidad de resultados en relación con la implementación, establecimiento, operación y monitoreo del SGSI donde incluye la administración de riesgos. Está alineada a los hallazgos del estudio cuando señala que la normatividad ISO-27001 tiene una relación significativa con la gestión de riesgos.

Con respecto a lo indicado en el estudio anterior podemos indicar que no están considerando otras normas como la ISO-31000 de administración de riesgos, pero que la norma ISO 27001 la cita en una de sus cláusulas.

Asimismo, podemos indicar que podemos recalcar la relevancia de participación de las partes involucradas en los resultados de la implementación del SGSI.

Razikin y Soewito (2022) en su recomendación en el diseño de soporte a decisiones de ciberseguridad, en la construcción de un sistema tecnológico aplicado a seguridad de información apoyado en la interpretación de riesgos y normatividad de ciberseguridad ISO/IEC 27001. Donde los resultados del ensayo de hipótesis al utilizar el chi-cuadrado de Pearson obtuvieron un valor p 000005221 <0,05, entonces la hipótesis nula se descarta. El valor p del chi-cuadrado de Pearson puede ser incorrecto, por lo que se necesita validación utilizando el método de prueba de Fisher; el valor del valor p es 0,00000005658 < 0,05, significando que se descarta la hipótesis nula. Entonces, basado en los dos resultados, valor p < 0,05, se concreta que ocurre una asociación entre los sistemas que implementan y no implementan recomendaciones basadas en ISO/IEC 27001 para la mitigación de ataques de ciberseguridad. Por ello se aprecia la relación que existe con la

presente investigación donde se identifica la conexión que hay con el desarrollo de la normatividad ISO-27001 y la administración de riesgos que ayuda a mitigar los ataques de ciberseguridad entre otros.

Asimismo, cabe indicar que se toma en cuenta la normatividad ISO-31000 en el presente estudio.

Pero hemos de considerar otros métodos de gestión de riesgos como el OCTAVE o elegir uno de acuerdo con las necesidades de la organización.

En el escenario Nacional, se encuentra alineado con el estudio de Rodríguez et al. (2020) donde afirman que existe efecto de la normatividad ISO-27001 en la información respecto a la seguridad y es importante que se establezcan controles para resguardar la información ante cualquier riesgo. Además, la relevancia de su estudio reside en la evaluación de seguridad en áreas donde se gestiona información crucial dentro de las instituciones. Se contempló treinta colaboradores de la organización respecto a la muestra, donde el éxito del estudio radica no solo en la implementación de la norma, también en el involucramiento de los colaboradores y debido a ellos se reduce el impacto de la vulnerabilidad de la empresa. En cuanto a la hipótesis de investigación, se registró un valor de Z= -3,828 (p= .005). Debido a que el valor de p es menor al 5% de significancia, se puede concluir que la aplicación de ISO-27001 incide en la información respecto a la seguridad de una organización privada en el año 2019. Así como para la presente investigación se tomaron como muestra 115 activos de información que fueron identificados por los involucrados y donde se obtuvo una relación significativa 0.325 entre la normatividad ISO-27001 en la administración de riesgos.

Sin embargo, a diferencia de Rodríguez en el desarrollo de la norma ISO-27001 los activos de información forman parte esencial de la administración del SGSI.

Por otro parte, en la presente investigación se podría dar mayor énfasis considerando las incidencias que afectan la integridad, disponibilidad y confidencialidad de seguridad de la información.

Huayllani (2020) tuvo como propósito evaluar el efecto del desarrollo del sistema respecto a la administración de seguridad según la normatividad ISO-27001 en la administración del riesgo. El enfoque fue hipotético-deductiva, con enfoque cuantitativo de aplicación práctica, de longitud temporal y carácter correlacional. El grupo de estudio comprendió a 145 empleados de la unidad de administración de inversiones de reconstrucción con cambios del MINSA. La recolección de datos se ejecutó por medio de dos instrumentos diseñados para medir las variables pertinentes. La evaluación de los resultados se realizó utilizando el índice de correlación de Spearman, permitiendo validar las hipótesis basadas en los datos recopilados. Los hallazgos indicaron una conexión positiva y significativa de las variables de gestión del riesgo y SGSI (0.856). Esto concuerda con los hallazgos de la investigación actual, donde se observa una correlación significativa.

Cabe indicar, que en la investigación presente se incluyó la norma ISO-31000 de administración de riesgos.

Pero, resalta que se deben tener evaluaciones periódicas de cumplimiento de sus aplicaciones de administración de información respecto a la seguridad.

Al conseguir lo encontrado de la investigación presente se observó que el método de Spearman entre la variable ISO 31000 independiente y la variable gestión de riesgos dependiente es 0.386, este coeficiente señala la intensidad y la dirección de la relación de las variables. Asimismo, se tiene asociación significativa del 0.001 (bilateral) a un nivel de significancia de las variables.

Está presente investigación se encuentra alineada con lo indicado de Tobi et al., (2019) que está considerando un enfoque de riesgos de activos críticos considerando la ISO 31000, en base al riesgo potencial se define un proceso como análisis de criticidad a través del cual se puede asignar la calificación de criticidad a los activos; donde la reacción adecuada depende de la actitud de la organización hacia el riesgo respecto a activos y grado de riesgo de activos. Donde el resultado de la criticidad es representado en una curva de desempeño.

No obstante, a diferencia de lo expresado por Tobi et al., (2019), en la investigación presente tomó también en atención la ISO-27001 para la administración de riesgos.

Luego de lo elaborado por Tobi et al., (2019), se podría considerar ampliar la evaluación de criticidad de los recursos de información en la investigación, para considerarlo como un factor adicional en la evaluación de riesgos.

Se encuentra alineado con lo señalado por Huaura (2019) menciona, su objetivo de precisar que la administración de riesgos de información respecto a su seguridad fundamentada según NTP-ISO/IEC-31000 influye en monitorear riesgos en organizaciones del ámbito de las telco, donde consideró para su investigación a los aliados de las organizaciones de telecomunicaciones que tienen más de 5000 colaboradores pertenecientes a la ciudad Lima. Se tomó una población para el estudio de 104 personas pertenecientes al sector de telecomunicaciones. Donde analiza la conexión existente sobre un set de variables en definir si es válida la hipótesis. El análisis manifiesta una moderada correlación positiva de las variables de administración de riesgos y seguridad de la información (0.592). Por ello indica que una administración de riesgos fundamentada en una normatividad NTP-ISO/IEC-31000 en las organizaciones del ámbito de telecomunicaciones incide en el monitoreo de seguridad conforme a los riesgos.

Se resalta lo concluido por Huaura (2019) podemos indicar en la investigación también se tuvo en cuenta la norma ISO-27001 en monitorear riesgos de información de la organización.

Asimismo, resaltamos la participación de la Alta Dirección como papel importante en administración de riesgos, ya que permite gestionar los riesgos y gestionar los cambios en base a las decisiones tomadas, que influye en minimizar riesgos y cumplimiento de los objetivos.

VI. CONCLUSIONES

Primera: Respecto al objetivo general y después de analizar los hallazgos de los indicadores se concluyó una relación significativa entre la ISO-27001 y la ISO-31000 con la gestión de riesgos de los activos de información de una empresa del sector de telecomunicaciones, Lima 2023. Obteniéndose un método de correlación Spearman de 0.325, entre la ISO 27001 con la gestión de riesgos e Índice de correlación de rango de Spearman de 0.352 entre la normatividad ISO-31000 con la gestión de riesgos.

Segunda: En base al objetivo específico 1 y luego de analizar los resultados de los indicadores se concluyó que hay una relación significativa de la ISO-27001 e ISO-31000 en el nivel de activos para la gestión de riesgos de los recursos de información de una organización de telecomunicaciones, Lima 2023. Con correlación de Spearman de 0.340 entre la norma ISO 27001 con la dimensión evaluación de activos e índice de correlación de 0.376 entre la norma ISO 31000 con la dimensión con la dimensión evaluación de activos.

Tercero: Respecto al objetivo específico 2, la evaluación de los indicadores concluyó que hay una relación significativa de la ISO-27001 e ISO-31000 en el nivel de riesgos para la gestión de riesgos de los activos de información de una empresa del sector de telecomunicaciones, Lima 2023. Obteniéndose un índice de correlación de Spearman de 0.294 entre la norma ISO 27001 con la dimensión análisis de riesgos y coeficiente de correlación Spearman de 0.309 entre la norma ISO 31000 con la dimensión análisis de riesgos.

VII. RECOMENDACIONES

Primera: En futuros estudios se recomienda a los investigadores, que profundicen la investigación considerando la norma ISO 27005, CSX Cybersecurity, COBIT, COSO, OCTAVE, MAGERIT, entre otras metodologías para gestión de riesgos.

Segunda: Se sugiere al representante de la seguridad respecto a la información realice el análisis de riesgo de manera periódica o en caso de algún cambio trascendental en la organización, que incluya actualizar los recursos de información, para poder estar protegidos ante las diferentes amenazas.

Tercera: Se recomienda al representante de la seguridad, realizar la gestión de riesgos con respaldo de la Alta dirección e incluir a los principales líderes en el alcance del SGSI, a fin de tomar decisiones oportunas ante cualquier tratamiento de riesgo.

Cuarta: Se aconseja al representante de la seguridad de información planificar auditorías internas en evaluación del cumplimiento y el sostenimiento de la norma ISO 27001.

Quinta: Se recomienda al representante de la seguridad de información elaborar y ejecutar capacitaciones periódicas sobre las últimas actualizaciones de la norma ISO 27001 y la Normatividad ISO 31000 para el personal de la empresa, y puedan estar actualizados en las normativas.

Sexta: Se recomienda al representante de la seguridad de información la evaluación de la adquisición de una herramienta para administrar y centralizar la seguridad respecto a los riesgos de la empresa.

REFERENCIAS

Araujo, T. (2017). Evaluación de Riesgo, Supervisión y Monitoreo en el Logro de Objetivos, en el Fondo de Aseguramiento Saludpol – Perú [tesis de Doctorado]. Universidad César Vallejo. https://repositorio.ucv.edu.pe/handle/20.500.12692/4360

Argerich, J. & Cruz Cázares, C. (2017). Definition sampling, and results in business angels' research: toward a consensus. *Emerald insight,* 55(2), 310-330. https://doi.org/10.1108/MD-07-2016-0487

Arias Gonzáles, J.L. (2022). Guía para elaborar la operacionalización de variables. *Espacio I+D, Innovación más Desarrollo*, 10(28). https://espacioimasd.unach.mx/index.php/Inicio/article/view/274

Baena Paz, G. (2017). *Metodología de la investigación*. https://books.google.com.pe/books?id=jzZCDwAAQBAJ&hl=es&source=gbs_book_similarbooks

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

Carballo Barcos, M. & Guelmes Valdés, E.L. (2016). Algunas consideraciones acerca de las variables en las investigaciones que se desarrollan en educación. *Universidad Y Sociedad*, 8(1), 140 -150. https://rus.ucf.edu.cu/index.php/rus/article/view/317

Chavez Salazar, V.H. (2016). Desarrollo de un modelo de seguridad de la información en ambientes educativos virtuales. *Educación Superior*, 1(1),

15-30. http://www.scielo.org.bo/scielo.php?script=sci_arttext&pid=S2518-82832016000100003&lng=es&tlng=es.

Cruz Amézquita, C. P., Sarmiento Melo, L.A., Sáenz Gómez, J.A., & Pedraza Nájar, X. L. (2018). Correlation of requirements for management integration in Colombian public entities. *SIGNOS - Investigación en Sistemas De gestión*, 10(1), 25–38. https://www.redalyc.org/journal/5604/560459732001/

Diéguez, M. y Cares, C. (2019). Comparación de dos enfoques cuantitativos para seleccionar controles de seguridad de la información. RISTI - Revista Ibérica de Sistemas e Tecnologias de Información, (32), 113-128. https://doi.org/10.17013/risti.32.113-128

Ferreira, R., Frogeri, R.F., Coelho.A., & Piurcosky.F. (2018). Information security management practices: study of the influencing factors in a brazilian air force institution. *JISTEM - Journal of Information Systems and Technology Management*, 15(1), 201815005. https://www.redalyc.org/journal/2032/203261710005/

Flores Muñoz, P., Muñoz Escobar, L., y Sánchez Acalo, T. (2019). Estudio de potencia de pruebas de normalidad usando distribuciones desconocidas con distintos niveles de no normalidad. *Perfiles*, 21 (1), 1 – 8. https://bit.ly/3Fc7WG7

Flores Tapia, C.E. y Flores Cevallos, K.L. (2021). Pruebas para comprobar la normalidad de datos en procesos productivos: Anderson-Darling, Ryan-Joiner, Shapiro-Wilk y Kolmogórov-Smirnov. *Societas*, 23(2), 83–106. https://revistas.up.ac.pa/index.php/societas/article/view/2302

Gaviria Peña, C. y Márquez Fernández, C.A. (2019). *Estadística descriptiva y probabilidad*. https://books.google.com.ec/books?id=YubhDwAAQBAJ&pg=PA33&dq=c

omo+se+hace+el+muestreo+aleatorio+simple&hl=es419&sa=X&ved=2ahUKEwjrqtHo8sL6AhVpRjABHTVaCZwQ6AF6BAgJEAI#v=onepage&q=como%20se%20hace%20el%20muestreo%20aleatorio%20simple&f=false

Gerson De La Cruz, R., Méndez Fernández, A.C., y Méndez Fernández. R.A. (2023). Seguridad de la información en el comercio electrónico basado en ISO 27001: Una revisión sistemática. *Universidad La Salle*, 4(1), 219-236. https://www.redalyc.org/journal/6738/673874721015/

Guevara Alban, G.P., Verdesoto Arguello, A.E., y Castro Molina, N.E. (2020). Metodologías de investigación educativa (descriptivas, experimentales, participativas, y de investigación-acción). *Recimundo*, 4(3), 163-173. https://www.recimundo.com/index.php/es/article/view/860

Guerra, E., Neira, H., Díaz, J.L., y Patiño, J. (2021). Desarrollo de un sistema de gestión para la seguridad de la información basado en metodología de identificación y análisis de riesgo en bibliotecas universitarias. *Información tecnológica*, 32(5), 145-156. https://dx.doi.org/10.4067/S0718-07642021000500145

Hernández Escobar, A.A., Ramos Rodríguez, M.P., Plasencia Lopez, B.M., Indacochea Ganchozo, B., Quimis Gomez, A.J., y Moreno Ponce, L.A. (2018). *Metodología de la investigación científica*. https://3ciencias.com/wp-content/uploads/2018/02/MIC_breve.pdf

Hernández Sampieri, R. y Mendoza Torres, C.P. (2018). *Metodología de la investigación: Las rutas cuantitativa cualitativa y mixta*. http://www.biblioteca.cij.gob.mx/Archivos/Materiales_de_consulta/Drogas_de_Abuso/Articulos/SampieriLasRutas.pdf

Hinojosa Pérez, J.A. (2017). *El arte de hacer una tesis: Para pos y pregrado con casos prácticos*. https://adolfohinojosa.wordpress.com/category/el-arte-de-hacer-una-tesis/.

Huaura, M. (2019). *Gestión de riesgos de seguridad de la información para empresas del sector telecomunicaciones, 2019* [tesis de Maestría]. Universidad Nacional Mayor de San Marcos. https://cybertesis.unmsm.edu.pe/handle/20.500.12672/11225

Huayllani, O. (2020). *Sistema de gestión de seguridad de la información y la gestión del riesgo en el Ministerio de Salud, 2019* [tesis de Maestría]. Universidad Cesar Vallejo https://repositorio.ucv.edu.pe/handle/20.500.12692/42775

International Organization for Standardization - ISO 27001: 2013. (2013). *Information technology Security techniques Information security management systems*. https://www.iso.org/contents/data/standard/05/45/54534.html

International Organization for Standardization - ISO 27000:2018. (2018). *Information technology Security techniques Information security management systems Overview and vocabulary*. https://www.iso.org/standard/73906.html

International Organization for Standardization - ISO 31000:2018. (2018). *Risk management Guidelines*. https://www.iso.org/standard/65694.html

International Organization for Standardization - ISO 27005:2018. (2018). *Information technology Security techniques Information security management systems*. https://www.iso.org/standard/75281.html

International Organization for Standardization - ISO 27002:2013. (2013). *Information technology Security techniques Code of practice for information security controls*. https://www.iso.org/standard/54533.html

Kamil, Y., Lund, S., & Islam, M.S. (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(3), 699-722. https://doi.org/10.1007/s10257-023-00646-y

Kitsios, F., Chatzidimitriou, E., & Kamariotou, M. (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

Kovalenko, K.E., Kovalenko, N.E., & León González, J.L. (2019). A variety of information security threats. Revista Universidad y Sociedad, 11(5), 256-261. http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2218-36202019000500256&lng=es&tlng=en..

Lizarzaburu Bolaños, E.R., Barriga, G., y Noriega, E. (2018). Gestión Integral de Riesgos y Antisoborno: Un enfoque operacional desde la perspectiva ISO 31000 e ISO 37001. *Revista Universidad Y Empresa*, 21(36), 79-118. https://doi.org/10.12804/revistas.urosario.edu.co/empresa/a.6089

Luna Serrano, E., Vallle Espinosa, M., y Osuna Lever, C. (2010). Los rasgos de un "buen profesional", según la opinión de estudiantes universitarios en México. *Revista electrónica de investigación educativa*, 12(1), 1-14. http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1607-40412010000300006&lng=es&tlng=es.

Lykhova, S., Servatiuk, L., Shamsutdinov, O., Sysoieva, V., y Hurina, D. (2022). International and national standards on societal information security. *Revista Científica General José María Córdova*, 20(38), 247–264. https://www.redalyc.org/journal/4762/476273700001/

Martínez Gonzales, M.A., Sánchez Villegas, A., Toledo Atucha, E., & Faulin Fajardo, J. (2020). *Bioestadística amigable*. https://www.edicionesjournal.com/Papel/9788491134077/Bioestad%C3%ADstica+Amigable

Mayayise, T. (2021). Extending unified theory of acceptance and use of technology with ISO/IEC 27001 security standard to investigate factors influencing Bring Your Own Device adoption in South Africa. *South African Journal of Information Management*, 23(1), 9. https://doi.org/10.4102/sajim.v23i1.1376

Otzen, T. y Manterola, C. (2017). Técnicas de Muestreo sobre una Población a Estudio. *International Journal of Morphology*, 35(1), 227-232. https://dx.doi.org/10.4067/S0717-95022017000100037

Portugal Dias, A. (2017). A more effective audit after COSO ERM 2017 or after ISO 31000:2009?. *Revista Perspectiva Empresarial*, 4(2), 73-82. https://www.redalyc.org/articulo.oa?id=672271531007

Pretorius, M. & Ngejane, H. (2019). Best Practices for Establishment of a National Information Security Incident Management Capability (ISIMC). *The African Journal of Information and Communication (AJIC)*, (24), 1-20. https://doi.org/10.23962/10539/28656

Ramos Mamami, R.G., Llanqui Argollo, R.R., & Cahuaya Ancco, R. (2023). Política informática y la gestión de la seguridad de la información en base a la norma ISO 27001. *Innovación y Software*, 4(1), 96-106.https://www.redalyc.org/journal/6738/673874721007/

Rantao, T. & Njenga, K. (2020). Predicting communication constructs towards determining information security policies compliance. *South African Journal of Information Management*, 22(1), 10. https://doi.org/10.4102/sajim.v22i1.1211

Razikin, K. & Soewito, B. (2022). Cybersecurity decision support model to designing information technology security system based on risk analysis and cybersecurity framework. *Egyptian Informatics Journal*, 23 (3), 383-404. https://doi.org/10.1016/j.eij.2022.03.001

Robles Pastor, B. (2019). Población y Muestra. *Pueblo Continente*, 30(1), 245-246. http://journal.upao.edu.pe/PuebloContinente/article/view/1269/1099

Rodríguez Baca, L.S., Cruzado Puente de la Vega, C.F., Mejía Corredor, C., y Alarcón Diaz, M.A. (2020). Aplicación de ISO 27001 y su influencia en la seguridad de la información de una empresa privada peruana. *Propósitos y Representaciones*, 8(3), 786. http://www.scielo.org.pe/scielo.php?script=sci_arttext&pid=S2307-79992020000400011

Sabillon, R. (2018). A Practical Model to Perform Comprehensive Cybersecurity Audits. *Enfoque UTE*, 9(1), 127 - 137. https://doi.org/10.29019/enfoqueute.v9n1.214

Sanchez Carlessi, H., Reyes Romero, C., & Mejia Saenz, K. (2018). *Manual de términos en investigación científica, tecnológica y humanística.* *https://www.urp.edu.pe/pdf/id/13350/n/libro-manual-de-terminos-en-investigacion*.pdf

Tobi Sogen, M. D., Siregar, R., Nguyen, P.T., Lydia, E.L., & Shankar, K. (2019). Design and Implementation of a Process of Risk-Based Criticality for Network Utilities Asset Management. *Religación*, 4(19), 280-285. https://revista.religacion.com/index.php/religacion/article/view/756

Tonysé de la Rosa, M. (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.

http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2218-36202021000500495&lng=es&tlng=es..

Toro Flores, Y.A., Rivas Almonte, F.U., Turpo Gebera, O., Cuadros Paz, L., Fernández Gambarini, W., & Valderrama Chauca, E. (2019). Sistema de gestión de comunicaciones para evaluar riesgos de seguridad. *Revista Universidad y Sociedad*, 11(1), 86-92. http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2218-36202019000100086&lng=es&tlng=es..

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

Satizábal Echavarría, I.C. & Acevedo Quintana, N.M. (2018). MePRiSIA: risk prevention methodology for academic information systems. *Revista Facultad de Ingeniería Universidad de Antioquia*, (89), 81–101. https://www.redalyc.org/journal/430/43060744011/

Zuña Macancela, E.R., Arce Ramírez, A.A., Romero Berrones, W.J., y Soledispa Baque, C.J. (2019). Análisis de la seguridad de la información en las PYMES de la ciudad de Milagro. Revista Universidad y Sociedad, 11(4), 487-492. http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2218-36202019000400487&lng=es&tlng=es.

ANEXOS

Anexo 1: Matriz de Consistencia y Operacionalización de Variables

MATRIZ OPERACIONALIZACIÓN DE VARIABLES						
Variable	**Definición Conceptual**	**Definición Operacional**	**Dimensiones**	**Indicadores**	**Instrumento**	**Escala de medición**
Norma ISO 27001	La norma ISO 27001 es quien define los requisitos regulatorios para el desarrollo y operación de un SGSI, incluido un conjunto de controles para controlar y mitigar los riesgos asociados con los activos de información que la organización busca proteger mediante la operación del SGSI.	La norma ISO 27001 , se desglosa en 14 capitulos de controles de seguridad de la información, con un indicador de nivel de madurez por cada capitulo.	Capítulos de Controles de Seguridad	Nivel de Madurez de los Capítulos de Controles de Seguridad	Ficha de Datos	Razón
NORMA ISO 31000	La norma ISO 31000, Este documento proporciona directrices sobre la gestión de riesgos que enfrentan las organizaciones. Este documento proporciona un enfoque común para la gestión de cualquier tipo de riesgo y no es específico para ninguna industria o sector.	La norma iso 31000 ,se va dividir en la dimensión contexto. Donde me va permitir medir el nivel de impacto del contexto en cada uno de los activos de información en base a sus indicadores.	Contexto	Nivel de Impacto del contexto interno y externo		
Variable	**Definición Conceptual**	**Definición Operacional**	**Dimensiones**	**Indicadores**	**Instrumento**	**Escala de medición**
Gestión de Riesgos	Según la norma ISO 27000, la gestión de riesgos son actividades coordinadas para dirigir y controlar una organización,en lo relativo al riesgo.	La gestión de riesgos me va permitir identificar los activos, realizar la evaluación de activos en base a la confidencialidad, integridad y disponibilidad. Asimismo se va analizar el riesgo inherente de cada activo de la información en base al impacto por probabilidad.	Evaluación de Activo	Nivel de Activo	Ficha de Datos	Razón
			Análisis del Riesgos	Nivel de riesgo		

TITULO: La Norma ISO 27001 y la norma ISO 31000 en la gestión de riesgos de los activos de información de una empresa del sector de telecomunicaciones, Lima 2023									
Problema general	**Objetivo general**	**Hipótesis general**	**Variable Independiente**	**Dimensiones**	**Indicadores**	**Tipo y diseño**	**Población y muestra**	**Técnicas e instrumentos**	**Método de análisis de datos**
¿Existe una relación de la norma ISO 27001 y la norma ISO 31000 en la gestión de riesgos de los activos de información de una empresa del sector de telecomunicaciones, Lima 2023?	Determinar la relación de la norma ISO 27001 y la norma ISO 31000 en la gestión de riesgos de los activos de información de una empresa del sector de telecomunicaciones, Lima 2023	Existe una relación significativa de la norma ISO 27001 y la norma ISO 31000 en la gestión de riesgos de los activos de información de una empresa del sector de telecomunicaciones, Lima 2023	Norma ISO 27001	Capítulos de Controles de Seguridad	Nivel de Madurez de los controles	**Tipo:** Aplicada **Diseño:** No experimental transversal descriptivo correlacional	**Población:** N= 162 activos de información **Tipo de muestreo** Probabilistico aleatorio simple **Tamaño de la muestra:** n=115	**Técnicas:** Análisis Documental **Instrumento:** Ficha de Datos	**Descriptiva:** Estadísticos descriptivos y pruebas. **Inferencial:** Confiabilidad - Alfa de Cronback Normalidad - Kolmogorov-Smirnov Análisis paramétrico - Coeficiente de correlación de Pearson
			Norma ISO 31000	Contexto	Nivel de Impacto del contexto interno y externo				
Problemas específicos	**Objetivos específicos**	**Hipótesis específicas**	**Variable Dependiente**	**Dimensiones**	**Indicadores**				
¿Existe una relación de la norma ISO 27001 y la normaISO 31000 en el nivel de activos de para la gestión de riesgos de los activos de información de una empresa del sector de telecomunicaciones, Lima 2023?	Determinar la relación de la norma ISO 27001 y la norma ISO 31000 en el nivel de activos para la gestión de riesgos de los activos de información de una empresa del sector de telecomunicaciones, Lima 2023	Existe una relación significativa de la norma ISO 27001 y la norma ISO 31000 en el nivel de activos para la gestión de riesgos de los activos de información de una empresa de telecomunicaciones, Lima 2023.	Gestión de riesgo	Evaluación de Activo	Nivel de Activo				
¿Existe una relación de la norma ISO 27001 y la norma ISO 31000 en el nivel de riesgos para la gestión de riesgos de los activos de información de una empresa del sector de telecomunicaciones, Lima 2023?	Determinar la relación de la norma ISO 27001 y la norma ISO 31000 el nivel de riesgos para la gestión de riesgos de los activos de información de una empresa del sector de telecomunicaciones, Lima 2023	Existe una relación significativa de la norma ISO 27001 y la norma ISO 31000 el nivel de riesgos para la gestión de riesgos de una de los activos de información empresa del sector de telecomunicaciones, Lima 2023		Análisis del Riesgos	Nivel de riesgo				

Anexo 2: Instrumento de Recolección de Datos

			Políticas de Seguridad de la Información	Organización de la Seguridad de la Información	Seguridad de los Recursos Humanos	Gestión de Activos	Control de Acceso	Criptografía	Seguridad Física y del Entorno	Seguridad de las Operaciones	Seguridad de las Comunicaciones	Adquisición, Desarrollo y Mantenimiento de Sistemas	Relaciones con los Proveedores	Gestión de Incidentes de Seguridad de la Información	Aspectos de la Seguridad de la Información en la Gestión de Continuidad del Negocio	Cumplimiento	DE01. Debido a los cambios coyunturales se estan actualizando los procesos y la organización debe de adecuarse a los mismos.	DE02. Alta rotación de personal, especialmente en los procesos de Implementación, Operación y Mantenimiento.	DE03. Plataforma de software no alineada al flujo del servicio que queremos brindar, software con 15 años de antigüedad.	DE04. Falta de métricas estandarizadas en la implementación del servicio.	DE05. Falta de control para mantener los contratos de soporte activos.	DE06.Los comerciales solicitan SLAs, mas ajustados de lo que se ofrece tecnicamente y ofrecen servicios personalizados.	DE07.Falta de automatización en control de activos.	DE08.No contar con un data center alterno	DE09.El proceso poco seguro de entrega de cuentas y contraseñas a los clientes.	DE10.Equipos en producción que estan fuera de soporte.	AM01. Debido a las restricciones declaradas por el Estado, se implementaran controles en acceso al Data center limitando el aforo.	AM02. Competidores con mayor cobertura a nivel de conectividad-TELCO (nivel nacional) y mejores certificaciones internacionales.	AM03. Elevada actividad de ataques externos	AM04. Incremento de competidores del rubro con ofertas agresivas.	AM05. Interrupción a la continuidad en la operación debido al estado de emergencias,pandemias,sismos, otros.	Nivel de Activo (Confidencialidad, Disponibilidad, Integridad)	Nivel de Riesgos (Impacto * Probabilidad)
N°	CAT	ACTIVOS DE INFORMACIÓN	**Norma ISO 31000**														**Norma ISO 31000**															**Gestión de Riesgos**	
			D1. Capítulos de controles de seguridad														**D2.Contexto**															**D3.**	**D4.**
			C1	**C2**	**C3**	**C4**	**C5**	**C6**	**C7**	**C8**	**C9**	**C10**	**C11**	**C12**	**C13**	**C14**	**D01**	**D02**	**D03**	**D04**	**D05**	**D06**	**D07**	**D08**	**D09**	**D10**	**AM01**	**AM02**	**AM03**	**AM04**	**AM05**	**NA**	**NR**

Anexo 3. Matriz Evaluación por juicio de expertos

CARTA DE PRESENTACIÓN

Señor Ingeniero:

Marlon Frank Acuña Benites

Presente

Asunto: **VALIDACIÓN DE INSTRUMENTOS A TRAVÉS DE JUICIO DE EXPERTO**.

Me es muy grato comunicarme con usted para expresarle mis saludos y así mismo, hacer de su conocimiento que, siendo estudiante del Programa de Maestría en Ingeniería de Sistemas con mención en Tecnologías de la Información de la Escuela de Posgrado de la UCV, en la sede Lima norte 202302, requiero validar los instrumentos con los cuales se recogerá la información necesaria para poder desarrollar mi investigación y con la que sustentaré mis competencias investigativas en la experiencia curricular de diseño y desarrollo del trabajo de investigación.

Los nombres de mis variables son: Norma ISO 27001, Norma ISO 31000 y Gestión de Riesgos, siendo imprescindible contar con la aprobación de expertos del tema para poder aplicar los instrumentos en mención, he considerado conveniente recurrir a usted, ante su connotada experiencia en temas educativos y/o investigación educativa.

El expediente de validación, que le hago llegar contiene:

- Carta de presentación.
- Formato de validación.
- Certificado de validez de contenido de los instrumentos.

Expresándole mis sentimientos de respeto y consideración me despido de usted, no sin antes agradecerle por la atención que dispense a la presente.

Atentamente.

.....

Fiorella Denisse Bernardo Infancion

Alumna del programa de maestría grupo 202302

D.N.I 43187871

Evaluación por juicio de expertos

Respetado juez: Usted ha sido seleccionado para evaluar el instrumento para medir las variables Norma ISO 27001, Norma ISO 31000 y Gestión de Riesgos. La evaluación del instrumento es de gran relevancia para lograr que sea válido y que los resultados obtenidos a partir de éste sean utilizados eficientemente; aportando al quehacer psicológico. Agradezco su valiosa colaboración.

1. Datos generales del juez:

Nombre del juez:	Marlon Frank Acuña Benites
Grado profesional:	Maestría ( ) Doctor (X)
Área de formación académica:	Clínica ( ) Social ( ) Educativa (X) Organizacional ( )
Áreas de experiencia profesional:	Investigación
Institución donde labora:	Universidad César Vallejo sede Lima Norte
Tiempo de experiencia profesional en el área:	2 a 4 años ( ) Más de 5 años (X)
Experiencia en Investigación (si corresponde)	

2. Propósito de la evaluación:

Validar el contenido del instrumento, por juicio de expertos.

3. Soporte teórico

Breve detalle de las variables de la investigación

VI1. Norma ISO 27001: Es quien define los requisitos regulatorios para el desarrollo y operación de un SGSI, incluido un conjunto de controles para controlar y mitigar los riesgos asociados con los activos de información que la organización busca proteger mediante la operación del SGSI

VI2. Norma ISO 31000: Este documento proporciona directrices sobre la gestión de riesgos que enfrentan las organizaciones. Este documento

proporciona un enfoque común para la gestión de cualquier tipo de riesgo y no es específico para ninguna industria o sector.

VD. Gestión de Riesgos: Son actividades coordinadas para dirigir y controlar una organización en lo relativo al riesgo.

Tabla detalle de desglose dimensión e indicadores

Variable	Dimensión	Indicador	Detalle
VI.1 NORMA ISO 27001	D1. Capítulos de controles de seguridad	1. Políticas de Seguridad de la Información 2. Organización de la Seguridad de la Información 3. Seguridad de los Recursos Humanos 4. Gestión de Activos 5. Control de Acceso 6. Criptografía 7. Seguridad Física y del Entorno 8. Seguridad de las Operaciones 9. Seguridad de las Comunicaciones 10. Adquisición, Desarrollo y Mantenimiento de Sistemas 11. Relaciones con los Proveedores 12. Gestión de Incidentes de Seguridad de la Información 13. Aspectos de la Seguridad de la Información en la Gestión de Continuidad del Negocio 14. Cumplimiento	El nivel de madurez de cada capítulo de controles de seguridad de la información para cada uno de los activos de información.
VI2. NORMA ISO 31000	D2. Contexto	1. Cambios en los procesos. 2. Alta rotación de personal. 3. Plataforma de software no alineada al flujo del servicio. 4. Falta de métricas estandarizadas. 5. Falta de control en los contratos de soporte. 6. Los comerciales solicitan SLAs, más ajustados. 7. Falta de automatización en control de activos. 8. No contar con un data center alterno. 9. El proceso de gestión de accesos poco seguro. 10. Equipos en producción que están fuera de soporte. 11. Controles en acceso con limitaciones. 12. Competidores con mayor cobertura. 13. Elevada actividad de ataques externos. 14. Incremento de competidores. 15. Interrupción a la continuidad.	El nivel de impacto del contexto definido como amenazas y debilidades en cada uno de los activos de información.
VD. GESTION DE RIESGOS	D3. Evaluación de activos	1. Nivel de activo.	El nivel del activo se identifica en base al nivel de confidencialidad, integridad y disponibilidad de cada activo de información.
	D4. Análisis de Riesgos	1. Nivel de riesgo.	Analiza el riesgo inherente de cada activo de la información.

Escala/ ÁREA	Subescala (dimensiones)	Definición
ORDINAL	Capítulos de Controles de Seguridad	Cada capítulo define controles de seguridad conteniendo una o más categorías principales de seguridad. Que se utilizan en el apartado 6.1.3 Tratamiento de riesgos de seguridad de la información de la norma ISO 27001.
	Contexto	Es poder definir los parámetros externos e internos a tener en cuenta cuando se gestiona el riesgo.
	Evaluación de Activos	Es parte de las actividades de la gestión de riesgos de seguridad de la información.
	Análisis de riesgos	Proceso que permite comprender la naturaleza de riesgo y determinar el nivel de riesgo.

4. <u>Presentación de instrucciones para el juez</u>

A continuación, a usted le presento la ficha de datos conformada por las 3 variables de mi investigación detalladas con sus dimensiones numeradas del D1 al D4 con su detalle respectivo, elaborado por Fiorella Denisse Bernardo Infancion. De acuerdo con los siguientes indicadores califique cada uno de los ítems según corresponda.

Categoría	Calificación	Indicador
CLARIDAD El ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas.	1. No cumple con el criterio	El indicador no es claro.
	2. Bajo Nivel	El indicador requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de estas.
	3. Moderado nivel	Se requiere una modificación muy específica de algunos de los términos del ítem.
	4. Alto nivel	El indicador es claro, tiene semántica y sintaxis adecuada.
COHERENCIA El ítem tiene relación	1. Totalmente en desacuerdo (no cumple con el criterio)	El indicador no tiene relación lógica con la dimensión.

lógica conla dimensión o indicador que está midiendo.	2. Desacuerdo (bajo nivel de acuerdo)	El indicador tiene una relación tangencial /lejana conla dimensión.
	3. Acuerdo (moderado nivel)	El indicador tiene una relación moderada con ladimensión que se está midiendo.
	4. Totalmente de Acuerdo (altonivel)	El indicador se encuentra está relacionado con ladimensión que está midiendo.
RELEVANCIA El ítem es esencialo importante, es decir debe ser incluido.	1. No cumple con el criterio	El indicador puede ser eliminado sin que se veaafectada la medición de la dimensión.
	2. Bajo Nivel	El indicador tiene alguna relevancia, pero otro ítempuede estar incluyendo lo que mide éste.
	3. Moderado nivel	El indicador es relativamente importante.
	4. Alto nivel	El indicador es muy relevante y debe ser incluido.

Leer con detenimiento los ítems y calificar en una escala de 1 a 4 su valoración, así como solicitamos brindesus observaciones que considere pertinente

1 No cumple con el criterio
2. Bajo Nivel
3. Moderado nivel
4. Alto nivel

Dimensiones del Instrumento:

Ficha de datos

N°	CAT	ACTIVOS DE INFORMACIÓN	Norma ISO 31000													Norma ISO 31000													Gestión de Riesgos	
			D1. Capítulos de controles de seguridad													D2. Contexto													D3.	D4.
			C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11	C12	C13	C14	D01	D02	D03	D04	D05	D06	D07	D08	D09	D10	AM01	AM02	AM03	AM04	AM05	NA	NR

Variable independiente 1 – Norma ISO 27001

D1. Capítulos de controles de seguridad

C1	Políticas de Seguridad de la Información
C2	Organización de la Seguridad de la Información
C3	Seguridad de los Recursos Humanos
C4	Gestión de Activos
C5	Control de Acceso
C6	Criptografía
C7	Seguridad Física y del Entorno
C8	Seguridad de las Operaciones
C9	Seguridad de las Comunicaciones
C10	Adquisición, Desarrollo y Mantenimiento de Sistemas
C11	Relaciones con los Proveedores

C12	Gestión de Incidentes de Seguridad de la Información
C13	Aspectos de la Seguridad de la Información en la Gestión de Continuidad del Negocio
C14	Cumplimiento

Variable independiente 2 – Norma ISO 31000

D2. Contexto

D01	Cambios en los procesos.
D02	Alta rotación de personal.
D03	Plataforma de software no alineada al flujo del servicio.
D04	Falta de métricas estandarizadas.
D05	Falta de control en los contratos de soporte.
D06	Los comerciales solicitan SLAs, más ajustados.
D07	Falta de automatización en control de activos.
D08	No contar con un data center alterno.
D09	El proceso de gestión de accesos poco seguro.
D10	Equipos en producción que están fuera de soporte.

AM01	Controles en acceso con limitaciones.
AM02	Competidores con mayor cobertura.
AM03	Elevada actividad de ataques externos.
AM04	Incremento de competidores.
AM05	Interrupción a la continuidad.

Variable Dependiente – Gestión de Riesgos

D3. Evaluación de Activos

NA	Nivel de Activo

D4. Análisis de Riesgos

NR	Nivel de riesgo

- **Primera dimensión**: Capítulos de controles de seguridad
  Objetivos de la Dimensión: Medir el grado de madurez de los controles de seguridad de la información.

Indicadores	Claridad				Coherencia				Relevancia				
	1.No cumple con el criterio.	2.Bajo Nivel	3.Moderado Nivel	4.Alto Nivel	1.No cumple con el criterio.	2.Bajo Nivel	3.Moderado Nivel	4.Alto Nivel	1.No cumple con el criterio.	2.Bajo Nivel	3.Moderado Nivel	4.Alto Nivel	Observaciones/ Recomendaciones
C1 Políticas de Seguridad de la Información				X				X				X	
C2 Organización de la Seguridad de la Información				X				X				X	
C3 Seguridad de los Recursos Humanos				X				X				X	
C4 Gestión de Activos				X				X				X	
C5 Control de Acceso				X				X				X	
C6 Criptografía				X				X				X	
C7 Seguridad Física y del Entorno				X				X				X	
C8 Seguridad de las Operaciones				X				X				X	
C9 Seguridad de las Comunicaciones				X				X				X	
C10 Adquisición, Desarrollo y Mantenimiento de Sistemas				X				X				X	
C11 Relaciones con los Proveedores				X				X				X	
C12 Gestión de Incidentes de Seguridad de la Información				X				X				X	
C13 Aspectos de la Seguridad de la Información en la Gestión de Continuidad del Negocio				X				X				X	
C14 Cumplimiento				X				X				X	

- **Segunda dimensión**: Contexto
  Objetivos de la Dimensión: Medir el impacto del contexto en los activos de información.

Indicadores	Claridad				Coherencia				Relevancia				
	1.No cumple con el criterio.	2.Bajo Nivel	3.Moderado Nivel	4.Alto Nivel	1.No cumple con el criterio.	2.Bajo Nivel	3.Moderado Nivel	4.Alto Nivel	1.No cumple con el criterio.	2.Bajo Nivel	3.Moderado Nivel	4.Alto Nivel	Observaciones/ Recomendaciones
D01 Cambios en los procesos.				X				X				X	
D02 Alta rotación de personal.				X				X				X	
D03 Plataforma de software no alineada al flujo del servicio.				X				X				X	
D04 Falta de métricas estandarizadas.				X				X				X	
D05 Falta de control en los contratos de soporte.				X				X				X	
D06 Los comerciales solicitan SLAs, más ajustados.				X				X				X	
D07 Falta de automatización en control de activos.				X				X				X	
D08 No contar con un data center alterno.				X				X				X	
D09 El proceso de gestión de accesos poco seguro.				X				X				X	
D10 Equipos en producción que están fuera de soporte.				X				X				X	
AM01 Controles en acceso con limitaciones.				X				X				X	
AM02 Competidores con mayor cobertura.				X				X				X	
AM03 Elevada actividad de ataques externos.				X				X				X	
AM04 Incremento de competidores.				X				X				X	
AM05 Interrupción a la continuidad.				X				X				X	

- **Tercera dimensión**: Evaluación de Activos
  Objetivos de la Dimensión: Identificar el nivel de activo en base a la confidencialidad, integridad y disponibilidad.

Indicadores	Claridad				Coherencia				Relevancia				
	1.No cumple con el criterio.	2.Bajo Nivel	3.Moderado Nivel	4.Alto Nivel	1.No cumple con el criterio.	2.Bajo Nivel	3.Moderado Nivel	4.Alto Nivel	1.No cumple con el criterio.	2.Bajo Nivel	3.Moderado Nivel	4.Alto Nivel	Observaciones/ Recomendaciones
NA. Nivel de Activo				X				X				X	

- **Cuarta dimensión**: Análisis de Riesgos
  Objetivos de la Dimensión: Identificar el nivel del riesgo inherente de los activos.

Indicadores	Claridad				Coherencia				Relevancia				
	1.No cumple con el criterio.	2.Bajo Nivel	3.Moderado Nivel	4.Alto Nivel	1.No cumple con el criterio.	2.Bajo Nivel	3.Moderado Nivel	4.Alto Nivel	1.No cumple con el criterio.	2.Bajo Nivel	3.Moderado Nivel	4.Alto Nivel	Observaciones/ Recomendaciones
NR. Nivel de Riesgo				X				X				X	

Observaciones (precisar si hay suficiencia): El instrumento SI presenta suficiencia

Opinión de aplicabilidad: Aplicable [X] Aplicable después de corregir [ ]

No aplicable [ ]

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

Especialidad del validador: Metodológo

18 de diciembre del 2023.

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

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

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

Firma del Experto validador

Anexo 4. Resultado de similitud del programa Turnitin

Anexo 5. Resultados de prueba de fiabilidad

Estadísticas de Fiabilidad	
Alfa de Cronbach	**Número de elementos**
0.744	31

La explicación de lo encontrado fue lo siguiente:

1. Las estadísticas de confiabilidad, específicamente el índice alfa de Cronbach, ofrecen insights sobre la congruencia dentro de la ficha de datos utilizada como instrumento de recopilación de información.
2. Índice de Confiabilidad de Cronbach, el resultado obtenido es 0.744, dentro del rango de 0 a 1. Valores próximos a 1 señalan una mayor coherencia entre los elementos del cuestionario. En este contexto, un valor de 0.744 indica una coherencia interna positiva, lo que señala que las preguntas están positivamente correlacionadas entre sí. Además, este resultado indica que el instrumento utilizado exhibe una confiabilidad sólida, asegurando mediciones estables y coherentes.

Número de elementos: Son los 31 indicadores del instrumento de recopilación de datos que se están evaluando para medir la consistencia interna; esto es, 29 indicadores de variables independientes y 2 indicadores de variable dependiente.

Anexo 6. Formulación de hipótesis para pruebas de normalidad y resultados de prueba de normalidad de variables

Se evidencia la formulación de hipótesis para pruebas de normalidad.

Pruebas de Normalidad	**Norma ISO 27001**	**Norma ISO 31000**	**Gestión de Riesgos**
Ho: Distribución normal	Ho: X = N (μ, σ2)	Ho: X = N (μ, σ2)	Ho: X = N (μ, σ2)
Ha: Distribución no normal	Ha: X <> N (μ, σ2)	Ha: X <> N (μ, σ2)	Ha: X <> N (μ, σ2)
Nivel de significancia: NC	0.95	0.95	0.95
Error: α	0.05	0.05	0.05
Prueba de normalidad	n >= 50 Kolmogorov-Smirnov	n >= 50 Kolmogorov-Smirnov	n >= 50 Kolmogorov-Smirnov
	n < 50 Shapiro-Wilk	n < 50 Shapiro-Wilk	n < 50 Shapiro-Wilk
Criterio de decisión	p-valor < 0.05 Rechazar Ho Aceptar Ha	p-valor < 0.05 Rechazar Ho Aceptar Ha	p-valor < 0.05 Rechazar Ho Aceptar Ha
	p-valor >= 0.05 Aceptar Ho Rechazar Ha	p-valor >= 0.05 Aceptar Ho Rechazar Ha	p-valor >= 0.05 Aceptar Ho Rechazar Ha

Se evidencia los resultados de prueba de normalidad de variables

Pruebas de Normalidad						
	Kolmogorov-Smirnova			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
ISO27001	0.318	115	<0.001	0.738	115	<0.001
ISO 31000	0.250	115	<0.001	0.846	115	<0.001
Riesgos	0.324	115	<0.001	0.711	115	<0.001

a. Ajuste de significación de Lilliefors

De acuerdo con los resultados de prueba de normalidad de variables, se observó que los indicadores de las variables independientes Norma ISO 27001 y Norma ISO 31000, junto con los indicadores relacionados con la variable dependiente "Gestión de Riesgos", muestran un p-valor igual a 0. Al compararlo con los criterios de la formulación de hipótesis para pruebas de normalidad y al verificar que el p-valor es menor a 0.05, se descarta la hipótesis nula que postula que los datos siguen una distribución normal. En su lugar, se respalda la hipótesis alternativa, llegando a la conclusión de que los datos no exhiben una distribución normal.