UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

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

ISO 27001 para la gestión de seguridad de la información en el área TI de una empresa industrial, Lima 2023

TESIS PARA OBTENER EL GRADO ACADÉMICO DE:

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

AUTOR:

Medina Pinillos, Jose Roberto (orcid.org/0000-0002-2870-7206)

ASESORES:

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

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

LÍNEA DE INVESTIGACIÓN:

Auditoría de Sistemas y Seguridad de la Información

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:

Desarrollo económico, empleo y emprendimiento

LIMA – PERÚ

2023

DEDICATORIA

Agradezco a Dios por bendecirme en este camino y haberme permitido concluir este gran sueño.

A mis padres José y Meri, a mi esposa Joanna, son ustedes el motivo principal de mi vida y el mejor ejemplo de familia.

AGRADECIMIENTO

A mis docentes de la UCV por compartir parte de su conocimiento con entrega y dedicación, muy en especial a mis amigos del Grupo 1 y a mi amiga De Los Ángeles ya que sin su apoyo constante no lo hubiera logrado.
A todos, muchas gracias.

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLA

ÍNDICE DE GRÁFICO Y FIGURAS

RESUMEN

La investigación presentó como objetivo general: determinar de qué manera ISO 27001 influye en la gestión de la seguridad de la información en el área TI de una empresa industrial, Lima 2023. La metodología fue cuantitativa, correlacional causal, básica, la población fue de 31 colaboradores del área TI de una empresa industrial, Lima 2023, la muestra fue de la totalidad de la población, siendo esta elegida por medio de un muestreo no probabilístico, censal, la técnica de recolección de datos empleada fue la encuesta y el instrumento el cuestionario; ISO 27001 y el de gestión de sistema de información. Se reflejó como resultado que la ISO 27001 influyó significativamente con la gestión de la seguridad de la información en el área TI de una empresa industrial, lo cual fue reflejando por medio de una $p<0.05$. Se concluyó que la variable ISO 27001 en un 22% influyó significativa en la gestión de la seguridad de la información. Se recomienda establecer un programa estratégico de implementación de la ISO 27001 para fortalecer la gestión de la seguridad de la información en este espacio, con la intención de continuar fortaleciendo este tipo de conocimientos y su práctica dentro del equipo de trabajo.

Palabras clave: ISO 27001, seguridad de la información, empresa industrial, área TI, colaboradores.

ABSTRACT

The research presented as a general objective: to determine how ISO 27001 influences the management of information security in the IT area of an industrial company, Lima 2023. The methodology was quantitative, causal correlational, basic, the population was 31 employees of the IT area of an industrial company, Lima 2023, the sample was from the entire population, being chosen by means of a non-probabilistic, census sampling, the data collection technique used was the survey and the instrument the questionnaire; ISO 27001 and the information system management. It was reflected as a result that ISO 27001 significantly influenced the management of information security in the IT area of an industrial company, which was reflected by means of a $p<0.05$. It was concluded that the ISO 27001 variable had a significant influence on information security management by 22%. It is recommended to establish a strategic program for the implementation of ISO 27001 to strengthen information security management in this space, with the intention of continuing to strengthen this type of knowledge and its practice within the work team.

Keywords: ISO 27001, information security, industrial company, IT area, collaborators.

I. INTRODUCCIÓN

Por medio de este proyecto, se lleva a cabo el proceso de determinación de la variable ISO 27001 para la gestión de seguridad de la información en una empresa industrial, dedicada al rubro de venta de colchones, para el área de TI.

Las organizaciones cuentan con una abundante cantidad de información que les ayuda a alcanzar el éxito, sin embargo, es importante destacar que, en algunos lugares del mundo, existen individuos conocidos como Hackers, los cuales poseen muchas habilidades en el manejo de los avances tecnológicos y pudieran cometer delitos informáticos, incluyendo el robo de información confidencial de las empresas (Kitsios, 2023). Al respecto, se resalta que estas para protegerse de este tipo de amenazas suelen adoptar normas de seguridad de estas informaciones, siendo una de las más prestigiosas las ISO 27001, cuyas certificaciones en la actualidad han aumentado de forma global en un 12% más en comparación con el año 2018 (Quset And Alkilani, 2022). Según Alexie (2021), en Moldavia, frecuentemente se están reportando casos referente a la poca eficiencia del resguardo de informaciones y confidencialidad de las comunicaciones empresariales, debido a la ausencia de políticas, procedimientos y controles adecuados en los procesos, conociéndose que son muy escasas las empresas que en este país poseen certificaciones de seguridad de la información, por lo que se recomendó adoptar las ISO 27001 dentro de su estructura de manejo en la seguridad de las informaciones, puesto que permiten brindar beneficios, en cuanto a la protección de los servicios y activos empresariales, incremento de la confianza y respaldo de clientes e inversionistas nacionales e internacionales, entre otros.

Dentro del territorio peruano, Narro (2021), en la ciudad de Cajamarca, bajo un enfoque cuantitativo y aplicado, ejecutó la realización de un estudio, cuya finalidad se basó en la determinación de como las SGSI inciden dentro del proceso de las gestiones de riesgo en activos de informaciones, por lo que se lograron identificar las ventajas y la eficacia del SGSI en la alineación de los procesos de la empresa, referente a las gestiones de riesgo de activos de las informaciones, señalándose como principales elementos con significancia en esta relación a la

supervisión (<0.05). Se concluyó que la implementación del SGSI mejora el conocimiento y tiene efectos positivos en las gestiones de riesgos de activos de las informaciones. Asimismo, se sugirió enfocar el proceso de aplicabilidad SGSI en las ISO 27001, para elevar los niveles de efectividad propuesto.

A nivel Local, Alemán (2023), en Lima, desarrolló un estudio cuantitativo, con una muestra de 78 colaboradores de una empresa, donde planteó la operatividad de las ISO 27001 dentro de la planificación y ejecución de los SGSI, obteniendo como resultados que este tipo de herramienta no solo contribuye a la protección de la información y a la realización efectiva de las proyecciones empresariales, sino que también puede generar confianza y credibilidad ante los clientes y socios comerciales, al garantizar la seguridad de su información. Lo que contribuye a la reducción de costos asociados al resguardo de informaciones, tales como; pérdida de datos o interrupción de servicios, lo que se traduce en una mayor eficiencia y rentabilidad en la operación de la empresa. Por lo tanto, la operatividad de las ISO 27001 dentro de la planificación y ejecución de los SGSI es una decisión estratégica que genera beneficios a largo plazo y contribuir al éxito de la organización en un entorno cada vez más digital y conectado.

En concordancia, se plantea el caso de una empresa industrial en Lima, que se desempeña en la actividad de hacer colchones, con 50 años aproximadamente dentro del mercado, donde llama la atención se ha venido generando situaciones respecto a la posible carencia de políticas en cuanto al resguardo de informaciones, debilidad en la modalidad de resguardo de los datos de la empresa, descontrol en el acceso de los usuarios a los mismos, fallas en el control de registro de uso y sus modificaciones, poco respaldos de informaciones, escasa empleabilidad de la creación de copias de registros, entre otras.

Ante todos estos planteamientos, se desarrolla la presente investigación, enfocada en las ISO 27001 para la gestión de seguridad de la Información en el área TI de una empresa industrial, Lima 2023. Planteándose como pregunta general: ¿De qué manera ISO 27001 influye en la gestión de la seguridad de la información en el área TI de una empresa industrial, Lima 2023?, y preguntas

específicas: ¿De qué manera ISO 27001 influye en la disponibilidad de la información en el área TI de una empresa industrial, Lima 2023?, ¿De qué manera ISO 27001 influye en la autenticidad de la información en el área TI de una empresa industrial, Lima 2023?, ¿De qué manera ISO 27001 influye en la integridad de la información en el área TI de una empresa industrial, Lima 2023?, ¿De qué manera ISO 27001 influye en la confidencialidad de la información en el área TI de una empresa industrial, Lima 2023? y ¿De qué manera ISO 27001 influye en la trazabilidad de la información en el área TI de una empresa industrial, Lima 2023?

Dentro de este contexto, se destaca como justificación práctica del estudio, que este se sustenta en la búsqueda de bienestar para la dinámica empresarial abordada, puesto la operatividad de las ISO 27001 en el área TI, busca proteger los recursos informativos de la empresa y mitigar los riesgos asociados a su manejo, posibilitándose se establezca un trabajo sistemático, completo y normado para la seguridad de la informaciones, lo que ayuda a la empresa a identificar y manejar los riesgos de manera efectiva, en función de este tipo de procesos, contribuyendo a reforzar su imagen ante los clientes y otras partes interesadas.

La justificación metodológica, se fundamenta en que ayuda considerablemente en que se colaborará con los procesos de protección y gestión de las informaciones de las empresas, planteando procedimientos, técnicas, herramientas propias del uso ISO 27001 para las gestiones de las informaciones en el área TI de una empresa industrial, permitiendo diseñar una solución procedimentalmente certificada y avalada por estándares internacionales reconocidas, la cual está enfocada en las gestiones de riesgos de los activos de informaciones. Debido a que el propósito es brindar un conocimiento detallado sobre una metodología que haga capaz de procurar se cumplan las normas, para minimizar amenazas para el manejo de las informaciones y alcanzar niveles de madurez eficiente en el modelo de SGSI, además pretende fortalecer las gestiones de riesgos y asegurar la protección de las informaciones de la organización.

Se justifica de forma teórica, al basarse en la perspectiva de que un adecuado SGSI, inicia con estrategias como la incorporación de las ISO 27001,

planteamientos que se fortalecen al desarrollar de análisis apoyado en teorías y temas académicos discutidos por la comunidad científica, por lo tanto, el estudio de investigación plantea alinear los conocimientos de los SGSI como práctica para fundamentar determinaciones dentro de la organización, siendo clave en cuanto a la inversión en seguridad de la información, sustentándose en fundamentos desarrollados a partir de estudios e investigaciones donde se implementan las ISO 27001. Por lo que partiendo de esta experiencia se provee de un material referencial actualizado, que será de gran relevancia para futuros investigadores.

Al respecto, se plantean los siguientes objetivos: Objetivo General; determinar de qué manera ISO 27001 influye en la gestión de la seguridad de la información en el área TI de una empresa industrial, Lima 2023. Objetivos específicos; determinar de qué manera ISO 27001 influye en la disponibilidad de la información en el área TI de una empresa industrial, Lima 2023, determinar de qué manera ISO 27001 influye en la autenticidad de la información en el área TI de una empresa industrial, Lima 2023, determinar de qué manera ISO 27001 influye en la integridad de la información en el área TI de una empresa industrial, Lima 2023, determinar de qué manera ISO 27001 influye en la confidencialidad de la información en el área TI de una empresa industrial, Lima 2023 y determinar de qué manera ISO 27001 influye en la trazabilidad de la información en el área TI de una empresa industrial, Lima 2023.

Las hipótesis de la investigación se estructuran de la siguiente forma: Hipótesis general; ISO 27001 influye significativamente en la gestión de la seguridad de la información en el área TI de una empresa industrial, Lima 2023. Hipótesis específicas: ISO 27001 influye significativamente en la disponibilidad de la información en el área TI de una empresa industrial, Lima 2023, ISO 27001 influye significativamente en la autenticidad de la información en el área TI de una empresa industrial, Lima 2023, ISO 27001 influye significativamente en la integridad de la información en el área TI de una empresa industrial, Lima 2023, ISO 27001 influye significativamente en la confidencialidad de la información en el área TI de una empresa industrial, Lima 2023 e ISO 27001 influye significativamente en la trazabilidad de la información en el área TI de una empresa industrial, Lima 2023.

II. MARCO TEÓRICO

La sección presentó la información teórica que brindó sustento al estudio, las cuales se encontraron relacionadas a las variables; ISO 27001 y gestión de seguridad de la información, plasmándose antecedentes de la investigación y bases teóricas.

En este sentido, se mencionan a continuación los antecedentes nacionales, citándose a: Ibarra (2023), quien determinó la incidencia de las ISO 27001:2013 en las gestiones de control de informaciones en una UGEL. Su metodología fue cuantitativa, pre-experimental, donde se incluyó a 47 empleados en la muestra, se recolecto información por medio de un cuestionario. Los resultados expuestos reflejaron que se halló una significancia <0.05, reconociéndose una incidencia directa entre la aplicación de estas normas en la gestión de las informaciones dentro de esta institución, también indicó que no existía influencia entre variable ISO 27001 y la dimensión autenticidad, siendo esto valorado por medio de una $p<0.05$, con una $t_o= 9,342$ y $t_c= 1.680$. Se concluyó que las normas mencionadas son una excelente herramienta para fortalecer los procesos de gestiones de las informaciones.

Alemán (2023), estableció como finalidad la aplicación de las ISO 27001 y su relacionamiento con el resguardo de las informaciones de una empresa consultora. La metodología fue cuantitativa, pre-experimental, su muestra fue de 78 colaboradores, el instrumento utilizado fue el cuestionario. Se obtuvo como hallazgo un valor de significancia menor a 0.05 y 78 grados de libertad, por lo que se estable que estas normas favorecen el control de seguridad de las informaciones, al contrastarse los resultados de las dimensiones; disponibilidad, adaptabilidad, accesibilidad, resguardo de la información, se halló que estas se relacionan con las ISO 27001, indicándose un sig. <0.05. Se concluye que las normas mencionadas son una herramienta indicada para optimizar los procesos de control para el resguardo de informaciones entro de la organización.

Cuenca (2023), se planteó establecer el diseño de SGSI según 27001 para el resguardo del activo TI en un espacio organizacional particular. La metodología

fue cuantitativa, aplicada, la muestra de 20 empleados, el instrumento fue el cuestionario. Como hallazgo se conoció de una interconexión positiva y con significancia entre los elementos estudiados (0.713; <0.05). Se concluyó como cierta la relación de las variables focalizadas, demostrándose que el fortalecer el proceso de las SGSI con las ISO 27001 es una acción determinante de la efectividad en el control de activos TI.

Huaney (2022), tuvo como propósito la demostración de como la estructuración de una data center puede ser mejorada con la incorporación de la seguridad de las informaciones enfocadas en ISO 27001. La investigación fue cuantitativa, explicativa, contando con 280 colaboradores de muestra, el cuestionario se usó para la obtención de datos. Entre sus resultados, se resaltó que la estructuración de data center dentro de la institución estudiada influyen en las ISO 27001, lo cual en su prueba de entrada arrojo ser deficiente en un 35.2% y en su prueba de salida se halló como eficiente en un 50.6%. Se concluyó que las ISO 27001 influyen de manera positiva dentro de la estructuración de una data center.

Escobar (2022), determinó como la implementación de ISO 27001 favorecen los sistemas de controles de delitos dentro del ámbito informático. La metodología fue cuantitativa, causal, el instrumento establecido fue el cuestionario, la muestra se constituyó con 100 personas pertenecientes al contexto de estudio. Se resaltó entre sus resultados que el nivel de aplicación de las ISO 27001 fue alto en un 88% y que el control del delito fue alto en un 86%, asimismo se determinó que las incorporaciones de las ISO 27001 favorecen la detección de estas infracciones en un 81.2% (Pseudo R cuadrado). Se concluye que la implementación de estas normas de seguridad es un proceso importante para controlar los delitos de carácter informático.

Ponte (2022), formuló como meta el establecimiento de las influencias de ISO27001 en el trabajo remoto en el periodo de pandemia en una organización. La metodología fue cuantitativa, correlacional, con 45 colaboradores de muestra, se empleó el cuestionario para tomar datos. Los resultados demostraron que existía significativamente una incidencia, al obtenerse < 0.05, evidenciándose que al incluir

ISO27001 dentro del desarrollo del teletrabajo en pandemia, la reducción de la deficiencia se calculó en un 44%, la optimización logro un nivel regular en un 22.2% y la eficiencia se elevó en el 66%. Se concluyó que la influencia de las ISO 27001 ha sido un acierto muy notorio dentro del desarrollo del teletrabajo, siendo sus aportes significantes para mejorar su aplicabilidad.

Duval et al., (2022), focalizó en su propósito la identificación de la importancia de los SGSI dentro del contexto educativo con el ITIL e ISO 27001. La metodología fue mixta, donde participaron 30 personas en su muestra, utilizándose la ficha de recojo de datos y los cuestionarios como instrumentos. Entre los hallazgos se indicó a la SGSI que no ha sido relevante dentro de la incorporación del ITIL e ISO 27001 en su capacidad de respuesta en base a la autenticidad de sus operaciones, siendo en su pre-test deficiente en un 84% y en el post-test en un 85% manteniendo casi los mismos niveles, asimismo se resaltó que la capacitación de los colaboradores en pre tes se definía como deficiente en un 91%. Se concluyó que la SGSI es un proceso de relevancia dentro del contexto educativo, el cual se fortalece al incorporar la ITIL e ISO 27001, potenciándose el rendimiento interno y permitiendo una mejor proyección de esta, con respecto a la capacidad de respuesta ante sus diversas demandas.

Córdoba (2021). Se propuso como propósito establecer la planificación estructural sistema computarizado para los SGSI fortalecidos en las ISO 27001 en una universidad colombiana. La metodología fue cuantitativa y tecnológica, la muestra estuvo constituida por 6 integrantes de la coordinación de sistemas e informática de la casa de estudio, los instrumentos aplicados fueron el cuestionario, lista de cotejo y registro de recojo de datos. Entre sus hallazgos, se conoció que en la empresa la aplicabilidad de las SGSI basadas en ISO 27001 es inexistente en un 63%, no se articulan las exigencias de la ley 1581 con las normas mencionadas en un 57%, se considera en un 91% no existe dentro de la institución el cumplimiento de algún control para hacer más satisfactorio el establecimiento de SGSI. En conclusión, se estima que es de carácter importante el desarrollo del diseño del sistema automatizado mencionado basados en las normas ISO 27001, el cual

brindará mayores controles para manejo de informaciones y permitirá se alinean aspectos requeridos en la ley dentro de la institución.

Bustamante et al., (2021), refirieron como propósito demostrar como la incorporación de las ISO 27001: 2013 y sus políticas incidían en la SGSI de una municipalidad. Se desarrolló una metodología cuantitativa, aplicada, cuya muestra se constituyó por 30 colaboradores, el instrumento aplicado fue el cuestionario. Se identificó como resultados que la incorporación de las ISO 27001: 2013 en las SGSI registraron un 90% de mejoras, siendo los resultados de la prueba de entrada 46% y salida 96%. En conclusión, se destaca que se asume como la presencialidad de una interrelación directa entre las variables de investigación, lo cual ha sido notorio en el antes y después de la aplicabilidad de las ISO 27001en las SGSI.

Arias (2020), se planteó la descripción del empleo de las ISO 27001 dentro del área TI de una empresa. Siendo el enfoque empleado cualitativo, una muestra de 3 trabajadores, se hizo uso de la guía de entrevista como instrumento. Los hallazgos expusieron que la aplicabilidad de estas normas es considerada beneficiosa, porque permite que las informaciones sean resguardadas y a la vez minimizan riegos como posibles sanciones, pérdidas económicas, fidelización del público, estableciéndose procesos como disponibilidad, integridad y lo confidencial de las informaciones. Se concluye que estas normas son muy funcionales y efectivas en su uso para gestionar la seguridad de las informaciones de la empresa, siendo que se fundamenta en tres características estratégicas para su control; disponibilidad, integridad y lo confidencial.

Seguidamente como antecedentes internacionales, se resalta la investigación desarrollada por los autores Shimels and Lessa (2023), los cuales desarrollaron como propósito en su estudio la evaluación de la madurez de SGSI en entidades bancarias. Su metodología se enfocó como cuantitativa, causal, cuyo tamaño muestral abordo 4 bancos que generaron la participación de 110 colaboradores, el cuestionario se utilizó para recoger datos. Entre los hallazgos se logró determinar que el índice de madurez de los bancos era de nivel 2.45, no alcanzando el nivel 3 definido, con respecto a la madurez de los SGSI esta oscila

entre 2.39 a 2.5, siendo el puntaje esperado 5, hallándose una brecha del 50%. En conclusión, se destaca que existe notable debilidad de los SGSI aplicados en los bancos haciéndose necesario la incorporación de los estándares de la ISO 27001 para fortalecer su aplicabilidad y lograr resultados esperados.

Sánchez (2022), desarrollo el establecimiento de una planificación de SGI fundamentado en ISO 27001 de una compañía. La metodología fue cualicuantitativa (mixta), la muestra fue de 675 organizaciones, se empleó para recolectar datos la ficha de observación y las guías de entrevistas. Entre sus resultados se conoció que dentro de la empresa el estatus de aplicación de las SGI es administrado en un 64% y que sus controles son deficientes en un 32%, estableciéndose como riesgos que se pudieran acarrear entre la valoración muy alta una fuga financiera superior a 50000000 de euros y como mínima una perdida inferior a 200mil euros. Se concluye que el establecimiento de una planificación de SGI fundamentada en ISO 27001 sería un recurso de relevancia para la empresa, el cual potenciaría este proceso de gestión de controles de seguridad a siendo de beneficios a la empresa.

Antunes et al., (2022), planteó como propósito la evaluación y mitigación de SGSI de ciberseguridad y seguridad de las informaciones a las PYMES en el marco de las auditorias. Se trato de una investigación con enfoque mixto, cuya muestra fue de 50 organizaciones, se ejecutó el cuestionario y guías de entrevistas para obtener datos. Entre los hallazgos se destacan que un 38% de estas organizaciones tenían más de 60 empleados, así mismo se conoció que el 60% de las empresas aplicaron un proceso de auditoria estándar y el 40% una auditoria completa. También se demostró que SGSI se hace más eficiente cuando se aplica basado en las ISO 27001, debido a todos los controles que facilita y que a la vez permite realizar informes, que pueden ser descargados en formato pdf. Se concluye que dentro de las empresas PYMES los SGSI permiten conducir las auditorias de ciberseguridad siendo estas más productivas al implementar los controles de ISO 27001.

Bokhari and Manzoor (2022), en su estudio plantearon conocer el impacto que tienen los SGSI en las finanzas de empresas. La metodología fue cuantitativa, correlacional, la muestra fue de 600 empresas, se ejecutó el cuestionario para obtener datos. Entre los hallazgos se conoció que el 14% pertenecían al área de fabricación, un 39% bancarias, 40% consultoras contables y 16% TI, donde el 60% tiene entre 1 a 15 años de establecidas. Al respecto, se determinó que la implementación de las SGSI es significativa en el progreso financiero de las empresas ($r = 0,735$, $p < 0,01$). Se concluyó que es de carácter importante aplicar las SGSI en todas las empresas, puesto que la misma otorga herramientas para elevar la eficiencia de las organizaciones, repercutiendo de forma positiva en su desempeño financiero.

Podrecca et al., (2022), planteó como objetivo conocer como la seguridad de información y creación de valor se generan por medio del impacto de las ISO/IEC 27001. Su desarrollo metodológico se fundó como cuantitativo, relacional, donde participaron 143 empresas estado unidense, se operativizo el uso del cuestionario para obtener datos. Entre los resultados, se estableció que dentro de la investigación el mayor número de empresas abordadas eran del área TI/ TIC en el 67%, donde el 100% poseen certificación a estas normas. También se conoció que el poseer esta certificación tiene un efecto positivo en la internalización de las empresas (sig. 0,0320; $p < 0,05$), brinda ganancias anuales (sig. 0,0326; $p < 0,05$) e impulsa la rentabilidad de la empresa (sig. 0,0043 <0,05), también es puntualizado qué al establecerse la interconexión entre las variables se determinó una p mayor a 0,05 y un rho= 0.305 lo que indica que no existe relación. Se concluye que las hizo son pieza fundamental para la creación de valor dentro de la empresa evidenciándose es su rentabilidad sin embargo se conoció qué estás normas no determinan influencia en la seguridad de la información por lo que se requiere sean aplicadas con mayor rigidez.

Kitsios et al., (2022), realizaron un estudio enfocado en el establecimiento de un marco evaluativo de riesgos desarrollado una empresa del rubro tecnológico de las informaciones implementando las ISO 27001 en sus SGSI. Metodológicamente se presentó como cuantitativa, explicativa, tomando (1) una

empresa como muestra, se operativizo el uso del cuestionario y las listas de observaciones para obtener datos. Entre los resultados se hizo el reconocimiento de 309 formas de amanezcas particulares, aplicándose 309 controles, en base a las SGSI todos fortalecidos con las ISO 27001 donde se evidencio una significancia de $p<0.05$, mitigándose un 83% de amenazas y logrando un nivel aceptable de los mismos, asimismo fue minimizando el impacto en el 17% restantes. Se concluyó que las estrategias de los SGSI para atender riesgo dentro de la empresa se vuelven más efectivos cuando se aplican las ISO 27001.

Al-Karaki and Sanaa (2022), se plantearon evaluar los SGSI basados en normas ISO, cuya metodología fue cuantitativa, causal, con una muestra de 25 empresas, se operativizo el uso la encuesta, lista de cotejo. Entre los hallazgos se conoció que según la muestra abordada el 50% desconocía que poseían un SGSI, refiriendo no se establecían formalmente sus políticas y no se comunicaban estas a los colaboradores, el 62% de los conocían sobre el tema ratificaron que este sistema es importante para la empresa y la seguridad de las informaciones. Al relacionarse la variable ISO 27001 con la trazabilidad se hayo $p<0.05$ y $R=0.456$, demostrando una relación media, positiva y significativa. Se ha concluido que los SGSI enfocados en ISO 27001 demostraron cambios sustanciales hacia el mejoramiento del resguardo de datos y las comunicaciones con énfasis en su trazabilidad.

Alsahafi et al., (2022), en su estudio evaluaron en qué medidas se establece el cumplimiento de las ISO 27001 en el contexto educativo del sector universitario con certificaciones otorgadas. Su metodología se enfocó como cuantitativa, cuyo tamaño muestral abordo 29 universidades, los instrumentos aplicados han sido la lista de observación y las entrevistas. Entre los resultados se conoció que el 64% de las empresas certificadas cumplen con NCA-ECC, sin embargo, al valorarse la influencia de las ISO 27001 respecto a SGSI se obtuvo una $p>0.05$ y 69 grados de libertad indicándose que esta no se establece en su dimensión disponibilidad. Se concluyó que dentro de estas organizaciones se debe prestar atención a la aplicación de las normas ISO 27001 para qué estás sean más eficientes en cuanto al a la seguridad de la información.

Mirtsch et al., (2021), se formularon la finalidad de profundizar conocimientos sobre la aplicación de SGSI fundamentados en ISO 27001. Fue cuantitativa, relacional, contó con 125 organizaciones como muestra, se operativizo el uso de los cuestionarios para obtener datos. Los hallazgos determinaron que la aplicación de estas normas dentro del área SGSI mejora notablemente el desempeño general de las empresas TIC y no TIC con una significancia de <0.05 en las siguientes áreas; aumenta la demanda de los clientes, potencia la imagen de la organización, eleva las ventas donde se toma en consideración las certificaciones de las empresas, asimismo se estableció que no se registró mejoras en cuanto a la confiabilidad las informaciones con una sig. 0.075. En conclusión, se logró brindar información comprobada y documentada referente a lo útil de emplear estas normas dentro de este ámbito de resguardo de la información en algunos aspectos evidenciándose limitaciones con respecto a la confiabilidad de los datos.

Gaitero et al., (2021), refirió como finalidad la valoración de la calidad de las certificaciones para la SGSI de PYMES. La metodología fue cuantitativa, causal, en esta se consultó a 26 PYMES, el instrumento fue; encuestas, listas de cotejo, fichas de recojo de dato. Al respecto se halló como resultados que el 50% de los encuestados destacaron que la implementación de las SGSI enfocadas en las ISO 27001 permitieron que las empresas elevaran sus niveles de eficiencia y efectividad en base confiabilidad de los datos, asimismo indicó en un 50% que se pueden notar los resultados obtenidos. Se concluyó que las SGSI enfocadas en las ISO 27001 son una excelente opción para ser aplicadas en el contexto de las PYMES españolas, puesto que su incidencia es positiva y satisfactoria

Mirtsch et al., (2021), cuyo objetivo fue generar información necesaria en cuanto para las incorporaciones de las ISO 27001 en el sector de la minería web. La metodología fue cuantitativa, causal, se trabajó con 2664 organizaciones como muestra, el cuestionario se usó para recabar datos. Entre los resultados se resaltó que el 29,7% de estas organizaciones en su portal refieren su certificación ISO/IEC 27001, comprobándose que su 100% formalmente se encuentran certificadas, un 5,4% manifiestan la intensión de lograr su acreditación con estas normas, asimismo se conoció que un 49% de las empresas certificadas se desempeñan brindando

atención TIC, lo que les permite tener mayor prestigio en su labor. Destacándose entre sus beneficios que poseer certificación les ha posibilitado desarrollar en un 62% más innovaciones en el área TIC que las que no poseen esta condición, en un 72% se proyectan ante los clientes como más rentables. Se concluye que la certificación ISO 27001 en el sector de minería web representa una gran oportunidad para fortalecer las proyecciones de éxito y expansión de estas organizaciones online.

Fonseca-Herrera et al., (2021), planteó el desarrollo de un modelo SGSI fundamentado en ISO 27001. El enfoque fue cuantitativo, la muestra de 69 empresas, se emplearon los cuestionarios y las entrevistas para la obtención de datos. Se conoció que la incorporación de las ISO 27001 no ha demostrado influencia en la mejora de la SGSI dentro del contexto abordado, lo cual se ha reflejado por medio de una $p > 0,05$ y $Z=-7,696_b$. Se concluye qué es necesario que dentro de la empresa los modelos de seguridad de gestión de la información sean reorganizados en pro del favorecimiento de la práctica de ISO 27001.

Zaini et al., (2020), determinó la incidencia de la SGSI en las agilidades organizacionales. cuantitativa, causal, donde se involucró a 250 personas como muestra, el cuestionario se utilizó como instrumento. Entre los resultados, se conoció que la agilidad empresarial, se relaciona significativamente <0.05 con los SGSI, por lo que se aprobó la hipótesis alterna al afirmar la relación entre las variables. Se concluyó que los SGSI son una herramienta fundamental para potenciar el desarrollo de las empresas, pudiendo estas desenvolverse de manera más eficiente y con más celeridad en su contexto.

Fathurohman and Witjaksono (2020), desarrollaron como propósito el establecimiento de la evaluación de los beneficios de la incorporación de ISO 27001: 2013 utilizando ANNEX Control al SGSI. Su metodología se enfocó como cuantitativa, experimental, con la participación de 56 colaboradores de un gobierno distrital en la muestra, se usaron los cuestionarios, fichas de recojo de datos y listas de cotejo para acumular informaciones. Entre los resultados se conoció que las evaluaciones desarrolladas del estudio de brechas al implementar SGSI con las

normas señaladas, mejoran en un 35% el manejo de activos, criptografías, seguridad en comunicación, asimismo se alcanzó un 29% de efectividad en las gestiones operativas de los sistemas, se demostró al obtenerse un valor de p>0.05; -0.237 que las ISO27001 no influyen en la mejora de las SGSI. Se concluyó que a pesar que las ISO27001 se constituyen como una estrategia organizativa para el cumplimiento de normas las mismas no han demostrado mejoras en el contexto de las SGSI.

Morales (2019), planteó el diseño de un Balanced ScoreCard para la gestión de controles de seguridad bajo lineamientos de ISO 27001 en unidades cooperativas de ahorro y crédito. La metodología fue cuantitativa, correlacional, se involucró a 58 colaboradores como participantes, cuestionarios y la lista de cotejo fueron los instrumentos. Como hallazgo se destacó que el 45% de los encuestados han manifestado que no existen lineamientos de política, ni normas de SGSI, el 39% indicó que la información más sensible se respalda por medio de un Cloud Backup. Concluyéndose que el diseño de un Balanced ScoreCard es una herramienta importante para potenciar el resguardo de la SGSI de estas cooperativas.

A continuación, se presentan las bases teóricas del estudio, planteándose la conceptualización de la variable: ISO 27001, donde se destaca que estas son definidas como un modelo aplicativo para garantizar el resguardo de las informaciones organizacionales, por medio del cual se brindan las pautas que se deben tener en cuenta para certificar confidencialidad, integridad y disponibilidad de las informaciones (Akinyemi et al., 2020). Estas ISO, indican una serie de aspectos para posibilitar la protección de las informaciones, la cual es considerada como toda forma, medio, herramienta y metodología que se usa con la finalidad de asegurar los registros de entrada, datos, destrucción, modificación o uso no permitido de ésta, para de esta forma protegerla de personas que busquen hacer un mal uso de las fuentes de infraestructura y estadísticas de dicha empresa (Podrecca and Sartor, 2023).

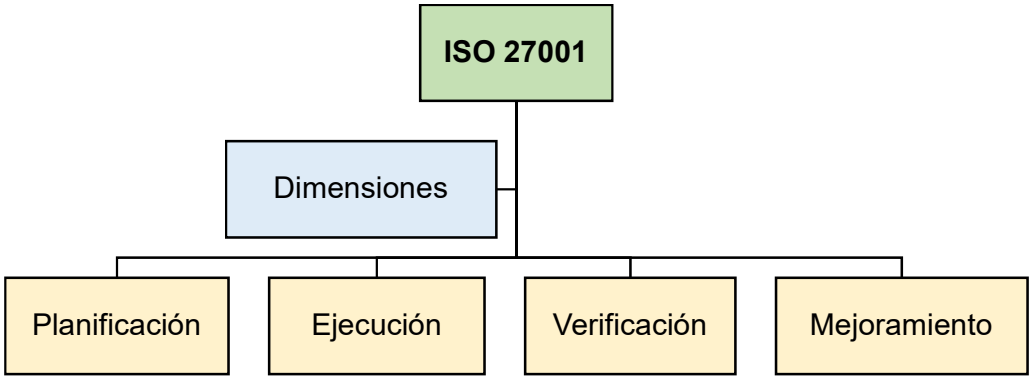
Las ISO 27001, avalan las habilidades que se apliquen, en función de resguardar el manejo de las informaciones (Culot et al., 2021). Esta norma de carácter internacional, se creó con el fin de brindar a las empresas un patrón que admita la implementación, monitoreo, revisión y manejo SGSI, siendo capaz de asegurar, de manera eficiente, la información que allí se maneje (Roy, 2020). Para Quset And Alkilani (2022), ISO 27001 tiene como base fundamental proteger que los datos sean íntegros, estén disponibles y se mantengan confidenciales, apoyando a descubrir las dificultades y los problemas que puedan afectar los hechos, mediante una evaluación de peligro para posteriormente, determinar qué se debe hacer evitando que se lleven a cabo estos obstáculos.

La variable ISO 27001 se explicó a nivel filosófico por medio de la teoría general de sistemas, cuyo mayor representante fue Von (1950), que se basa en el dominio de la investigación de componentes, como también en el reconocimiento de los elementos externos e internos que persiguen el mismo objetivo (Constantino, 2019). Asimismo, Martínez, (2019), asevera que la teoría de sistema tiene analogía, puesto que es un proceso integrador dirigido a un desarrollo directo, con el fin de alcanzar un adecuado beneficio. Esta teoría de sistema se vincula con la variable de estudio, ya que se aplicarán estas las normas, en el proceso de inspección de la SGSI, con el fin de reducir y evitar pérdidas de informaciones, mejorando el manejo de dicha seguridad e incrementando la eficiencia de los trabajadores en las posibles acciones que pongan en peligro tal seguridad (Tatiara et al., 2018). Por medio de la incorporación de estos lineamientos, se busca reducir las pérdidas de información, regular y controlar su uso, evitar posibles ciberataques, optimizar la seguridad e incrementar la competitividad de los trabajadores (Grishaeva, 2021).

Para el estudio de la ISO 27001 como variable de investigación se han desarrollado como dimensiones las siguientes:

Figura 1

Dimensiones de la gestión del manejo de información



Fuente: Elaboración propia

Planificación: involucra los entornos de la empresa, donde se determinan los logros del SGSI por medio del establecimiento de aspectos fundamentales y su cumplimiento (Rincón, 2019). Se trata de un proceso donde se prevén cursos de acciones para el desempeño de la operatividad en la consecución de objetivos propuestos (Alemán, 2023).

Ejecución: se refiere al trabajo realizado para la operativización de las acciones. Se trata de un proceso dinámico que activa la funcionalidad de los procesos planificados (Martín, 2021). Esta dimensión es fundamental para la aplicabilidad de las normas ISO 27001:2013, puesto que se basa en la realización de los temas específicos con respecto al control de seguridad de información (Roy, 2020).

Verificación: señala las exigencias para valorar y estudiar el propósito de la empresa y el establecimiento de la realización de las acciones planificadas y las ejecutadas (Martín, 2021). Este implica al proceso de autenticación que se desarrolla por medio de las normas ISO 27001:2013 el cual permite proteger las informaciones (Martín, 2021).

Mejoramiento: precisa las exigencias para las modificaciones obligatorias en pro de potencializar los procesos de los SGSI, permitiendo corregir los errores realizados hasta llegar a mejorarlos para el adecuado ejercicio de la empresa, teniendo como base la mejora continua (López et al., 2019).

Seguidamente, se plantea la conceptualización de la variable dependiente que refiere a la gestión de la seguridad de la información, que alude a una serie de disposiciones que permiten el resguardo de los datos importantes de las organizaciones, considerados como uno de los activos más relevantes de ellas (Ibarra, 2023). Asimismo, este refiere que es un proceso de conservación de la integridad, disponibilidad y confiabilidad de las informaciones de las empresas (Bokhari and Manzoor, 2022). Indican el establecimiento de un conglomerado de actividades procedimentales y metodológicas que permiten identificar riesgos y plantear alternativas para su reducción y erradicación (Orozova et al., 2019).

En ilación, se asume que el SGSI es de suma importancia para garantizar la protección y legalidad de los datos, ya que admite precisar los controles y tratamientos que se pondrán en marcha para conservar los datos bien resguardados (Ruiz et al., 2022). Asimismo, instaura las políticas que deben conocer y llevar a cabo los miembros de la compañía, para así tener en cuenta cuáles son los problemas que se pueden presentar y de qué forma se llegarán a aplacar (Chen et al., 2022)

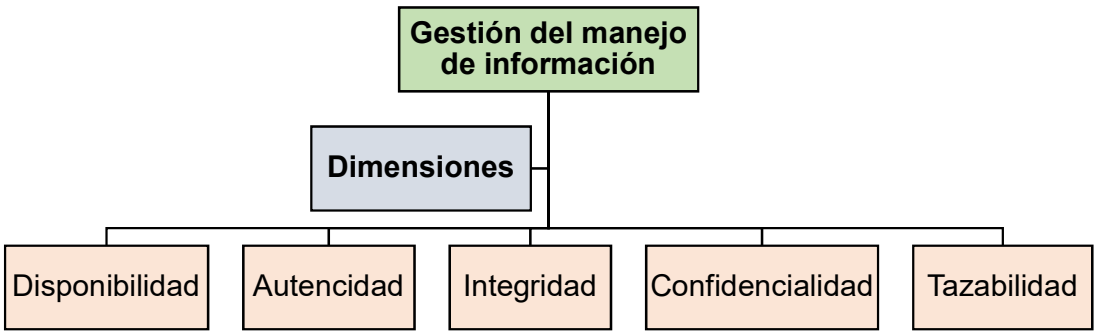
La mencionada variable se explica a nivel filosófico por medio de la teoría de la información, que ha sido planteada por Shannon y Weaver (1940), que está enfocada en el proceso de difusión y procesamiento de la mismas, valorando como se presentan las informaciones y los parámetros que la regulan (Solana-González, 2019). Esta es una teoría de gran relevancia, que busca aplicar una estructuración segura de los sistemas de informaciones y comunicaciones, precaviendo que sus procesamientos sean eficientes (Bolek et al., 2023). Desde esta perspectiva, esta teoría se relaciona con la variable en cuestión, puesto que también se centra en la conducción y trasmisión de las informaciones, enfocándose en que estos sean procesados de la manera más idónea posibles, tratando de evitar situaciones de

riesgo, las cuales pudieran comprometer a la empresa (Annika and Fredrik, 2022). En correspondencia, esta teoría fortalece esta variable, permitiendo optimizar las técnicas presentadas, minimizando coste y resguardando los SGSI (Zuña et al., 2019).

Seguidamente se presentan las dimensiones de la variable, las cuales harán posible su desarrollo y viabilidad

Figura 2

Dimensiones de la gestión del manejo de información



Fuente: Elaboración propia

Disponibilidad: indica la condición que refiere al acceso otorgado, en cuanto al manejo de las informaciones y los sistemas por medio del cual se establece contacto con los datos que se requieren para su revisión o manipulación (Ruiz et al., 2022). La disponibilidad de la información hace referencia que las nóminas estén accesibles cuando lo requieran (Rodríguez et al., 2020). Es fundamental impedir que en el sistema se ocasionen inconvenientes o que cualquier sujeto pretenda tener acceso de forma arbitraria a los programas e información de la empresa (Bokhari and Manzoor, 2022).

Integridad: busca proteger los datos libres de cambios no permitidos (Bolek et al., 2023). Para una compañía, la integridad es resguardar adecuadamente la información tal como se funda, sin que sea manipulada o alterada por personas no autorizadas (Ruiz et al., 2022). La integridad de las informaciones de las

organizaciones se fundamenta en las habilidades necesarias que avalen el resguardo, y que se cuente con el apoyo suficiente de los datos (Somepalli et al., 2020). La información inscrita debe ser la correcta y adecuada, no tener errores o cualquier tipo de manipulación, la transparencia de la información está referida a la veracidad de los mismos (Barafort And Mesquida, 2017).

Confidencialidad: refiere a un proceso de privacidad de las informaciones de una empresa y a su debido resguardo. Siendo su preservación importante para certificar que la información privada o secreta no sea divulgada o revelada a personas no autorizadas (Ruiz et al., 2022). Este requerimiento es aplicable mediante el acopio, transferencia y procesamiento de los datos (Topa and Karyda, 2019). En la confidencialidad, la información manejada solo será aprovechada por las personas autorizadas, por lo tanto, ésta no debe ser operada ni manipulada por personal ajeno a la empresa (Ključnikov et al., 2023).

Autenticidad: esta toma en cuenta que la información proporcionada sea directamente de los usuarios o entes encargados de su manejo (Duval et al., 2022). La cual debe ser verificada para asegurarse que los datos suministrados sean precisos (Manas and Sarbeswar, 2020). En la autenticidad de la información, pueden ocurrir alteraciones en el origen de los datos, siendo que por medio de los sistemas de gestión de información se prevean elementos para garantizar este proceso (Annika and Fredrik, 2022).

Trazabilidad: indica el control que se tendrá sobre las informaciones y su desarrollo partiendo desde su línea inicial de tiempo hasta sus últimas modificaciones (Zambrano-Izurieta et al., 2023). Refiere a todas las operaciones predeterminadas e independientes que admitan saber la historia, trayectoria y ubicación de los activos de información, lo que consiste en ejecutar un rastreo de estos desde su elaboración hasta la recepción final, luego de atravesar todas las etapas de transporte logístico necesario (Chen, 2022). La trazabilidad es primordial para examinar los sucesos y reconocer a las posibles amenazas hacia estos activos (Solana-González et al., 2019).

III. METODOLOGÍA

3.1 Tipo y diseño de investigación

Tipo de Investigación

Este ha sido desarrollado como básico, también conocida con el calificativo de pura, siendo aquella que busca producir saberes y conocimientos científicos a nivel conceptual y teórica referente al fenómeno abordado (Arias, 2019). Esta brindó la oportunidad de ampliar el marco referencial de las variables desarrollas, ofreciendo un enfoque actulizado.

Enfoque de Investigación

Se trató del cuantitativo, al emplearse de manera sistemática la incorporación del lenguaje cuantificable, estableciéndose un sistema de hipótesis para su verificación o rechazo (Hernández-Sampieri y Mendoza, 2018). Siendo este un aspecto fundamental, porque las variables de estudio requirieron ser valoradas para lograr la obtención de resultados y plantear de manera óptima conclusiones y recomendaciones respectivas.

Nivel de investigación

Se ha empleado como nivel el correlacional causal, puesto que se busca conocer la asociación o relaciones que se generan entre las variables abordadas (Hernández-Sampieri y Mendoza, 2018). En relación al estudio propuesto, este nivel se mostró como el más acertado para brindar respuesta al objetivo planteado, siendo capaz de satisfacer la interrogante de investigación, posibilitando generar respuesta coherente a esta realidad.

Diseño de investigación

Se gestó como no experimental, refiriéndose al diseño que excluye en su ejecución el control intencional y deliberado del fenómeno de estudio, debido a que se busca que estas sean estudiadas en su contexto natural, tal cual se presentan en su cotidianidad (Arias, 2020). En consideración, se indicó que se desarrolló un corte

transversal, por tomarse como referencia para el desarrollo del estudio una única unidad de tiempo (Baena, 2017).

3.2 Variables y operacionalización

Variable independiente: ISO 27001

Definición conceptual: Indica un modelo aplicativo para garantizar la SGSI de una organización, por medio del cual se brindan las pautas que se deben tener en cuenta para proteger la disponibilidad, confidencialidad e integridad de las informaciones (Akinyemi et al., 2020).

Definición operacional: ISO27001, se valoró por medio de la implementación de un instrumento que posee un total de 25 ítems, el cual abordó 4 dimensiones; planificación (16 ítems), ejecución (3 ítems), verificación (3 ítems) y mejoramiento (3 ítems), en una escala de likert, tipo ordinal.

Indicadores: Liderazgo, planeamiento, soporte, operaciones, evaluaciones de desempeño, mejora- continua.

Escala de medición: Ordinal

Variable dependiente: Gestión de la seguridad de la información

Definición conceptual: Se comprende como una serie de disposiciones, políticas y normas que permiten el resguardo de los datos importantes de las organizaciones, los cuales son considerados como uno de los activos más relevantes de ellas (Ibarra, 2023).

Definición operacional: Esta se valoró a través del empleo de un cuestionario, que posee un total de 24 preguntas, el cual aborda 5 dimensiones; disponibilidad

(5 ítems), autenticidad (5 ítems), integridad (4 ítems), confidencialidad (5 ítems) y mejora continua (3), en una escala de likert, tipo ordinal.

Indicadores:

Estabilidad de red, acceso 24 horas, capacidades tecnológicas, anchos de banda, controles de los usuarios, políticas de seguridad, administración de equipos, vulnerabilidad de las informaciones, protección de datos, copia de seguridad, soporte técnico, administración del sistema, políticas institucionales, seguimiento de procesos, privilegios de acceso, y rastreo de usuario.

Escala de medición: Ordinal

Operacionalización de las variables

Esta refiere al proceso que se desarrolló para la definición de cada una de las variables del estudio, en función de la medición de sus diversas caracterizaciones. Con respecto al presente estudio, este instrumento permitió se establezcan cada una de las variables que se abordaron como foco de interés, especificando sus definiciones conceptuales, operacionales, dimensiones, indicadores, ítems y escalas de mediciones (ver anexo 1).

3.3 Población, muestra y muestreo

Población: Esta hace alusión a la totalidad de la unidad de estudio abordada, la cual guarda coincidencia en cuanto a su delimitación tiempo y espacio (Maldonado, 2018). En correspondencia este estudio, estuvo constituido por 31 personas que prestan servicio en el área mencionada de la empresa en cuestión, en Lima, durante el 2023.

Muestra: Esta indicó a un fragmento de la población, la cual ha sido asumida como representativa por poseer las mismas características distintivas, pudiendo ser los generalizados los resultados obtenidos (Arias, 2020). La muestra del estudio ha sido de 31 personas que prestan servicio en el área mencionada de la empresa en

cuestión, en Lima, durante el 2023. Tomándose la totalidad de la población por considerarse un número reducido y manejable.

Muestreo: El muestreo indicó el procedimiento que se desarrolla para hacer posible el cálculo de la muestra (Baena, 2017). Para efectos del estudio, se aplicó el muestreo no probabilístico, en su tipología censal, procediéndose a validar la totalidad de la población como muestra, al considerarse pequeña (31 trabajadores) y manejable, teniendo acceso a ella y disponibilidad.

3.4 Técnicas e instrumentos de recolección de datos

Técnica: En esta ocasión se emplearon las encuestas, las cuales posibilitaron se recojan datos de manera organizada dentro de un proceso de investigación, haciendo foco de atención al objeto de estudio (Maldonado, 2018).

Instrumento: Fue empleado el cuestionario, que refirió a una estructura estandarizada de manera coherente, precisa y sistemática, que se centró en plantear preguntas que permitieran cumplir con los objetivos de investigación (Arias, 2019).

En correspondencia con la presente investigación se aplicaron dos cuestionarios, uno para cada variable, los cuales a continuación se describen:

Para la variable; ISO27001, se empleó el cuestionario desarrollado por Alemán (2023), de procedencia peruana, el cual fue adaptado por el investigador. Este presentó como propósito; evaluar la implementación de las ISO27001. Este instrumento se encontró estructurado por un total de 25 preguntas, el cual abordó 4 dimensiones; Planificación (16 ítems), ejecución (3 ítems), verificación (3 ítems) y mejoramiento (3 ítems), en una escala de likert, tipo ordinal, donde se estimó un tiempo de aplicación de 15 minutos aproximados, siendo administrado de manera grupal e individual.

La validez del instrumento es un proceso riguroso que se desarrolla en función de medir la precisión, claridad y coherencia del instrumento de acuerdo a

los objetivos planteados, siendo reconocidos como aplicables (Pino, 2018). Para efectos del estudio, se menciona que fue desarrollada en su versión original a través del juicio de experto, donde se consultó a tres profesionales de gran experiencia en la materia y con capacidad de desarrollar dicha evaluación, en cuanto a; claridad, pertinencia y relevancia, siendo valorado finalmente como aplicable. Los especialistas que validaron el instrumento fueron; Dr. Frank Acuña, Mg. Giancarlo Sánchez, Mg. Juan Pérez.

En cuanto a la adaptación desarrollada por el investigador, la validación se desarrolló por medio del juicio de expertos, participando tres especialistas en la materia, los cuales se mencionan a continuación; Dr. Marlon Acuña, Mg. Walter Pérez y Mg. Carlos Huerta, determinando el instrumento como aplicable.

La confiabilidad es un procedimiento que se realiza para valorar la fiabilidad del instrumento a ser aplicado, lo que permitió conocer si este brinda confianza para que se recaben datos capaces de dar respuesta al problema planteado (Baena, 2017). La confiabilidad del instrumento mencionado en su presentación original, para la variable dependiente, fue calculada por el coeficiente alfa cronbach, una vez aplicada una prueba piloto a 10 trabajadores, cuyos resultados arrojaron un índice de .938, siendo este calificado como muy confiable. Respecto la confiabilidad desarrollada por el investigador, esta se desarrolló por medio del alfa cronbach, estableciéndose inicialmente un piloto de prueba constituido por 15 integrantes de la población objeto de estudio, obteniéndose un índice de .903, el cual es considerado con una fiabilidad excelente.

Referente a la variable, denominada; gestión de la seguridad de la información se utilizó el instrumento realizado por Ibarra (2023), con procedencia peruana, el cual ha sido adaptado por el investigador, cuyo objetivo fue estudiar el SGSI de una organización. Este cuestionario estuvo estructurado por un total de 24 preguntas, el cual abordó 5 dimensiones; Disponibilidad (5 ítems), autenticidad (5 ítems), integridad (4 ítems), confidencialidad (5 ítems) y trazabilidad (5), en una escala de likert, tipo ordinal, donde se estima un tiempo de aplicación de 15 minutos aproximados, siendo administrado de manera grupal e individual.

La validación del instrumento original fue desarrollada empleando el juicio de experto, donde se consultó a tres ingenieros de gran experiencia en la materia y con capacidad de desarrollar dicha evaluación, donde se tomó en referencia la claridad, pertinencia y relevancia, siendo valorado finalmente como aplicable. Los especialistas que validaron el instrumento fueron; Dr. Pedro Lezama, Dr. Marlo Acuña, Dr. Elvis Ponte.

En cuanto a la adaptación desarrollada por el investigador, la validación se desarrolló utilizando el juicio de expertos, participando tres especialistas en la materia, los cuales se mencionan a continuación; Dr. Marlon Acuña, Mg. Walter Pérez y Mg. Carlos Huerta, determinando el instrumento como aplicable.

En cuanto a la confiabilidad del cuestionario en su formato original, para la variable dependiente, se operativizó un procesamiento estadístico basado en el alfa cronbach, aplicándose para ello una prueba piloto a 15 trabajadores, cuyos resultados arrojaron un índice de .859, siendo este calificado como bueno y confiable. Respecto la confiabilidad desarrollada por el investigador, esta se desarrolló por medio del alfa cronbach, estableciéndose inicialmente un piloto de prueba constituido por 15 integrantes de la población objeto de estudio, obteniéndose un índice de .887, el cual es considerado con una fiabilidad excelente.

3.5 Procedimiento

Para el abordaje de este estudio, se pidió autorización a la gerencia de TI de la empresa industrial, donde se expuso por medio de un oficio escrito, las motivaciones del estudio, el tema, objetivos, posibles beneficios y justificaciones, asimismo se expresó que se abordaría el Área TI como población objetivo, aclarando respecto a la incorporación de la figura del consentimiento informado, el cual debe ser firmado por cada colaborador para demostrar su participación voluntaria, debido a que esta será libre, decidiendo ellos de manera personal responder los cuestionarios aplicados. También se aclaró que estos instrumentos se aplicarían de manera presencial.

Una vez recibido la permisología correspondiente por parte de la coordinación gerencial de esta área, se procedió a tener contacto con los posibles

participantes, recabando informaciones importantes, referente a datos requeridos para sustentar la investigación. Siendo que por medio de este acercamiento se explicó el motivo del estudio y se invitó a los 31 colaboradores a participar, explicándose que los datos serian manejados siguiendo el cumplimiento de la confidencialidad, anonimato, beneficencia y no maleficiencia. De esta forma, se procedió a entregar el consentimiento informado para su firma y posterior a ello se aplicarán los instrumentos. Al finalizar la recabación de datos se tabularon los mismos y se procesaron para su respectivo análisis y procesamiento estadísticos.

3.6 Método de análisis de datos

En correspondencia se hace necesario mencionar que los datos que han sido producto de la indagación emprendida, fueron tabulados en una hoja de excel, de forma organizada, siendo exportados posteriormente al programa SPSS versión 27, donde inicialmente se desarrolló un análisis descriptivo de los datos, los cuales se plasmaron por medio de cuadros y gráficos estadísticos de frecuencias absolutas y porcentuales.

Posteriormente se planteó el análisis inferencial para el cual inicialmente se calculó la normalidad de los datos, aplicando kolmogorov Smirnov, al considerarse que se trata de una totalidad muestral mayor a 30. Una vez conocida sus resultados se indicó que la naturaleza de los datos correspondía a una un tipo de distribución que ha sido calificada como no normal, aplicándose pruebas no paramétricas para determinar cómo influyó una variable con respecto a la otra, siendo por ello que se aplicó la regresión lógica para la determinación de los diferentes objetivos planteados, lo que también permitió el desarrollo del proceso de contrastación de hipótesis, por medio del cual se rechazaron y aprobaron algunos supuesto expresado a través la hipótesis nula o alterna.

3.7 Aspectos éticos

Durante el proceso de estudio, han sido considerados primordialmente el aspecto de autenticidad como principio ético existente en dicho estudio, puesto que éste se fundamentó en la recolección e indagación de información para sostener el desarrollo de las variables y dar a conocer las fuentes oportunas que beneficiaron

el progreso de la investigación. Siendo las fuentes bibliográficas correctamente citadas, según lo estipulado por los parámetros de la American Psychological Association (APA) séptima (7ma) edición, pudiéndose comprobar la autoría de los aportes teóricos citados. Sin embargo, para estar aún más seguros que no se ha cometido ningún tipo de plagio en el desarrollo de la investigación, se sometido el contenido del estudio a una revisión ejecutada a través del programa “turnitin”, el cual fue el determinante para constatar la originalidad del mismo. De igual manera, se resaltaron valores como el respeto, a las normas que se reflejan en documentos tan valiosos como la Resolución de Consejo Universitario N° 0470-2022/UCV, donde existe un establecimiento formal del código de ética en investigación de la Universidad Cesar Vallejo, según el oficio N° 0283-2022.

IV. RESULTADOS

4.1 Estadística Descriptiva

Se visualiza el desarrollo de la presentación de los resultados descriptivos, en los que se presentan tablas y gráficos estadísticos en los que se plasman frecuencias absolutas y porcentuales de los niveles de cada variable y sus dimensiones.

Variable 1: ISO 27001

Tabla 1

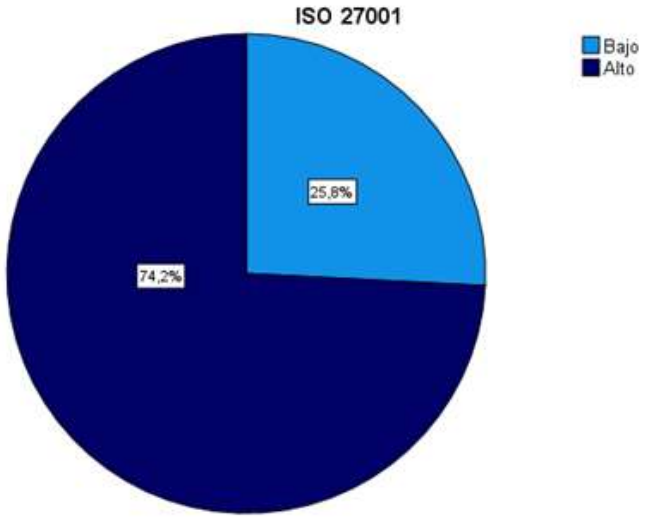
Nivel de la variable ISO 27001

		Frecuencia	Porcentaje
Válido	Bajo	8	25,8
	Alto	23	74,2
	Total	31	100,0

Por medio de la tabla 1, figura 3, se visualiza que la variable ISO 27001 ha sido calificada por los colaboradores del área TI de una empresa industrial con un nivel alto en un 74.2%, asimismo un 25.8% lo valoro como bajo

Figura 3

Nivel de ISO 27001



Dimensiones de la variable ISO 27001

Dimensión: planificación

Tabla 2

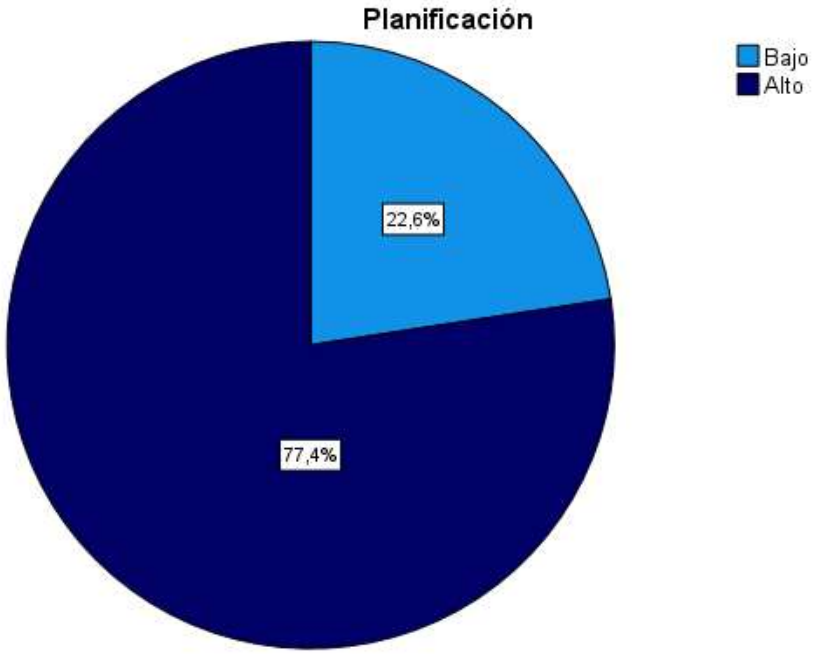
Nivel de la planificación

		Frecuencia	Porcentaje
Válido	Bajo	7	22,6
	Alto	24	77,4
	Total	31	100,0

Por medio de la tabla 2, figura 4, se visualiza que la dimensión planificación ha sido calificada por los colaboradores del área TI de una empresa industrial con un nivel alto en un 77.4%, asimismo un 22.6% se valoró como nivel bajo.

Figura 4

Nivel de la planificación



Dimensión: ejecución

Tabla 3

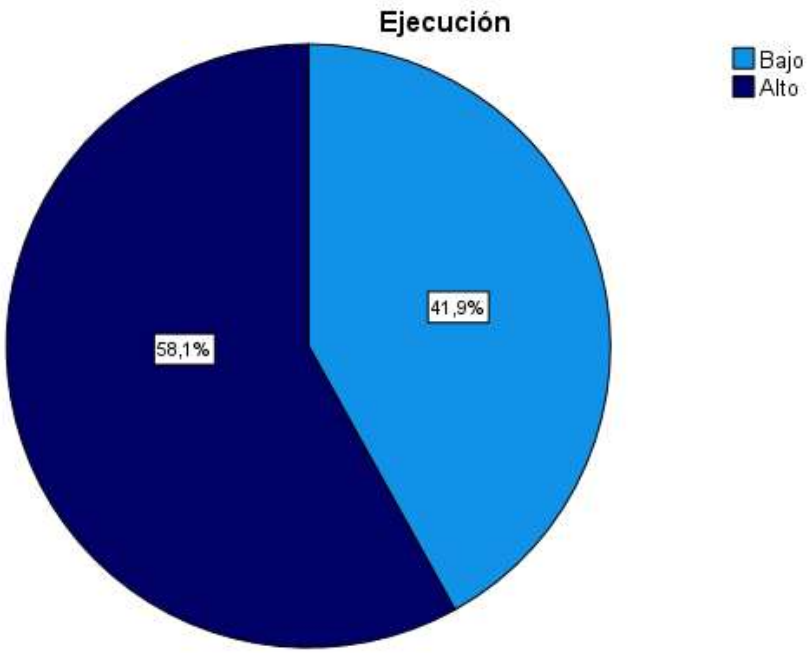
Nivel de la ejecución

		Frecuencia	Porcentaje
Válido	Bajo	13	41,9
	Alto	18	58,1
	Total	31	100,0

Por medio de la tabla 3, figura 5, se visualiza que la dimensión ejecución ha sido calificada por los colaboradores del área TI de una empresa industrial con un nivel alto en un 58.1%, asimismo un 41.9% se valoró como nivel bajo

Figura 5

Nivel de la ejecución



.

Dimensión: verificación

Tabla 4

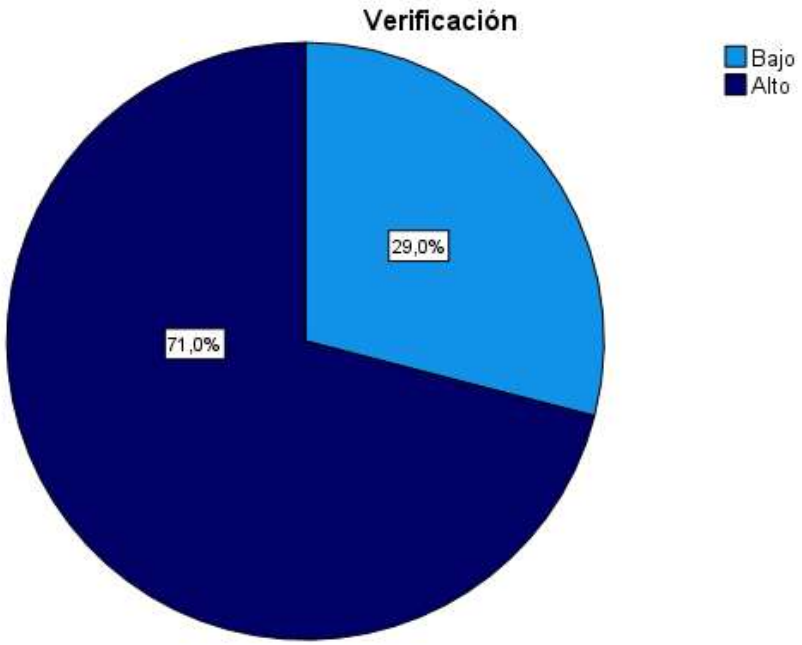
Nivel de la verificación

		Frecuencia	Porcentaje
Válido	Bajo	9	29,0
	Alto	22	71,0
	Total	31	100,0

Por medio de la tabla 4, figura 6, se visualiza que la dimensión verificación ha sido calificada por los colaboradores del área TI de una empresa industrial con un nivel alto en un 71%, asimismo un 29% se valoró como nivel bajo.

Figura 6

Nivel de la verificación



Dimensión: mejoramiento

Tabla 5

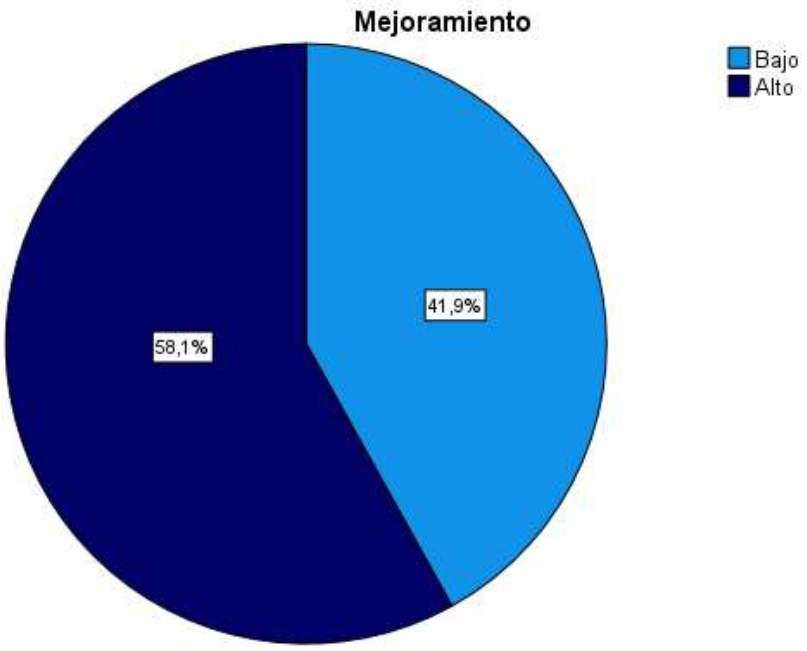
Nivel de mejoramiento

		Frecuencia	Porcentaje
Válido	Bajo	13	41,9
	Alto	18	58,1
	Total	31	100,0

Por medio de la tabla 5, figura 7, se visualiza que la dimensión mejoramiento ha sido calificada por los colaboradores del área TI de una empresa industrial con un nivel alto en un 58.1%, asimismo un 41.9% se valoró como nivel bajo.

Figura 7

Nivel de mejoramiento



Variable 2: Gestión de Seguridad de la Información

Tabla 6

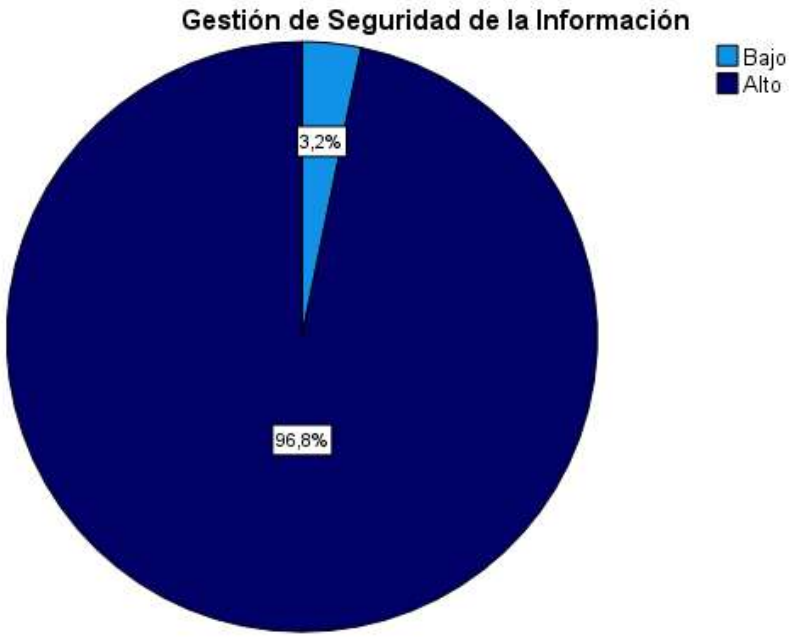
Nivel de la variable Gestión de Seguridad de la Información

		Frecuencia	Porcentaje
Válido	Bajo	1	3,2
	Alto	30	96,8
	Total	31	100,0

Por medio de la tabla 6, figura 8, se visualiza que esta variable ha sido calificada por los colaboradores del área TI de una empresa industrial con un nivel alto en un 96.8%, asimismo un 3.2% se valoró como nivel bajo.

Figura 8

Nivel de la variable Gestión de Seguridad de la Información



Dimensiones de la Variable Gestión de Seguridad de la Información

Dimensión: disponibilidad

Tabla 7

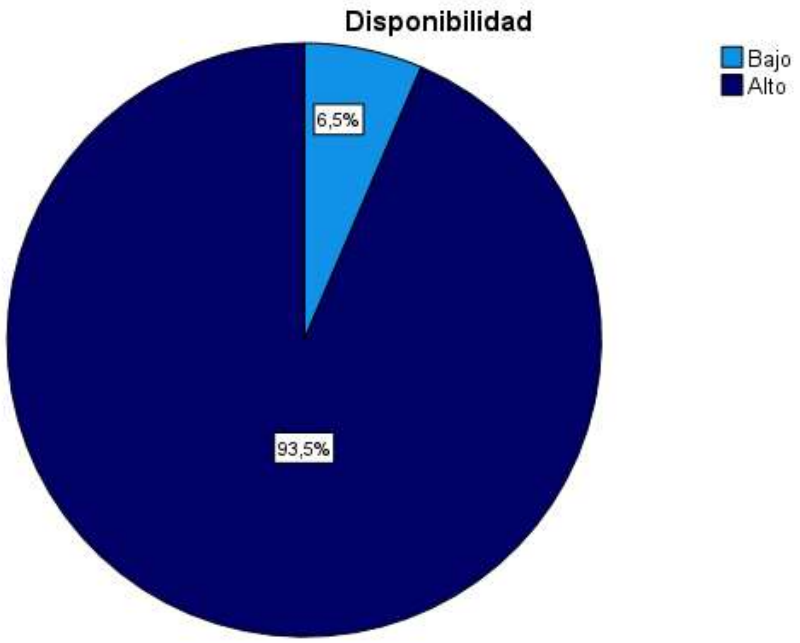
Nivel de la disponibilidad

		Frecuencia	Porcentaje
Válido	Bajo	2	6,5
	Alto	29	93,5
	Total	31	100,0

Por medio de la tabla 7, figura 9, se visualiza que la dimensión disponibilidad ha sido calificada por los colaboradores del área TI de una empresa industrial con un nivel alto en un 93.5%, asimismo un 6.5% se valoró como nivel bajo.

Figura 9

Nivel de la disponibilidad



Dimensión: autenticidad

Tabla 8

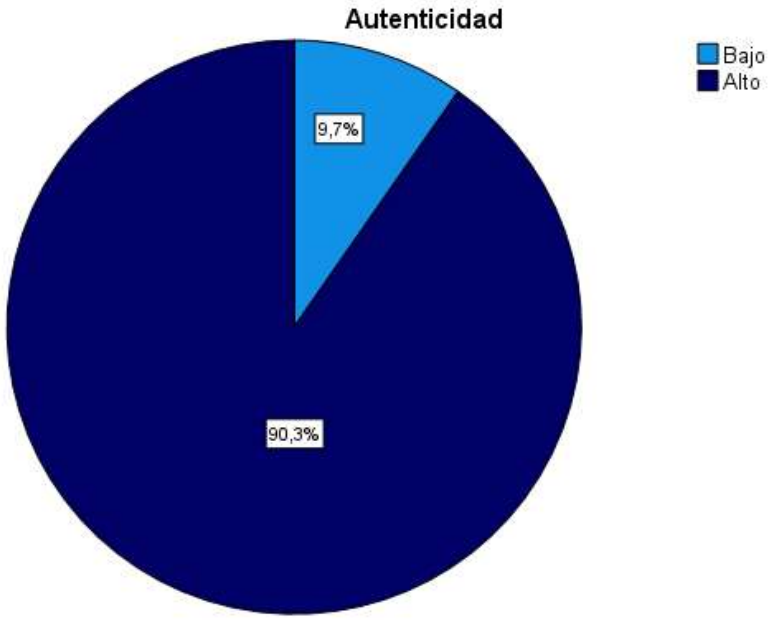
Nivel de la autenticidad

		Frecuencia	Porcentaje
Válido	Bajo	3	9,7
	Alto	28	90,3
	Total	31	100,0

Por medio de la tabla 8, figura 10, se visualiza que la dimensión Autenticidad ha sido calificada por los colaboradores del área TI de una empresa industrial con un nivel alto en un 90.3%, asimismo un 9.7% se valoró como nivel bajo.

Figura 10

Nivel de la Autenticidad



Dimensión: integridad

Tabla 9

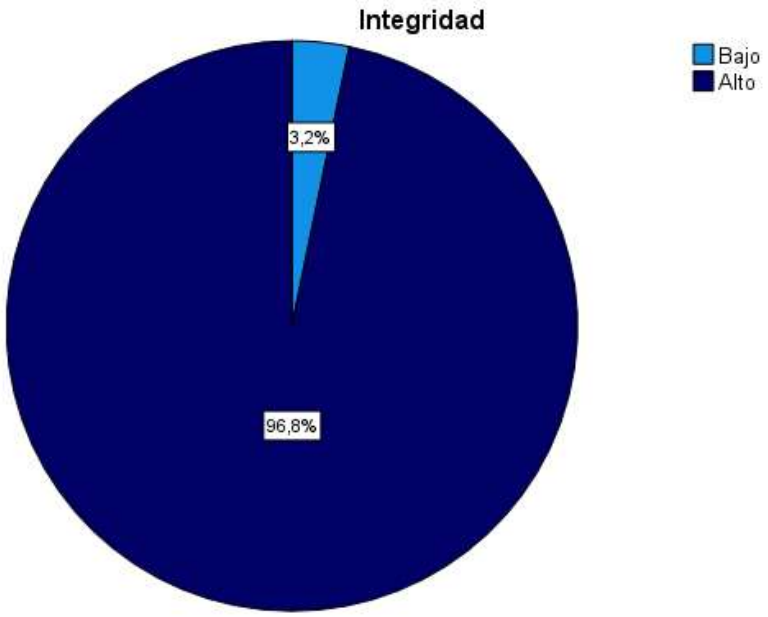
Nivel de la integridad

		Frecuencia	Porcentaje
Válido	Bajo	1	3,2
	Alto	30	96,8
	Total	31	100,0

Por medio de la tabla 9, figura 11, se visualiza que la dimensión integridad ha sido calificada por los colaboradores del área TI de una empresa industrial con un nivel alto en un 96.8%, asimismo un 3.2% se valoró como nivel bajo.

Figura 11

Nivel de la n integridad



Dimensión: confidencialidad

Tabla 10

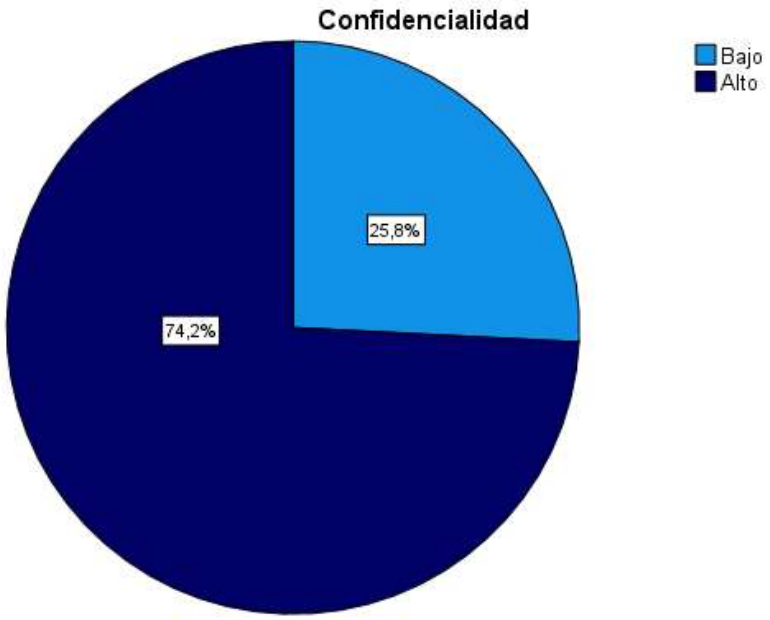
Nivel de la confidencialidad

		Frecuencia	Porcentaje
Válido	Bajo	8	25,8
	Alto	23	74,2
	Total	31	100,0

Por medio de la tabla 10, figura 12, se visualiza que la dimensión confidencialidad ha sido calificada por los colaboradores del área TI de una empresa industrial con un nivel alto en un 74.2%, asimismo un 25.8% se valoró como nivel bajo.

Figura 12

Nivel de la confiabilidad



Dimensión: trazabilidad

Tabla 11

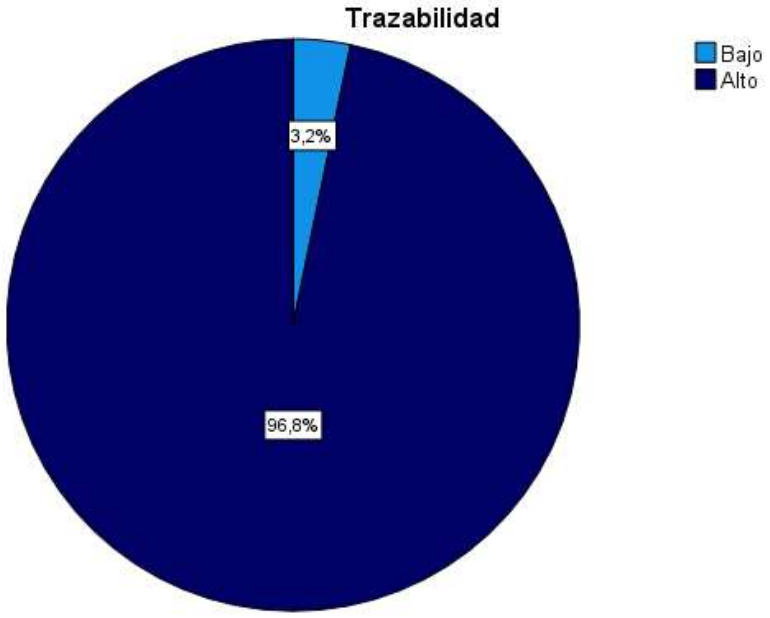
Nivel de la trazabilidad

		Frecuencia	Porcentaje
Válido	Bajo	1	3,2
	Alto	30	96,8
	Total	31	100,0

Por medio de la tabla 11, figura 13, se visualiza que la dimensión trazabilidad ha sido calificada por los colaboradores del área TI de una empresa industrial con un nivel alto en un 96.8%, asimismo un 3.2% se valoró como nivel bajo.

Figura 13

Nivel de la trazabilidad



4.2 Resultados Inferenciales

4.2.1 Prueba de normalidad

Tabla 12

Prueba de normalidad Kolmogorov-Smirnov hipótesis general

	Estadístico	gl	Sig.
ISO 27001	,143	31	,107
Gestión de Seguridad de la Información	,117	31	,200*

La tabla 12, exhiben los hallazgos estadísticos referentes al cálculo de la distribución de los datos refrentes a las variables acontecidas, donde se visualizó un índice de significancia estadística mayor a >0.05, el cual permitió se aceptará la H_0, donde se estableció la normalidad de los datos dejando como constancia de la dinámica de los mismos.

Tabla 13

Prueba de normalidad Kolmogorov-Smirnov hipótesis especifica 1

	Estadístico	gl	Sig.
ISO 27001	,143	31	,107
Disponibilidad	,203	31	,002

Se observan en la tabla 13, los hallazgos reflejados por medio del calculó estadístico de la normalidad, hallándose un índice de significancia >0.05 para la variable ISO 27001 y <0.05 para la dimensión disponibilidad, rechazándose la H_0 lo que ha posibilitado asumir que no existe normalidad de la disposición de los datos suministrados al respecto.

Tabla 14

Prueba de normalidad Kolmogorov-Smirnov hipótesis especifica 2

	Estadístico	gl	Sig.
ISO 27001	,143	31	,107
Autenticidad	,131	31	,190

La tabla 14, muestra los hallazgos reflejados por medio del cálculo de la normalidad de los datos, en la cual se reseñó una significancia >0.05 para las variables, aceptándose la H_0 lo que ha posibilitado asumir la normalidad de la disposición de los datos suministrados al respecto.

Tabla 15

Prueba de normalidad Kolmogorov-Smirnov hipótesis especifica 3

	Estadístico	gl	Sig.
ISO 27001	,143	31	,107
Integridad	,203	31	,002

Se observan en la tabla 15, los hallazgos reflejados por medio del cálculo de la normalidad de los datos, indican una significancia >0.05 para la variable ISO 27001 y <0.05 para la dimensión integridad, rechazándose la H_0 lo que ha posibilitado asumir que no existe normalidad de la disposición de los datos suministrados al respecto.

Tabla 16

Prueba de normalidad Kolmogorov-Smirnov hipótesis especifica 4

	Estadístico	gl	Sig.
ISO 27001	,143	31	,107
Confidencialidad	,313	31	,000

Se observan en la tabla 16, los hallazgos reflejados por medio de la aplicabilidad de prueba en cuestión, indican que se obtuvo una significancia >0.05 para la variable ISO 27001 y <0.05 para la dimensión confidencialidad, rechazándose la H_0 lo que ha posibilitado asumir que no existe normalidad en la disposición de los datos suministrados al respecto.

Tabla 17

Prueba de normalidad Kolmogorov-Smirnov hipótesis especifica 5

	Estadístico	gl	Sig.
ISO 27001	,143	31	,107
Trazabilidad	,127	31	,200*

Se observan en la tabla 17, los resultados de la normalidad de los datos, los cuales dejan al descubierto una significancia >0.05 para las variables, aceptándose la H_0 donde se establece que los datos poseen una distribución normal

4.2.2 Contrastación de hipótesis

a) Contrastación de la hipótesis general

H_1= ISO 27001 SI influye significativamente en la gestión de la seguridad de la información en el área TI de una empresa industrial, Lima 2023

H_0= ISO 27001 NO influye significativamente en la gestión de la seguridad de la información en el área TI de una empresa industrial, Lima 2023

Tabla 18

Información de ajuste del modelo para la hipótesis general

Información de ajuste del modelo				
	Criterios de ajuste de modelo	Pruebas de la razón de verosimilitud		
Modelo	Logaritmo de la verosimilitud -2	Chi-cuadrado	gl	Sig.
Sólo intersección	11,665			
Final	6,070	5,594	1	,018

En cuanto a la tabla 18, se visualiza una significancia <0.05, lo que permite indicar que los hallazgos referenciados se ajustan al modelo de regresión lógica, donde se señala una influencia de la variable Principal con relación a la variable secundaria, desarrollada dentro del área empresarial que ha sido tomada como referente de estudio.

Tabla 19

Prueba Pseudo R cuadrado de la V1 en la V2

Pseudo R cuadrado	
Cox y Snell	,165
Nagelkerke	,220
McFadden	,130

La tabla 19, destaca un coeficiente de Nagelkerke que permite establecer que la variable las ISO 27001 influye en un 22% en la gestión de la seguridad de la información de la población objeto de abordaje.

Tabla 20

Estimaciones de parámetro de la influencia de la V1 en la V2

Gestión de Seguridad de la Información[a]		B	Desv. Error	Wald	gl	Sig.	Exp(B)	95% de intervalo de confianza para Exp(B) Límite inferior	Límite superior
Bajo	Intersección	-,875	,532	2,705	1	,100			
	[ISO 27001=1]	1,792	,796	5,069	1	,024	6,000	1,261	28,547
	[ISO 27001=2]	0[b]	.	.	0	.	.	.	.

En la tabla 20, referida a las estimaciones de parámetro de la influencia de la V1 en la V2, se visualiza una significancia <0.05, validando la veracidad de la H_1 que refiere a que la variable principal SI influye significativamente en la variable secundaria del estudio, desarrollada dentro del área empresarial que ha sido tomada como referente de estudio.

b) Contrastación de la primera hipótesis especifica

H_1= ISO 27001 SI influye significativamente en la disponibilidad de la información en el área TI de una empresa industrial, Lima 2023

H_0= ISO 27001 NO influye significativamente en la disponibilidad de la información en el área TI de una empresa industrial, Lima 2023

Tabla 21

Información de ajuste del modelo para la primera hipótesis especifica

Información de ajuste de los modelos				
	Criterios de ajuste de modelo	Pruebas de la razón de verosimilitud		
Modelo	Logaritmo de la verosimilitud -2	Chi-cuadrado	gl	Sig.
Sólo intersección	11,412			
Final	6,046	5,366	1	,021

En cuanto a la tabla 21, se visualiza una significancia <0.05, lo que permite indicar que los hallazgos referenciados se ajustan al modelo de regresión lógica, donde se señala que si influye la variable ISO 27001 en la disponibilidad de la información de la población objeto de estudio.

Tabla 22

Prueba Pseudo R cuadrado de la V1 en la V2

Pseudo R cuadrado	
Cox y Snell	,159
Nagelkerke	,214
McFadden	,127

La tabla 22, resalta un coeficiente de Nagelkerke que permite establecer que la variable las ISO 27001 SI influye en un 21.4% en la disponibilidad de la información en el área TI mencionada.

Tabla 23

Estimaciones de parámetro de la influencia de la V1 en la V2

Gestión de Seguridad de la Información[a]		B	Desv. Error	Wald	gl	Sig.	Exp(B)	95% de intervalo de confianza para Exp(B) Límite inferior	Límite superior
Bajo	Intersección	-1,179	,572	4,249	1	,039			
	[ISO 27001=1]	1,766	,799	4,891	1	,027	5,850	1,222	27,994
	[ISO 27001=2]	0[b]	.	.	0	.	.	.	.

En la tabla 23, referida a las estimaciones de parámetro de la influencia de la V1 en la V2, se visualiza una significancia <0.05, lo que permite asumir que ISO 27001 influye de manera significativa en la dimensión de la variable secundaria que ha sido valorada dentro del área empresarial que ha sido tomada como referente de estudio.

c) Contrastación de la segunda hipótesis especifica

H_1= ISO 27001 SI influye significativamente en la autenticidad de la información en el área TI de una empresa industrial, Lima 2023

H_0= ISO 27001 NO influye significativamente en la autenticidad de la información en el área TI de una empresa industrial, Lima 2023

Tabla 24

Información de ajuste del modelo para la segunda hipótesis especifica

Información de ajuste de los modelos				
	Criterios de ajuste de modelo	Pruebas de la razón de verosimilitud		
Modelo	Logaritmo de la verosimilitud -2	Chi-cuadrado	gl	Sig.
Sólo intersección	6,399			
Final	6,391	,009	1	,925

En cuanto a la tabla 24, se determina una significancia >0.05, lo que permite indicar que los hallazgos referenciados no se ajustan al modelo de regresión lógica, donde se señala que la ISO 27001 no influye en la autenticidad de la información del área empresarial en cuestión. Estableciéndose la aceptación de la variable nula.

d) Contrastación de la tercera hipótesis especifica

H_1= ISO 27001 SI influye significativamente en la integridad de la información en el área TI de una empresa industrial, Lima 2023

H_0= ISO 27001 NO influye significativamente en la integridad de la información en el área TI de una empresa industrial, Lima 2023

Tabla 25

Información de ajuste del modelo para la tercera hipótesis especifica

Información de ajuste de los modelos				
	Criterios de ajuste de modelo	Pruebas de la razón de verosimilitud		
Modelo	Logaritmo de la verosimilitud -2	Chi-cuadrado	gl	Sig.
Sólo intersección	8,292			
Final	5,906	2,386	1	,122

En cuanto a la tabla 25, se visualiza una significancia >0.05, lo que permite indicar que los hallazgos referenciados no se ajustan al modelo de regresión lógica, donde se señala que no se refleja existencia de influencias de la variable ISO 27001 en la integridad de la información desarrollada dentro del área empresarial que ha sido tomada como referente de estudio. Estableciéndose la aceptación de la variable nula.

e) Contrastación de la cuarta hipótesis especifica

H_1= ISO 27001 SI influye significativamente en la confidencialidad de la información en el área TI de una empresa industrial, Lima 2023

H_0= ISO 27001 NO influye significativamente en la confidencialidad de la información en el área TI de una empresa industrial, Lima 2023

Tabla 26

Información de ajuste del modelo para la cuarta hipótesis especifica

Información de ajuste de los modelos				
	Criterios de ajuste de modelo	Pruebas de la razón de verosimilitud		
Modelo	Logaritmo de la verosimilitud -2	Chi-cuadrado	gl	Sig.
Sólo intersección	8,292			
Final	5,906	2,386	1	,122

En cuanto a la tabla 26, se visualiza una significancia >0.05, lo que permite indicar que los hallazgos referenciados no se ajustan al modelo de regresión lógica, donde se señala que variable ISO 27001 no influye en la confidencialidad de la información del área en cuestión. Estableciéndose la aceptación de la variable nula.

f) Contrastación de la quinta hipótesis especifica

H_1= ISO 27001 SI influye significativamente en la trazabilidad de la información en el área TI de una empresa industrial, Lima 2023.

H_0= ISO 27001 NO influye significativamente en la trazabilidad de la información en el área TI de una empresa industrial, Lima 2023.

Tabla 27

Información de ajuste del modelo para la quinta hipótesis especifica

Información de ajuste de los modelos				
	Criterios de ajuste de modelo	Pruebas de la razón de verosimilitud		
Modelo	Logaritmo de la verosimilitud -2	Chi-cuadrado	gl	Sig.
Sólo intersección	8,892			
Final	6,273	2,619	1	,106

En cuanto a la tabla 27, se visualiza una significancia >0.05, lo que permite indicar que los hallazgos referenciados no se ajustan al modelo de regresión lógica, donde se señala que la variable ISO 27001 no influye en la trazabilidad de la información desarrollada dentro del área empresarial que ha sido tomada como referente de estudio. Estableciéndose la aceptación de la variable nula.

V. DISCUSIÓN

El estudio se focalizó en el abordaje de la variable ISO 27001 y su posible capacidad de influenciar la gestión de seguridad de la información dentro del contexto del área TI de una empresa industrial, ubicada en Lima 2023, la cual se constituye como un hecho de relevancia porque permite proveer a la organización en cuestión de datos necesarios para fortalecer su estructura organizativa, en cuanto a la gestión de la seguridad de uno de sus activos más importantes como lo es la información.

Inicialmente se hará mención al objetivo general, respecto al cual se obtuvo como resultados que las ISO 27001 poseían influencia significativa respecto a la variable secundaria la cual ha sido denominada; gestión de la seguridad de la información del área en cuestión dentro de la empresa industrial, lo cual fue reflejando por medio de una $p<0.05$ un coeficiente de Nagelkerke de 22%. Encontrándose estos hallazgos relacionados con lo planteado por Cuenca (2023), quien al abordar el estudio de estas variables halló la existencia de una interconexión positiva, moderada y significativa reflejadas en una Rho= 0.713; $p<0.05$, presentando este autor en su investigación similitudes con el mencionado estudio, donde coincidentemente tomaron en cuenta el uso de las encuestas como técnicas y de los cuestionarios para instrumentar la forma de obtener los datos requeridos, fundamentados en el hecho de que estas le permiten recabar informaciones referente a sus variables de estudio de forma más organizada y enfocadas en el objeto de investigación, siendo este una pieza clave en la aportación de contestaciones idóneas a las interrogantes que se abordaron y poder comprobar las hipótesis planteadas. Estos estudios también guardan afinidad al haberse basado en una población pequeña como unidad de estudio, la cual estuvo constituida por 20 personas. Ambas investigaciones destacaron que las normas ISO 27001 son una excelente herramienta para apoyar los procesos estructurales de las empresas, en cuanto al resguardo de las informaciones, siendo por ello que fundamentaron su estudio para comprobar la influencia de las mismas.

Sin embargo, los resultados señalados en su exposición encontraron antagonismo en los planteamientos formulados por Fathurohman & Witjaksono (2020), quienes desarrollaron un estudio en indonesia, en el cual puntualizaron como hallazgo de relevancia que los SGSI eran una variable que no registraron mejoras notables por la implementación de las normas ISO 27001 en la que reflejaron una $p>0.05$; $r=-0.237$, pudiéndose atribuir estos resultados a la cultura de los países donde se desarrollan los estudios, también se podría explicar esta discrepancia, porque que el tratamiento estadístico que se ofrece a los datos obtenidos son diferentes, al ser ellos netamente experimental, asimismo adoptando un tipo de investigación aplicado diferente al de la investigación en cuestión, que se planteó como básico y no experimental.

Continuando con la sección actual, se hace alusión al primer objetivo específico; en el cual se ha resaltado una significancia $p<0.05$ con un coeficiente de Nagelkerke del 21.4%, que deja al descubierto la influencia ejercida por la variable principal del estudio ISO 27001 respecto a la dimensión disponibilidad de la seguridad de la información que se desarrolla dentro del contexto focalizado. Exaltando estos resultados que se encuentran en ilación y respaldado por la investigación ejercida por Alemán (2023), en la cual se expuso como resultados al calcular la interconexión entre ISO 27001 y la disponibilidad, demostrando el hecho de que existía una incidencia de la variable en la mejora de la dimensión mencionada, lo que se reflejó por medio de una $p<0.05$ y de 78 grado de libertad. Estas han sido investigaciones que presentan semejanzas al abordar de manera responsable este tópico de estudio, aplicando un enfoque cuantitativo en su metodología, explicando que este sería propicio para abordar el fenómeno de estudio, haciendo posible manejar aspectos cuantificables que le permitieron generar resultados numéricos, también se resaltó como recurrencia que la variable ISO 27001 presentó las mismas dimensiones en ambos estudios; planificación, ejecución, verificación y mejora continua, lo que refleja que se medirán de manera similar, con un instrumento que presenta una escala de likert en la que se disponen 5 opciones de contestaciones.

En este sentido, se plantea en contraposición los hallazgos mencionados por Alsahafi et al., (2022), quienes por medio de su estudio refirieron que no se registró influencias notables de forma estadística sig.0.78, entre las normas ISO 27001 respecto a su inclusión como aspecto relevante para potenciar el sistema de gestión de ciberseguridad de las informaciones dentro de la dimensión disponibilidad. Diferenciándose este estudio con los planteamientos iniciales al considerarse que este se desarrolla dentro del territorio árabe saudita, en el contexto educativo del sector universitario con certificaciones otorgadas, en la cual la población estuvo enmarcada por 29 instituciones educativas, asumiéndose como instrumento la lista de observación.

Respecto al segundo objetivo; se obtuvo una significancia $p>0.05$ con 1 grado de libertad, lo que permitió indicar que no existía influencias de ISO 27001 en la autenticidad de la información del área en cuestión. En correspondencia los autores Duval et al., (2022), entre sus determinaciones reflejaron que las SGSI no habían sido relevante dentro de la incorporación del ITIL e ISO 27001 en su capacidad de respuesta en base a la autenticidad de sus operaciones, siendo en su pre-test deficiente en un 84% y en el post-test en un 85% manteniendo casi los mismos niveles, asimismo se resaltó que la capacitación de los colaboradores en pre-test se definía como deficiente en un 91%. Dichas investigaciones guardan parecidos al evidenciarse que sus autores mostraron interés en plantear un modelo SGSI enriquecido con los lineamientos de las normas internacionales ISO 27001, justificando de manera firme que se trataban de dos variables de gran relevancia que valían la pena de ser estudiadas para conocer más a fondo su interrelación. Asimismo se resalta que el mencionado estudios, también se interconecta con la presente investigación por asumir como base filosófica que explica la variable ISO 27001 a la teoría de los sistemas, planteando que se trata de un proceso integrador que se estructura en pro de generar la consolidación de resultados, los cuales pueden ser satisfactorios o no pero que dependerá en su mayoría de la forma como sea administrado en su concepción global cada uno de sus elementos, puesto que ellos son relevantes y potencian la acción reguladora que se requiere.

Como contradicción presentada se indican los hallazgos encontrados por Ibarra (2023) en su investigación quien al realizar el cruce de la mencionada variable ISO 27001 con la dimensión confiabilidad, expuso que sus resultados fueron adversos a los presentados anteriormente, declarando que si se gestaba de forma notoria una relación significativa entre ISO 27001 que denotaron una incidencia en la autenticidad de los SGSI determinándose un $p<0.05$, con una t_o= 9,342 y t_c= 1.680, resultados que pueden estar mostrando estos valores por desarrollar procedimientos estadísticos diversos al de la investigación de referencia, al conocerse que el autor citado desarrollo un estudio pre experimental en el cual estipulaba una manipulación a las variables de estudio, para así conocer su reacción y posible comportamiento en el contexto proyectado, cuyo estadístico aplicado para el cálculos de sus valores fue T de Student. En este orden de ideas, se demarcan como notable discrepancia que se indica que se aplicaron dos momentos de cogida de muestras, situación que no fue realizada en la investigación que se referencia. También se conoció sin asociación, en cuanto al contexto donde esta se fundamentó, obedeciendo al espacio educativo a nivel administrativo, específicamente dentro de la UGEL Bolognesi en Ancash y el del presente estudio en una empresa industrial.

En cuanto al tercer objetivo específico; fue notorio la obtención de resultados que indicaron una significancia $p>0.05$ y 1 grado de libertad, que fue la base de la toma decisiones que permitió señalar que no existían influencias de la variable independiente referente a la dimensión integridad de la información la organización que se abordó. Siendo estos resultados comparables a los que expuestos por los autores Podrecca et al., (2022), quienes mostraron asociación, por medio de su estudio desarrollado en Italia, donde reseñaron que las ISO 27001 no se relacionan significativamente con la integridad de la información del área TI/TIC, determinándose una p mayor a 0,05 y un Rho= 0.305. El estudio refiere concomitancia con puntualizado, al inclinarse por el estudio de la variable ISO 27001 al sostener que se trataba de uno de los sistemas de certificaciones más importantes a nivel mundial, acoplándose con la presente investigación al emplear el mismo estadístico para su prueba de normalidad, el cual fue kolmogorov Smirnov, por tratarse de que también poseía una población de estudio mayor a 30

personas. Asimismo, este autor muestra concurrencia al plantear como dimensión la integridad, asumiéndola como un elemento que deja en evidencia la honestidad, trasparencia y con que se debe tratar las informaciones dentro de las organizaciones, siendo un valor fundamental para el resguardo y seguridad del flujo informativo, exponiendo el cuidado que se debe ejercer en los accesos que se otorgan a los usuarios para que accedan a bases de datos y demás elementos informativos.

En desacuerdo surgen las fundamentaciones desarrolladas por Kitsios et al., (2022), quienes a través de su estudio ha manifestado por medio de una $p<0.05$ y una mitigación del 83% de amenazas del contexto que las ISO27001 influyen positivamente en un nivel aceptable en la dimensión integridad de las SGSI, puesto que el autor expresó que dentro del contexto de la seguridad de la información se estima necesario resguardar de manera muy estricta el acceso a los datos, pudiendo mostrar variaciones estos estudios al desarrollarse dentro de una empresa que cuyo rubro es la tecnológico donde se abordaron 309 formas de amenazas particulares, aplicándose 309 controles, en base a las SGSI todos fortalecidos con las ISO 27001.

Seguidamente se menciona el cuarto objetivo específico; donde se ha evidenciado que se obtuvo una significancia $p>0.05$ con 1 grado de libertad, lo que permitió indicar que los hallazgos referenciados dejan constancia de que no existe influencias de la variable ISO 27001 en cuanto a la confidencialidad de las informaciones de la organización resaltada. Estando los hallazgos en concordancia con lo planteado por Mirtsch et al., (2021), quienes abordaron el estudio de la temática referida, obteniendo dentro de sus resultados una sig. 0.076 la aplicabilidad de las ISO 27001 en referencia al elemento confiabilidad de las SGSI. Los mencionados estudios guardan conformidad, al enfocarse en aplicar de manera rigurosa el método científico reconociendo, que este es un procedimiento que reviste de importancia por cuando es conocido mundialmente y es capaz de aportar objetividad, confiabilidad y validez a los resultados obtenidos, pudiendo ser estos proyectados de manera general y empleado para sustentar posteriores investigaciones en pro de generar mayores referentes para el abordaje de estas

variables, pudiendo demostrarse mayor variedad de realidades al respecto. Esta investigación a pesar de desarrollarse en un contexto social europeo con costumbres y modos de pensar diferentes, muestra igualdades, al considerarse a la seguridad de la información como elemento de gran relevancia dentro de las organizaciones y que por lo tanto debe ser centro de estructuras consolidadas para su manejo eficiente.

En contraste, los autores Gaitero et al., (2021), difieren en sus determinaciones de lo reflejado en la investigación actual, reseñando al respecto que se conoció que el 50% de los encuestados destacaron que la implementación de las SGSI enfocadas en las ISO 27001 permitieron que las empresas elevaran sus niveles de eficiencia y efectividad en base confiabilidad de los datos, asimismo indicó en un 50% que se pueden notar los resultados obtenidos. Los cuales pueden estar sujetos a incongruencias, respecto al tipo de criterio de inclusión de la población que han propuesto para su estudio, puesto a que su unidad de estudio estaba basada en las PYMES, donde sus datos fueron procesados por medio de la descripción porcentual de los mismos.

Finalmente, respecto al quinto objetivo específico; Se obtuvo como respuesta que la variable ISO 27001 no influye en el comportamiento de la dimensión trazabilidad de la información del espacio laboral resaltados dentro de la empresa objeto de abordaje, reflejándose una $p> 0.05$ y 1 grado de libertad. Estos planteamientos tienen concordancia con lo establecido por los autores Fonseca-Herrera et al., (2021), quienes destacan en sus resultados no existía dentro de su contexto influencia de las ISO 27001 en la dimensión trazabilidad con una $p>0.05$ y $Z=-7,696b$. Los cuales en su estudio muestran analogía con esta investigación por tomar en consideración el desarrollo de bases filosóficas para brindar una comprensión más profunda de las variables que se focalizan, estableciéndose a estas como elementos integrales que siempre ha sido del interés de las organizaciones y que van tomando relevancia con el tiempo, en la medida que las personas asumen las informaciones y la privacidad de las mismas como requisitos indispensables dentro de sus negocios. Asimismo, estos estudios se vinculan, debido a que toman como sustentos estudios científicos actuales de diversas

nacionalidades en pro de estudiar la pluralidad de los posibles matices que plantean las variables de acuerdo a cada cultura. Es interesante ver entre las coincidencias que esta investigación plantea como objetivo determinar las posibles influencias entre variables, indicando por medio de algunas de sus interpretaciones que era necesario que dentro de la organización los modelos de seguridad de las gestiones de las informaciones sean reorganizados para la aplicabilidad satisfactoria de ISO27001.

En confrontación Al-Karaki and Sanaa (2022), señala entre sus hallazgos al desarrollar el cruce entre las ISO 27001 en virtud de conocer su relacionamiento con la trazabilidad que se denotó una $p< 0.05$ y $r=0.456$, demostrando una relación media, positiva y significativa, sirviéndole estos valor para sustentar que si existe interrelación como se afirmó en su hipótesis de investigación, lo cual es un elemento que deja al descubierto que en el contexto abordado por este autor se le da importancia a la ruta de tiempo que han recorrido las informaciones, estableciéndola como aspecto de relevancia para poder llevar control de las mismas, a la vez que se asume como un mecanismo de resguardo y seguridad para monitorear el curso de acción que siguen cada uno de los usuarios con accesos a las informaciones. La mencionada investigación refiere discrepancias en cuanto a sus conclusiones donde señala que los SGSI enfocados en ISO 27001 demostraron cambios sustanciales hacia el mejoramiento de los procesos de gestiones de las informaciones de la organización.

VI. CONLUSIONES

1. Se determinó con respecto al objetivo general que ISO 27001, influyó significativamente en un 22% en la gestión de la seguridad de la información en el área TI de una empresa industrial, Lima 2023, obteniéndose un valor de $p<0.05$.

2. En cuanto al primer objetivo específico, se determinó por medio de una $p<0.05$ que ISO 27001, influyó significativamente en un 21.4% en la disponibilidad de la información en el área TI de una empresa industrial, Lima 2023.

3. Referente al segundo objetivo específico, se determinó por medio de una $p>0.05$ que ISO 27001, influyó con 1 grado de libertad en la autenticidad de la información en el área TI de una empresa industrial, Lima 2023.

4. Se determinó en base al tercero objetivo específico por medio de la obtención de una $p>0.05$ que ISO 27001 influyó con 1 grado de libertad en la integridad de la información en el área TI de una empresa industrial, Lima 2023.

5. Se determinó como conclusión referente al cuarto objetivo específico que ISO 27001 influyó con 1 grado de libertad en la confidencialidad de la información en el área TI de una empresa industrial, Lima 2023, por medio de una $p>0.05$.

6. Referente al quinto objetivo específico, se determinó que ISO 27001 influyó con 1 grado de libertad en la trazabilidad de la información en el área TI de una empresa industrial, Lima 2023, lo que se determinó al obtenerse una $p>0.05$.

VII. RECOMENDACIONES

1. Se recomienda que el gerente del área TI, impulse en la empresa el desarrollo de un programa estratégico de implementación de las ISO 27001 para fortalecer la gestión de la seguridad de la información en este espacio, con la intención de continuar fortaleciendo este tipo de conocimientos y su práctica dentro del equipo de trabajo.

2. Se recomienda que el gerente del área TI, tomando en consideración la disponibilidad de la gestión de la seguridad de la información diseñe planificaciones con este objetivo, asumiendo cómo importante mantener presente la funcionalidad de la ISO 27001.

3. Se recomienda que el gerente del área TI, establezca un análisis FODA dentro del espacio laboral para desarrollar medidas de seguridad focalizadas en la autenticidad de la gestión de la seguridad de la información, con el fin de que sean acatadas por todos los integrantes del espacio laboral, en función de la administración del manejo de la misma.

4. Se recomienda que el gerente del área TI, consulte con los especialistas de sistema en cuanto al manejo de la gestión de la seguridad de la información para establecer pautas para fortalecimiento de la aplicación de las normas ISO 27001 en pro de consolidar la integridad de la misma

5. Se recomienda que el gerente del área TI, establezca mecanismos más especializados para garantizar la confidencialidad de la información dentro del área TI, haciendo continuamente cambio de claves de acceso al servidor y base de datos empresarial para evitar posibles situaciones negativas en el futuro con respecto a este elemento

6. Se recomienda que el gerente del área TI, ejerza un control más exacto y preciso de la trazabilidad de las informaciones, lo cual será fundamental para manejar y valorar las diferentes rutas que se activen en el tratamiento de estas.

REFERENCIAS

Akinyemi, I., Schatz, D. & Bashroush, R. (2020). SWOT analysis of information security management system ISO 27001. *International Journal of Services Operations and Informatics, 10*(4), 269-287. doi:10.1504/IJSOI.2020.111297

Annika, K. & Fredrik, K. (2022). Standardizing information security – a structurational analysis. *Information & Management, 59* (3), 562-573. https://doi.org/10.1016/j.im.2022.103623.

Al-Karaki, J. & Sanaa, A. (2022). GoSafe: On the practical characterization of the overall security posture of an organization information system using smart auditing and ranking. *Journal of King Saud University - Computer and Information Sciences, 34*(6), 3079-3095. https://doi.org/10.1016/j.jksuci.2020.09.011.

Alemán, F. (2023). *Norma ISO 27001 para el Control de la Seguridad de Información en una Consultoría Privada, Lima 2023*. [Universidad Cesar Vallejo, Tesis de Maestría]. https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/106824/Aleman_BFY-SD.pdf?sequence=1&isAllowed=y

Alexei, A. (2021). Ensuring information security in public organizations in the Republic of Moldova through the ISO 27001 standard. *Journal of Social Sciences, 4*(1), 84-94. ISSN 2587-3490. DOI: 10.52326/jss.utm.2021.4(1).11

Alsahafi, T., Halboob, W. & Almuhtadi, J. (2022). Compliance with saudi NCA-ECC based on ISO/IEC 27001. *Tehnicki Vjesnik, 29*(6), 2090-2097. doi:10.17559/TV-20220307162849

Antunes, M., Maximiano, M. & Gomes, R. (2022). A client-centered information security and cybersecurity auditing framework. *Applied Sciences (Switzerland), 12*(9); 1-38. doi:10.3390/app12094102

Arias, E. (2020). *Implementación de la norma ISO 27001 en el Departamento de Tecnología de Información de la empresa Esvicsac, Callao.* [Universidad Cesara Vallejo, Tesis de Maestría]. https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/47276/Arias_QES-SD.pdf?sequence=1&isAllowed=y

Arias, F. (2019). Revista de Actividad Física y Científica. Revista científica, 11(1), 7.

Arias, G., J. (2020). Proyecto de tesis. (1era ed.) Arequipa- Perú. Biblioteca Nacional del Perú N° 2020-05577. www.agogocursos.com

Baena, G. (2017*). Metodología de la Investigación*. Grupo editorial Patria 2017.

Barafort, A. And Mesquida, A. (2017). Integrating risk management in IT settings from ISO standards and management systems perspectives. *Computer Standards & Interfaces, 54* (3), 176-185, https://doi.org/10.1016/j.csi.2016.11.010.

Bolek, V., Romanová, A. & Korcek, F. (2023). The Information Security Management Systems in E-Business. *Journal of global information management, 31*(1); 1-29. https://dl.acm.org/doi/abs/10.4018/JGIM.316833

Bokhari, S. and Manzoor, S. (2022) Impact of Information Security Management System on Firm Financial Performance: Perspective of Corporate Reputation and Branding. *American Journal of Industrial and Business Management*, **12**, 934-954. doi: 10.4236/ajibm.2022.125048.

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

Chen L, Xie Z, Zhen J, Dong K. (2021). The Impact of Challenge Information Security Stress on Information Security Policy Compliance: The Mediating Roles of Emotions. *Psychol Res Behav Manag, 11*(15); 1177-1191. doi: 10.2147/PRBM.S359277.

Chen, Y. (2022) Information security management: compliance challenges and new directions. *Journal of Information Technology Case and Application Research, 24*(4), 243-249, DOI: 10.1080/15228053.2022.2148979

Constantino, J. (2019). *Elaboración de un plan de implementación de la ISO 27001-SOC*. [Universitat Oberta de Catalunya, Tesis de Maestría]. https://openaccess.uoc.edu/handle/10609/96948

Córdoba, J. (2021). *Diseño de un sistema automatizado de gestión de la seguridad de la información basado en la Norma ISO/IEC 27001:2013 para dar cumplimiento a la Ley 1581 de 2012 de protección de datos personales en el departamento de sistemas de una institución universitaria en Colombia.* [Universidad Peruana Unión, Tesis de Maestría]. https://repositorio.upeu.edu.pe/bitstream/handle/20.500.12840/4789/Javier_Tesis_Maestro_2021.pdf?sequence=1&isAllowed=y

Cuenca, E. (2023). *SGSI según ISO/IEC 27001:2013 para el control de activos de TI en una empresa privada de Outsourcing, Lima 2023.* [Universidad Cesar Vallejo, Tesis de Maestría]. https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/109516/Cuenca_NEE-SD.pdf?sequence=1&isAllowed=y

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

Duval, E., Delgado, J. y Mendoza, A. (2022). Importancia de la gestión de seguridad de la información en instituciones educativas con ITIL e ISO 27001. *Revista de investigación y sistema e informática, 15*(4); 113-126. DOI: https://doi.org/10.15381/risi.v15i1.23362

Escobar, J. (2022). *Implementación ISO 27001 para el Control de Delitos Informáticos en la División de Prensa DIRCII PNP, Lima, 2022.* [Universidad Cesara Vallejo, Tesis de Maestría]. https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/99731/Escobar_GJA-SD.pdf?sequence=4&isAllowed=

Fathurohman, A. & Witjaksono, R. W. (2020). Analysis and Design of Information Security Management System Based on ISO 27001: 2013 Using ANNEX Control (Case Study: District of Government of Bandung City). *Bulletin of Computer Science and Electrical Engineering, 1*(1), 1–11. https://doi.org/10.25008/bcsee.v1i1.2

Fonseca-Herrera, O., Rojas, A. & Florez, H. (2021). A model of an information security management system based on NTC-ISO/IEC 27001 standard. *IAENG International Journal of Computer Science, 48*(2), 1-10. https://www.researchgate.net/publication/362062660_A_Model_of_an_Information_Security_Management_System_Based_on_NTC-ISOIEC_27001_Standard

Gaitero, D., Genero, M. & Piattini, M. (2021). System quality and security certification in seven weeks: A multi-case study in Spanish SMEs. *Journal of Systems and Software, 178*(1), 356- 368. https://doi.org/10.1016/j.jss.2021.110960

Grishaeva, S. (2021). Development and Implementation of Privacy Information Management for Compliance with International Standard ISO 27701:2019. *Information Technologies, 6 (1),* 192-200, doi: 10.1109/ITQMIS53292.2021.9642925.

Huaney, J. (2022*). Infraestructura de un data center para la seguridad de la información (ISO 27001) de la Municipalidad Provincial de Huaraz – 2021.* [Universidad Peruana De Ciencias E Informática, Tesis de Maestría]. https://repositorio.upci.edu.pe/bitstream/handle/upci/725/Huaney%20-%20Tesis%20Oficial%20-%20OK.pdf?sequence=1&isAllowed=y

Hernández-Sampieri, R., y Mendoza, C. (2018). *Metodología de la investigación.* Las rutas cuantitativas, cualitativas y Mc. Graw Hill Educación.

Ibarra, L. (2023). *ISO 27001:2013 para la gestión del manejo de información en la UGEL Bolognesi, Ancash 2023.* [Universidad Cesara Vallejo, Tesis de Maestría]. https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/109468/Ibarra_CL-SD.pdf?sequence=1&isAllowed=y

Kitsios, F., Chatzidimitriou, E. & Kamariotou, M. (2022). Developing a Risk Analysis Strategy Framework for Impact Assessment in Information Security Management Systems: A Case Study in IT Consulting Industry. *Sustainability 14*(3), 1269. https://doi.org/10.3390/su14031269. https://doi.org/10.3390/su14031269

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 (Switzerland), 15*(7) doi:10.3390/su15075828

Ključnikov, A., Mura, L. & Sklenár, D. (2019). Information security management in SMEs: factors of success. *Entrepreneurship and Sustainability Issues, VsI Entrepreneurship and Sustainability Center, 6*(4); 2081-2094. https://ideas.repec.org/a/ssi/jouesi/v6y2019i4p2081-2094.html

López, I. M., Guarda, T. and Oliveira, P. (2019). Implementation of ISO 27001 Standards as GDPR Compliance Facilitator*. Journal of Information Systems*

Engineering & Management, 4(2), em0089. https://doi.org/10.29333/jisem/5888

Maldonado, J. (2018). *Metodologia de la investigacion social*. colombia: Ediciones de la U.

Manas, N. & Sarbeswar, H. (2020). A Review Article on Information Security Management. *International Journal of Advanced Research in Engineering and Technology, 51*(5); 551–567. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3878639

Martín, T. (2021). Automatización de un sistema de gestión de seguridad de la información basado en la Norma ISO/IEC 27001. *Revista Universidad y Sociedad*, *13*(5), 495-506. http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2218-36202021000500495&lng=es&tlng=es.

Martínez, A. (2019*). Importancia de la implementación de un sistema de gestión de seguridad de la información (SGSI) en las empresas bajo la iso 27001.* [Universidad Militar Nueva Granada, Tesis de Posgrado]. https://repository.unimilitar.edu.co/bitstream/handle/10654/34863/MartinezLopezAdrianaMilena.pdf?sequence=1&isAllowed=y

Mirtsch, M., Blind, K., Koch, C. & Dudek, G. (2021). Information security management in ICT and non-ICT sector companies: A preventive innovation perspective. *Computers and Security, 109*(1); 210-236. doi:10.1016/j.cose.2021.102383

Mirtsch, M., Kinne, J., & Blind, K. (2021). Exploring the adoption of the international information security management system standard ISO/IEC 27001: A web mining-based analysis. *IEEE Transactions on Engineering Management, 68*(1), 87-100. doi:10.1109/TEM.2020.2977815

Morales, L. (2019). *Balanced ScoreCard para seguridad de la información bajo el estándar ISO 27001 en Cooperativas de Ahorro y Crédito* [Universidad Técnica De Ambato, Tesis de Maestría]. https://repositorio.uta.edu.ec/bitstream/123456789/29216/1/Tesis_%20t1537msi.pdf

Narro, S. (2021). *El sistema de gestión de seguridad de la información y la gestión de riesgos en el área informática de una universidad pública, región cajamarca 2020.* [Universidad Privada del Norte, Tesis de Maestría]. https://repositorio.upn.edu.pe/bitstream/handle/11537/30041/Narro%20Mestanza%20Sarita%20Morelia.pdf?sequence=1&isAllowed=y

Orozova, D., Kaloyanova, K. & Todorova, M. (2019). Introducing information security concepts and standards in higher education. *TEM Journal, 8*(3), 1017-1024. doi:10.18421/TEM83-46

Pino, R. (2018). *Metodología de la investigación* (2da. Ed.). Lima: Editorial San Marcos E.I.R.L.

Podrecca, M., Culot, G., Nassimbeni, G. & Sartor, M. (2022). Information security and value creation: The performance implications of ISO/IEC 27001. *Computers in Industry, 142(2); 116-145.* doi:10.1016/j.compind.2022.103744

Podrecca, M. & Sartor, M. (2023). Forecasting the diffusion of ISO/IEC 27001: A grey model approach. *TQM Journal, 35*(9), 123-151. doi:10.1108/TQM-07-2022-0220

Ponte, E. (2022). *Seguridad de la información (ISO27001) para el desarrollo de teletrabajo en tiempos de Covid-19. Empresa OSIR E.I.R.L., Ancash – 2022.* [Universidad Cesara Vallejo, Tesis de Maestría]. https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/94036/Ponte_QEJ-SD.pdf?sequence=1&isAllowed=y

Qusef A, & Alkilani H. (2022). The effect of ISO/IEC 27001 standard over open-source intelligence. *PeerJ Comput Sci, 6*(8); 116-138. doi: 10.7717/peerj-cs.810

Rincón, J. (2019). *Plan de implementación de la norma ISO/IEC ISO 27001:2013 para un operador de información PILA.* [Universitat Oberta de Catalunya, Tesis de Maestría]. https://www.lareferencia.info/vufind/Record/ES_6a8b96fa784855a8c6e5b7dec0cbc747

Resolución de Consejo Universitario N° 0470-2022/UCV. (2022). Código de Ética en Investigación de la Universidad César Vallejo.

Rodríguez, L., Cruzado, C., Mejía, C. y Alarcón, M. (2020). Aplicación de ISO 27001 y su influencia en la seguridad de la información de una empresa privada peruana. *Propósitos y Representaciones, 8*(3), e786. doi: http://dx.doi.org/10.20511/pyr2020.v8n3.786

Romano, J. (2019). *Plan de implementación de la ISO/IEC 27001:2013 en la empresa Gespa*. [Universitat Oberta de Catalunya, Tesis de Maestría]. http://hdl.handle.net/10609/97027

Roy, P. (2020). A High-Level Comparison between the NIST Cyber Security Framework and the ISO 27001 Information Security Standard. *2020 National Conference on Emerging Trends on Sustainable Technology and Engineering Applications (NCETSTEA)*, Durgapur, India, 35(1); 1-3, doi: 10.1109/NCETSTEA48365.2020.9119914.

Ruiz, L. C., Amado, M. L., Carrasco, J. R. & Andrade-Arenas, L. (2022). Implementation of information security audit for the sales system in a peruvian company. *International Journal on Advanced Science, Engineering and Information Technology, 12*(3), 1189-1195. DOI:10.18517/ijaseit.12.3.13969

Sánchez, E. (2022). *Propuesta de Plan De Implementación De La Norma ISO/IEC 27001.* [Universitat Oberta de Catalunya, Tesis de Maestría]. https://openaccess.uoc.edu/bitstream/10609/145849/11/esanchezhernTFM0622memoria.pdf

Solana-González, P., Vanti, A. & Souza, K. (2019). Multicriteria analysis of the compliance for the improvement of information security. *Journal of Information Systems and Technology Management – Jistem USP, 16*(1), 234-242. https://www.tecsi.org/jistem/index.php/jistem/article/download/3071/718

Shimels, T. & Lessa, L. (2023), Maturity of information systems' security in Ethiopian banks: case of selected private banks. *International Journal of Industrial Engineering and Operations Management*, *Vol. ahead-of-print No. ahead-of-print*. https://doi.org/10.1108/IJIEOM-10-2021-0014

Somepalli, S., Tangella, S. & Yalamanchili, S. (2020). Information Security Management. *HOLISTICA – Journal of Business and Public Administration. 11*(2); 1-16. https://www.researchgate.net/publication/343700567_Information_Security_Management

Tatiara, A., Fajar, A., Siregar, B. & Gunawan, W. (2018). Analysis of factors that inhibiting implementation of Information Security Management System (ISMS) based on ISO 27001. *Journal of Physics: Conference Series, 978*(2); 1-7. DOI 10.1088/1742-6596/978/1/012039

Topa, I. & Karyda, M. (2019). From theory to practice: Guidelines for enhancing information security management. *Information and Computer Security, 27*(3), 326-342. doi:10.1108/ICS-09-2018-0108

Zaini, M.K., Masrek, M.N. and Abdullah Sani, M.K.J. (2020). The impact of information security management systems on organizational agility. *Information and Computer Security, 28*(5), 681-700. https://doi.org/10.1108/ICS-02-2020-0020

Zambrano-Izurieta, J. P., Mendoza-Barberán, M. G., & Farez-Arias, M. (2023). Funcionalidades de la Trazabilidad en el Desarrollo del Modelo de Comercio Electrónico B2C. *Economía Y Negocios*, *14* (1), 135–148. https://doi.org/10.29019/eyn.v14i1.1057

Zuña, E., Arce, A., Romero, W. and Soledispa, C. (2019). Analysis of information security in SMEs in the city of Milagro. *University and Society Magazine, 11*(4), 487-492. http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2218-36202019000400487&lng=es&tlng=es.

ANEXOS

Anexo 1: Operacionalización de la variable

VARIABLES	D. CONCEPTUAL	D. OPERACIONAL	DIMENSIONES	INDICADORES	ÍTEMS	ESCALA
ISO 27001	Son definidas como un modelo aplicativo para garantizar la seguridad de la información de una empresa, por medio del cual se brindan las pautas que se deben tener en cuenta para asegurar la integridad, disponibilidad y confidencialidad de la información (Akinyemi et al., 2020).	La variable ISO27001, se medirá por medio de un cuestionario que posee un total de 25 preguntas, el cual aborda 4 dimensiones; Planificación (16 ítems), ejecución (3 ítems), verificación (3 ítems) y mejora continua (3), en una escala de likert, tipo ordinal.	Planificación	Liderazgo, planeamiento, soporte	1-16	Ordinal
			Ejecución	Operaciones,	17-19	
			Verificación	Evaluaciones de desempeño	20- 23	
			Mejoramiento	Mejora continua	24-25	
Gestión de la Seguridad de la Información	Se determinan como una serie de disposiciones, políticas y normas que permiten el resguardo de los datos importantes de las organizaciones, los cuales son considerados como	La variable se medirá por medio del cuestionario Gestión de la Seguridad de la Información, que posee un total de 24 preguntas, el cual aborda 5 dimensiones;	Disponibilidad	Acceso las 24 horas, Estabilidad de la red, capacidades tecnológicas, anchos de banda,	1-5	Ordinal
			Autenticidad	políticas de seguridad,	6- 10	

	uno de los activos más relevantes de ellas (Ibarra, 2023).	Disponibilidad (5 ítems), autenticidad (5 ítems), integridad (4 ítems), confidencialidad (5 ítems) Trazabilidad (3), en una escala de likert, tipo ordinal.		controles de los usuarios, Administración de equipos, vulnerabilidad de la información,		
			Integridad	copia de seguridad, soporte técnico, administración del sistema,	11-15	
			Confidencialidad	Protección de los datos, Privilegios de acceso, Políticas institucionales,	16- 20	
			Trazabilidad	seguimiento de procesos. rastreo de usuario,	21- 24	

Anexo 2: Validación por juicio de expertos

Variable ISO 27001

5. <u>Presentación de instrucciones para el juez</u>:

A continuación, a usted le presento el cuestionario ISO 27001, elaborado por Alemán Balladares Fernando Yasmani, en el año 2023. 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 ítem no es claro.
	2. Bajo Nivel	El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por laordenación de estas.
	3. Moderado nivel	Se requiere una modificación muy específica de algunos de los términos del ítem.
	4. Alto nivel	El ítem es claro, tiene semántica y sintaxis adecuada.
COHERENCIA El ítem tiene relación lógica con la dimensión o indicador que está midiendo.	1. totalmente en desacuerdo (no cumple con el criterio)	El ítem no tiene relación lógica con la dimensión.
	2. Desacuerdo (bajo nivel de acuerdo)	El ítem tiene una relación tangencial /lejana conla dimensión.
	3. Acuerdo (moderado nivel)	El ítem tiene una relación moderada con la dimensión que se está midiendo.
	4. Totalmente de Acuerdo (alto nivel)	El ítem se encuentra está relacionado con la dimensión que está midiendo.
RELEVANCIA El ítem es esencial o importante, es decir debe ser incluido.	1. No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión.
	2. Bajo Nivel	El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide éste.
	3. Moderado nivel	El ítem es relativamente importante.
	4. Alto nivel	El ítem 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:

- **Primera dimensión**: Planificación
- Objetivos de la Dimensión: evaluar la implementación de las ISO 27001 una organización.

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Liderazgo	1	4	4	4	
	2	4	4	4	
	3	4	4	4	
	4	4	4	4	
	5	4	4	4	
Planificación	6	4	4	4	
	7	4	4	4	
	8	4	4	4	
	9	4	4	4	
	10	4	4	4	
Soporte	11	4	4	4	
	12	4	4	4	
	13	4	4	4	
	14	4	4	4	
	15	4	4	4	
	16	4	4	4	

- **Segunda dimensión**: Ejecución
- Objetivos de la Dimensión: evaluar la implementación de las ISO 27001 una organización.

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Operación	17	4	4	4	
	18	4	4	4	
	19	4	4	4	

- **Tercera dimensión**: Verificación
- Objetivos de la Dimensión: evaluar la implementación de las ISO 27001 una organización.

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Evaluación del desempeño	20	4	4	4	
	21	4	4	4	
	22	4	4	4	
	23	4	4	4	

- **Cuarta dimensión**: Mejoramiento
- Objetivos de la Dimensión: evaluar la implementación de las ISO 27001 una organización.

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Mejora - continuidad	24	4	4	4	
	25	4	4	4	

Observaciones (precisar si hay suficiencia): HAY 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: Metodólogo.

[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

26 de mayo del 2023

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

Firma del Experto validador

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

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

5. <u>Presentación de instrucciones para el juez</u>:

A continuación, a usted le presento el Cuestionario ISO 27001 elaborado por Alemán Balladares Fernando Yasmani, en el año 2023. 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 ítem no es claro.
	2. Bajo Nivel	El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por laordenación de estas.
	3. Moderado nivel	Se requiere una modificación muy específica de algunos de los términos del ítem.
	4. Alto nivel	El ítem es claro, tiene semántica y sintaxis adecuada.
COHERENCIA El ítem tiene relación lógica con la dimensión o indicador que está midiendo.	1. totalmente en desacuerdo (no cumple con el criterio)	El ítem no tiene relación lógica con la dimensión.
	2. Desacuerdo (bajo nivel de acuerdo)	El ítem tiene una relación tangencial /lejana conla dimensión.
	3. Acuerdo (moderado nivel)	El ítem tiene una relación moderada con la dimensión que se está midiendo.
	4. Totalmente de Acuerdo (alto nivel)	El ítem se encuentra está relacionado con la dimensión que está midiendo.
RELEVANCIA El ítem es esencial o importante, es decir debe ser incluido.	1. No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión.
	2. Bajo Nivel	El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide éste.
	3. Moderado nivel	El ítem es relativamente importante.
	4. Alto nivel	El ítem 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 <u>No</u> cumple con el criterio
2. Bajo Nivel
3. Moderado nivel
4. Alto nivel

Dimensiones del instrumento:

- **Primera dimensión**: Planificación
- Objetivos de la Dimensión: evaluar la implementación de las ISO 27001 una organización.

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Liderazgo	1	4	4	4	
	2	4	4	4	
	3	4	4	4	
	4	4	4	4	
	5	4	4	4	
Planificación	6	4	4	4	
	7	4	4	4	
	8	4	4	4	
	9	4	4	4	
	10	4	4	4	
Soporte	11	4	4	4	
	12	4	4	4	
	13	4	4	4	
	14	4	4	4	
	15	4	4	4	
	16	4	4	4	

- **Segunda dimensión**: Ejecución
- Objetivos de la Dimensión: evaluar la implementación de las ISO 27001 una organización.

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Operación	17	4	4	4	
	18	4	4	4	
	19	4	4	4	

- **Tercera dimensión**: Verificación
- Objetivos de la Dimensión: evaluar la implementación de las ISO 27001 una organización.

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Evaluación del desempeño	20	4	4	4	
	21	4	4	4	
	22	4	4	4	
	23	4	4	4	

- **Cuarta dimensión**: Mejoramiento
- Objetivos de la Dimensión: evaluar la implementación de las ISO 27001 una organización.

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Mejora - continuidad	24	4	4	4	
	25	4	4	4	

Observaciones (precisar si hay suficiencia): HAY SUFICIENCIA

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

Apellidos y nombres del juez validador: Mg. Carlos Antonio Huerta Michiline

Especialidad del validador: Maestría en Dirección de Sistemas y Tecnologías de la Información

26 de mayo del 2023

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

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

Firma del Experto validador

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

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

5. <u>Presentación de instrucciones para el juez</u>:

A continuación, a usted le presento el cuestionario gestión seguridad de la información elaborado por Ibarra Caqui, Lucio, en el año 2023. 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 ítem no es claro.
	2. Bajo Nivel	El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por laordenación de estas.
	3. Moderado nivel	Se requiere una modificación muy específica de algunos de los términos del ítem.
	4. Alto nivel	El ítem es claro, tiene semántica y sintaxis adecuada.
COHERENCIA El ítem tiene relación lógica con la dimensión o indicador que está midiendo.	1. totalmente en desacuerdo (no cumple con el criterio)	El ítem no tiene relación lógica con la dimensión.
	2. Desacuerdo (bajo nivel de acuerdo)	El ítem tiene una relación tangencial /lejana conla dimensión.
	3. Acuerdo (moderado nivel)	El ítem tiene una relación moderada con la dimensión que se está midiendo.
	4. Totalmente de Acuerdo (alto nivel)	El ítem se encuentra está relacionado con la dimensión que está midiendo.
RELEVANCIA El ítem es esencial o importante, es decir debe ser incluido.	1. No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión.
	2. Bajo Nivel	El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide éste.
	3. Moderado nivel	El ítem es relativamente importante.
	4. Alto nivel	El ítem 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:

- **Primera dimensión**: Planificación
- Objetivos de la Dimensión: evaluar la implementación de las ISO 27001 una organización.

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Liderazgo	1	4	4	4	
	2	4	4	4	
	3	4	4	4	
	4	4	4	4	
	5	4	4	4	
Planificación	6	4	4	4	
	7	4	4	4	
	8	4	4	4	
	9	4	4	4	
	10	4	4	4	
Soporte	11	4	4	4	
	12	4	4	4	
	13	4	4	4	
	14	4	4	4	
	15	4	4	4	
	16	4	4	4	

- **Segunda dimensión**: Ejecución
- Objetivos de la Dimensión: evaluar la implementación de las ISO 27001 una organización.

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Operación	17	4	4	4	
	18				
	19				

- **Tercera dimensión**: Verificación
- Objetivos de la Dimensión: evaluar la implementación de las ISO 27001 una organización.

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Evaluación del desempeño	20	4	4	4	
	21	4	4	4	
	22	4	4	4	
	23	4	4	4	

- **Cuarta dimensión**: Mejoramiento
- Objetivos de la Dimensión: evaluar la implementación de las ISO 27001 una organización.

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Mejora - continuidad	24	4	4	4	
	25	4	4	4	

Observaciones (precisar si hay suficiencia): HAY SUFICIENCIA

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

Apellidos y nombres del juez validador: Mg. Pérez Sánchez Walter Yvan

Especialidad del validador: Maestría en Supply Chain Management

26 de mayo del 2023

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

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

Firma del Experto validador

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

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

Variable Gestión de la Seguridad de la Información

5. Presentación de instrucciones para el juez:

A continuación, a usted le presento el cuestionario gestión seguridad de la información elaborado por Ibarra Caqui, Lucio, en el año 2023. 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 ítem no es claro.
	2. Bajo Nivel	El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por laordenación de estas.
	3. Moderado nivel	Se requiere una modificación muy específica de algunos de los términos del ítem.
	4. Alto nivel	El ítem es claro, tiene semántica y sintaxis adecuada.
COHERENCIA El ítem tiene relación lógica con la dimensión o indicador que está midiendo.	1. totalmente en desacuerdo (no cumple con el criterio)	El ítem no tiene relación lógica con la dimensión.
	2. Desacuerdo (bajo nivel de acuerdo)	El ítem tiene una relación tangencial /lejana conla dimensión.
	3. Acuerdo (moderado nivel)	El ítem tiene una relación moderada con la dimensión que se está midiendo.
	4. Totalmente de Acuerdo (alto nivel)	El ítem se encuentra está relacionado con la dimensión que está midiendo.
RELEVANCIA El ítem es esencial o importante, es decir debe ser incluido.	1. No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión.
	2. Bajo Nivel	El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide éste.
	3. Moderado nivel	El ítem es relativamente importante.
	4. Alto nivel	El ítem 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:

- **Primera dimensión**: Disponibilidad
- Objetivos de la Dimensión: Estudiar el SGSI de una organización

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Acceso las 24 horas	1	4	4	4	
	2	4	4	4	
Estabilidad de la red	3	4	4	4	
Capacidad tecnológica	4	4	4	4	
Ancho de banda	5	4	4	4	

- **Segunda dimensión**: Autenticidad
- Objetivos de la Dimensión: Estudiar el SGSI de una organización

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Política de seguridad	6	4	4	4	
Control de usuarios	7	4	4	4	
Administración de equipos	8	4	4	4	
	9	4	4	4	
Vulneración de información	10	4	4	4	

- **Tercera dimensión**: Integridad
- Objetivos de la Dimensión: Estudiar el SGSI de una organización

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Copias de seguridad	11	4	4	4	
	12	4	4	4	
Soporte técnico	13	4	4	4	
Administración de los sistemas	14	4	4	4	
	15	4	4	4	

- **Cuarta dimensión**: Confiabilidad
- Objetivos de la Dimensión: Estudiar el SGSI de una organización

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Protección de datos	16	4	4	4	
	17	4	4	4	
Privilegios de acceso	18	4	4	4	
	19	4	4	4	
Políticas institucionales	20	4	4	4	

Dimensiones del instrumento:

- **Quinta dimensión**: Trazabilidad
- Objetivos de la Dimensión: Estudiar el SGSI de una organización

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Seguimiento de los procesos.	21	4	4	4	
	22	4	4	4	
Rastreo de usuarios	23	4	4	4	
	24	4	4	4	

Observaciones (precisar si hay suficiencia): HAY SUFICIENCIA

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

Apellidos y nombres del juez validador: Mg. Carlos Antonio Huerta Michiline

Especialidad del validador: Maestría en Dirección de Sistemas y Tecnologías de la Información

26 de mayo del 2023

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

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

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

Firma del Experto validador

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

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

5. <u>Presentación de instrucciones para el juez</u>:

A continuación, a usted le presento el cuestionario gestión seguridad de la información elaborado por Ibarra Caqui, Lucio, en el año 2023. 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 ítem no es claro.
	2. Bajo Nivel	El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por laordenación de estas.
	3. Moderado nivel	Se requiere una modificación muy específica de algunos de los términos del ítem.
	4. Alto nivel	El ítem es claro, tiene semántica y sintaxis adecuada.
COHERENCIA El ítem tiene relación lógica con la dimensión o indicador que está midiendo.	1. totalmente en desacuerdo (no cumple con el criterio)	El ítem no tiene relación lógica con la dimensión.
	2. Desacuerdo (bajo nivel de acuerdo)	El ítem tiene una relación tangencial /lejana conla dimensión.
	3. Acuerdo (moderado nivel)	El ítem tiene una relación moderada con la dimensión que se está midiendo.
	4. Totalmente de Acuerdo (alto nivel)	El ítem se encuentra está relacionado con la dimensión que está midiendo.
RELEVANCIA El ítem es esencial o importante, es decir debe ser incluido.	1. No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión.
	2. Bajo Nivel	El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide éste.
	3. Moderado nivel	El ítem es relativamente importante.
	4. Alto nivel	El ítem 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 <u>No</u> cumple con el criterio
2. Bajo Nivel
3. Moderado nivel
4. Alto nivel

Dimensiones del instrumento:

- **Primera dimensión**: Disponibilidad
- Objetivos de la Dimensión: Estudiar el SGSI de una organización

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Acceso las 24 horas	1	4	4	4	
	2	4	4	4	
Estabilidad de la red	3	4	4	4	
Capacidad tecnológica	4	4	4	4	
Ancho de banda	5	4	4	4	

- **Segunda dimensión**: Autenticidad
- Objetivos de la Dimensión: Estudiar el SGSI de una organización

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Política de seguridad	6	4	4	4	
Control de usuarios	7	4	4	4	
Administración	8	4	4	4	
de equipos	9	4	4	4	
Vulneración de información	10	4	4	4	

- **Tercera dimensión**: Integridad
- Objetivos de la Dimensión: Estudiar el SGSI de una organización

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Copias de seguridad	11	4	4	4	
	12	4	4	4	
Soporte técnico	13	4	4	4	
Administración	14	4	4	4	
de los sistemas	15	4	4	4	

- **Cuarta dimensión**: Confiabilidad
- Objetivos de la Dimensión: Estudiar el SGSI de una organización

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Protección de datos	16	4	4	4	
	17	4	4	4	

- **Quinta dimensión**: Trazabilidad
- Objetivos de la Dimensión: Estudiar el SGSI de una organización

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Seguimiento de los procesos.	21	4	4	4	
	22	4	4	4	
Rastreo de usuarios	23	4	4	4	
	24	4	4	4	

Observaciones (precisar si hay suficiencia): HAY SUFICIENCIA

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

Apellidos y nombres del juez validador: Mg. Carlos Antonio Huerta Michiline

Especialidad del validador: Maestría en Supply Chain Management

26 de mayo del 2023

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

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

Firma del Experto validador

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

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

5. <u>Presentación de instrucciones para el juez</u>:

A continuación, a usted le presento el cuestionario gestión seguridad de la información elaborado por Ibarra Caqui, Lucio, en el año 2023. 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 ítem no es claro.
	2. Bajo Nivel	El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por laordenación de estas.
	3. Moderado nivel	Se requiere una modificación muy específica de algunos de los términos del ítem.
	4. Alto nivel	El ítem es claro, tiene semántica y sintaxis adecuada.
COHERENCIA El ítem tiene relación lógica con la dimensión o indicador que está midiendo.	1. totalmente en desacuerdo (no cumple con el criterio)	El ítem no tiene relación lógica con la dimensión.
	2. Desacuerdo (bajo nivel de acuerdo)	El ítem tiene una relación tangencial /lejana conla dimensión.
	3. Acuerdo (moderado nivel)	El ítem tiene una relación moderada con la dimensión que se está midiendo.
	4. Totalmente de Acuerdo (alto nivel)	El ítem se encuentra está relacionado con la dimensión que está midiendo.
RELEVANCIA El ítem es esencial o importante, es decir debe ser incluido.	1. No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión.
	2. Bajo Nivel	El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide éste.
	3. Moderado nivel	El ítem es relativamente importante.
	4. Alto nivel	El ítem 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 <u>No</u> cumple con el criterio
2. Bajo Nivel
3. Moderado nivel
4. Alto nivel

Dimensiones del instrumento:

- **Primera dimensión**: Disponibilidad
- Objetivos de la Dimensión: Estudiar el SGSI de una organización

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Acceso las 24 horas	1	4	4	4	
	2	4	4	4	
Estabilidad de la red	3	4	4	4	
Capacidad tecnológica	4	4	4	4	
Ancho de banda	5	4	4	4	

- **Segunda dimensión**: Autenticidad
- Objetivos de la Dimensión: Estudiar el SGSI de una organización

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Política de seguridad	6	4	4	4	
Control de usuarios	7	4	4	4	
Administración de equipos	8	4	4	4	
	9	4	4	4	
Vulneración de información	10	4	4	4	

- **Tercera dimensión**: Integridad
- Objetivos de la Dimensión: Estudiar el SGSI de una organización

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Copias de seguridad	11	4	4	4	
	12	4	4	4	
Soporte técnico	13	4	4	4	
Administración de los sistemas	14	4	4	4	
	15	4	4	4	

- **Cuarta dimensión**: Confiabilidad
- Objetivos de la Dimensión: Estudiar el SGSI de una organización

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Protección de datos	16	4	4	4	
	17	4	4	4	
Privilegios de acceso	18	4	4	4	
	19	4	4	4	
Políticas institucionales	20	4	4	4	

- **Quinta dimensión**: Trazabilidad
- Objetivos de la Dimensión: Estudiar el SGSI de una organización

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Seguimiento de los procesos.	21	4	4	4	
	22	4	4	4	
Rastreo de usuarios	23	4	4	4	
	24	4	4	4	

Observaciones (precisar si hay suficiencia): HAY SUFICIENCIA

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

Apellidos y nombres del juez validador: Mg. Walter Yvan Pérez Sánchez

Especialidad del validador: Maestría en Supply Chain Management

26 de mayo del 2023

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

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

Firma del Experto validador

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

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

Anexo 3: Instrumentos de recolección de datos

Cuestionario: ISO 27001

Fecha: / /

Sexo: Femenino [ ] Masculino [ ]

Tiempo de trabajo dentro del área TI:

Autor: Alemán (2023), adaptado para la investigación

Instrucciones: estimado usuario, el siguiente cuestionario tiene la intención de evaluar ***la implementación de las ISO 27001 en la empresa***. Las opiniones podrían ayudar a optimizar la gestión de la misma, en lo que se pueda perfeccionar, ese es el motivo principal para que conteste con la sinceridad del caso. Debe marcar sólo una de las alternativas, colocando un aspa (X) en el cuadro que corresponda según la siguiente valoración.

Valoración	Categoría
1	Nunca
2	Casi nunca
3	A veces
4	Casi siempre
5	Siempre

Preguntas:

	DIMENSIÓN 1: Planificación	1	2	3	4	5
1	Dentro del área TI el cumplimiento de los objetivos de seguridad de la información se encuentra enfocados en base a las ISO 27001					
2	El equipo del área TI asegura la integración de los requisitos de la ISO 27001 en los procesos de la empresa					
3	Existe apoyo en el área TI para la contribución efectiva de la ISO 27001					
4	En el área TI se establecen política de seguridad de la información					
5	En el área TI se suelen definir roles y responsabilidades para seguridad de la información					
6	En el área TI se realizan análisis de riesgo de la seguridad de la información					

7	La empresa se define y aplican proceso de valoración de riesgo de la seguridad de la información					
8	En la empresa se estructuran planes de tratamiento de riesgo de la seguridad de la información					
9	La empresa suele tener documentado los objetivos de la seguridad de la información					
10	La empresa plantea un plan de mejoras basados en el cumplimiento de los objetivos					
11	La empresa proporciona los recursos necesarios para la gestión de la seguridad informática en el área TI					
12	Se desarrollan evaluaciones de desempeño acerca de la seguridad información dentro de la empresa					
13	Se desarrollan políticas de seguridad de información					
14	Se definen canales de atención para la de la seguridad de información					
15	En la empresa se cuentan con la documentación de la seguridad de información para asegurar efectividad					
16	Se controla la información requerida para una gestión de seguridad; disponible y protegida					
	DIMENSIÓN 2: Ejecución					
17	Se plantea una planificación, ejecución y control de procesos para la gestión de seguridad de información					
18	Se llevan a cabo evaluaciones de riesgos planificadas					
19	En la empresa se activan planes de tratamiento de riesgos					
	DIMENSIÓN 3: Verificación					
20	La empresa realiza el seguimiento, análisis y evaluación de la gestión de seguridad de información					
21	La empresa realiza auditorías internas					
22	La alta dirección revisa su gestión de seguridad de información para asegurar su eficacia					
23	La alta dirección toma decisiones y medidas en base a los resultados obtenidos por la gestión de seguridad de información					
	DIMENSIÓN 4: Mejoramiento					
24	La empresa controla y corrige las normas de cumplimiento de la seguridad de información					
25	La empresa mejora continuamente la educación y efectividad de la gestión y efectividad de la gestión					

Cuestionario: Gestión de seguridad de la información

Fecha: / /

Sexo: Femenino [ ] Masculino [ ]

Tiempo de trabajo dentro del área TI:

Autor: Ibarra (2023), adaptado para la investigación

Instrucciones: estimado usuario, el siguiente cuestionario tiene la intención de ***evaluar la gestión de seguridad de la información***. Las opiniones podrían ayudar a optimizar la gestión de la misma, en lo que se pueda perfeccionar, ese es el motivo principal para que conteste con la sinceridad del caso. Debe marcar sólo una de las alternativas, colocando un aspa (X) en el cuadro que corresponda según la siguiente valoración.

Valoración	Categoría
1	Nunca
2	Casi nunca
3	A veces
4	Casi siempre
5	Siempre

Preguntas:

	DIMENSIÓN 1: Disponibilidad	1	2	3	4	5
1	Se encuentra con acceso a los sistemas de información durante las 24 horas del día					
2	Es necesario que el área TI cuente con acceso a los sistemas de información durante las 24 horas del día					
3	La red de datos actual permite que los servicios de sistemas de información se mantengan disponibles durante las 24 horas del día					
4	La capacidad tecnológica del área TI requiere se optimice					
5	El ancho de banda de internet con que cuenta el área TI de la empresa permite trabajar con normalidad y evita saturación de datos					
	DIMENSIÓN 2: Autenticidad					
6	El área TI se suelen contar con políticas de seguridad para el acceso de los usuarios a su información					
7	Se cuenta con un control de usuarios basados en un servidor de dominio					

8	Los usuarios que se conectan de manera remota presentan identificación de nombres de equipo					
9	Es necesario mejorar la modalidad actual de acceder a los sistemas por escritorio remoto					
10	Se ha registrado durante los últimos 6 meses intentos de vulneración de las informaciones					
	DIMENSIÓN 3: Integridad					
11	El área TI realiza copias de seguridad de los sistemas de información de manera periódica					
12	Los usuarios que realizan trabajos remotos, poseen una carpeta compartida en el servidor para almacenar su información					
13	Cuando se presentan inconvenientes con los equipos de computadoras se cuenta con un personal que brinda soporte de manera oportuna					
14	El área TI cuenta con un administrador del sistema para brindar soporte de conexiones o inconsistencias presentadas					
15	Se presentan problemas en los sistemas como; información duplicada o reporte sin información.					
	DIMENSIÓN 4: Confidencialidad					
16	El área TI cuenta con lineamientos que permiten la protección de datos de los trabajadores y usuarios					
17	Se puede extraer informaciones del Área TI por medio de dispositivos como USB					
18	Se cuenta con un administrador que facilita los privilegios de los usuarios, de acuerdo a sus necesidades					
19	Todos los usuarios tienen los mismos accesos al sistema					
20	El área TI cuenta con políticas internas que sancionan a los trabajadores que vulneren la confiabilidad de información					
	Dimensión 5: Trazabilidad					
21	La política que presenta el área TI es que cada usuario es responsable de las acciones realizadas en los sistemas de información.					
22	Se cuenta con un control de acciones en el sistema para detectar los cambios que se realizan en el sistema					
23	El área TI suele contar con un sistema que permite monitorear a nivel de red el acceso a los sistemas de información de manera interna o externa.					
24	Se suele conta con un firewall para realizar la protección de información de los clientes.					

Cuestionario: ISO 27001

Fecha: 15/05/2023

Sexo: Femenino [ ] Masculino [X]

Tiempo de trabajo dentro del área TI: 5 años

Instrucciones: estimado usuario, el siguiente cuestionario tiene la intención de evaluar ***la implementación de las ISO 27001 en la empresa***. Las opiniones podrian ayudar a optimizar la gestión de la misma, en lo que se pueda perfeccionar, ese es el motivo principal para que conteste con la sinceridad del caso. Debe marcar sólo una de las alternativas, colocando un aspa (X) en el cuadro que corresponda según la siguiente valoración.

Valoración	Categoría
1	Nunca
2	Casi nunca
3	A veces
4	Casi siempre
5	Siempre

Preguntas:

	DIMENSIÓN 1: Planificación	1	2	3	4	5
1	Dentro del área TI el cumplimiento de los objetivos de seguridad de la información se encuentra enfocados en base a las ISO 27001		X			
2	El equipo del área TI asegura la integración de los requisitos de la ISO 27001 en los procesos de la empresa		X			
3	Existe apoyo en el área TI para la contribución efectiva de la ISO 27001	X				
4	En el área TI se establecen política de seguridad de la información				X	
5	En el área TI se suelen definir roles y responsabilidades para seguridad de la información				X	
6	En el área TI se realizan análisis de riesgo de la seguridad de la información				X	
7	La empresa se define y aplican proceso de valoración de riesgo de la seguridad de la información			X		
8	En la empresa se estructuran planes de tratamiento de riesgo de la seguridad de la información			X		
9	La empresa suele tener documentado los objetivos de la seguridad de la información			X		

10	La empresa plantea un plan de mejoras basados en el cumplimiento de los objetivos				X	
11	La empresa proporciona los recursos necesarios para la gestión de la seguridad informática en el área TI				X	
12	Se desarrollan evaluaciones de desempeño acerca de la seguridad información dentro de la empresa			X		
13	Se desarrollan políticas de seguridad de información				X	
14	Se definen canales de atención para la de la seguridad de información			X		
15	En la empresa se cuentan con la documentación de la seguridad de información para asegurar efectividad			X		
16	Se controla la información requerida para una gestión de seguridad; disponible y protegida			X		
	DIMENSIÓN 2: ejecución					
17	Se plantea una planificación, ejecución y control de procesos para la gestión de seguridad de información				X	
18	Se llevan a cabo evaluaciones de riesgos planificadas			X		
19	En la empresa se activan planes de tratamiento de riesgos		X			
	DIMENSIÓN 3: Verificación					
20	La empresa realiza el seguimiento, análisis y evaluación de la gestión de seguridad de información				X	
21	La empresa realiza auditorías internas				X	
22	La alta dirección revisa su gestión de seguridad de información para asegurar su eficacia			X		
23	La alta dirección toma decisiones y medidas en base a los resultados obtenidos por la gestión de seguridad de información			X		
	DIMENSIÓN 4: mejoramiento					
24	La empresa controla y corrige las normas de cumplimiento de la seguridad de información				X	
25	La empresa mejora continuamente la educación y efectividad de la gestión y efectividad de la gestión				X	

¡Muchas gracias!

Cuestionario: Gestión de seguridad de la información

Fecha: 15/05/2023

Sexo: Femenino [ ] Masculino [X]

Tiempo de trabajo dentro del área TI: 5 años

Instrucciones: estimado usuario, el siguiente cuestionario tiene la intención de ***evaluar la gestión de seguridad de la información***. Las opiniones podrían ayudar a optimizar la gestión de la misma, en lo que se pueda perfeccionar, ese es el motivo principal para que conteste con la sinceridad del caso. Debe marcar sólo una de las alternativas, colocando un aspa (X) en el cuadro que corresponda según la siguiente valoración.

Valoración	Categoría
1	Nunca
2	Casi nunca
3	A veces
4	Casi siempre
5	Siempre

Preguntas:

	DIMENSIÓN 1: Disponibilidad	1	2	3	4	5
1	Se encuentra con acceso a los sistemas de información durante las 24 horas del día					X
2	Es necesario que el área TI cuente con acceso a los sistemas de información durante las 24 horas del día					X
3	La red de datos actual permite que los servicios de sistemas de información se mantengan disponibles durante las 24 horas del día					X
4	La capacidad tecnológica del área TI requiere se optimice				X	
5	El ancho de banda de internet con que cuenta el área TI de la empresa permite trabajar con normalidad y evita saturación de datos				X	
	DIMENSIÓN 2: Autenticidad					
6	El área TI se suelen contar con políticas de seguridad para el acceso de los usuarios a su información					X
7	Se cuenta con un control de usuarios basados en un servidor de dominio					X
8	Los usuarios que se conectan de manera remota presentan identificación de nombres de equipo					X
9	Es necesario mejorar la modalidad actual de acceder a los sistemas por escritorio remoto		X			

10	Se ha registrado durante los últimos 6 meses intentos de vulneración de las informaciones		X			
	DIMENSIÓN 3: Integridad					
11	El área TI realiza copias de seguridad de los sistemas de información de manera periódica					X
12	Los usuarios que realizan trabajos remotos, poseen una carpeta compartida en el servidor para almacenar su información				X	
13	Cuando se presentan inconvenientes con los equipos de computadoras se cuenta con un personal que brinda soporte de manera oportuna				X	
14	El área TI cuenta con un administrador del sistema para brindar soporte de conexiones o inconsistencias presentadas					X
15	Se presentan problemas en los sistemas como; información duplicada o reporte sin información.		X			
	DIMENSIÓN 4: Confidencialidad					
16	El área TI cuenta con lineamientos que permiten la protección de datos de los trabajadores y usuarios					X
17	Se puede extraer informaciones del Área TI por medio de dispositivos como USB				X	
18	Se cuenta con un administrador que facilita los privilegios de los usuarios, de acuerdo a sus necesidades					X
19	Todos los usuarios tienen los mismos accesos al sistema	X				
20	El área TI cuenta con políticas internas que sancionan a los trabajadores que vulneren la confiabilidad de información		X			
	Dimensión 5: Trazabilidad					
21	La política que presenta el área TI es que cada usuario es responsable de las acciones realizadas en los sistemas de información.				X	
22	Se cuenta con un control de acciones en el sistema para detectar los cambios que se realizan en el sistema				X	
23	El área TI suele contar con un sistema que permite monitorear a nivel de red el acceso a los sistemas de información de manera interna o externa.					X
24	Se suele conta con un firewall para realizar la protección de información de los clientes.					X

¡Muchas gracias!

Cuestionario: ISO 27001

Fecha: 03 / 05 / 2023

Sexo: Femenino [ ] Masculino [X]

Tiempo de trabajo dentro del área TI: 17 AÑOS, 8 MESES

Instrucciones: estimado usuario, el siguiente cuestionario tiene la intención de evaluar ***la implementación de las ISO 27001 en la empresa***. Las opiniones podrían ayudar a optimizar la gestión de la misma, en lo que se pueda perfeccionar, ese es el motivo principal para que conteste con la sinceridad del caso. Debe marcar sólo una de las alternativas, colocando un aspa (X) en el cuadro que corresponda según la siguiente valoración.

Valoración	Categoría
1	Nunca
2	Casi nunca
3	A veces
4	Casi siempre
5	Siempre

Preguntas:

	DIMENSIÓN 1: Planificación	1	2	3	4	5
1	Dentro del área TI el cumplimiento de los objetivos de seguridad de la información se encuentra enfocados en base a las ISO 27001				X	
2	El equipo del área TI asegura la integración de los requisitos de la ISO 27001 en los procesos de la empresa				X	
3	Existe apoyo en el área TI para la contribución efectiva de la ISO 27001					X
4	En el área TI se establecen política de seguridad de la información					X
5	En el área TI se suelen definir roles y responsabilidades para seguridad de la información				X	
6	En el área TI se realizan análisis de riesgo de la seguridad de la información			X		
7	La empresa se define y aplican proceso de valoración de riesgo de la seguridad de la información			X		
8	En la empresa se estructuran planes de tratamiento de riesgo de la seguridad de la información				X	
9	La empresa suele tener documentado los objetivos de la seguridad de la información				X	

10	La empresa plantea un plan de mejoras basados en el cumplimiento de los objetivos				X	
11	La empresa proporciona los recursos necesarios para la gestión de la seguridad informática en el área TI				X	
12	Se desarrollan evaluaciones de desempeño acerca de la seguridad información dentro de la empresa			X		
13	Se desarrollan políticas de seguridad de información			X		
14	Se definen canales de atención para la de la seguridad de información					X
15	En la empresa se cuentan con la documentación de la seguridad de información para asegurar efectividad				X	
16	Se controla la información requerida para una gestión de seguridad: disponible y protegida				X	
	DIMENSIÓN 2: ejecución					
17	Se plantea una planificación, ejecución y control de procesos para la gestión de seguridad de información				X	
18	Se llevan a cabo evaluaciones de riesgos planificadas			X		
19	En la empresa se activan planes de tratamiento de riesgos			X		
	DIMENSIÓN 3: Verificación					
20	La empresa realiza el seguimiento, análisis y evaluación de la gestión de seguridad de información				X	
21	La empresa realiza auditorías internas					X
22	La alta dirección revisa su gestión de seguridad de información para asegurar su eficacia					X
23	La alta dirección toma decisiones y medidas en base a los resultados obtenidos por la gestión de seguridad de información				X	
	DIMENSIÓN 4: mejoramiento					
24	La empresa controla y corrige las normas de cumplimiento de la seguridad de información				X	
25	La empresa mejora continuamente la educación y efectividad de la gestión y efectividad de la gestión			X		

¡Muchas gracias!

Cuestionario: Gestión de seguridad de la información

Fecha: 15/05/2023

Sexo: Femenino [ ] Masculino [X]

Tiempo de trabajo dentro del área TI:

Instrucciones: estimado usuario, el siguiente cuestionario tiene la intención de ***evaluar la gestión de seguridad de la información***. Las opiniones podrían ayudar a optimizar la gestión de la misma, en lo que se pueda perfeccionar, ese es el motivo principal para que conteste con la sinceridad del caso. Debe marcar sólo una de las alternativas, colocando un aspa (X) en el cuadro que corresponda según la siguiente valoración.

Valoración	Categoría
1	Nunca
2	Casi nunca
3	A veces
4	Casi siempre
5	Siempre

Preguntas:

	DIMENSIÓN 1: Disponibilidad	1	2	3	4	5
1	Se encuentra con acceso a los sistemas de información durante las 24 horas del día					X
2	Es necesario que el área TI cuente con acceso a los sistemas de información durante las 24 horas del día			X		
3	La red de datos actual permite que los servicios de sistemas de información se mantengan disponibles durante las 24 horas del día					X
4	La capacidad tecnológica del área TI requiere se optimice			X		
5	El ancho de banda de internet con que cuenta el área TI de la empresa permite trabajar con normalidad y evita saturación de datos			X		
	DIMENSIÓN 2: Autenticidad					
6	El área TI se suelen contar con políticas de seguridad para el acceso de los usuarios a su información				X	
7	Se cuenta con un control de usuarios basados en un servidor de dominio					X
8	Los usuarios que se conectan de manera remota presentan identificación de nombres de equipo					X
9	Es necesario mejorar la modalidad actual de acceder a los sistemas por escritorio remoto			X		

10	Se ha registrado durante los últimos 6 meses intentos de vulneración de las informaciones	X				
	DIMENSIÓN 3: Integridad					
11	El área TI realiza copias de seguridad de los sistemas de información de manera periódica					X
12	Los usuarios que realizan trabajos remotos, poseen una carpeta compartida en el servidor para almacenar su información				X	
13	Cuando se presentan inconvenientes con los equipos de computadoras se cuenta con un personal que brinda soporte de manera oportuna			X		
14	El área TI cuenta con un administrador del sistema para brindar soporte de conexiones o inconsistencias presentadas				X	
15	Se presentan problemas en los sistemas como; información duplicada o reporte sin información.	X				
	DIMENSIÓN 4: Confidencialidad					
16	El área TI cuenta con lineamientos que permiten la protección de datos de los trabajadores y usuarios				X	
17	Se puede extraer informaciones del Área TI por medio de dispositivos como USB			X		
18	Se cuenta con un administrador que facilita los privilegios de los usuarios, de acuerdo a sus necesidades				X	
19	Todos los usuarios tienen los mismos accesos al sistema	X				
20	El área TI cuenta con políticas internas que sancionan a los trabajadores que vulneren la confiabilidad de información					X
	Dimensión 5: Trazabilidad					
21	La política que presenta el área TI es que cada usuario es responsable de las acciones realizadas en los sistemas de información.				X	
22	Se cuenta con un control de acciones en el sistema para detectar los cambios que se realizan en el sistema			X		
23	El área TI suele contar con un sistema que permite monitorear a nivel de red el acceso a los sistemas de información de manera interna o externa.			X		
24	Se suele conta con un firewall para realizar la protección de información de los clientes.			X		

¡Muchas gracias!

Cuestionario: ISO 27001

Fecha: 15 / 05 / 2023

Sexo: Femenino [ ] Masculino [X]

Tiempo de trabajo dentro del área TI: 3 años y 2 meses

Instrucciones: estimado usuario, el siguiente cuestionario tiene la intención de evaluar ***la implementación de las ISO 27001 en la empresa***. Las opiniones podrían ayudar a optimizar la gestión de la misma, en lo que se pueda perfeccionar, ese es el motivo principal para que conteste con la sinceridad del caso. Debe marcar sólo una de las alternativas, colocando un aspa (X) en el cuadro que corresponda según la siguiente valoración.

Valoración	Categoría
1	Nunca
2	Casi nunca
3	A veces
4	Casi siempre
5	Siempre

Preguntas:

	DIMENSIÓN 1: Planificación	1	2	3	4	5
1	Dentro del área TI el cumplimiento de los objetivos de seguridad de la información se encuentra enfocados en base a las ISO 27001				X	
2	El equipo del área TI asegura la integración de los requisitos de la ISO 27001 en los procesos de la empresa			X		
3	Existe apoyo en el área TI para la contribución efectiva de la ISO 27001		X			
4	En el área TI se establecen política de seguridad de la información			X		
5	En el área TI se suelen definir roles y responsabilidades para seguridad de la información				X	
6	En el área TI se realizan análisis de riesgo de la seguridad de la información				X	
7	La empresa se define y aplican proceso de valoración de riesgo de la seguridad de la información		X			
8	En la empresa se estructuran planes de tratamiento de riesgo de la seguridad de la información			X		
9	La empresa suele tener documentado los objetivos de la seguridad de la información			X		

10	La empresa plantea un plan de mejoras basados en el cumplimiento de los objetivos			X		
11	La empresa proporciona los recursos necesarios para la gestión de la seguridad informática en el área TI				X	
12	Se desarrollan evaluaciones de desempeño acerca de la seguridad información dentro de la empresa		X			
13	Se desarrollan políticas de seguridad de información				X	
14	Se definen canales de atención para la de la seguridad de información				X	
15	En la empresa se cuentan con la documentación de la seguridad de información para asegurar efectividad			X		
16	Se controla la información requerida para una gestión de seguridad; disponible y protegida				X	
	DIMENSIÓN 2: ejecución					
17	Se plantea una planificación, ejecución y control de procesos para la gestión de seguridad de información		X			
18	Se llevan a cabo evaluaciones de riesgos planificadas			X		
19	En la empresa se activan planes de tratamiento de riesgos		X			
	DIMENSIÓN 3: Verificación					
20	La empresa realiza el seguimiento, análisis y evaluación de la gestión de seguridad de información			X		
21	La empresa realiza auditorías internas					X
22	La alta dirección revisa su gestión de seguridad de información para asegurar su eficacia			X		
23	La alta dirección toma decisiones y medidas en base a los resultados obtenidos por la gestión de seguridad de información			X		
	DIMENSIÓN 4: mejoramiento					
24	La empresa controla y corrige las normas de cumplimiento de la seguridad de información			X		
25	La empresa mejora continuamente la educación y efectividad de la gestión y efectividad de la gestión	X				

¡Muchas gracias!

Cuestionario: Gestión de seguridad de la información

Fecha: 15/ 05 / 2023

Sexo: Femenino [ ] Masculino [X]

Tiempo de trabajo dentro del área TI: 7 años y 2 meses

Instrucciones: estimado usuario, el siguiente cuestionario tiene la intención de ***evaluar la gestión de seguridad de la información***. Las opiniones podrían ayudar a optimizar la gestión de la misma, en lo que se pueda perfeccionar, ese es el motivo principal para que conteste con la sinceridad del caso. Debe marcar sólo una de las alternativas, colocando un aspa (X) en el cuadro que corresponda según la siguiente valoración.

Valoración	Categoría
1	Nunca
2	Casi nunca
3	A veces
4	Casi siempre
5	Siempre

Preguntas:

	DIMENSIÓN 1: Disponibilidad	1	2	3	4	5
1	Se encuentra con acceso a los sistemas de información durante las 24 horas del día					X
2	Es necesario que el área TI cuente con acceso a los sistemas de información durante las 24 horas del día					X
3	La red de datos actual permite que los servicios de sistemas de información se mantengan disponibles durante las 24 horas del día				X	
4	La capacidad tecnológica del área TI requiere se optimice			X		
5	El ancho de banda de internet con que cuenta el área TI de la empresa permite trabajar con normalidad y evita saturación de datos				X	
	DIMENSIÓN 2: Autenticidad					
6	El área TI se suelen contar con políticas de seguridad para el acceso de los usuarios a su información				X	
7	Se cuenta con un control de usuarios basados en un servidor de dominio				X	
8	Los usuarios que se conectan de manera remota presentan identificación de nombres de equipo					X
9	Es necesario mejorar la modalidad actual de acceder a los sistemas por escritorio remoto				X	

10	Se ha registrado durante los últimos 6 meses intentos de vulneración de las informaciones		X			
	DIMENSIÓN 3: Integridad					
11	El área TI realiza copias de seguridad de los sistemas de información de manera periódica					X
12	Los usuarios que realizan trabajos remotos, poseen una carpeta compartida en el servidor para almacenar su información				X	
13	Cuando se presentan inconvenientes con los equipos de computadoras se cuenta con un personal que brinda soporte de manera oportuna				X	
14	El área TI cuenta con un administrador del sistema para brindar soporte de conexiones o inconsistencias presentadas					X
15	Se presentan problemas en los sistemas como; información duplicada o reporte sin información.		X			
	DIMENSIÓN 4: Confidencialidad					
16	El área TI cuenta con lineamientos que permiten la protección de datos de los trabajadores y usuarios				X	
17	Se puede extraer informaciones del Área TI por medio de dispositivos como USB	X				
18	Se cuenta con un administrador que facilita los privilegios de los usuarios, de acuerdo a sus necesidades					X
19	Todos los usuarios tienen los mismos accesos al sistema	X				
20	El área TI cuenta con políticas internas que sancionan a los trabajadores que vulneren la confiabilidad de información		X			
	Dimensión 5: Trazabilidad					
21	La política que presenta el área TI es que cada usuario es responsable de las acciones realizadas en los sistemas de información.				X	
22	Se cuenta con un control de acciones en el sistema para detectar los cambios que se realizan en el sistema				X	
23	El área TI suele contar con un sistema que permite monitorear a nivel de red el acceso a los sistemas de información de manera interna o externa.				X	
24	Se suele conta con un firewall para realizar la protección de información de los clientes.					X

¡Muchas gracias!

Anexo 4: Permiso de la institución

UNIVERSIDAD CÉSAR VALLEJO

POS GRA DO

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

Lima, 11 de mayo de 2023
Carta P. 0058-2023-UCV-VA-EPG-F01/J

Mt
Carlos Antonio Huerta Michiline
Maestro en Dirección de Sistemas y Tecnologías de la Información
Productos Paraíso del Perú SAC

De mi mayor consideración:

Es grato dirigirme a usted, para presentar a Medina Pinillos, José Roberto; identificado con DNI N° 43355207 y con código de matrícula N° 7002817285; estudiante del programa de MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN quien, en el marco de su tesis conducente a la obtención de su grado de MAESTRO, se encuentra desarrollando el trabajo de investigación titulado:

ISO 27001 para la Gestión de Seguridad de la Información en el área TI de una empresa industrial, Lima 2023

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

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

Atentamente,

ESCUELA DE POSGRADO UCV JEFATURA CAMPUS LIMA NORTE

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

PRODUCTOS PARAÍSO DEL PERÚ S.A.C.
Paraíso
CARLOS HUERTA MICHILINE
IT MANAGER

Anexo 5: ASPECTOS ADMINISTRATIVOS

4.1 Recursos y presupuesto

4.1.1 Recursos humanos

En función de la investigación realizada, se considerarán como necesario una serie de acciones desarrolladas por el investigador, en función de cubrir satisfactoriamente los objetivos planteados, tomándose como costo de los recursos humanos las inversiones que se desarrollarán en cuanto a; material bibliográfico, trasporte, manejo y procesamiento de base de datos. En este sentido se presenta la tabla 1.

Tabla 1

Presupuesto de recursos humanos.

Recursos	Descripción	Monto
Material bibliográfico	Referencias utilizadas	S/ 40. 00
Trasporte	Traslado	S/ 100. 00
Base de datos	Recojo, manejo y procesamiento	S/ 1,200. 00
Total		S/ 1,340.00

4.1.2 Recursos de Hardware

En este apartado se tomará como referencia a los equipos que se emplearan para la elaboración de la investigación a desarrollarse, considerándose en este particular una laptop. En conformidad se plantea la tabla 2.

Tabla 2

Presupuesto de recursos de hardware

Recursos	Descripción	Monto
Equipo	Laptop Hacer Nitro 5 (Modelo AN515-54-59ED)	S/ 4,000. 00
Total		S/ 4,000.00

4.1.2 Recursos de Software

Se indica que en la realización de la investigación se emplearán como recurso Software el programa estadístico Statistical Package for the Social sciencies (SPSS) versión 27 para el procesamiento de datos, por medio del cual se establecerán valores descriptivos e inferenciales que se obtendrán en el estudio. Al respecto, estas se especifican por medio de la tabla 3.

Tabla 3

Presupuesto de recursos de software

Recursos	Descripción	Monto
Licencia	Statistical Package for the Social sciencies (SPSS) versión 27	S/ 356. 00
Total		S/ 356. 00

4.1.4 Presupuesto

Para hacer la presentación del presupuesto se tomarán los montos totales de los presupuestos anteriormente establecidos; planteándose la sumatoria general como el coste total de la investigación.

Tabla 4

Presupuesto total

Sumatoria de costos	Monto
Recursos humanos	S/ 1,340.00
Recursos de hardware	S/ 4,000.00
Recursos de software	S/ 356. 00
Presupuesto total	S/ 5,696.00

4.2 Financiamiento

Para la presente investigación se hace referencia a que la totalidad del presupuesto estimado será cubierto por medio del autofinanciamiento, siendo el investigador, quien disponiendo de sus propuso recursos solventará los costos generados.

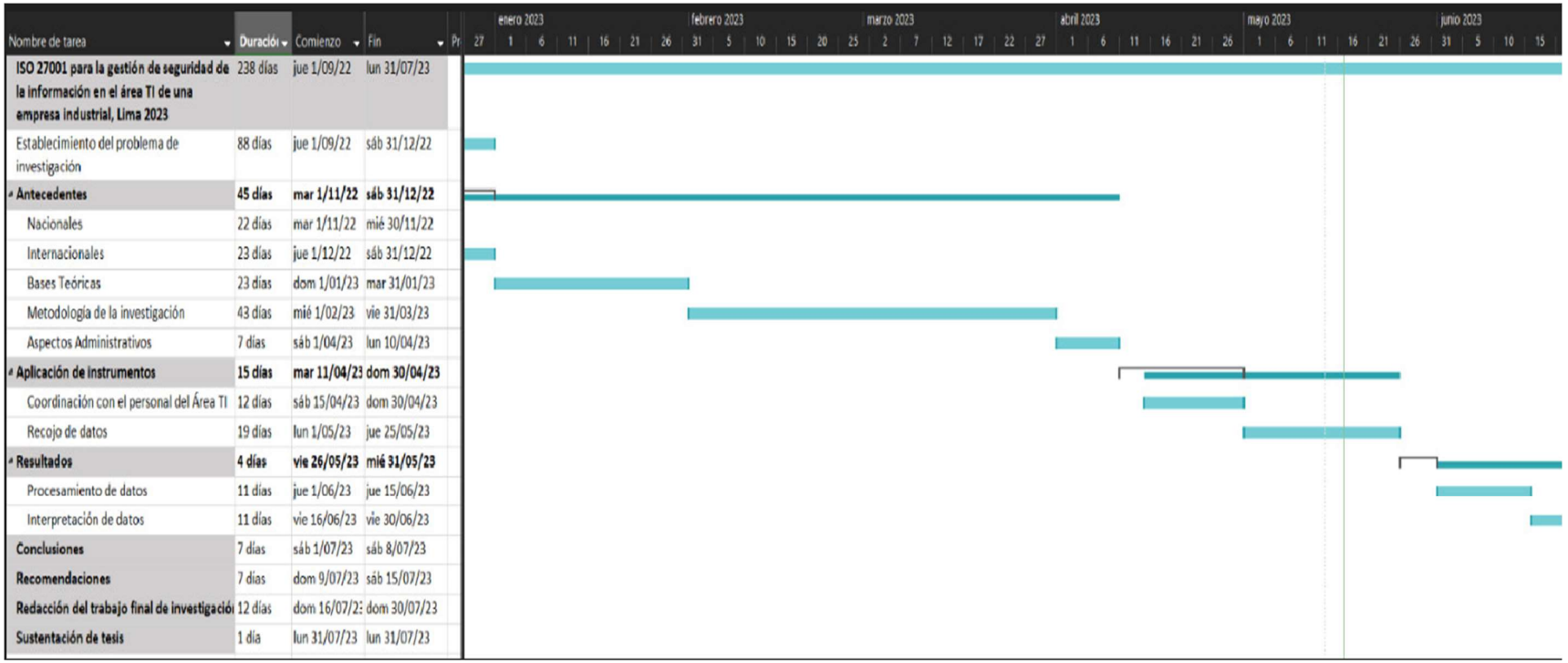
Tabla 5

Financiamiento

Entidad financiera	Monto	Porcentaje (%)
Autofinanciamiento	S/ 5,696.00	100%

4.3 Cronograma de Ejecución

En cuanto al estudio planteado, se presenta el cronograma de ejecución donde se refleja el tiempo empleado para las tareas llevadas a cabo.



Nombre de tarea	Duración	Comienzo	Fin
ISO 27001 para la gestión de seguridad de la información en el área TI de una empresa industrial, Lima 2023	238 días	jue 1/09/22	lun 31/07/23
Establecimiento del problema de investigación	88 días	jue 1/09/22	sáb 31/12/22
Antecedentes	**45 días**	**mar 1/11/22**	**sáb 31/12/22**
Nacionales	22 días	mar 1/11/22	mié 30/11/22
Internacionales	23 días	jue 1/12/22	sáb 31/12/22
Bases Teóricas	23 días	dom 1/01/23	mar 31/01/23
Metodología de la investigación	43 días	mié 1/02/23	vie 31/03/23
Aspectos Administrativos	7 días	sáb 1/04/23	lun 10/04/23
Aplicación de instrumentos	**15 días**	**mar 11/04/23**	**dom 30/04/23**
Coordinación con el personal del Área TI	12 días	sáb 15/04/23	dom 30/04/23
Recojo de datos	19 días	lun 1/05/23	jue 25/05/23
Resultados	**4 días**	**vie 26/05/23**	**mié 31/05/23**
Procesamiento de datos	11 días	jue 1/06/23	jue 15/06/23
Interpretación de datos	11 días	vie 16/06/23	vie 30/06/23
Conclusiones	7 días	sáb 1/07/23	sáb 8/07/23
Recomendaciones	7 días	dom 9/07/23	sáb 15/07/23
Redacción del trabajo final de investigación	12 días	dom 16/07/23	dom 30/07/23
Sustentación de tesis	1 día	lun 31/07/23	lun 31/07/23

Anexo 6: Fotos de la investigación (Lineamiento propuesto para la aplicación de la ISO 27001 en la Gestión de la Seguridad de la Información)

	Política de SGSI	
	Código	PO-SGSI-001
	Versión / Fecha	00 / 26.06.2023
	Última revisión	16.06.2023
	Revisado	Gerencia de TI
	Aprobado	Gerente de TI

1. OBJETIVO

El presente documento tiene como objetivo crear un sistema global de seguridad de la información que permita alcanzar el nivel de seguridad requerido por la empresa de acuerdo con las necesidades del negocio y los riesgos en los procesos de negocio.

La Política General de Seguridad de Información y los documentos asociados (normas y procedimientos) tienen los siguientes objetivos:

- Cumplir con los niveles de autorización y responsabilidad de la información (uso, divulgación, manejo y retención) establecidos para el desarrollo normal de los negocios. La delegación comienza con una solicitud de la administración del condado para aumentar el acceso a su personal y compartir la responsabilidad con cada miembro del personal autorizado.
- Reducir la posibilidad de que eventos inesperados interrumpan su negocio y reduzca el impacto de fallas en equipos, medios, procesamiento y equipos de comunicaciones.
- Proteger la información y cómo se procesa, almacena y transmite del uso no autorizado o divulgación accidental, error, fraude, sabotaje, invasión de la privacidad y otras actividades que podrían dañar o comprometer la información.
- Establecer, difundir y controlar la normativa relacionada con la protección de la información y los sistemas de la empresa.
- Cumplir con los estándares legales y reglamentarios establecidos por la ley y las autoridades de control correspondientes en relación con la seguridad de la información y los medios contenidos en ella.
- Educar y capacitar a los empleados sobre sus responsabilidades para mantener la seguridad de la información y el uso justo, y crear una cultura organizacional que incorpore la seguridad de la información como un aspecto relevante del negocio práctico de la empresa.

2. ALCANCE

Este documento y los documentos asociados establecen la PGSI para los usuarios de la empresa que deberá ser de conocimiento y cumplimiento obligatorio del personal, permanente o temporal, así como del personal de las compañías contratadas por la Empresa en tanto realicen tareas para ésta.

Este documento cubre los siguientes temas:

- Política de Seguridad de la Información
- Organización para la administración de Seguridad de Información
- Seguridad física y lógica de los equipos
- Administración de las operaciones y comunicaciones
- Controles de acceso
- Administración de la Continuidad de los Negocios
- Capacitación del personal
- Cumplimiento

3. NORMA O DOCUMENTOS DE REFERENCIA

- Norma ISO/IEC 27001 Sistema de Gestión de Seguridad de la Información.

	Política de SGSI	
	Código	PO-SGSI-001
	Versión / Fecha	00 / 26.06.2023
	Última revisión	16.06.2023
	Revisado	Gerencia de TI
	Aprobado	Gerente de TI

4. CONCEPTOS GENERALES

La información que utiliza una empresa ya sea información de clientes o información propia de la empresa, debe considerarse uno de sus activos más importantes. Esta información puede existir en una variedad de formas y puede imprimirse, almacenarse electrónicamente, transmitirse manual o electrónicamente, mostrarse gráficamente o mostrarse en una conversación. Independientemente de la forma en que se obtenga la información, o cómo se distribuya o almacene, siempre debe protegerse adecuadamente, porque la información no es solo inherente a los riesgos operativos asociados con los sistemas y tecnologías de la información.

La seguridad de la información garantiza la disponibilidad, integridad y confidencialidad de la información que es esencial para mantener una ventaja competitiva, cumplir con las leyes y reglamentos y proteger la imagen de una empresa. Nuestra información y los sistemas que la sustentan pueden ser objeto de amenazas tales como fraude, sabotaje, espionaje industrial, vandalismo, ataques de piratas y virus informáticos; estas amenazas ponen en riesgo cada vez mayor a nuestros sistemas informáticos y de información.

5. RESPONSABILIDADES

5.1. Gerencia de TI

- Cumplir con lo establecido en el presente procedimiento.
- Proporcionar las herramientas, ambientes y recursos materiales necesarios para la ejecución de las capacitaciones.
- Asegurar la inducción de los nuevos colaboradores.
- Administrar los registros de inducción y capacitaciones en materia de seguridad de la información.
- Mantener actualizados los legajos de personal con los certificados de capacitación.

5.2. Gerencias y Subgerencias

- Asegurar, motivar y facilitar la participación de los Jefes, Coordinadores, Supervisores y personal bajo su cargo en las actividades de capacitación en seguridad de la información.
- Identificar necesidades de capacitación del personal bajo su cargo.

5.3. Jefes, Coordinadores y Supervisores

- Asegurar, motivar y facilitar la participación del personal bajo su cargo en las actividades de capacitación en seguridad de la información.
- Asegurar que los proveedores in house bajo su cargo estén capacitados en seguridad de la información.
- Identificar necesidades de capacitación del personal bajo su cargo.
- Entrenar al personal en las funciones propias de su puesto de trabajo, considerando los lineamientos de seguridad de la información establecidos.

	Política de SGSI	
	Código	PO-SGSI-001
	Versión / Fecha	00 / 26.06.2023
	Última revisión	16.06.2023
	Revisado	Gerencia de TI
	Aprobado	Gerente de TI

6. MARCO NORMATIVO

6.1. Estructura de la Política de Seguridad de la Información

Los documentos sobre la política de seguridad de la información de la compañía incluyen los siguientes documentos:

- Política de seguridad de información, este documento
- Normas y procedimientos
- Estándares tecnológicos

6.2. Preparación y aprobación

Las normativas, procedimientos y estándares de la política de seguridad de la información serán desarrolladas al interior de la Empresa.

El Gerente de TI efectuará la revisión y una primera aprobación de las normativas elaboradas y posteriormente la Gerencia General previa evaluación, las aprobará. Posterior a ello la Gerencia de TI publicara los documentos aprobados.

6.3. Capacitación

Todos los empleados y usuarios externos deben recibir una formación adecuada a las funciones asignadas en la empresa, que debe incluir responsabilidades relacionadas con la seguridad de la información, uso de recursos, obligaciones legales y controles de negocio, así como formación en el uso correcto de las aplicaciones de tratamiento de la información. Esta capacitación debe ser actualizada constantemente. La Gerencia de RRHH debe incluir temas de seguridad de la información en el programa de capacitación de la empresa. Este equipo de liderazgo se coordinará con la Gerencia de TI en el alcance y la implementación. Esta capacitación debe categorizarse de acuerdo con el rol que desempeñará el empleado en la empresa y debe impartirse en un lenguaje claro y sencillo. Este entrenamiento debe entonces ser reforzado por una comunicación ocasional sobre el tema. Se deben llevar registros del proceso de formación en el que han participado los empleados.

	Política de SGSI	
	Código	PO-SGSI-001
	Versión / Fecha	00 / 26.06.2023
	Última revisión	16.06.2023
	Revisado	Gerencia de TI
	Aprobado	Gerente de TI

7. Política de Seguridad de la Información

7.1. Aspectos Generales

- Todo el personal de la empresa debe conocer sus responsabilidades respecto a la seguridad de la información.
- El personal que efectuara tareas críticas para la empresa debe pasar por un proceso de reclutamiento riguroso en el que se le indique claramente las responsabilidades que están asociadas a su función dentro de la misma.
- Un requisito fundamental para obtener niveles apropiados de seguridad de información en la empresa es la colaboración de todo el personal. Para conseguir su participación es imprescindible establecer políticas de sensibilización y concientización que permitan al personal conocer y asumir las políticas de seguridad de información.
- El incumplimiento de las políticas de seguridad de información conducirá a acciones disciplinarias que serán definidas por el área de Recursos Humanos de empresa, de acuerdo con la gravedad de la falta.
- Cuando una persona haga uso de su periodo vacacional, él o los usuarios de acceso a los distintos sistemas que utiliza, deberán ser temporalmente deshabilitados para evitar que personal no autorizado intente utilizar dichas cuentas para efectuar alguna acción no autorizada.
- Cuando una persona cesa en la empresa, el área de RRHH deberá comunicar vía correo electrónico al Área de TI para que sus credenciales sean deshabilitadas y posteriormente eliminadas de ser necesario.

7.2. Seguridad física y lógica

7.3. Sala de Comunicaciones y servidores

- Estas áreas deben de estar físicamente protegidas contra accesos no autorizados, daños e interferencias (control biométrico, grupo electrógeno, entre otros).
- La infraestructura eléctrica y el cableado en general deberán estar convenientemente ordenados a fin de prevenir cortocircuitos y fallos en los equipos. Así mismo, en la Sala de Servidores, los circuitos y redes informáticas deberán estar identificados y rotulados.
- El acceso a estas Áreas sólo estará permitido a personal autorizado y a terceros que realizan trabajos en estas instalaciones, los que deberán estar permanentemente supervisados por personal de la Empresa.

7.4. Seguridad de los equipos

- Todos los equipos informáticos de la empresa deberán estar tanto física como lógicamente protegidos.
- Se deben de establecer contraseñas de acceso a computadoras de escritorio, portátiles, entre por otros por periodos de inactividad (al no utilizar el equipo por más de 15 minutos, este se bloqueará automáticamente).

7.5. Acceso por usuarios

- La contraseña de cada usuario es personal e intransferible. Cada usuario es responsable del correcto uso de su contraseña, por lo tanto, todas las operaciones realizadas con su cuenta de usuario y contraseña serán de su entera responsabilidad.

- Una contraseña debe constar de mínimo ocho (8) caracteres: Uso de mayúsculas y minúsculas, números y símbolos. Las contraseñas deben ser cambiadas de manera obligatoria cada 90 días.
- La contraseña no puede coincidir con el nombre del usuario, no debe ser usada para otro servicio de la empresa, ni debe ser reutilizable (contraseña antigua)
- Las cuentas de usuario serán bloqueadas luego de tres (3) intentos fallidos de inicio de sesión. Estos intentos de accesos fallidos serán registrados y revisados con el usuario para conocer las causas de este error cuando solicite restablecer su contraseña.

7.6. Incidentes de Seguridad de la Información

Un incidente de seguridad de la información es cualquier evento no deseado o inesperado que compromete las operaciones de la empresa y afecta la confidencialidad, disponibilidad y/o integridad de la información o que representa una violación a las Políticas de Seguridad de la Información.

- El colaborador al momento de identificar un incidente de seguridad debe inmediatamente comunicarlo al Área de TI, vía correo electrónico, anexo telefónico o numero celular. En el caso de incidentes relacionados con correos del tipo Phishing, el usuario debe adjuntar el mismo en el correo, y luego de eso, eliminarlo de su cuenta de correo de manera inmediata.
- Es responsabilidad de los colaboradores de la empresa reportar los incidentes de seguridad de la información que tengan una probabilidad de materializar un riesgo.
- Si el incidente implica la infección por algún tipo de software malicioso como virus, troyano u otro, entonces el comunicado NO debe ser hecho por correo desde el equipo afectado, para evitar que la infección se siga transmitiendo a través de la red.
- El personal de TI debe conocer los procedimientos de respuesta a incidentes, que considera al menos las etapas de:
    - Identificación y reporte
    - Contención
    - Recuperación
    - Solución

7.7. Operaciones y comunicaciones

El personal de la empresa debe de seguir las siguientes políticas para una adecuada administración de sus procesos:

7.7.1. Control preventivo

- Todas las estaciones de trabajo de la empresa y locales remotos deben cumplir con el uso del software antivirus aprobado (actualmente es el Kaspersky Endpoint Security).
- En caso de ocurrir una infección por virus u otro tipo de ataque sobre una estación de trabajo, el usuario deberá manejarlo como un incidente de seguridad de información, reportándolo al Área de TI para que se proceda a solucionar el incidente.

- Los usuarios no deben usar ningún software que no haya sido revisado por el área de TI, para evitar la infección por virus o ataques de cualquier tipo. Además de esto, en caso de ser un software que requiera licenciamiento, NO podrá ser instalada una versión no original.
- El antivirus instalado en las estaciones de trabajo, debe ser permanentemente actualizados, bajo responsabilidad del área de TI.
- Los responsables de los controles preventivos del área de TI deberán emitir un informe mensual de los eventos de virus u otros ataques ocurridos en la plataforma de la Empresa, este informe debe ser entregado a la Gerencia de TI.

7.7.2. Seguridad de la Red

- Toda conexión externa a la red de la empresa deberá ser autorizada por la Gerencia de TI y estar acorde a la norma de conexiones externas, así mismo toda la información que se transmita deberá contar con un nivel de seguridad adecuado de acuerdo con su clasificación.
- Con el fin de garantizar un funcionamiento y mantenimiento adecuados, el responsable del mantenimiento de las Redes debe documentar y mantener actualizado el esquema de la Red de la empresa. Dicha documentación deberá estar a disposición del personal autorizado, cada vez que éste la requiera.

7.7.3. Copias de seguridad

- La disponibilidad de los sistemas operativos, aplicaciones en producción y base de datos, son la parte fundamental del plan de continuidad de negocio, por lo que es necesario asegurar que se contará con la disponibilidad de dicha información mediante un adecuado procedimiento de respaldo en base a copias de seguridad periódicas, locales y externas, de Software Base, Datos (bases de datos, archivos críticos en cinta) e Inventario de las copias de respaldo realizadas.
- Las copias de respaldo realizadas deberán almacenarse adicionalmente en una ubicación diferente a los sistemas respaldados, que cuente con fácil acceso y niveles de seguridad adecuados, evitando su pérdida en caso de siniestro de gran magnitud y asegurando el acceso adecuado en caso de contingencia.

7.7.4. Copias de correo electrónico

- El correo electrónico se pone a disposición del personal de la empresa para el desarrollo exclusivo de sus funciones laborales, el servicio de correo puede ser proporcionado tanto a nivel interno como externo.
- Todo correo electrónico que contenga información confidencial deberá tener en el Asunto "subject" la palabra CONFIDENCIAL, a modo de rotulación.
- La Política de Uso del Correo Electrónico aprobada por la Gerencia General de la Empresa, detalla todos los aspectos que deben ser considerados. El colaborador deberá cumplir con lo señalado en esta.

7.7.5. Seguridad en Internet

- El acceso a Internet se provee como una herramienta para el desarrollo exclusivo de la actividad laboral del personal de la empresa. El acceso deberá ser aprobado por la Gerencia respectiva.

- La Política de Uso de Internet aprobada por la Gerencia General de la Empresa, detalla todos los aspectos que deben ser considerados.

7.8. Control de Acceso

- La autorización de acceso a la información, por parte de los usuarios debe ser realizada de acuerdo con sus atribuciones, funciones y/o tareas a desarrollar. Estas deben ser asignadas por la gerencia correspondiente. Será responsabilidad del jefe directo definir el perfil de acceso de sus subordinados.
- Será responsabilidad del jefe directo definir el personal de reemplazo temporal para las funciones y tareas desarrolladas en su área, para períodos de vacaciones y licencias médicas. El acceso realizado por el personal de backup, deberá ser efectuado utilizando su cuenta personal, no puede utilizar la cuenta de la persona que reemplaza.
- El acceso a los recursos de información de la empresa es a través de usuarios y contraseñas. El área de TI es la responsable de la creación, administración y eliminación de los usuarios.
- El acceso a las aplicaciones deberá estar adecuadamente restringido sólo para usuarios con autorización, así mismo las aplicaciones deben contar con una adecuada estructura de perfiles de usuario que restrinja los accesos de acuerdo con las funciones y responsabilidades de los empleados de la Empresa.

7.8.1. Monitoreo y uso de sistemas de acceso

- Los sistemas de comunicaciones y servidores que contengan información sensible, valiosa o crítica de la Empresa deberán contar con un registro de eventos de seguridad de información relevante, para detectar lo siguiente:
  - Intentos fallidos de contraseñas.
  - Intentos de usar privilegios no autorizados.
  - Cambios a privilegios de usuarios.
  - Modificaciones a software de sistemas.
  - Accesos a las opciones del sistema a la cual está autorizado.
- Los eventos de seguridad antes mencionados deberán ser almacenados y el acceso de este debe estar permitido sólo a personal autorizado. Estos eventos serán de mucha utilidad para la corrección de errores, recuperación de violaciones de seguridad, auditorías e iniciativas relacionadas.

7.8.2. Acceso por parte del Área de TI

- El personal del área de TI está autorizado, previo consentimiento del usuario para revisar archivos de los usuarios con el propósito de resolver problemas inesperados tales como los generados por virus o caídas del sistema. En tal caso están obligados a notificar a los usuarios que se ha tomado tal acción. Si se efectuaron copias de los archivos éstas deben eliminarse.
- El Gerente de TI o a quien él designe en su reemplazo, podrán hacer uso de herramientas de hardware y/o software que pudieran evaluar o comprometer la seguridad de los sistemas de información, previa autorización de la Gerencia General y para propósitos de evaluar la seguridad de los sistemas (análisis de vulnerabilidades, Ethical Hacking). Esta autorización deberá ser otorgada por un período de tiempo limitado.

7.8.3. Control de cumplimiento de la PSGSI

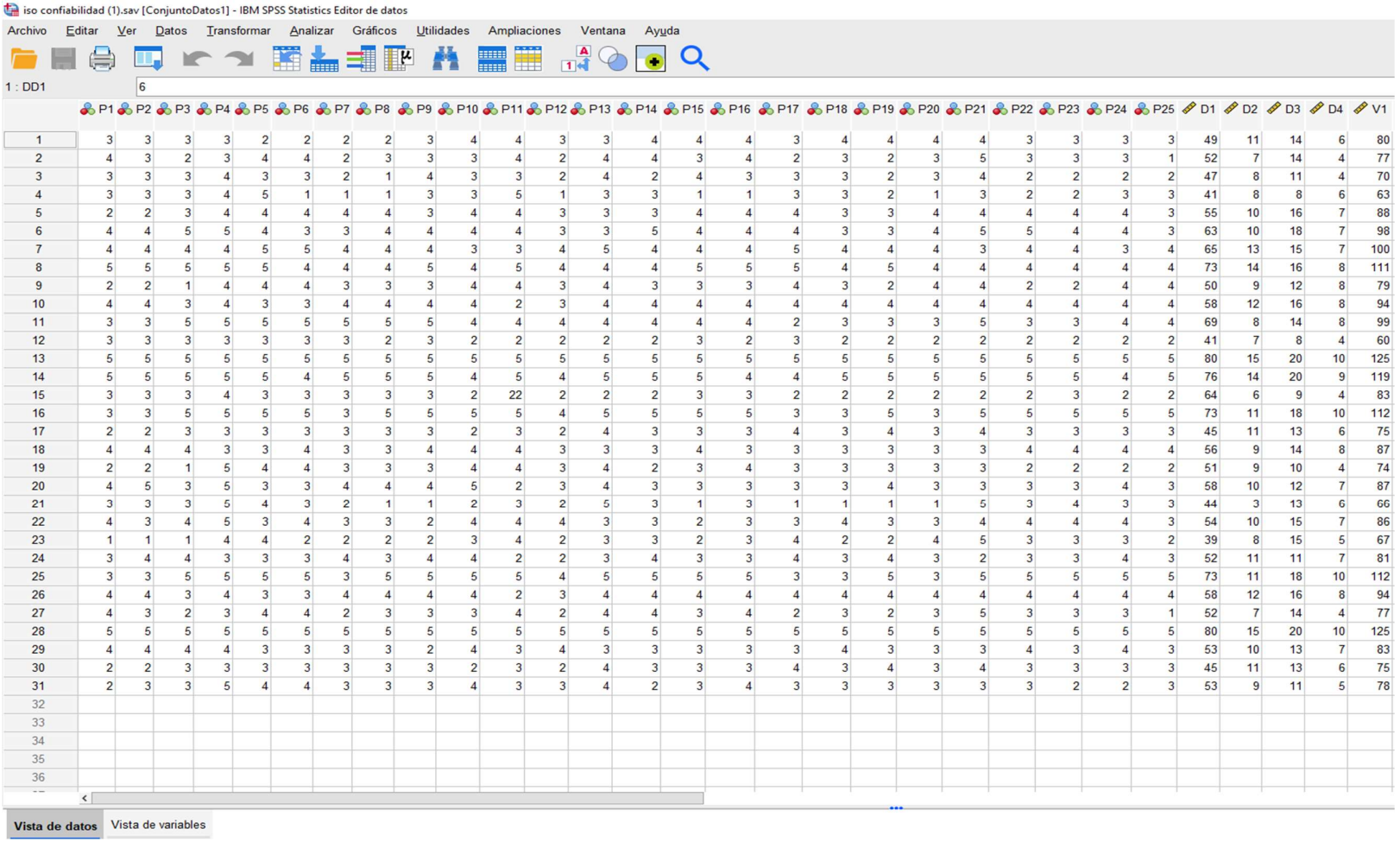
Dado que la empresa pone a disposición de los empleados internos o terceros los recursos de la información con el objeto de que éstos desarrollen su trabajo y funciones asignadas y que estas facilidades son sólo entregadas para que sean utilizadas para el propósito del negocio, se considera que los empleados no manejan información personal, por lo que los siguientes procesos de monitoreo y control son responsabilidad y derecho de la Empresa:

- La Gerencia General o quien ésta delegue se reserva el derecho de examinar todos los datos guardados o transmitidos en sus sistemas, correo electrónico, directorios de archivos personales, disco duro, carpetas compartidas, OneDrive, y cualquier otra información mantenida o transmitida en los sistemas de la Empresa. Esta revisión se realizará para asegurar la conformidad con las políticas de seguridad, para el apoyo a la ejecución de investigaciones internas y para ayudar al control de la administración de los sistemas de la Información.
- La Empresa se reserva el derecho de supervisar, acceder, recuperar, leer, y/o descubrir comunicaciones del personal cuando:
  - Exista una verdadera necesidad comercial que no pueda ser satisfecha a través de otros medios.
  - El personal involucrado no está disponible y el tiempo sea crítico para una actividad comercial.
  - Exista una causa razonable para sospechar de una actividad delictiva o violación a las políticas de seguridad de la información.
  - Sea requerida por la ley o regulación, para una supervisión.

8. Anexos

Anexo 7: Base de Datos

Variable: ISO 27001



iso confiabilidad (1).sav [ConjuntoDatos1] - IBM SPSS Statistics Editor de datos

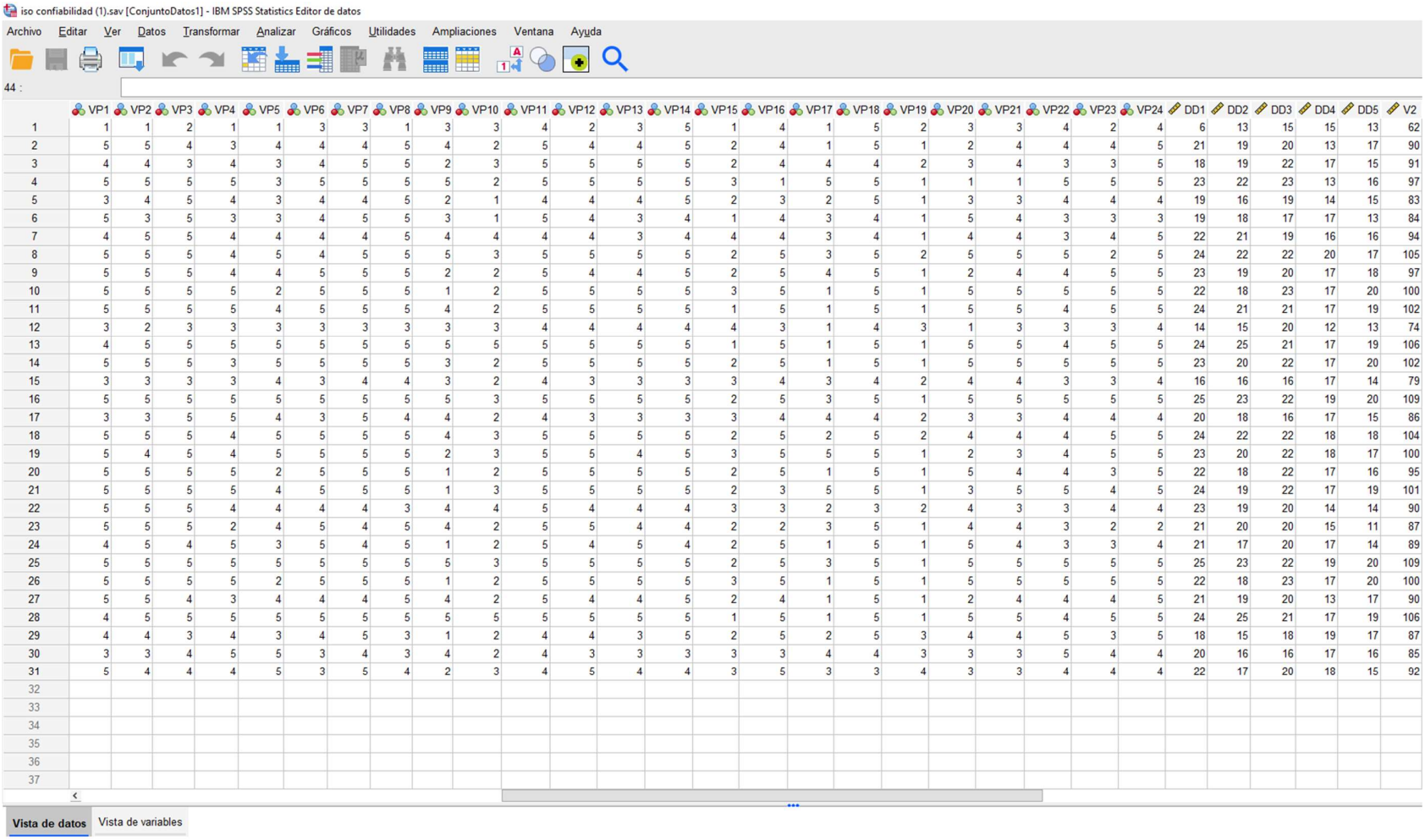
Archivo Editar Ver Datos Transformar Analizar Gráficos Utilidades Ampliaciones Ventana Ayuda

1 : DD1 6

	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14	P15	P16	P17	P18	P19	P20	P21	P22	P23	P24	P25	D1	D2	D3	D4	V1
1	3	3	3	3	2	2	2	2	3	4	4	3	3	4	4	4	3	4	4	4	4	3	3	3	3	49	11	14	6	80
2	4	3	2	3	4	4	2	3	3	3	4	2	4	4	3	4	2	3	2	3	5	3	3	3	1	52	7	14	4	77
3	3	3	3	4	3	3	2	1	4	3	3	2	4	2	4	3	3	3	2	3	4	2	2	2	2	47	8	11	4	70
4	3	3	3	4	5	1	1	1	3	3	5	1	3	3	1	1	3	3	2	1	3	2	2	3	3	41	8	8	6	63
5	2	2	3	4	4	4	4	4	3	4	4	3	3	3	4	4	4	3	3	4	4	4	4	4	3	55	10	16	7	88
6	4	4	5	5	4	3	3	4	4	4	4	3	3	5	4	4	4	3	3	4	5	5	4	4	3	63	10	18	7	98
7	4	4	4	4	5	5	4	4	4	3	3	4	5	4	4	4	5	4	4	4	3	4	4	3	4	65	13	15	7	100
8	5	5	5	5	5	4	4	4	5	4	5	4	4	4	5	5	5	4	5	4	4	4	4	4	4	73	14	16	8	111
9	2	2	1	4	4	4	3	3	3	4	4	3	4	3	3	3	4	3	2	4	4	2	2	4	4	50	9	12	8	79
10	4	4	3	4	3	3	4	4	4	4	2	3	4	4	4	4	4	4	4	4	4	4	4	4	4	58	12	16	8	94
11	3	3	5	5	5	5	5	5	5	4	4	4	4	4	4	4	2	3	3	3	5	3	3	4	4	69	8	14	8	99
12	3	3	3	3	3	3	3	2	3	2	2	2	2	2	3	2	3	2	2	2	2	2	2	2	2	41	7	8	4	60
13	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	80	15	20	10	125
14	5	5	5	5	5	4	5	5	5	4	5	4	5	5	5	4	4	5	5	5	5	5	5	4	5	76	14	20	9	119
15	3	3	3	4	3	3	3	3	3	2	22	2	2	2	3	3	2	2	2	2	2	2	3	2	2	64	6	9	4	83
16	3	3	5	5	5	5	3	5	5	5	5	4	5	5	5	5	3	3	5	3	5	5	5	5	5	73	11	18	10	112
17	2	2	3	3	3	3	3	3	3	2	3	2	4	3	3	3	4	3	4	3	4	3	3	3	3	45	11	13	6	75
18	4	4	4	3	3	4	3	3	4	4	4	3	3	3	4	3	3	3	3	3	3	4	4	4	4	56	9	14	8	87
19	2	2	1	5	4	4	3	3	3	4	4	3	4	2	3	4	3	3	3	3	3	2	2	2	2	51	9	10	4	74
20	4	5	3	5	3	3	4	4	4	5	2	3	4	3	3	3	3	3	4	3	3	3	4	3	3	58	10	12	7	87
21	3	3	3	5	4	3	2	1	1	2	3	2	5	3	1	3	1	1	1	1	5	3	4	3	3	44	3	13	6	66
22	4	3	4	5	3	4	3	3	2	4	4	4	3	3	2	3	3	4	3	3	4	4	4	4	3	54	10	15	7	86
23	1	1	1	4	4	2	2	2	2	3	4	2	3	3	2	3	4	2	2	4	5	3	3	3	2	39	8	15	5	67
24	3	4	4	3	3	3	4	3	4	4	2	2	3	4	3	3	4	3	4	3	2	3	3	4	3	52	11	11	7	81
25	3	3	5	5	5	5	3	5	5	5	5	4	5	5	5	5	3	3	5	3	5	5	5	5	5	73	11	18	10	112
26	4	4	3	4	3	3	4	4	4	4	2	3	4	4	4	4	4	4	4	4	4	4	4	4	4	58	12	16	8	94
27	4	3	2	3	4	4	2	3	3	3	4	2	4	4	3	4	2	3	2	3	5	3	3	3	1	52	7	14	4	77
28	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	80	15	20	10	125
29	4	4	4	4	3	3	3	3	2	4	3	4	3	3	3	3	3	4	3	3	3	4	3	4	3	53	10	13	7	83
30	2	2	3	3	3	3	3	3	3	2	3	2	4	3	3	3	4	3	4	3	4	3	3	3	3	45	11	13	6	75
31	2	3	3	5	4	4	3	3	3	4	3	3	4	2	3	4	3	3	3	3	3	3	2	2	3	53	9	11	5	78
32																														
33																														
34																														
35																														
36																														

Vista de datos Vista de variables

Variable: Gestión de la seguridad de la información



iso confiabilidad (1).sav [ConjuntoDatos1] - IBM SPSS Statistics Editor de datos

Archivo Editar Ver Datos Transformar Analizar Gráficos Utilidades Ampliaciones Ventana Ayuda

44 :

	VP1	VP2	VP3	VP4	VP5	VP6	VP7	VP8	VP9	VP10	VP11	VP12	VP13	VP14	VP15	VP16	VP17	VP18	VP19	VP20	VP21	VP22	VP23	VP24	DD1	DD2	DD3	DD4	DD5	V2
1	1	1	2	1	1	3	3	1	3	3	4	2	3	5	1	4	1	5	2	3	3	4	2	4	6	13	15	15	13	62
2	5	5	4	3	4	4	4	5	4	2	5	4	4	5	2	4	1	5	1	2	4	4	4	5	21	19	20	13	17	90
3	4	4	3	4	3	4	5	5	2	3	5	5	5	5	2	4	4	4	2	3	4	3	3	5	18	19	22	17	15	91
4	5	5	5	5	3	5	5	5	5	2	5	5	5	5	3	1	5	5	1	1	1	5	5	5	23	22	23	13	16	97
5	3	4	5	4	3	4	4	5	2	1	4	4	4	5	2	3	2	5	1	3	3	4	4	4	19	16	19	14	15	83
6	5	3	5	3	3	4	5	5	3	1	5	4	3	4	1	4	3	4	1	5	4	3	3	3	19	18	17	17	13	84
7	4	5	5	4	4	4	4	5	4	4	4	4	3	4	4	4	3	4	1	4	4	3	4	5	22	21	19	16	16	94
8	5	5	5	4	5	4	5	5	5	3	5	5	5	5	2	5	3	5	2	5	5	5	2	5	24	22	22	20	17	105
9	5	5	5	4	4	5	5	5	2	2	5	4	4	5	2	5	4	5	1	2	4	4	5	5	23	19	20	17	18	97
10	5	5	5	5	2	5	5	5	1	2	5	5	5	5	3	5	1	5	1	5	5	5	5	5	22	18	23	17	20	100
11	5	5	5	5	4	5	5	5	4	2	5	5	5	5	1	5	1	5	1	5	5	4	5	5	24	21	21	17	19	102
12	3	2	3	3	3	3	3	3	3	3	4	4	4	4	4	3	1	4	3	1	3	3	3	4	14	15	20	12	13	74
13	4	5	5	5	5	5	5	5	5	5	5	5	5	5	1	5	1	5	1	5	5	4	5	5	24	25	21	17	19	106
14	5	5	5	3	5	5	5	5	3	2	5	5	5	5	2	5	1	5	1	5	5	5	5	5	23	20	22	17	20	102
15	3	3	3	3	4	3	4	4	3	2	4	3	3	3	3	4	3	4	2	4	4	3	3	4	16	16	16	17	14	79
16	5	5	5	5	5	5	5	5	5	3	5	5	5	5	2	5	3	5	1	5	5	5	5	5	25	23	22	19	20	109
17	3	3	5	5	4	3	5	4	4	2	4	3	3	3	3	4	4	4	2	3	3	4	4	4	20	18	16	17	15	86
18	5	5	5	4	5	5	5	5	4	3	5	5	5	5	2	5	2	5	2	4	4	4	5	5	24	22	22	18	18	104
19	5	4	5	4	5	5	5	5	2	3	5	5	4	5	3	5	5	5	1	2	3	4	5	5	23	20	22	18	17	100
20	5	5	5	5	2	5	5	5	1	2	5	5	5	5	2	5	1	5	1	5	4	4	3	5	22	18	22	17	16	95
21	5	5	5	5	4	5	5	5	1	3	5	5	5	5	2	3	5	5	1	3	5	5	4	5	24	19	22	17	19	101
22	5	5	5	4	4	4	4	3	4	4	5	4	4	4	3	3	2	3	2	4	3	3	4	4	23	19	20	14	14	90
23	5	5	5	2	4	5	4	5	4	2	5	5	4	4	2	2	3	5	1	4	4	3	2	2	21	20	20	15	11	87
24	4	5	4	5	3	5	4	5	1	2	5	4	5	4	2	5	1	5	1	5	4	3	3	4	21	17	20	17	14	89
25	5	5	5	5	5	5	5	5	5	3	5	5	5	5	2	5	3	5	1	5	5	5	5	5	25	23	22	19	20	109
26	5	5	5	5	2	5	5	5	1	2	5	5	5	5	3	5	1	5	1	5	5	5	5	5	22	18	23	17	20	100
27	5	5	4	3	4	4	4	5	4	2	5	4	4	5	2	4	1	5	1	2	4	4	4	5	21	19	20	13	17	90
28	4	5	5	5	5	5	5	5	5	5	5	5	5	5	1	5	1	5	1	5	5	4	5	5	24	25	21	17	19	106
29	4	4	3	4	3	4	5	3	1	2	4	4	3	5	2	5	2	5	3	4	4	5	3	5	18	15	18	19	17	87
30	3	3	4	5	5	3	4	3	4	2	4	3	3	3	3	3	4	4	3	3	3	5	4	4	20	16	16	17	16	85
31	5	4	4	4	5	3	5	4	2	3	4	5	4	4	3	5	3	3	4	3	3	4	4	4	22	17	20	18	15	92
32																														
33																														
34																														
35																														
36																														
37																														

Vista de datos Vista de variables

Anexo 8: Matriz de Consistencia

Matriz de Consistencia
Título: ISO 27001 para la Gestión de Seguridad de la Información en el área TI de una empresa industrial, Lima 2023
Autor: Medina Pinillos, Jose Roberto

Problema	**Objetivos**	**Hipótesis**	**Variable 1:** ISO 27001				
			Dimensiones	**Indicadores**	**Ítem**	**Escala**	**Nivel**
General: ¿De qué manera ISO 27001 influye en la gestión de la seguridad de la información en el área TI de una empresa industrial, Lima 2023?	**General:** Determinar de qué manera ISO 27001 influye en la gestión de la seguridad de la información en el área TI de una empresa industrial, Lima 2023	**General:** ISO 27001 influye significativamente en la gestión de la seguridad de la información en el área TI de una empresa industrial, Lima 2023.	Planificación	Liderazgo, planeamiento, soporte	1-16	Escala de likert Siempre (5) casi siempre (4) A veces (3) Casi nunca (2) Nunca (1)	Ordinal
			Ejecución	Operaciones	17-19		
			Verificación	Evaluaciones de desempeño	20- 23		
			Mejoramiento	Mejora continua	24-25		
Específicos: ¿De qué manera ISO 27001 influye en la disponibilidad de la información en el área TI de una empresa industrial, Lima 2023?	**Específicos:** Determinar de qué manera ISO 27001 influye en la disponibilidad de la información en el área TI de una empresa industrial, Lima 2023	**Especificas:** ISO 27001 influye significativamente en la disponibilidad de la información en el área TI de una empresa industrial, Lima 2023	**Variable 2:** Gestión de Seguridad de la Información				
			Dimensiones	**Indicadores**	**Ítem**	**Escala**	**Nivel**
¿De qué manera ISO 27001 influye en la autenticidad de la información en el área TI de una empresa industrial, Lima 2023?	Determinar de qué manera ISO 27001 influye en la autenticidad de la información en el área TI de una empresa industrial, Lima 2023	ISO 27001 influye significativamente en la autenticidad de la información en el área TI de una empresa industrial, Lima 2023	Disponibilidad	Acceso las 24 horas, Estabilidad de la red, capacidades tecnológicas, anchos de banda,	1-5	Escala de likert Siempre (5) casi siempre (4) A veces (3) Casi nunca (2) Nunca (1)	Ordinal
¿De qué manera ISO 27001 influye en la integridad de la información en el área TI de una empresa industrial, Lima 2023?	Determinar de qué manera ISO 27001 influye en la integridad de la información en el área TI de una empresa industrial, Lima 2023	ISO 27001 influye significativamente en la integridad de la información en el área TI de una empresa industrial, Lima 2023	Autenticidad	políticas de seguridad, controles de los usuarios, Administración de equipos, vulnerabilidad de la información,	6- 10		
¿De qué manera ISO 27001 influye en la	Determinar de qué manera ISO 27001 influye en la	ISO 27001 influye significativamente en la	Integridad	copia de seguridad, soporte técnico, administración del sistema,	11-15		

<table>
<tr><td>confidencialidad de la información en el área TI de una empresa industrial, Lima 2023?
¿De qué manera ISO 27001 influye en la trazabilidad de la información en el área TI de una empresa industrial, Lima 2023?</td><td>confidencialidad de la información en el área TI de una empresa industrial, Lima 2023
Determinar de qué manera ISO 27001 influye en la trazabilidad de la información en el área TI de una empresa industrial, Lima 2023.</td><td>confidencialidad de la información en el área TI de una empresa industrial, Lima 2023

ISO 27001 influye significativamente en la trazabilidad de la información en el área TI de una empresa industrial, Lima 2023.</td><td>Confidencialidad

Trazabilidad</td><td>Protección de los datos,
Privilegios de acceso,
Políticas institucionales,
seguimiento de procesos.
rastreo de usuario,</td><td>16- 20

21- 24</td><td></td><td></td></tr>
<tr><td>Tipo y diseño de investigación</td><td>Población y muestra</td><td>Técnicas e instrumentos</td><td colspan="5">Estadística a utilizar</td></tr>
<tr><td>Enfoque:
Cuantitativa</td><td rowspan="2">Población:
31 trabajador del área TI de una empresa industrial</td><td>Variable 1:</td><td colspan="5" rowspan="4">DESCRIPTIVA:
Se procesaron los datos empleando el programa SPSS versión 27, por medio del cual se presentarán resultados descriptivos representados en tablas y gráficos estadísticos de distribución absolutas y porcentuales

INFERENCIAL:
Para el cálculo de los resultados inferenciales se empleó la regresión lineal.</td></tr>
<tr><td>Nivel:
Correlacional causal</td><td>Técnicas: Encuesta.</td></tr>
<tr><td>Diseño:
No experimental-trasversal</td><td rowspan="2">Tipo de muestreo:
No probabilístico- censal</td><td>Instrumentos:
Cuestionario</td></tr>
<tr><td>Tipo:
básica</td><td>Tamaño de muestra: 31 trabajador del área TI de una empresa industrial</td><td>Variable 2:
Técnicas: Encuesta.</td></tr>
<tr><td></td><td></td><td>Instrumentos:
Cuestionario</td></tr>
</table>

UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

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

Declaratoria de Autenticidad del Asesor

Yo, ACUÑA BENITES MARLON FRANK, docente de la ESCUELA DE POSGRADO MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA NORTE, asesor de Tesis titulada: "ISO 27001 para la Gestión de Seguridad de la Información en el Área TI de una Empresa Industrial, Lima 2023", cuyo autor es MEDINA PINILLOS JOSE ROBERTO, constato que la investigación tiene un índice de similitud de 10.00%, verificable en el reporte de originalidad del programa Turnitin, el cual ha sido realizado sin filtros, ni exclusiones.

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

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

LIMA, 31 de Julio del 2023

Apellidos y Nombres del Asesor:	**Firma**
ACUÑA BENITES MARLON FRANK **DNI:** 42097456 **ORCID:** 0000-0001-5207-9353	Firmado electrónicamente por: MACUNABE el 31-07-2023 22:58:42

Código documento Trilce: TRI - 0632191

INVESTIGA UCV