

**UNIVERSIDAD NACIONAL
TORIBIO RODRÍGUEZ DE MENDOZA DE AMAZONAS**



**FACULTAD DE INGENIERÍA DE SISTEMAS Y MECÁNICA
ELÉCTRICA
ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS**

**TESIS PARA OBTENER
EL TÍTULO PROFESIONAL DE
INGENIERO DE SISTEMAS**

**INFLUENCIA DE LA ISO/IEC 27001:2022 EN LA
SEGURIDAD DE LA INFORMACIÓN DE EMPRESA
ELÉCTRICA**

Autor: Bach. Keymer Alexis Bustamante Campos

Asesor: Mg. Ivan Adrianzén Olano

Registro:

CHACHAPOYAS – PERÚ

2024

DEDICATORIA

A mis padres, Antonio Bustamante y Marleny Campos, hermanos y amigos, quienes han sido fuente constante de amor y apoyo. Este logro no es solo mío, sino de todos ustedes que han estado a mi lado en este emocionante viaje académico.

Keymer Alexis Bustamante Campos

AGRADECIMIENTO

A los profesionales, Mg. Ivan Adrianzén Olano, Mg. Luis Manuel Sánchez Fernández e Ing. Elvis Eduardo Otiniano Amambal por su orientación, sabiduría y paciencia durante el exigente recorrido académico.

A la alta dirección y colaboradores de EMSEU S.A.C. por acogerme y compartir conmigo sus conocimientos y experiencias.

A mi familia y aquellas personas que contribuyeron en mi crecimiento personal. Este logro no habría sido posible sin el aporte y respaldo de cada uno de ustedes.

Keymer Alexis Bustamante Campos

**AUTORIDADES DE LA UNIVERSIDAD NACIONAL TORIBIO RODRÍGUEZ
DE MENDOZA DE AMAZONAS**

Ph. D. JORGE LUIS MAICELO QUINTANA

Rector

Dr. OSCAR ANDRÉS GAMARRA TORRES

Vicerrector Académico

Dra. MARÍA NELLY LUJÁN ESPINOZA

Vicerrectora de Investigación

Dr. ÍTALO MALDONADO RAMÍREZ

Decano de la Facultad de Ingeniería de Sistemas y Mecánica Eléctrica

VISTO BUENO DEL ASESOR DE LA TESIS



UNTRM

REGLAMENTO GENERAL
PARA EL OTORGAMIENTO DEL GRADO ACADÉMICO DE
BACHILLER, MAESTRO O DOCTOR Y DEL TÍTULO PROFESIONAL


ANEXO 3-L

VISTO BUENO DEL ASESOR DE TESIS PARA OBTENER EL TÍTULO PROFESIONAL

El que suscribe el presente, docente de la UNTRM ()/Profesional externo (), hace constar que ha asesorado la realización de la Tesis titulada INFLUENCIA DE LA ISO/IEC 27001:2022 EN LA SEGURIDAD DE LA INFORMACIÓN DE EMPRESA ELÉCTRICA del egresado KEYMER ALEXIS BUSTAMANTE CAMPOS de la Facultad de INGENIERÍA DE SISTEMAS Y MECÁNICA ELÉCTRICA Escuela Profesional de INGENIERÍA DE SISTEMAS de esta Casa Superior de Estudios.

El suscrito da el Visto Bueno a la Tesis mencionada, dándole pase para que sea sometida a la revisión por el Jurado Evaluador, comprometiéndose a supervisar el levantamiento de observaciones que formulen en Acta en conjunto, y estar presente en la sustentación.

Chachapoyas, 11 de DICIEMBRE de 2023



Firma y nombre completo del Asesor
ADRIANZEN OLAND IVAN

JURADO EVALUADOR DE LA TESIS



Mg. EDER NICANOR FIGUEROA PISCOYA

Presidente



Mg. CARLOS LUIS LOBATÓN ARENAS

Secretario



Mg. ROBERTO CARLOS SANTA CRUZ ACOSTA

Vocal

CONSTANCIA DE ORIGINALIDAD DE LA TESIS



UNTRM

REGLAMENTO GENERAL
PARA EL OTORGAMIENTO DEL GRADO ACADÉMICO DE
BACHILLER, MAESTRO O DOCTOR Y DEL TÍTULO PROFESIONAL

ANEXO 3-Q

CONSTANCIA DE ORIGINALIDAD DE LA TESIS PARA OBTENER EL TÍTULO PROFESIONAL

Los suscritos, miembros del Jurado Evaluador de la Tesis titulada:

INFLUENCIA DE LA ISO/IEC 27001:2022 EN LA SEGURIDAD DE LA INFORMACIÓN DE EMPRESA ELÉCTRICA

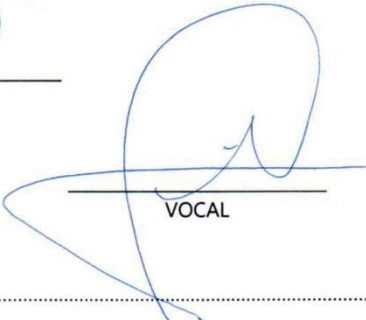
presentada por el estudiante ()/egresado (x) Kaymer Alexis Bustamante Compas
de la Escuela Profesional de Ingeniería de Sistemas
con correo electrónico institucional 7197696472@untrm.edu.pe

después de revisar con el software Turnitin el contenido de la citada Tesis, acordamos:

- La citada Tesis tiene 20 % de similitud, según el reporte del software Turnitin que se adjunta a la presente, el que es menor (x) / igual () al 25% de similitud que es el máximo permitido en la UNTRM.
- La citada Tesis tiene _____ % de similitud, según el reporte del software Turnitin que se adjunta a la presente, el que es mayor al 25% de similitud que es el máximo permitido en la UNTRM, por lo que el aspirante debe revisar su Tesis para corregir la redacción de acuerdo al Informe Turnitin que se adjunta a la presente. Debe presentar al Presidente del Jurado Evaluador su Tesis corregida para nueva revisión con el software Turnitin.

Chachapoyas, 26 de 03 del 2024


SECRETARIO


VOCAL


PRESIDENTE

OBSERVACIONES:

.....
.....

RESUMEN TURNITIN


TESIS INFLUENCIA DE LA ISO/IEC 27001:2022 EN LA SEGURIDAD DE LA INFORMACIÓN DE EMPRESA ELÉCTRICA

INFORME DE ORIGINALIDAD

20%	20%	4%	8%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	hdl.handle.net Fuente de Internet	8%
2	repositorio.ucv.edu.pe Fuente de Internet	3%
3	Submitted to Universidad Cesar Vallejo Trabajo del estudiante	1%
4	repositorio.upn.edu.pe Fuente de Internet	1%
5	Submitted to Escuela de Posgrado Newman Trabajo del estudiante	1%
6	repositorio.unc.edu.pe Fuente de Internet	1%
7	worldwidescience.org Fuente de Internet	1%
8	repositorio.uwiener.edu.pe Fuente de Internet	<1%
9	repositorio.uta.edu.ec Fuente de Internet	


Mr. EVER NICANOR FIGUEROA PIZARRO
Presidente del Jurado Evaluador.

ACTA DE SUSTENTACIÓN DE LA TESIS



UNTRM

REGLAMENTO GENERAL
PARA EL OTORGAMIENTO DEL GRADO ACADÉMICO DE
BACHILLER, MAESTRO O DOCTOR Y DEL TÍTULO PROFESIONAL

ANEXO 3-5

ACTA DE SUSTENTACIÓN DE TESIS PARA OBTENER EL TÍTULO PROFESIONAL

En la ciudad de Chachapoyas, el día 14 de mayo del año 2024 siendo las 10:00 horas, el aspirante: Keymer Alexis Bustamante Campos, asesorado por Mg. Iván Adrián Olano defiende en sesión pública presencial (X) / a distancia () la Tesis titulada: Influencia de la ISO/IEC 27001:2022 en la Seguridad de la Información de empresa eléctrica, para obtener el Título Profesional de Ingeniero de sistemas, a ser otorgado por la Universidad Nacional Toribio Rodríguez de Mendoza de Amazonas; ante el Jurado Evaluador, constituido por:

Presidente: Mg. Eder Nicanor Figueroa Piscocoya

Secretario: Mg. Carlos Luis Lobatón Arenas

Vocal: M. Roberto Carlos Santa Cruz Acosta

Procedió el aspirante a hacer la exposición de la Introducción, Material y métodos, Resultados, Discusión y Conclusiones, haciendo especial mención de sus aportaciones originales. Terminada la defensa de la Tesis presentada, los miembros del Jurado Evaluador pasaron a exponer su opinión sobre la misma, formulando cuantas cuestiones y objeciones consideraron oportunas, las cuales fueron contestadas por el aspirante.

Tras la intervención de los miembros del Jurado Evaluador y las oportunas respuestas del aspirante, el Presidente abre un turno de intervenciones para los presentes en el acto de sustentación, para que formulen las cuestiones u objeciones que consideren pertinentes.

Seguidamente, a puerta cerrada, el Jurado Evaluador determinó la calificación global concedida a la sustentación de la Tesis para obtener el Título Profesional, en términos de:

Aprobado (X) por Unanimidad (X) / Mayoría () Desaprobado ()

Otorgada la calificación, el Secretario del Jurado Evaluador lee la presente Acta en esta misma sesión pública. A continuación se levanta la sesión.

Siendo las 11:00 horas del mismo día y fecha, el Jurado Evaluador concluye el acto de sustentación de la Tesis para obtener el Título Profesional.


SECRETARIO


VOCAL


PRESIDENTE

OBSERVACIONES:

.....

ÍNDICE O CONTENIDO GENERAL

DEDICATORIA	ii
AGRADECIMIENTO	iii
AUTORIDADES DE LA UNIVERSIDAD NACIONAL TORIBIO RODRÍGUEZ DE MENDOZA DE AMAZONAS	iv
VISTO BUENO DEL ASESOR DE LA TESIS	v
JURADO EVALUADOR DE LA TESIS	vi
CONSTANCIA DE ORIGINALIDAD DE LA TESIS.....	vii
RESUMEN TURNITIN	viii
ACTA DE SUSTENTACIÓN DE LA TESIS.....	ix
ÍNDICE O CONTENIDO GENERAL	x
ÍNDICE DE TABLAS	xii
ÍNDICE DE FIGURAS	xiii
RESUMEN	1
ABSTRACT.....	xv
I. INTRODUCCIÓN	16
II. MATERIAL Y MÉTODOS.....	19
2.1. Tipo y diseño de investigación.....	19
2.2. Población, muestra y muestreo	19
2.3. Técnica e instrumento de recolección de datos.....	21
2.4. Procedimiento de recolección de datos	22
2.5. Método de análisis de datos	22
2.6. Análisis de datos	22
III. RESULTADOS	23
3.1. Resultados del pre-test	23
3.2. Cumplimiento de la ISO/IEC 27001:2022.....	27
3.3. Resultados del pos-test.....	32

3.4. Prueba de normalidad.....	36
3.5. Prueba de hipótesis.....	38
IV. DISCUSIÓN	42
V. CONCLUSIONES	45
VI. RECOMENDACIONES.....	46
VII. REFERENCIAS BIBLIOGRÁFICAS	47
ANEXOS	53

ÍNDICE DE TABLAS

Tabla 1 <i>Distribución de la muestra</i>	20
Tabla 2 <i>Resultados del pre-test de la seguridad de la información</i>	23
Tabla 3 <i>Resultados del pre-test de la dimensión integridad</i>	24
Tabla 4 <i>Resultados del pre-test de la dimensión confidencialidad</i>	25
Tabla 5 <i>Resultados del pre-test de la dimensión disponibilidad</i>	26
Tabla 6 <i>Resultados del cumplimiento de la ISO/IEC 27001:2022</i>	27
Tabla 7 <i>Resultados de la dimensión planificación</i>	28
Tabla 8 <i>Resultados de la dimensión ejecución</i>	29
Tabla 9 <i>Resultados de la dimensión verificación</i>	30
Tabla 10 <i>Resultados de la dimensión mejoramiento</i>	31
Tabla 11 <i>Resultados del pos-test de la seguridad de la información</i>	32
Tabla 12 <i>Resultados del pos-test de la dimensión integridad</i>	33
Tabla 13 <i>Resultados del pos-test de la dimensión confidencialidad</i>	34
Tabla 14 <i>Resultados del pos-test de la dimensión disponibilidad</i>	35
Tabla 15 <i>Prueba de normalidad de hipótesis general</i>	36
Tabla 16 <i>Prueba de normalidad de hipótesis específica 1</i>	37
Tabla 17 <i>Prueba de normalidad de hipótesis específica 2</i>	37
Tabla 18 <i>Prueba de normalidad de hipótesis específica 3</i>	37
Tabla 19 <i>Prueba de hipótesis general</i>	38
Tabla 20 <i>Prueba de hipótesis específica 1</i>	39
Tabla 21 <i>Prueba de hipótesis específica 2</i>	40
Tabla 22 <i>Prueba de hipótesis específica 3</i>	41

ÍNDICE DE FIGURAS

Figura 1 <i>Resultados del pre-test de la seguridad de la información</i>	24
Figura 2 <i>Resultados del pre-test de la dimensión integridad</i>	25
Figura 3 <i>Resultados del pre-test de la dimensión confidencialidad</i>	26
Figura 4 <i>Resultados del pre-test de la dimensión disponibilidad</i>	27
Figura 5 <i>Resultados del cumplimiento de la ISO/IEC 27001:2022</i>	28
Figura 6 <i>Resultados de la dimensión planificación</i>	29
Figura 7 <i>Resultados de la dimensión ejecución</i>	30
Figura 8 <i>Resultados de la dimensión verificación</i>	31
Figura 9 <i>Resultados de la dimensión mejoramiento</i>	32
Figura 10 <i>Resultados del pos-test de la seguridad de la información</i>	33
Figura 11 <i>Resultados del pos-test de la dimensión integridad</i>	34
Figura 12 <i>Resultados del pos-test de la dimensión confidencialidad</i>	35
Figura 13 <i>Resultados del pos-test de la dimensión disponibilidad</i>	36

RESUMEN

El objetivo de esta investigación fue determinar la influencia de la ISO/IEC 27001:2022 en la seguridad de la información en EMSEU S.A.C. La metodología que se utilizó fue aplicada bajo un diseño pre experimental, en el que se evaluó un conjunto de individuos antes y después del tratamiento. La población estuvo integrada por 60 empleados, de donde se seleccionó una muestra de 35 mediante un muestreo no probabilístico por conveniencia, basado en criterios para incluir y excluir individuos. La técnica que se usó en la recopilación de datos fue la encuesta, y el instrumento fue el cuestionario. La validez del instrumento se determinó con el juicio de expertos, mientras el nivel de confiabilidad se midió empleando el coeficiente alfa de Cronbach. El análisis estadístico integró el análisis descriptivo con el inferencial y se ejecutó en SPSS.

Como resultados, se logró que antes de la aplicación del tratamiento, el 88.6% de los encuestados expresó su desacuerdo, y el 11.4% manifestó no estar ni de acuerdo ni en desacuerdo. En contraste, después de la implementación exitosa del estándar, el 91,4% expresó estar de acuerdo y el 8.6% estar totalmente de acuerdo con la seguridad de la información. Al existir diferencia significativa con tendencia positiva entre el pre y post-test, donde $p < 0.05$, se excluyó la H_0 y se admitió la H_a . En conclusión, el estándar ISO/IEC 27001:2022 influye de manera significativa en la seguridad de la información y en sus dimensiones.

Palabras clave: ISO/IEC 27001, Gestión, Políticas, Seguridad de la información, Integridad, Confidencialidad, Disponibilidad.

ABSTRACT

The objective of this research was to determine the influence of ISO/IEC 27001:2022 on information security at EMSEU S.A.C. The methodology used was applied under a pre-experimental design, in which a set of individuals was evaluated before and after the treatment. The population consisted of 60 employees, from which a sample of 35 was selected by non-probabilistic convenience sampling, based on criteria for including and excluding individuals. The technique used in data collection was the survey, and the instrument was the questionnaire. The validity of the instrument was determined by expert judgment, while the level of reliability was measured using Cronbach's alpha coefficient. The statistical analysis integrated descriptive and inferential analysis and was performed in SPSS.

As results, it was found that before the implementation of the treatment, 88.6% of the respondents expressed disagreement, and 11.4% expressed neither agreement nor disagreement. In contrast, after the successful implementation of the standard, 91.4% expressed agreement and 8.6% strongly agreed with information security. As there was a significant difference with a positive trend between the pre- and post-test, where $p < 0.05$, H_0 was excluded and H_a was admitted. In conclusion, the ISO/IEC 27001:2022 standard significantly influences information security and its dimensions.

Key words: ISO/IEC 27001, Management, Policies, Information security, Integrity, Confidentiality, Availability.

I. INTRODUCCIÓN

Hoy en día, el avance de las soluciones informáticas ha hecho que las empresas dependan cada vez más de ellas para aplicar sus estrategias y alcanzar así sus objetivos (Fathurohman & Witjaksono, 2020). Sin embargo, esta dependencia también ha aumentado el riesgo de vulnerabilidades informáticas y actos maliciosos que comprometen la seguridad de aplicativos de información, redes o dispositivos IoT (Llano et al., 2021).

A nivel mundial, las vulnerabilidades informáticas y las ciberamenazas han aumentado considerablemente en alcance, complejidad y eficacia (Fortinet, 2022). Por ello, según Microsoft (2022), existe una creciente necesidad de asegurar la información, ya que es uno de los activos con más valor en las organizaciones. IBM (2022), en su informe lo demuestra: 4,35 millones dólares, es el coste total promedio global de las vulneraciones a la información, de las cuales, Verizon (2022), en su reporte anual, menciona que el 82% de las vulnerabilidades se debe al factor humano, es decir, se dan a partir de errores humanos.

En ese contexto, en el ámbito regional, el informe de Kaspersky (2022), señala que Latinoamérica se ha transformado en el epicentro de amenazas financieras, debido a que, desgraciadamente, se ha comprobado que las malas prácticas y el uso de piratería continúa siendo un importante vector que pone en riesgo a la información. Por otro lado, ESET (2022), afirma que más del 60% de las organizaciones se esfuerzan por mejorar su preparación en cuanto a protección de la información, dado que les preocupa el robo de la misma.

A escala nacional, las tecnologías de la información también están ganando mayor importancia, por lo que se han tomado medidas necesarias para poner en marcha un gobierno con normativas claras que permitan salvaguardar la información (Altamirano, 2021). No obstante, el informe anual de ESET (2022), muestra que Perú es el país donde más brechas de seguridad informática se detectan, con un 18%, frente al 17% de México, el 12% de Colombia, el 11% de Argentina y el 9% de Ecuador.

Ahora bien, la empresa responsable de distribuir la energía eléctrica en Utcubamba, denominada EMSEU S.A.C., se encuentra en una fase estratégica de mejora continua, orientada a adoptar e integrar las TIC en sus departamentos y áreas, incluyendo procesos

empresariales, modelos de operación, cultura, estrategia y estructura organizativa. Esto con el fin de optimizar significativamente la calidad con la que presta sus servicios, lo que a su vez resulta de manera positiva en los usuarios y la comunidad en general.

Impulso que no solo fortalece su competitividad en el panorama empresarial actual, sino que también la posiciona como una entidad a la vanguardia en un panorama digital de constante evolución. En vista que las TIC no solo buscan ser un factor clave, sino una pieza fundamental para impulsar y mantener el éxito operativo, dado que permiten adaptarse ágilmente a las demandas cambiantes del mercado y aseguran una experiencia de usuario optimizada y eficiente. Además, fomenta la innovación, genera nuevas oportunidades y promueve el desarrollo sostenible, reforzando así la contribución de la empresa al progreso económico-social.

Sin embargo, se encuentra ante diversos retos en lo que respecta a la protección de su información, dado que no posee un sistema capaz de gestionar y garantizar la protección de sus datos críticos, incluyendo procesos de negocio, información de usuarios y transacciones financieras. Por otra parte, la falta de políticas claras y la ausencia de medidas preventivas efectivas han llevado a la empresa a experimentar incidentes de seguridad que ponen en riesgo su capacidad para prestar sus servicios.

Esta situación es especialmente preocupante en un contexto donde los ciberataques y las violaciones de seguridad son cada vez más frecuentes y sofisticadas. Sin las medidas adecuadas, la empresa se encuentra expuesta a múltiples amenazas, como robos de información, ataques cibernéticos. Asimismo, enfrenta desafíos internos, como la utilización incorrecta de los recursos informáticos, y la poca sensibilización de lo relevante que puede ser resguardar los datos corporativos sensibles.

En síntesis, debido a la ausencia de un SGSI, EMSEU S.A.C. se encuentra en una posición vulnerable que la expone a diversos riesgos como el robo o pérdida de información, interrupción sus actividades y errores humanos, los cuales pueden comprometer la integridad, confidencialidad y disponibilidad de la información.

En consecuencia, se hizo imperativa la necesidad de abordar y llevar a cabo la presente investigación, enmarcando la norma como estrategia organizacional para fortalecer y sostener la información de forma segura. Todo esto teniendo en cuenta la siguiente

interrogante: ¿Cuál es la influencia de la ISO/IEC 27001:2022 en la seguridad de la información de EMSEU S.A.C.?

Dicho esto, tras examinar antecedentes y literatura relevante, fue posible reconocer tres dimensiones fundamentales a considerar en la protección de la información: integridad, que tiene por indicadores la exactitud, consistencia y completitud, para evitar la modificación no autorizada; confidencialidad, que tiene por indicadores el control de accesos y protección de datos, para prevenir la divulgación y el uso no autorizado; y disponibilidad, que tiene por indicadores el rendimiento, capacidad de respuesta y capacidad de recuperación, para mantener y disponer de la información cuando sea necesario.

Por otra parte, el estudio se basó en la necesidad de generar y aportar información significativa sobre cómo incide la norma en la preservación de la información. De igual manera, se justificó en la necesidad de constatar como la aplicación de esta norma permite optimizar la administración, gestión o control del manejo de la información. Asimismo, buscó abordar un problema específico bajo la evaluación y aplicación de conocimiento existente, proporcionando de este modo un fundamento sólido para la toma de decisiones a través de una exploración aplicada de tipo pre experimental.

En vista de aquello, como hipótesis, se planteó lo siguiente: La ISO/IEC 27001:2022 influye significativamente en la seguridad de la información de EMSEU S.A.C. En función de: 1.- La ISO/IEC 27001:2022 influye significativamente en la integridad de la información de EMSEU S.A.C.; 2.- La ISO/IEC 27001:2022 influye significativamente en la confidencialidad de la información de EMSEU S.A.C.; y 3.- La ISO/IEC 27001:2022 influye significativamente en la disponibilidad de la información de EMSEU S.A.C.

II. MATERIAL Y MÉTODOS

2.1. Tipo y diseño de investigación

Según su finalidad o propósito, la investigación se divide en dos tipos: básica, que busca generar conocimiento teórico sin una aplicación práctica; y aplicada, que tiene como fin adquirir y aplicar conocimiento en la solución de problemas concretos en situaciones específicas (Arias & Covinos, 2021). En función a dichas premisas, el estudio fue clasificado como investigación aplicada al poner en práctica conocimiento existente del estándar ISO/IEC 27001:2022 para optimizar una situación determinada en un escenario real mediante la implementación efectiva de un SGSI.

En investigación se aborda el diseño como estrategias que se utilizan para realizar un estudio y se clasifica en dos tipos: diseño experimental, que busca cuantificar los cambios relacionados de una variable en otra; y diseño no experimental, que se enfoca en evaluar a los participantes en su entorno natural sin intervenir en las variables, se divide en transversal y longitudinal (Polanía et al., 2020). En esa línea, la investigación se efectuó bajo un diseño pre experimental, llevando a cabo una evaluación a un conjunto de participantes antes y después de aplicar un estímulo, buscando analizar y comprender de manera precisa los efectos resultantes.

$$G \quad O_1 \rightarrow X \rightarrow O_2$$

Donde:

- G : Representa el conjunto de participantes bajo investigación.
- O_1 : Corresponde a la evaluación de la variable antes del estímulo.
- X : Representa el estímulo o tratamiento administrado.
- O_2 : Corresponde a la evaluación de la variable después del estímulo.

2.2. Población, muestra y muestreo

Población

En concordancia con Mucha et al. (2021), es la agrupación de individuos con características similares de donde se pretende obtener información y sobre el cual se va a concluir. Por tal razón, la población lo constituían 60 trabajadores; personal administrativo, técnicos, y de servicios (limpieza y vigilancia).

Muestra

Para Feria et al. (2019), es la parte representativa tomada de una población de estudio para demostrar lo se quiere conseguir sin recurrir a toda la población. En tal sentido, la investigación, considerando criterios que se establecieron para incluir o excluir a los participantes, se basó en una muestra de 35 personas, como se detalla más adelante:

Tabla 1

Distribución de la muestra

Tipo	Cantidad de personas
Administrativos	20
Técnicos	15
Total	35

Nota. Tabla que presenta cómo estaba distribuida la muestra de la investigación.

Muestreo

Según Hernández & Carpio (2019), es la técnica, método o procedimiento que nos permite seleccionar los elementos representativos de una población. Por ello, en el estudio, se hizo uso del método no probabilístico basado en o por conveniencia, donde se establecieron criterios para incluir o excluir a los participantes en la selección.

Criterio de inclusión:

- Administrativos contratados en plantilla.
- Técnicos contratados en plantilla con acceso a la plataforma de registro de consumo eléctrico.

Criterio de exclusión:

- Administrativos que poseen contrato de servicios.
- Técnicos contratados en plantilla sin acceso a la plataforma de registro de consumo eléctrico.
- Personal de servicios (limpieza y vigilancia).

2.3. Técnica e instrumento de recolección de datos

Técnica

De acuerdo con Sánchez (2022), es un proceso formalizado que admite la obtención de datos de manera confiable con el propósito de analizar un fenómeno, verificar una hipótesis o explorar una pregunta de investigación. En tal sentido, en el estudio se aplicó la encuesta, técnica que utiliza cuestionarios estandarizados o entrevistas estructuradas para adquirir información de una muestra sin interferir en el entorno (Arias, 2020).

Instrumento

Arias & Covinos (2021), afirma que un instrumento de investigación es el medio o herramienta que se utiliza para compilar datos o información de forma sistematizada y estructurada. En función a esto, en el estudio se optó por aplicar el cuestionario, instrumento que comprende una sucesión estructurada de enunciados o interrogantes relacionadas con la hipótesis, que se presentan a una muestra, con el fin de reunir datos cuantitativos o respuestas específicas (Useche et al., 2019).

Validez y confiabilidad

Para López et al. (2019), la validez es la capacidad del instrumento de medida para evaluar o capturar, de manera precisa y sin error, aquello que se supone debe medir. Mientras que, según Arias, (2020), la confiabilidad alude a la homogeneidad y estabilidad de las mediciones o resultados obtenidos al aplicar el instrumento a lo largo del tiempo y en diversas condiciones.

Bajo esas premisas, la validez se precisó mediante el juicio de expertos, proceso donde 05 especialistas cualificados en el campo de estudio, evalúan la idoneidad, claridad, coherencia y relevancia del instrumento (Tarazona, 2020). Por otro lado, para instaurar el nivel de confiabilidad se empleó el coeficiente alfa de Cronbach, medida que permite analizar la congruencia de un grupo de ítems en un test o cuestionario presentado con una escala tipo Likert (Toro et al., 2022).

2.4. Procedimiento de recolección de datos

Según lo establecido por Sánchez (2022), implica un conjunto de acciones que permiten recopilar información relevante y necesaria para evaluar el impacto o relación antes y después de la introducción de un estímulo o tratamiento. Por lo tanto, en el estudio se optó por recopilar los datos en dos etapas, tal y como se describe a continuación:

Primera etapa (Pre-test): Medición inicial, efectuada antes de aplicar cualquier intervención o tratamiento, consistió en la aplicación del instrumento previamente validado en los 35 elementos de la muestra. El propósito fue establecer el punto de referencia para evaluar los cambios que puedan ocurrir como resultado de la influencia de la norma.

Segunda etapa (Pos-test): La medición final, después de administrar el estímulo, se efectuó utilizando el mismo instrumento en los 35 elementos de la muestra, con el objetivo de contrastar y evaluar cualquier diferencia con respecto a las mediciones iniciales. Este análisis incluyó el ordenamiento, distribución y tratamiento de los datos en SPSS, software estadístico.

2.5. Método de análisis de datos

Según Yuni & Urbano (2020), se trata de un conjunto de procedimientos sistematizados utilizados para inspeccionar y procesar datos con el fin de obtener información, detectar patrones, realizar inferencias y generar conclusiones. Por lo que, en él estudió, se eligió combinar el análisis descriptivo, que permite sintetizar y describir los datos obtenidos, con el inferencial, que se emplea para sacar conclusiones más allá de la muestra observada.

2.6. Análisis de datos

Conforme a Rivadeneira et al. (2020), es el proceso de sacar conclusiones sobre un tema en particular a partir del examen e interpretación de datos, utilizando métodos, técnicas o modelos estadísticos. Bajo ese punto de vista, en la investigación, el proceso inició con la tabulación y distribución de los datos dentro del software SPSS, y finalizó con la interpretación de los descubrimientos, la exposición a detalle de los resultados y la generación de conclusiones.

III. RESULTADOS

Apartado en el que se expone el producto de la evaluación de los datos recabados durante la ejecución de los objetivos. Para ello, se realizó una evaluación de la percepción del cumplimiento de la implementación del estándar, así como de la retroalimentación de la muestra antes y después de llevar a cabo cualquier intervención o tratamiento.

Este proceso implicó revisar críticamente los datos con el objetivo de entender el impacto de las acciones tomadas y determinar la influencia de las intervenciones. Además, buscó obtener una visión integral de cómo se han traducido los objetivos en la realidad.

En tal sentido, este análisis resultó fundamental para comprender de manera descriptiva e inferencial cómo la adopción del estándar influye en la seguridad de la información, contemplando sus tres principales pilares: integridad, confidencialidad y disponibilidad.

3.1. Resultados del pre-test

Variable: Seguridad de la información

Tabla 2

Resultados del pre-test de la seguridad de la información

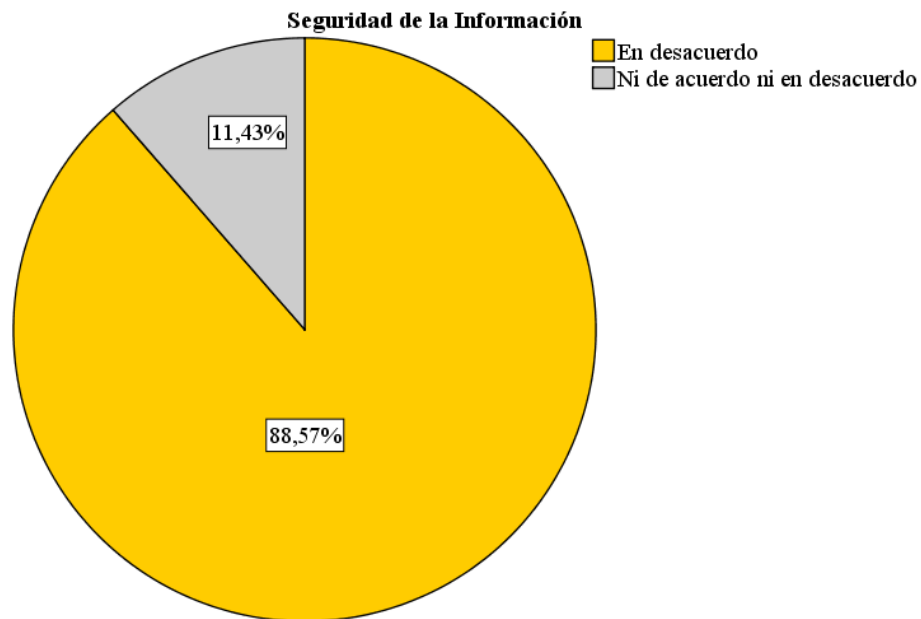
	Seguridad de la Información	Frecuencia	Porcentaje
	En desacuerdo	31	88,6
Válido	Ni de acuerdo ni en desacuerdo	4	11,4
	Total	35	100,0

Nota. Tabla que presenta los resultados del análisis de la seguridad de la información previa implementación de la ISO/IEC 27001:2022.

Del total de encuestados, el 88.6% expresó su desacuerdo con la seguridad de la información. Por otro lado, el 11.4% manifestó no estar ni de acuerdo ni en desacuerdo, debido al desconocimiento del tema o a la falta de una opinión firme como respuesta. Estos resultados indican que la mayor parte de los encuestados carecía de una percepción positiva respecto a la seguridad de la información, destacando la necesidad de la implementación del estándar internacional.

Figura 1

Resultados del pre-test de la seguridad de la información



Dimensión: Integridad

Tabla 3

Resultados del pre-test de la dimensión integridad

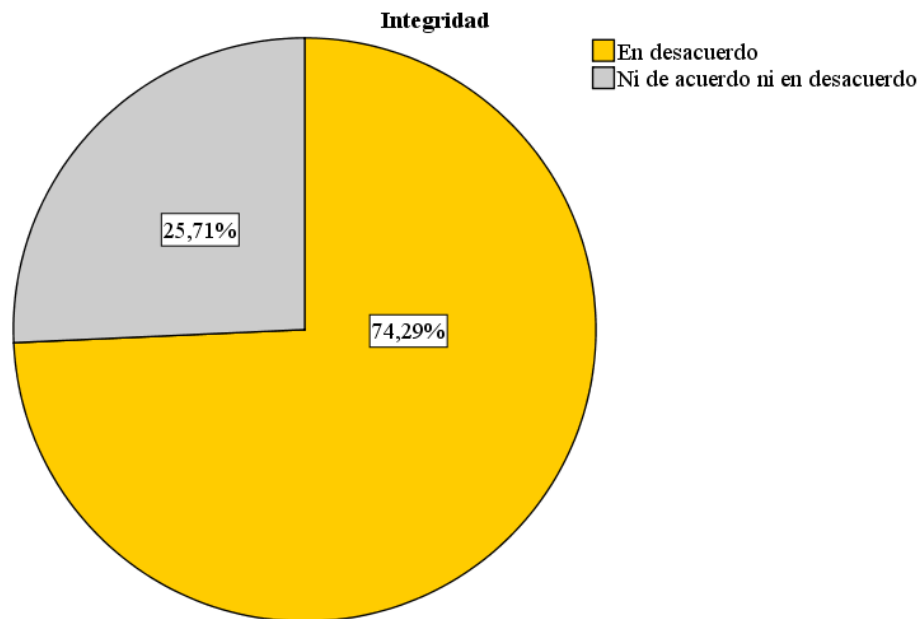
	Integridad	Frecuencia	Porcentaje
	En desacuerdo	26	74,3
Válido	Ni de acuerdo ni en desacuerdo	9	25,7
	Total	35	100,0

Nota. Tabla que presenta los resultados del análisis de la integridad previa implementación de la ISO/IEC 27001:2022.

Del total de encuestados, el 74.3% expresó su desacuerdo en relación con la integridad. Por otro lado, el 25.7% manifestó no estar ni de acuerdo ni en desacuerdo, debido al desconocimiento del tema o a la falta de una opinión firme como respuesta. Estos resultados indican que la mayor parte de los encuestados carecía de una percepción positiva respecto a la integridad de la información.

Figura 2

Resultados del pre-test de la dimensión integridad



Dimensión: Confidencialidad

Tabla 4

Resultados del pre-test de la dimensión confidencialidad

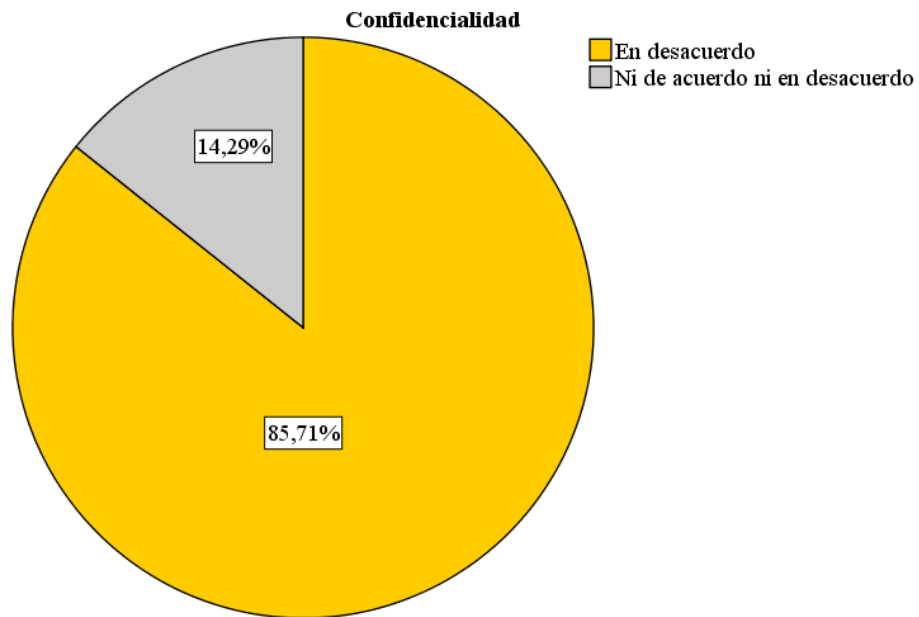
Confidencialidad		Frecuencia	Porcentaje
	En desacuerdo	30	85,7
Válido	Ni de acuerdo ni en desacuerdo	5	14,3
	Total	35	100,0

Nota. Tabla que presenta los resultados del análisis de la confidencialidad previa implementación de la ISO/IEC 27001:2022.

Del total de encuestados, el 85.7% expresó su desacuerdo en relación con la confidencialidad. Por otro lado, el 14.3% manifestó no estar ni de acuerdo ni en desacuerdo, debido al desconocimiento del tema o a la falta de una opinión firme como respuesta. Estos resultados indican que la mayor parte de los encuestados carecía de una percepción positiva respecto a la confidencialidad de la información.

Figura 3

Resultados del pre-test de la dimensión confidencialidad



Dimensión: Disponibilidad

Tabla 5

Resultados del pre-test de la dimensión disponibilidad

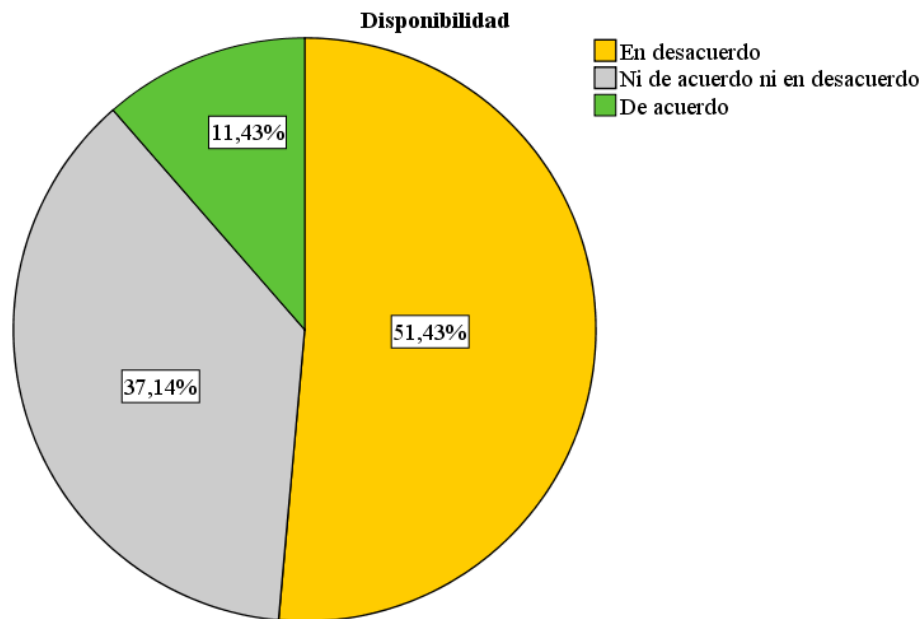
	Disponibilidad	Frecuencia	Porcentaje
Válido	En desacuerdo	18	51,4
	Ni de acuerdo ni en desacuerdo	13	37,1
	De acuerdo	4	11,4
	Total	35	100,0

Nota. Tabla que presenta los resultados del análisis de la disponibilidad previa implementación de la ISO/IEC 27001:2022.

Del total de encuestados, el 51,4% expresó su desacuerdo en relación con la disponibilidad. Por otro lado, el 11,4% expresó estar de acuerdo; mientras que, el 14,3% manifestó no estar ni de acuerdo ni en desacuerdo. Estos resultados indican que, a pesar de tener una cantidad de encuestados con percepción positiva, la mayor parte aún carecía de esta respecto a la disponibilidad de la información.

Figura 4

Resultados del pre-test de la dimensión disponibilidad



3.2. Cumplimiento de la ISO/IEC 27001:2022

Variable: ISO/IEC 27001:2022

Tabla 6

Resultados del cumplimiento de la ISO/IEC 27001:2022

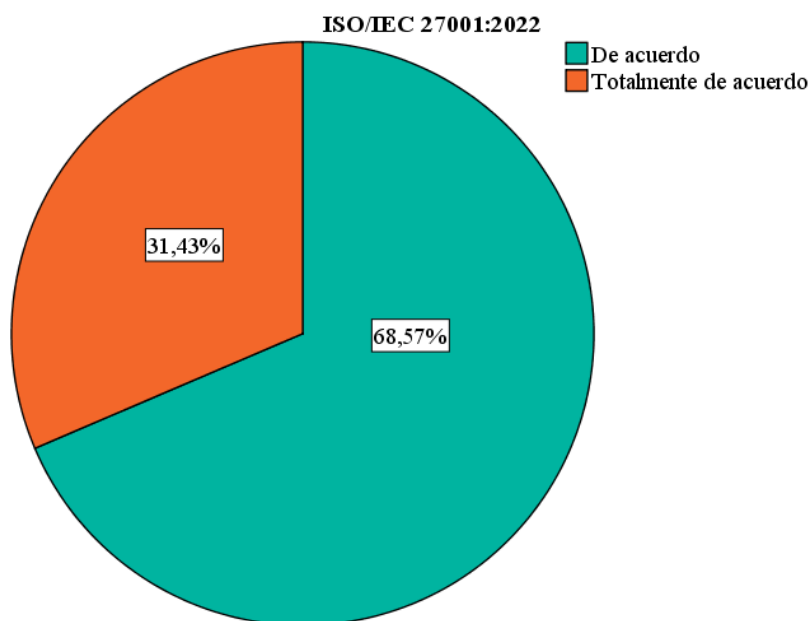
ISO/IEC 27001:2022	Frecuencia	Porcentaje
De acuerdo	24	68,6
Válido Totalmente de acuerdo	11	31,4
Total	35	100,0

Nota. Tabla que presenta los resultados del análisis de la percepción del cumplimiento de la implementación de la ISO/IEC 27001:2022.

Del total de encuestados, el 68,6% expresó estar de acuerdo y el 31,4% estar totalmente de acuerdo con el cumplimiento de la implementación. Estos resultados indican que los encuestados presentaban una percepción positiva respecto al cumplimiento de la implementación del estándar, destacando el conocimiento de su aplicación.

Figura 5

Resultados del cumplimiento de la ISO/IEC 27001:2022



Dimensión: Planificación

Tabla 7

Resultados de la dimensión planificación

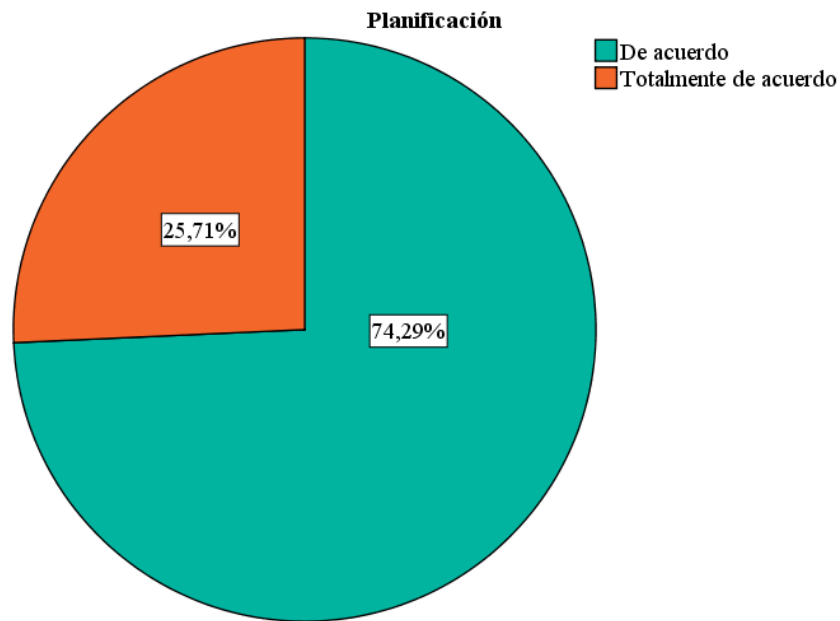
	Planificación	Frecuencia	Porcentaje
	De acuerdo	26	74,3
Válido	Totalmente de acuerdo	9	25,7
	Total	35	100,0

Nota. Tabla que presenta los resultados del análisis de la percepción del cumplimiento de la planificación en la implementación de la ISO/IEC 27001:2022.

Del total de encuestados, el 74,3% expresó estar de acuerdo y el 25,7% estar totalmente de acuerdo con el cumplimiento de la planificación. Estos resultados indican que los encuestados presentaban una percepción positiva respecto al cumplimiento de la planificación de la implementación del estándar.

Figura 6

Resultados de la dimensión planificación



Dimensión: Ejecución

Tabla 8

Resultados de la dimensión ejecución

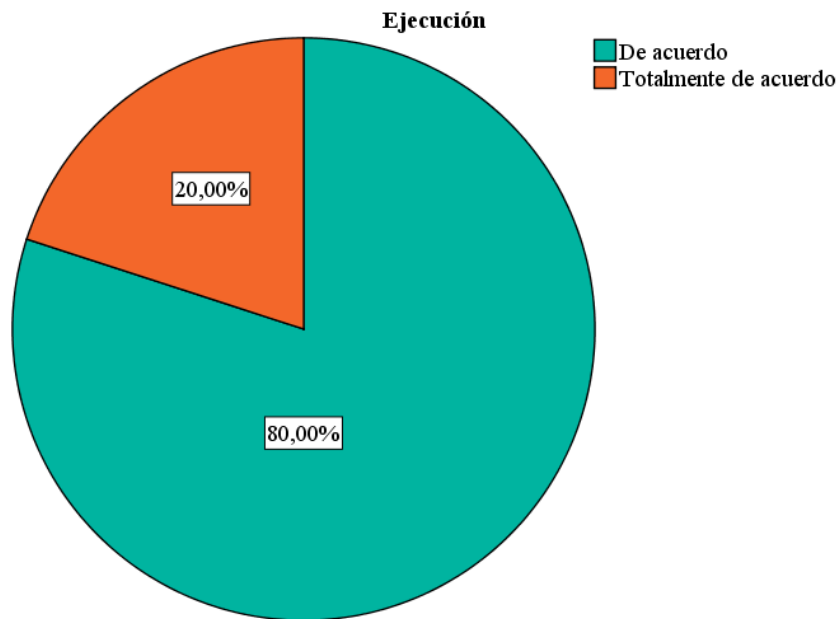
Ejecución		Frecuencia	Porcentaje
	De acuerdo	28	80,0
Válido	Totalmente de acuerdo	7	20,0
	Total	35	100,0

Nota. Tabla que presenta los resultados del análisis de la percepción del cumplimiento de la ejecución en la implementación de la ISO/IEC 27001:2022.

Del total de encuestados, el 80,0% expresó estar de acuerdo y el 20,0% estar totalmente de acuerdo con el cumplimiento de la ejecución. Estos resultados indican que los encuestados presentaban una percepción positiva respecto al cumplimiento de la ejecución en la implementación del estándar.

Figura 7

Resultados de la dimensión ejecución



Dimensión: Verificación

Tabla 9

Resultados de la dimensión verificación

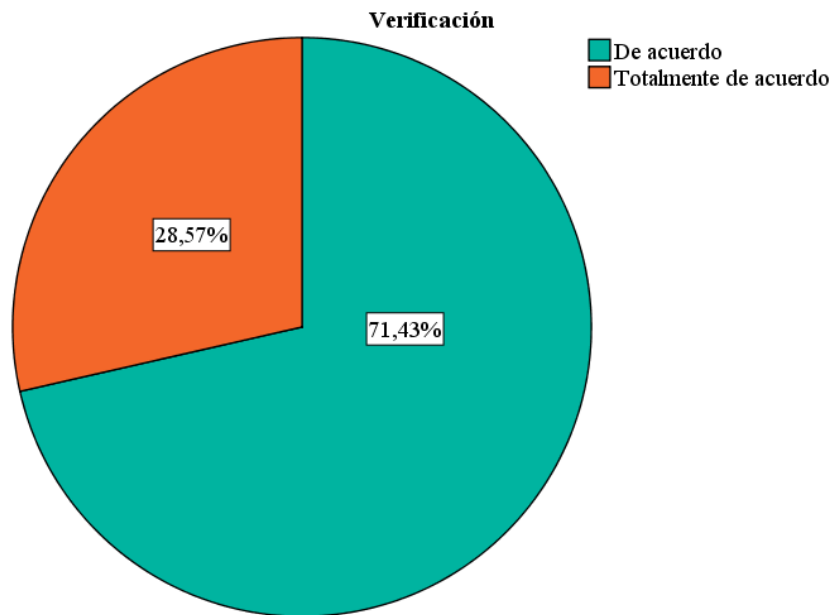
	Verificación	Frecuencia	Porcentaje
	De acuerdo	25	71,4
Válido	Totalmente de acuerdo	10	28,6
	Total	35	100,0

Nota. Tabla que presenta los resultados del análisis de la percepción del cumplimiento de la verificación en la implementación de la ISO/IEC 27001:2022.

Del total de encuestados, el 71,4% expresó estar de acuerdo y el 28,6% estar totalmente de acuerdo con el cumplimiento de la verificación. Estos resultados indican que los encuestados presentaban una percepción positiva respecto al cumplimiento de la verificación en la implementación del estándar.

Figura 8

Resultados de la dimensión verificación



Dimensión: Mejoramiento

Tabla 10

Resultados de la dimensión mejoramiento

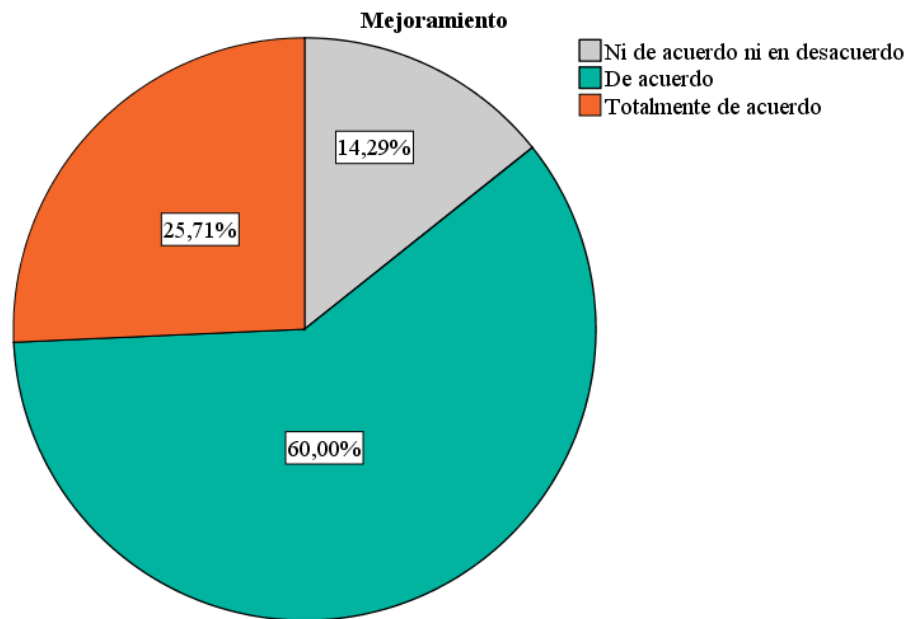
	Mejoramiento	Frecuencia	Porcentaje
Válido	Ni de acuerdo ni en desacuerdo	5	14,3
	De acuerdo	21	60,0
	Totalmente de acuerdo	9	25,7
	Total	35	100,0

Nota. Tabla que presenta los resultados del análisis de la percepción del cumplimiento del mejoramiento en la implementación de la ISO/IEC 27001:2022.

Del total de encuestados, el 60,0% expresó estar de acuerdo y el 25,7% estar totalmente de acuerdo con el cumplimiento del mejoramiento; mientras que, el 14,3% manifestó no estar ni de acuerdo ni en desacuerdo. Estos resultados indican que la mayor parte de encuestados presentaban una percepción positiva; Sin embargo, una pequeña parte mostraba una percepción neutra debido a la falta de una opinión firme respecto al cumplimiento del mejoramiento en la implementación del estándar.

Figura 9

Resultados de la dimensión mejoramiento



3.3. Resultados del pos-test

Variable: Seguridad de la información

Tabla 11

Resultados del pos-test de la seguridad de la información

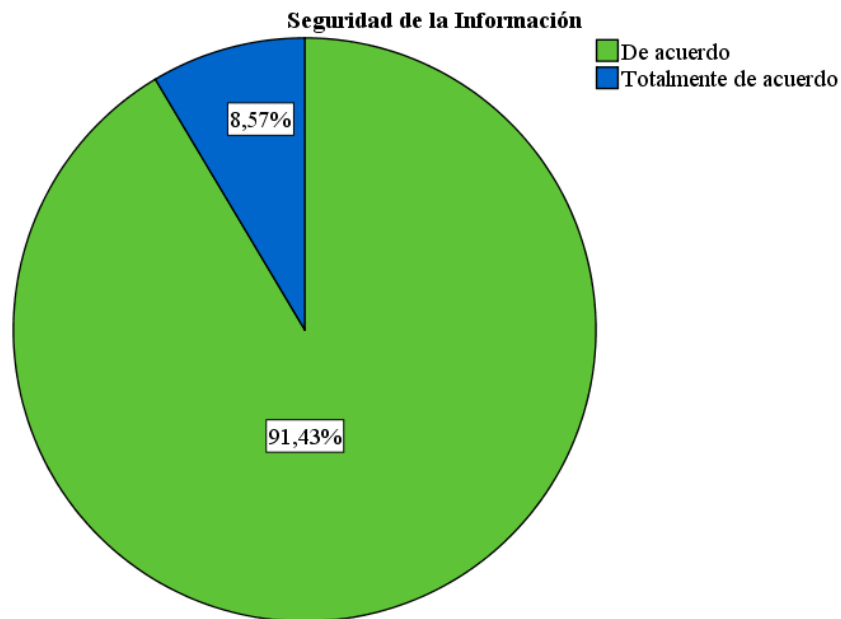
Seguridad de la Información	Frecuencia	Porcentaje
De acuerdo	32	91,4
Válido Totalmente de acuerdo	2	8,6
Total	35	100,0

Nota. Tabla que presenta los resultados del análisis de la seguridad de la información después de la implementación de la ISO/IEC 27001:2022.

Del total de encuestados, el 91,4% expresó estar de acuerdo y el 8,6% estar totalmente de acuerdo con la seguridad de la información. Estos resultados indican que los encuestados presentaban una percepción positiva respecto a la seguridad de la información, destacando la implementación exitosa del estándar internacional.

Figura 10

Resultados del pos-test de la seguridad de la información



Dimensión: Integridad

Tabla 12

Resultados del pos-test de la dimensión integridad

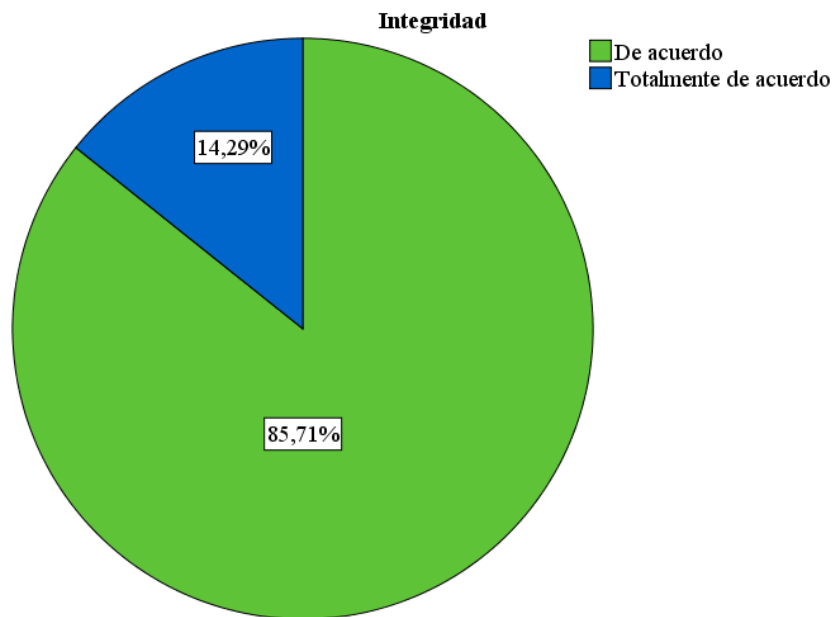
	Integridad	Frecuencia	Porcentaje
	De acuerdo	30	85,7
Válido	Totalmente de acuerdo	5	14,3
	Total	35	100,0

Nota. Tabla que presenta los resultados del análisis de la integridad después de la implementación de la ISO/IEC 27001:2022.

Del total de encuestados, el 85,7% expresó estar de acuerdo y el 14,3% estar totalmente de acuerdo en relación con la integridad. Estos resultados indican que los encuestados presentaban una percepción positiva respecto a la integridad de la información.

Figura 11

Resultados del pos-test de la dimensión integridad



Dimensión: Confidencialidad

Tabla 13

Resultados del pos-test de la dimensión confidencialidad

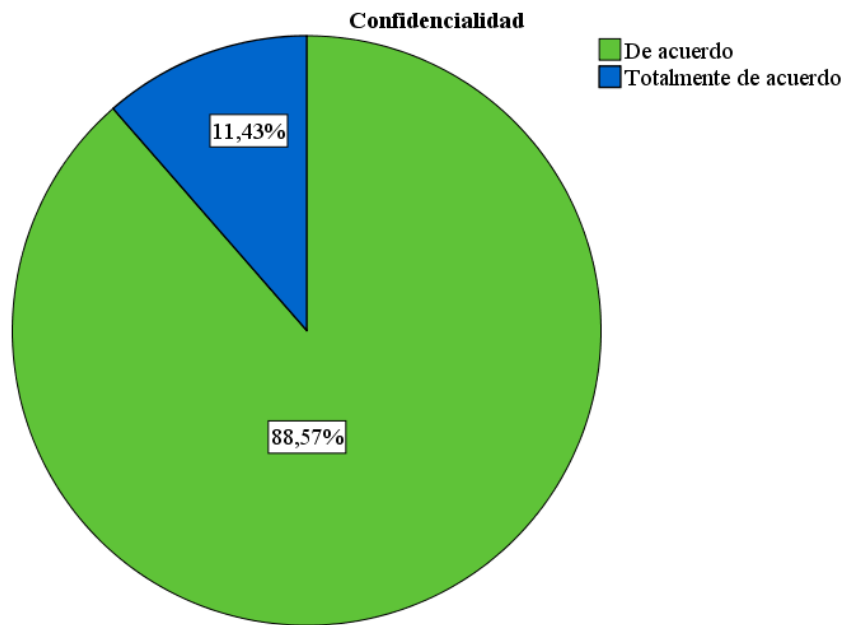
	Confidencialidad	Frecuencia	Porcentaje
	De acuerdo	31	88,6
Válido	Totalmente de acuerdo	4	11,4
	Total	35	100,0

Nota. Tabla que presenta los resultados del análisis de la confidencialidad después de la implementación de la ISO/IEC 27001:2022.

Del total de encuestados, el 88,6% expresó estar de acuerdo y el 11,4% manifestó estar totalmente de acuerdo en relación con la confidencialidad. Estos resultados indican que los encuestados presentaban una percepción positiva respecto a la confidencialidad de la información.

Figura 12

Resultados del pos-test de la dimensión confidencialidad



Dimensión: Disponibilidad

Tabla 14

Resultados del pos-test de la dimensión disponibilidad

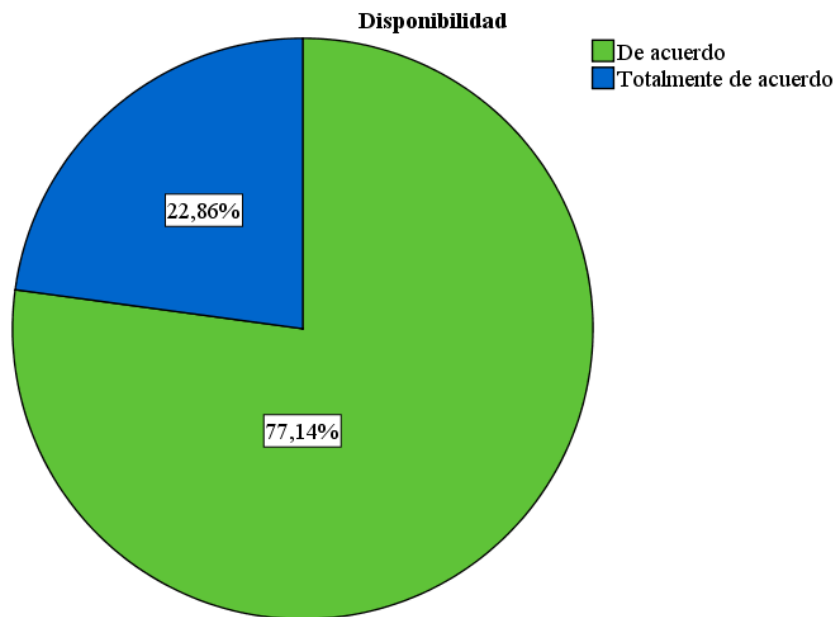
	Disponibilidad	Frecuencia	Porcentaje
	De acuerdo	27	77,1
Válido	Totalmente de acuerdo	8	22,9
	Total	35	100,0

Nota. Tabla que presenta los resultados del análisis de la disponibilidad después de la implementación de la ISO/IEC 27001:2022.

Del total de encuestados, el 77,1% expresó estar de acuerdo y el 22,9% manifestó estar totalmente de acuerdo en relación con la disponibilidad. Estos resultados indican que los encuestados presentaban una percepción positiva respecto a la disponibilidad de la información.

Figura 13

Resultados del pos-test de la dimensión disponibilidad



3.4. Prueba de normalidad

Proceso mediante el cual se estableció si la configuración de datos generados por la muestra sigue, o no, una distribución gaussiana o normal.

Tabla 15

Prueba de normalidad de hipótesis general

	Shapiro-Wilk		
	Estadístico	gl	p
Seguridad de la Información	,317	35	,000

Nota. Tabla que presenta los resultados de la prueba de normalidad de la seguridad de la información.

En la Tabla 15, dado que ($p=0$) es menor que ($\alpha=0.05$), se excluyó la H_0 y se admitió la H_a , indicando que los datos no se distribuyen de manera normal. Por lo tanto, se optó por la aplicación de métodos estadísticos no paramétricos, al considerarlos como los más idóneos para analizar datos que no siguen una distribución normal.

Tabla 16*Prueba de normalidad de hipótesis específica 1*

	Shapiro-Wilk		
	Estadístico	gl	p
Integridad	,418	35	,000

Nota. Tabla que presenta los resultados de la prueba de normalidad de la integridad de la información.

En la Tabla 16, dado que ($p=0$) de la dimensión integridad es menor que ($\alpha=0.05$), se excluyó la H_0 y se admitió la H_a , indicando que los datos no se distribuyen de manera normal.

Tabla 17*Prueba de normalidad de hipótesis específica 2*

	Shapiro-Wilk		
	Estadístico	gl	p
Confidencialidad	,372	35	,000

Nota. Tabla que presenta los resultados de la prueba de normalidad de la confidencialidad de la información.

En la Tabla 17, dado que ($p=0$) de la dimensión confidencialidad es menor que ($\alpha=0.05$), se excluyó la H_0 y se admitió la H_a , indicando que los datos no se distribuyen de manera normal.

Tabla 18*Prueba de normalidad de hipótesis específica 3*

	Shapiro-Wilk		
	Estadístico	gl	p
Disponibilidad	,521	35	,000

Nota. Tabla que presenta los resultados de la prueba de normalidad de la disponibilidad de la información.

En la Tabla 18, dado que ($p=0$) de la dimensión disponibilidad es menor que ($\alpha=0.05$), se excluyó la H_0 y se admitió la H_a , indicando que los datos no se distribuyen de manera normal.

3.5. Prueba de hipótesis

Proceso en el cual se evaluó la validez de sus afirmaciones o hipótesis a través del análisis de datos muestrales.

Hipótesis general

H_0 : La ISO/IEC 27001:2022 no influye significativamente en la seguridad de la información de EMSEU S.A.C.

H_a : La ISO/IEC 27001:2022 influye significativamente en la seguridad de la información de EMSEU S.A.C.

Tabla 19

Prueba de hipótesis general

Prueba de rangos con signo de Wilcoxon			
N total			35
Estadístico de prueba			630,000
Error estándar			56,258
Estadístico de prueba estandarizado			5,599
Sig. asintótica (prueba bilateral)			,000
Hipótesis nula	Prueba	p	Decisión
La mediana de diferencias entre Seguridad de la Información Pre-test y Seguridad de la Información Pos-test es igual a 0.	Prueba de rangos con signo de Wilcoxon para muestras relacionadas	,000	Rechace la hipótesis nula.

Nota. Tabla que presenta los resultados de la prueba de rangos con signo de Wilcoxon de la seguridad de la información.

En la Tabla 19, dado que ($p=0$) es menor que ($\alpha=0.05$), se excluyó la H_0 y se admitió la H_a , indicando que entre las medias del pre y pos-test existe diferencia significativa positiva. En consecuencia, se determinó que el estándar ISO/IEC 27001:2022 influye significativamente en la seguridad de la información.

Hipótesis específicas

HE1o: La ISO/IEC 27001:2022 no influye significativamente en la integridad de la información de EMSEU S.A.C.

HE1a: La ISO/IEC 27001:2022 influye significativamente en la integridad de la información de EMSEU S.A.C.

Tabla 20

Prueba de hipótesis específica 1

Prueba de rangos con signo de Wilcoxon			
N total			35
Estadístico de prueba			630,000
Error estándar			56,723
Estadístico de prueba estandarizado			5,553
Sig. asintótica (prueba bilateral)			,000
Hipótesis nula	Prueba	p	Decisión
La mediana de diferencias entre Integridad Pre-test e Integridad Pos-test es igual a 0.	Prueba de rangos con signo de Wilcoxon para muestras relacionadas	,000	Rechace la hipótesis nula.

Nota. Tabla que presenta los resultados de la prueba de rangos con signo de Wilcoxon de la integridad de la información.

En la Tabla 20, dado que ($p=0$) es menor que ($\alpha=0.05$), se excluyó la HE1o y se admitió la HE1a, indicando que entre las medias del pre y pos-test existe diferencia significativa positiva. En consecuencia, se determinó que el estándar ISO/IEC 27001:2022 influye significativamente en la integridad de la información.

HE2o: La ISO/IEC 27001:2022 no influye significativamente en la confidencialidad de la información de EMSEU S.A.C.

HE2a: La ISO/IEC 27001:2022 influye significativamente en la confidencialidad de la información de EMSEU S.A.C.

Tabla 21

Prueba de hipótesis específica 2

Prueba de rangos con signo de Wilcoxon			
N total			35
Estadístico de prueba			630,000
Error estándar			55,185
Estadístico de prueba estandarizado			5,708
Sig. asintótica (prueba bilateral)			,000
Hipótesis nula	Prueba	p	Decisión
La mediana de diferencias entre Confidencialidad Pre-test y Confidencialidad Pos-test es igual a 0.	Prueba de rangos con signo de Wilcoxon para muestras relacionadas	,000	Rechace la hipótesis nula.

Nota. Tabla que presenta los resultados de la prueba de rangos con signo de Wilcoxon de la confidencialidad de la información.

En la Tabla 21, dado que ($p=0$) es menor que ($\alpha=0.05$), se excluyó la HE2o y se admitió la HE2a, indicando que entre las medias del pre y pos-test existe diferencia significativa positiva. En consecuencia, se determinó que el estándar ISO/IEC 27001:2022 influye significativamente en la confidencialidad de la información.

HE3o: La ISO/IEC 27001:2022 no influye significativamente en la disponibilidad de la información de EMSEU S.A.C.

HE3a: La ISO/IEC 27001:2022 influye significativamente en la disponibilidad de la información de EMSEU S.A.C.

Tabla 22*Prueba de hipótesis específica 3*

Prueba de rangos con signo de Wilcoxon			
N total		35	
Estadístico de prueba		528,000	
Error estándar		51,927	
Estadístico de prueba estandarizado		5,084	
Sig. asintótica (prueba bilateral)		,000	
Hipótesis nula	Prueba	p	Decisión
La mediana de diferencias entre 1 Disponibilidad Pre-test y Disponibilidad Pos-test es igual a 0.	Prueba de rangos con signo de Wilcoxon para muestras relacionadas	,000	Rechace la hipótesis nula.

Nota. Tabla que presenta los resultados de la prueba de rangos con signo de Wilcoxon de la disponibilidad de la información.

En la Tabla 22, dado que ($p=0$) es menor que ($\alpha=0.05$), se excluyó la HE3o y se admitió la HE3a, indicando que entre las medias del pre y pos-test existe diferencia significativa positiva. En consecuencia, se determinó que el estándar ISO/IEC 27001:2022 influye significativamente en la disponibilidad de la información.

IV. DISCUSIÓN

El estudio se concentró en evaluar la influencia de la implementación de la ISO/IEC 27001:2022 en la seguridad de la información en EMSEU S.A.C., entidad responsable de la distribución de energía eléctrica en Utcubamba, Amazonas, Perú. Adicionalmente, buscó proporcionar información crucial para fortalecer la estructura organizativa, abordando la relevancia estratégica de la gestión concierne al resguardo de uno de los activos más críticos: la información. Para concretar este análisis, se contextualizó a la organización, se realizaron exhaustivas revisiones, se evaluaron riesgos para identificar posibles vulnerabilidades y se establecieron estrategias para mitigar amenazas potenciales. En ese contexto, después de la recolección y validación de datos, respaldado por un enfoque que integró el análisis descriptivo con el inferencial, se logró obtener resultados significativos con relación a las preguntas e hipótesis planteadas, contribuyendo con una comprensión más profunda para la generación de conclusiones.

En cuanto a los resultados, en relación con los objetivos, pregunta e hipótesis general, de acuerdo con la Tabla 2 y Figura 1 en el pre-test antes de la aplicación del tratamiento, el 88.6% de los encuestados expresó su desacuerdo, mientras que el 11.4% manifestó no estar ni de acuerdo ni en desacuerdo con la seguridad de la información. Asimismo, en conformidad con la Tabla 11 y Figura 10 en el pos-test, teniendo en cuenta que el 68,6% expresó estar de acuerdo y 31,4% estar totalmente de acuerdo con la implementación; el 91,4% expresó estar de acuerdo y el 8.6% estar totalmente de acuerdo con la seguridad de la información, destacando una percepción positiva. En la prueba de hipótesis general, acorde a la Tabla 19, dado que $p < 0.05$, se excluyó la H_0 y se admitió la H_a , determinando así la existencia de influencia significativa del estándar en la seguridad de la información.

Resultado que se asocia con lo propuesto por Rodríguez et al. (2020), autores que, tras aplicar y examinar dominios específicos de la norma, para optimizar la cobertura y defensa de la información, lograron reconocer que el despliegue de dicho estándar verdaderamente influye en la protección de uno de los activos más críticos de las empresas privadas peruanas. Esto al observar en la entidad en estudio una mejora porcentual de su seguridad. Asimismo, se vincula con lo mencionado por Fonseca et al. (2021), quienes, en una empresa colombiana de hidrocarburos, tras orientar un piloto de sistema de gobierno para fortalecer la información con las especificaciones dadas por la norma, lograron determinar que la aplicación del piloto basado en el estándar sirve de

base para la aplicación de un eficiente SGSI, e influye significativamente en el resguardo la información, atendiendo la confidencialidad, integridad y disponibilidad.

Siguiendo con la sección, en relación con las preguntas e hipótesis específicas, de acuerdo con la Tabla 3 y Figura 2, de la dimensión integridad se pudo observar que, en el pre-test antes de la aplicación del tratamiento, el 74,3% de los encuestados expresó su desacuerdo, mientras que el 25,7% manifestó no estar ni de acuerdo ni en desacuerdo. Asimismo, acorde con la Tabla 12 y Figura 11, en el pos-test, teniendo en cuenta la implementación exitosa del estándar; el 85,7% expresó estar de acuerdo y el 14,3% estar totalmente de acuerdo, destacando una percepción positiva. En la prueba de hipótesis, conforme a la Tabla 20, dado que $p < 0.05$, se excluyó la HE1o y se admitió la HE1a, determinando así la existencia de influencia significativa del estándar en la integridad de la información.

Resultado que se vincula con lo establecido por Bustamante et al. (2021), autores que examinaron la información, su gestión y la seguridad de la misma en un organismo estatal bajo las directivas de la ISO 27001, logrando implantar con éxito políticas de seguridad que garantizaban las tres dimensiones fundamentales de la información, haciendo énfasis en la integridad, al observar un aumento porcentual del 46% al 100%, cambio percibido y reconocido por más del 90% de los colaboradores. Mientras que difiere con lo planteado por Medina (2023), quien después de concentrarse en explorar la norma y su influencia en el gobierno de la seguridad de la información en el departamento TI de una industria, logró evidenciar que el estándar a pesar de tener influencia en el gobierno de la seguridad, evidenciando un 22% según un coeficiente de Nagelkerke, con una significancia de $p < 0,05$. En lo que concierne a la dimensión de integridad, no evidenció alguna influencia significativa, al alcanzar una significancia con 1 grado de libertad.

De igual forma, de acuerdo con la Tabla 4 y Figura 3, de la dimensión confidencialidad se pudo observar que, en el pre-test antes de la aplicación del tratamiento, el 85,7% de los encuestados expresó su desacuerdo, mientras que el 14,3% manifestó no estar ni de acuerdo ni en desacuerdo. Asimismo, conforme con la Tabla 13 y Figura 12, en el pos-test, teniendo en cuenta la implementación exitosa del estándar; el 88,6% expresó estar de acuerdo y el 11,4% estar totalmente de acuerdo, destacando una percepción positiva. En la prueba de hipótesis, acorde a la Tabla 21, dado que $p < 0.05$, se excluyó la HE2o y se admitió la HE2a, determinando así la existencia de influencia significativa del estándar en la confidencialidad de la información.

Resultado que se relaciona con lo planteado por Aguinaga (2021), quien mediante un estudio de las repercusiones de la adopción de un SGSI alineado al estándar, logró identificar mejoras en los tres aspectos primordiales de la información, especialmente la confidencialidad, aspecto que experimentó un incremento notable en comparación con su valor de referencia inicial. En contraste, no guarda relación completa con lo sugerido por Ticona (2021), quien después de estudiar los efectos positivos que la implantación de la norma tiene sobre la protección de la información en los sistemas integrados de una firma, logró determinar según el Rho de Spearman, con un valor de 0.204, que el estándar no generó un progreso en la confidencialidad de la información. Esto debido a que los sistemas ya contaban con una base sólida establecida de seguridad y ya existía una percepción positiva de la confidencialidad.

Por último, de acuerdo con la Tabla 5 y Figura 4, de la dimensión disponibilidad se pudo observar que, en el pre-test antes de la aplicación del tratamiento, el 51,4% de los encuestados expresó su desacuerdo y el 37,1% manifestó no estar ni de acuerdo ni en desacuerdo; mientras que, el 11,4% expresó estar de acuerdo. Asimismo, conforme con la Tabla 14 y Figura 13, en el pos-test, teniendo en cuenta la implementación exitosa del estándar; el 77,1% expresó estar de acuerdo y el 22,9% estar totalmente de acuerdo, destacando una percepción positiva. En la prueba de hipótesis, acorde a la Tabla 22, dado que $p < 0.05$, se excluyó la HE3o y se admitió la HE3a, determinando así la existencia de influencia significativa del estándar en la disponibilidad de la información.

Resultado que se adhiere a lo presentado por Chicaiza & Torres (2020), autores que tras ejecutar un modelo preventivo con base en la ISO 27001:2013 para la generación de un régimen de protección informática en una firma privada, lograron evidenciar con base en las percepciones de los encuestados un notable incremento de los indicadores de la disponibilidad de la información, siendo este representado por un 77,80%. A su vez, se adhiere a lo señalado por Torres & Asqui (2023), quienes llevaron a cabo la implantación y evaluación de la ISO 27001 en una institución educativa con el fin de potenciar la seguridad de la información, logrando demostrar que implantar el estándar de forma efectiva permite mejorar la disponibilidad de la información, reduciendo la tasa de incidentes de 130 a 20, donde el umbral promedio pasó de 61.83% a 15.67%, beneficiando así a la institución, sus colaboradores y estudiantes con acceso fácil a la información, sin problemas y con menor riesgo.

V. CONCLUSIONES

En conformidad con el objetivo, problema e hipótesis general, considerando los resultados del pre-test, la implantación exitosa del estándar, la valoración de la percepción del cumplimiento de la implementación, los hallazgos del pos-test, la tabulación y la prueba general de la hipótesis, que detalló la existencia de una diferencia significativa con tendencia positiva entre las medias del pre y pos-test, donde $p < 0.05$; se determinó que la ISO/IEC 27001:2022 influye de forma significativa en la seguridad de la información en EMSEU S.A.C.

De manera similar, en cuanto al primer problema e hipótesis específica, que se vincula con la integridad de la información; al existir una diferencia significativa con tendencia positiva entre las medias del pre y pos-test, donde $p < 0.05$; se determinó que la ISO/IEC 27001:2022 influye de forma significativa en la integridad de la información en EMSEU S.A.C.

Asimismo, en lo que respecta al segundo problema e hipótesis específica, que se vincula con la confidencialidad de la información; al existir una diferencia significativa con tendencia positiva entre las medias del pre y pos-test, donde $p < 0.05$; se determinó que la ISO/IEC 27001:2022 influye de forma significativa en la confidencialidad de la información en EMSEU S.A.C.

Por último, en lo que concierne al tercer problema e hipótesis específica, que se vincula con la disponibilidad de la información; al existir una diferencia significativa con tendencia positiva entre las medias del pre y pos-test, donde $p < 0.05$; se determinó que la ISO/IEC 27001:2022 influye de forma significativa en la disponibilidad de la información en EMSEU S.A.C.

VI. RECOMENDACIONES

Proteger la información en las organizaciones es esencial; en ese sentido, la adopción de estándares reconocidos, como la ISO 27001, proporciona una referencia integral y completa para la gestión efectiva. Después de explorar a fondo sus implicaciones y con base en los hallazgos obtenidos, se formulan las siguientes recomendaciones para impulsar la cultura de seguridad proactiva de la organización en estudio, así como para servir de guía en futuras investigaciones:

A la alta dirección, se recomienda la adopción de un proceso de perfeccionamiento continuo para el SGSI, fundamentado en los descubrimientos derivados de auditorías internas y la retroalimentación de las partes interesadas. Esto con el propósito de fortalecer de manera proactiva su estructura ante las demandas cambiantes del entorno.

De igual forma, se recomienda garantizar la aprobación y conformidad de los requisitos del estándar de manera formal para adquirir la certificación ISO 27001. Esto con el propósito de demostrar y certificar el involucramiento de la entidad con la información y su resguardo.

Asimismo, se recomienda implementar sesiones de formación destinadas a concientizar a los trabajadores sobre la trascendencia de la información al encontrarse de forma segura. Esto con el propósito de forjar un entendimiento más detallado de su papel individual en la preservación de la seguridad.

Por otra parte, para estudios futuros, se recomienda establecer con la alta dirección un compromiso sólido para respaldar activamente la implementación del estándar. Esto con el propósito de asegurar la entrega de recursos y que las iniciativas en seguridad de la información sean debidamente priorizadas.

Del mismo modo, se recomienda ejecutar un estudio antes de la adopción de la ISO/IEC 27001. Esto con el propósito de instaurar indicadores clave que permitirán generar una base sólida para valorar la seguridad de la información, el contexto en el que se opera, los peligros asociados y su comportamiento a lo largo del tiempo.

VII. REFERENCIAS BIBLIOGRÁFICAS

- Aguinaga, W. (2021). Sistema de gestión alineado a la norma ISO/IEC 27001:2013 para la seguridad de la información en una institución financiera, Chachapoyas-Amazonas, 2021. En *Repositorio Institucional - UCV*. Universidad César Vallejo. <https://repositorio.ucv.edu.pe/handle/20.500.12692/63185>
- 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. [https://doi.org/10.52326/JSS.UTM.2021.4\(1\).11](https://doi.org/10.52326/JSS.UTM.2021.4(1).11)
- Altamirano, K. (2021). La seguridad de la información en la administración pública. En Universidad de Lima (Ed.), *Construyendo un mundo inteligente para la sostenibilidad. Actas del III Congreso Internacional de Ingeniería de Sistemas* (pp. 77-95). Universidad de Lima. <https://hdl.handle.net/20.500.12724/13917>
- Arias, J. (2020). *Técnicas e instrumentos de investigación científica*. www.cienciaysociedad.org
- Arias, J., & Covinos, M. (2021). *Diseño y metodología de la investigación*. Enfoques Consulting EIRL. <http://hdl.handle.net/20.500.12390/2260>
- Astudillo, C., & Cabrera, A. (2019). Políticas de gestión de seguridad de la información, fundamentadas en la norma ISO/IEC 27001, centro de datos diseñado con el estándar ANSI/TIA 942. *Dominio de las Ciencias*, 5(3), 132. <https://doi.org/10.23857/dc.v5i3.929>
- Barzaga, O., Vélez, H., Nevárez, J., & Arroyo, M. (2019). Gestión de la información y toma de decisiones en organizaciones educativas. *Revista de ciencias sociales*, 25(2), 120-130. <https://dialnet.unirioja.es/servlet/articulo?codigo=7025997>
- Bustamante, S., Valles, M., Cuellar, I., & 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. <https://doi.org/https://doi.org/10.29019/enfoqueute.743>

- Carvalho, C., & Marques, E. (2019). Adapting ISO 27001 to a Public Institution. En IEEE Xplore (Ed.), *2019 14th Iberian Conference on Information Systems and Technologies (CISTI)*. IEEE Xplore. <https://doi.org/10.23919/CISTI.2019.8760870>
- Chicaiza, D., & Torres, C. (2020). *Plan de seguridad informática basado en la norma iso 27001, para proteger la información y activos de la empresa privada Megaprofer S.A.* <https://repositorio.uta.edu.ec/jspui/handle/123456789/30690>
- Culot, G., Nassimbeni, G., Podrecca, M., & Sartor, M. (2021). The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda. *TQM Journal*, 33(7), 76-105. <https://doi.org/10.1108/TQM-09-2020-0202/FULL/PDF>
- Damian, J. (2023). ISO/IEC 27000. *High Tech Engineering Journal*, 3(2), 80-84. <https://doi.org/10.46363/high-tech.v3i2.3>
- Duan, Y., Sun, X., Che, H., Cao, C., Li, Z., & Yang, X. (2019). Modeling Data, Information and Knowledge for Security Protection of Hybrid IoT and Edge Resources. *IEEE Access*, 7, 99161-99176. <https://doi.org/10.1109/ACCESS.2019.2931365>
- ESET. (2022). *ESET Security Report Latinoamérica 2022*. <https://doi.org/https://www.eset.com/latam/security-report/>
- Evans, N., & Price, J. (2020). Development of a holistic model for the management of an enterprise's information assets. *International Journal of Information Management*, 54, 102193. <https://doi.org/10.1016/j.ijinfomgt.2020.102193>
- 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/https://doi.org/10.25008/bcsee.v1i1.2>
- Feria, H., Blanco, M., & Valledor, R. (2019). *La dimensión metodológica del diseño de la investigación científica*.

- Figuroa, J., Rodríguez, R., Bone, C., & Saltos, J. (2018). La seguridad informática y la seguridad de la información. *Polo del Conocimiento*, 2(12), 145. <https://doi.org/10.23857/pc.v2i12.420>
- Fonseca, O. A., Rojas, A. E., & 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), 213-222. https://www.iaeng.org/IJCS/issues_v48/issue_2/IJCS_48_2_01.pdf
- Fortinet. (2022). *Informe FortiGuard Labs: Año 2021*. <https://www.fortinet.com/lat/corporate/about-us/newsroom/press-releases/2022/fortiguard-labs-reporte-ciberataques-america-latina-2021>
- Guerra, E., Neira, H., Díaz, J. L., & Patiño, J. (2021). Desarrollo de un sistema de gestión para la seguridad de la información basado en metodología de identificación y análisis de riesgo en bibliotecas universitarias. *Información tecnológica*, 32(5), 145-156. <https://doi.org/10.4067/S0718-07642021000500145>
- Hernández, C., & Carpio, N. (2019). Introducción a los tipos de muestreo. *Alerta, Revista científica del Instituto Nacional de Salud*, 2(1), 75-79. <https://doi.org/10.5377/ALERTA.V2I1.7535>
- IBM. (2022). *Coste de la vulneración de datos 2022*. <https://www.ibm.com/es-es/reports/data-breach>
- INCIBE. (2020). *Protección de la información*. https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_proteccion-de-la-informacion.pdf
- ISO. (2022). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection - Information security management systems - Requirements*.
- Kaspersky. (2022). *Panorama de amenazas América Latina*. <https://latam.kaspersky.com/blog/panorama-amenazas-latam-2022/25509/>
- Li, D., Landström, A., Fast, Å., & Almström, P. (2019). Human-Centred Dissemination of Data, Information and Knowledge in Industry 4.0. *Procedia CIRP*, 84, 380-386.

- Llano, A., Gaibor, M., Cruz, C., & Cadena, J. (2021). Importancia de políticas de seguridad Informática de acuerdo a las ISO 27001 para pequeñas y medianas empresas del Ecuador. *Ciencias de la Ingeniería y Aplicadas*, 5(2), 82-98. <http://investigacion.utc.edu.ec/revistasutc/index.php/ciya/article/view/374>
- López, R., Avello, R., Palmero, D., Sánchez, S., & Quintana, M. (2019). Validación de instrumentos como garantía de la credibilidad en las investigaciones científicas. *Revista Cubana de Medicina Militar*, 48(2(Sup)), 441-450. <https://revmedmilitar.sld.cu/index.php/mil/article/view/390>
- Mamani, J., Valenzuela, J., Huaraz, S., & Andrade, L. (2022). The Implementation of Information Security for the Inventory System in a Municipality of Lima-Perú. *International Journal on Advanced Science, Engineering and Information Technology*, 12(1), 101-113. <https://doi.org/10.18517/IJASEIT.12.1.13914>
- Medina, J. (2023). *ISO 27001 para la gestión de seguridad de la información en el área TI de una empresa industrial, Lima 2023*. <https://repositorio.ucv.edu.pe/handle/20.500.12692/121182>
- Microsoft. (2022). *Microsoft Digital Defense Report 2022*. <https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report-2022>
- Mucha, L., Chamorro, R., Oseda, M., & Alania, R. (2021). Evaluación de procedimientos empleados para determinar la población y muestra en trabajos de investigación de posgrado. *Desafíos*, 12(1), e253-e253. <https://doi.org/10.37711/DESAFIOS.2021.12.1.253>
- Polanía, C., Cardona, F., Castañeda, G., Vargas, I., Calvache, O., & Abanto, W. (2020). *Metodología de investigación Cuantitativa & Cualitativa*. Institución Universitaria Antonio José Camacho y Universidad César Vallejo. <https://doi.org/10.1/JQUERY.MIN.JS>
- Pratama, A., Zaki, A., Fiddarain, S., & Buyung, A. (2023). Implementation of ISO 27001: 2013 in Information System Security at ANNUR PRIMA Islamic Education Foundation. *Jurnal Sains dan Teknologi (JSIT)*, 3(1), 68-73. <https://doi.org/10.47233/JSIT.V3I1.488>

- Ramírez, E., & Rinconc, M. (2022). La importancia de la seguridad de la información en el sector público en Colombia. *Revista Ibérica de Sistemas e Tecnologías de Informação*, 46(6), 87-99. <https://doi.org/10.17013/risti.46.87-99>
- Rivadeneira, J., De La Hoz, A., & Barrera, M. (2020). Análisis general del SPSS y su utilidad en la estadística. *E-IDEA Journal Of Business Sciences*, 2(4), 17-25. <https://revista.estudioidea.org/ojs/index.php/eidea/article/view/19>
- Rodríguez, L., Cruzado, C., Mejía, C., & 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), 786. <https://doi.org/10.20511/PYR2020.V8N3.786>
- Sánchez, D. (2022). Técnicas e instrumentos de recolección de datos en investigación. *TEPEXI Boletín Científico de la Escuela Superior Tepeji del Río*, 9(17), 38-39. <https://doi.org/10.29057/ESTR.V9I17.7928>
- Sánchez, P., García, J., Triana, A., & Perez, L. (2021). Medida del nivel de seguridad informática de las pequeñas y medianas empresas (PYMEs) en Colombia. *Información tecnológica*, 32(5), 121-128. <https://doi.org/10.4067/S0718-07642021000500121>
- Segura, M. (2022). Diseño de un sistema de gestión de seguridad de la información: Caso de estudio Universidad Nacional Intercultural Fabiola Salazar Leguía. En *Repositorio Institucional - USS*. Universidad Señor de Sipán. <http://repositorio.uss.edu.pe/handle/20.500.12802/10186>
- Sepúlveda, S., & Cravero, A. (2021). Diseño de una política de seguridad de la información: una propuesta. *Revista Ibérica de Sistemas e Tecnologías de Informação*, 285-295. <https://www.proquest.com/docview/2647406666/6F59D4DA8E584037PQ/2>
- Szczepaniuk, E., Szczepaniuk, H., Rokicki, T., & Klepacki, B. (2020). Information security assessment in public administration. *Computers & Security*, 90, 101709. <https://doi.org/10.1016/j.cose.2019.101709>

- Tarazona, H. (2020). Observaciones para la construcción y validación de instrumentos de investigación. *Desafíos*, 11(2), e213. <https://doi.org/10.37711/desafios.2020.11.2.213>
- Ticona, H. (2021). Uso de la norma ISO 27001 y su influencia en la seguridad de información de la empresa Ico el año 2021. En *Universidad Privada del Norte*. Universidad Privada del Norte. <https://repositorio.upn.edu.pe/handle/11537/28162>
- Toro, R., Peña, M., Avendaño, B., Mejía, S., & Bernal, A. (2022). Análisis Empírico del Coeficiente Alfa de Cronbach según Opciones de Respuesta, Muestra y Observaciones Atípicas. *Revista Iberoamericana de Diagnóstico y Evaluación Psicológica*, 63(2), 17-30. <https://doi.org/10.21865/RIDEP63.2.02>
- Torres, J., & Asqui, J. (2023). *27001 para mejorar la seguridad de la información en una institución educativa*, Lima 2022. <https://hdl.handle.net/20.500.13053/8519>
- Useche, M., Artigas, W., Queipo, B., & Perozo, É. (2019). *Técnicas e instrumentos de recolección de datos cuali-cuantitativos*. (Vol. 1). Universidad de la Guajira. <https://repositoryinst.uniguajira.edu.co/handle/uniguajira/467>
- Verizon. (2022). 2022 Data Breach Investigations Report. En *Verizon*. <https://www.verizon.com/business/resources/reports/dbir/>
- Yungán, J., & Narváez, C. (2022). Aplicación de la Norma ISO 27001 para la seguridad de los Sistemas de Información. *Dominio de las Ciencias*, 8(3). <https://doi.org/10.23857/dc.v8i3>
- Yuni, J., & Urbano, C. (2020). *Metodología y técnicas para Investigar: recursos para la elaboración de proyectos, análisis de datos y redacción científica*. Brujas. [/ri.conicet.gov.ar/handle/11336/160315](https://ri.conicet.gov.ar/handle/11336/160315)

ANEXOS

Anexo 1. Operacionalización de variables

Variable	Definición conceptual	Definición operacional	Dimensión	Indicadores	Instrumento	Escala
Variable independiente ISO/IEC 27001:2022	Norma internacional que detalla los criterios esenciales para establecer, conservar y mejorar continuamente un sistema de gestión de seguridad de la información en una organización (Carvalho & Marques, 2019).	La ISO/IEC 27001:2022 se midió con un cuestionario tipo escala de Likert con un total de 25 ítems comprendido en 4 dimensiones: Planificación (12 ítems), Ejecución (5 ítems), Verificación (5 ítems) y Mejoramiento (3 ítems).		Liderazgo	Cuestionario	Ordinal (Escala de Likert)
			Planificación	Planificación		
			Ejecución	Operación		
			Verificación	Desempeño		
Variable dependiente Seguridad de la información	Conjunto de actividades y procedimientos que coordinan esfuerzos para asegurar que se almacene, procese y transmita la información de manera confidencial e íntegra, y esté disponible en todo momento (Fathurohman & Witjaksono, 2020).	La seguridad de la información fue medida con un cuestionario tipo escala de Likert con un total de 25 ítems comprendido en 3 dimensiones: Integridad (9 ítems), Confidencialidad (8 ítems) y Disponibilidad (8 ítems).	Integridad	Exactitud	Cuestionario	Ordinal (Escala de Likert)
				Consistencia		
				Completitud		
			Confidencialidad	Control de acceso		
				Protección de datos		
				Rendimiento		
	Disponibilidad	Capacidad de respuesta				
		Capacidad de recuperación				

Anexo 2. Matriz de consistencia

Problema General	Objetivo General	Hipótesis General	Variables - Dimensión - Indicadores		
¿Cuál es la influencia de la ISO/IEC 27001:2022 en la seguridad de la información de EMSEU S.A.C.?	Determinar la influencia de la ISO/IEC 27001:2022 en la seguridad de la información de EMSEU S.A.C.	La ISO/IEC 27001:2022 influye significativamente en la seguridad de la información de EMSEU.	Variable Independiente ISO/IEC 27001:2022 Variable Dependiente Seguridad de la información		
Problemas Específicos	Objetivos Específicos	Hipótesis Específicas	Dimensiones	Indicadores	Escala
PE1: ¿Cuál es la influencia de la ISO/IEC 27001:2022 en la integridad de la información de EMSEU S.A.C.?	OE1: Realizar una evaluación situacional de la seguridad de la información de EMSEU S.A.C.	HE1: La ISO/IEC 27001:2022 influye significativamente en la integridad de la información de EMSEU S.A.C.	Integridad	Exactitud Consistencia Compleitud	
PE2: ¿Cuál es la influencia de la ISO/IEC 27001:2022 en la confidencialidad de la información de la de EMSEU S.A.C.?	OE2: Implementar la ISO/IEC 27001:2022 para mejorar la seguridad en la información de EMSEU S.A.C.	HE2: La ISO/IEC 27001:2022 influye significativamente en la confidencialidad de la información de EMSEU S.A.C.	Confidencialidad	Control de acceso Protección de datos	Ordinal (Escala de Likert)
PE3: ¿Cuál es la influencia de la ISO/IEC 27001:2022 en la disponibilidad de la información de EMSEU S.A.C.?	OE3: Evaluar la influencia de la ISO/IEC 27001:2022 en la seguridad de la información de EMSEU S.A.C.	HE3: La ISO/IEC 27001:2022 influye significativamente en la disponibilidad de la información de EMSEU S.A.C.	Disponibilidad	Rendimiento Capacidad de respuesta Capacidad de recuperación	
Metodología	Población, Muestra y Muestreo	Técnicas e Instrumentos	Estadística por utilizar		
Tipo: Aplicada	Población: 60 Trabajadores	Técnica: Encuesta	Análisis descriptivo: Para resumir y describir los datos obtenidos. Análisis inferencial: Para generar conclusiones más allá de la muestra.		
Enfoque: Cuantitativa	Muestra: 20 administrativos y 15 técnicos	Instrumento: Cuestionario			
Diseño: Pre experimental	Muestreo: No probabilístico por conveniencia				

Anexo 3. Instrumentos de investigación

CUESTIONARIO N.º 01

El presente cuestionario tiene como objetivo recopilar información para llevar a cabo un análisis de la implementación del estándar internacional ISO/ IEC 27001:2022 en la Empresa Municipal de Servicios Eléctricos Utcubamba S.A.C.

Instrucciones:

Lea cuidadosamente y responda marcando con una "X" en el recuadro correspondiente la opción que mejor refleje su opinión o experiencia en relación con cada enunciado. Sea honesto(a); responda de manera intuitiva y evite respuestas neutras. Recuerde que no existe respuesta correcta o incorrecta. La valoración a tener en cuenta es del 1 al 5, donde 1 es "Totalmente en desacuerdo", 2 es "En desacuerdo", 3 es "Ni de acuerdo ni en desacuerdo", 4 es "De acuerdo" y 5 es "Totalmente de acuerdo".

Ítem	Enunciado	Alternativas				
		1	2	3	4	5
Dimensión 1: Planificación						
01	La organización demuestra un sólido proceso de identificación y clasificación de sus activos de información.					
02	La organización define claramente los límites de aplicabilidad para un Sistema de Gestión de Seguridad de la Información.					
03	La alta dirección de la organización demuestra liderazgo y compromiso para la instauración de un Sistema de Gestión de Seguridad de la Información.					
04	La organización formula y establece políticas de seguridad de la información que se alinean con sus objetivos estratégicos.					
05	La organización establece de manera efectiva roles y responsabilidades para garantizar la seguridad de la información.					
06	La organización identifica y evalúa de forma integral riesgos y oportunidades relacionados con la seguridad de la información.					
07	La organización define y aplica planes para el tratamiento de riesgos vinculados a la seguridad de la información.					
08	La organización formula objetivos de seguridad de la información con planes concretos para su consecución.					
09	La organización proporciona recursos necesarios para establecer, implementar y mejorar continuamente un Sistema de Gestión de Seguridad de la Información.					
10	La organización lleva a cabo acciones para concientizar y adquirir la competencia necesaria de un Sistema de Gestión de Seguridad de la Información.					

11	La organización determina la necesidad de comunicación para la efectividad de un Sistema de Gestión de la Seguridad de la Información.								
12	La organización documenta la información necesaria para la planificación y operación de un Sistema de Gestión de Seguridad de la Información.								
Dimensión 2: Ejecución									
13	La organización planifica, implementa y controla los procesos para cumplir los requisitos de un Sistema de Gestión de Seguridad de la Información.								
14	La organización asegura que procesos, productos o servicios de fuentes externas cumplan los requisitos de un Sistema de Gestión de Seguridad de la Información.								
15	La organización realiza evaluaciones de riesgos de la seguridad de la información a intervalos planificados.								
16	La organización implementa un plan de tratamiento para los riesgos de la seguridad de la información.								
17	La organización documenta la información de los resultados de las evaluaciones y tratamiento de los riesgos de la seguridad de la información.								
Dimensión 3: Verificación									
18	La organización realiza el seguimiento, análisis y evaluación de la gestión de la seguridad de la información.								
19	La organización evalúa el desempeño de la seguridad de la información y la eficacia del Sistema de Gestión de Seguridad de la Información.								
20	La organización realiza auditorías internas para garantizar el cumplimiento y la calidad del Sistema de Gestión de Seguridad de la Información.								
21	La alta dirección de la organización revisa de manera periódica la idoneidad, adecuación y eficacia del Sistema de Gestión de Seguridad de la Información.								
22	La alta dirección toma decisiones sobre oportunidades de mejora en el Sistema de Gestión de Seguridad de la Información.								
Dimensión 4: Mejoramiento									
23	La organización de manera continua mejora la idoneidad, adecuación y eficacia del Sistema de Gestión de Seguridad de la Información.								
24	La organización controla las normas de cumplimiento de la seguridad de la información.								
25	La organización corrige de manera efectiva las normas de cumplimiento de la seguridad de la información.								

¡Gracias por su participación y valiosa contribución con el estudio!

CUESTIONARIO N.º 02

El presente cuestionario tiene como objetivo recopilar información para llevar a cabo un análisis de la seguridad de la información en la Empresa Municipal de Servicios Eléctricos Utcubamba S.A.C.

Instrucciones:

Lea cuidadosamente y responda marcando con una "X" en el recuadro correspondiente la opción que mejor refleje su opinión o experiencia en relación con cada enunciado. Sea honesto(a); responda de manera intuitiva y evite respuestas neutras. Recuerde que no existe respuesta correcta o incorrecta. La valoración a tener en cuenta es del 1 al 5, donde 1 es "Totalmente en desacuerdo", 2 es "En desacuerdo", 3 es "Ni de acuerdo ni en desacuerdo", 4 es "De acuerdo" y 5 es "Totalmente de acuerdo".

Ítem	Enunciado	Alternativas				
		1	2	3	4	5
Dimensión 1: Integridad						
01	La organización cuenta con medidas o políticas de seguridad para proteger la información confidencial.					
02	La organización emplea métodos de validación para asegurar la autenticidad e integridad de la información.					
03	La organización limita la capacidad de escribir o actualizar información crítica en las bases de datos solo a usuarios autorizados.					
04	La organización dispone de mecanismos efectivos para identificar y responder posibles amenazas que puedan poner en riesgo la información.					
05	La organización realiza pruebas frecuentes de la infraestructura de red y sistemas para garantizar su capacidad de resistencia ante posibles ataques.					
06	La organización cuenta con firewalls o medidas de seguridad perimetral para proteger la información contra amenazas externas.					
07	La organización utiliza antivirus y antimalware para prevenir infecciones que puedan comprometer la información.					
08	La organización realiza de manera periódica copias de seguridad para facilitar la recuperación de información en caso de daño o pérdida.					
09	La organización lleva a cabo revisiones periódicas de seguridad para identificar posibles alteraciones no autorizadas en la información.					
Dimensión 2: Confidencialidad						
10	La organización proporciona accesos según roles y responsabilidades para limitar de manera apropiada el acceso a la información.					

11	La organización cuenta con políticas de control para garantizar la protección de información confidencial.						
12	La organización posee métodos sólidos para identificar a los usuarios y autenticar su acceso a la información.						
13	La organización posee controles de seguridad lógica y física para prevenir el acceso no autorizado a los sistemas y servidores.						
14	La organización utiliza técnicas de cifrado para garantizar la seguridad de la información durante su almacenamiento y transmisión.						
15	La organización promueve y garantiza la actualización regular de contraseñas para prevenir accesos a la información no autorizados.						
16	La organización promueve una cultura de responsabilidad individual sobre la importancia de mantener la confidencialidad de la información.						
17	La organización cuenta con políticas internas que sancionan a los empleados que vulneren la confiabilidad de la información.						
Dimensión 3: Disponibilidad							
18	La organización posee infraestructura de red adecuada para garantizar la disponibilidad de los sistemas y servicios de información.						
19	La organización cuenta con servicio de internet de calidad que permite realizar los trabajos diarios de manera eficiente.						
20	La organización realiza actualizaciones regulares de software y hardware para asegurar que los sistemas de información estén protegidos.						
21	La organización cuenta con acceso a los sistemas y servicios de información las 24 horas del día.						
22	La organización dispone de la información con facilidad para llevar a cabo tareas diarias.						
23	La organización cuenta con personal calificado para dar respuesta a situaciones inesperadas que podrían afectar el acceso o disponibilidad de la información.						
24	La organización realiza mantenimientos preventivos y correctivos de la infraestructura de red para evitar interrupciones no deseadas.						
25	La organización cuenta con estrategias para mantener la continuidad del negocio en caso de eventos inesperados o desastres naturales.						

¡Gracias por su participación y valiosa contribución con el estudio!

Anexo 4. Validación de instrumentos

VALIDACIÓN DE INSTRUMENTOS

El presente documento tiene como objetivo validar los instrumentos de la investigación “Influencia de la ISO/IEC 27001:2022 en la seguridad de la información de empresa eléctrica” mediante el juicio de expertos, para garantizar la idoneidad, coherencia y consistencia de su contenido.

Categoría	Calificación	Indicador
Idoneidad Los ítems tienen la capacidad de recopilar la información deseada.	1 - No cumple con el criterio	El ítem no recopila la información deseada de la dimensión.
	2 - Bajo nivel	El ítem recopila algún aspecto de la información deseada de la dimensión.
	3 - Moderado nivel	El ítem recopila varios aspectos de la dimensión, pero no corresponde a la dimensión total.
	4 - Alto nivel	El ítem recopila en su totalidad la información deseada de la dimensión.
Claridad Los ítems se comprenden fácilmente; su sintáctica y semántica es adecuada.	1 - No cumple con el criterio	El ítem no se comprende fácilmente.
	2 - Bajo nivel	El ítem requiere modificaciones para mejorar su comprensión.
	3 - Moderado nivel	El ítem requiere una modificación específica para mejorar su comprensión.
	4 - Alto nivel	El ítem se comprende fácilmente, su sintáctica y semántica es adecuada.
Coherencia Los ítems guardan relación lógica con la dimensión.	1 - No cumple con el criterio	El ítem no guarda relación lógica con la dimensión.
	2 - Bajo nivel	El ítem guarda mínima relación lógica con la dimensión.
	3 - Moderado nivel	El ítem guarda moderada relación lógica con la dimensión.
	4 - Alto nivel	El ítem guarda total relación lógica con la dimensión.
Relevancia Los ítems son esenciales o importantes para ser incluidos.	1 - No cumple con el criterio	El ítem puede ser eliminado sin afectar la medición de la dimensión.
	2 - Bajo nivel	El ítem tiene relevancia, pero otro ítem también incluye lo que mide.
	3 - Moderado nivel	El ítem es relativamente importante para medir la dimensión.
	4 - Alto nivel	El ítem es relevante y debe ser incluido para medir la dimensión.

INSTRUCCIONES

Lea cuidadosamente los ítems y responda en el recuadro correspondiente el valor de la opción que mejor refleje su opinión. Sea honesto(a); no existe respuesta correcta o incorrecta. Considere la valoración del 1 al 4, donde 1 es “No cumple con el criterio”, 2 es “Bajo nivel”, 3 es “Moderado nivel”, 4 es “Alto nivel”. Además, por favor, proporcione las observaciones que considere pertinentes.

CUESTIONARIO N.º 01						
Autor	Keymer Alexis Bustamante Campos					
Objetivo	Recopilar información para llevar a cabo un análisis de la implementación del estándar internacional ISO/ IEC 27001:2022 en la Empresa Municipal de Servicios Eléctricos Utcubamba S.A.C.					
Dimensión 1: Planificación						
Indicadores	Ítem	Idoneidad	Claridad	Coherencia	Relevancia	Observaciones
Liderazgo	01	4	4	4	4	
	02	4	4	4	4	
	03	4	4	4	4	
	04	4	4	4	4	
	05	4	4	4	4	
Planificación	06	4	4	4	4	
	07	4	4	4	4	
	08	4	4	4	4	
Soporte	09	4	4	4	4	
	10	4	4	4	4	
	11	4	4	4	4	
	12	4	4	4	4	
Dimensión 2: Ejecución						
Indicadores	Ítem	Idoneidad	Claridad	Coherencia	Relevancia	Observaciones
Operación	13	4	3	3	4	
	14	4	4	4	4	
	15	4	4	4	4	
	16	4	4	4	4	
	17	4	4	4	4	
Dimensión 3: Verificación						
Indicadores	Ítem	Idoneidad	Claridad	Coherencia	Relevancia	Observaciones
Desempeño	18	4	4	4	4	
	19	4	4	4	4	
	20	4	4	4	4	
	21	4	3	3	4	
	22	4	4	4	4	
Dimensión 4: Mejoramiento						
Indicadores	Ítem	Idoneidad	Claridad	Coherencia	Relevancia	Observaciones
Mejora	23	4	3	3	4	
	24	4	4	4	4	
	25	4	4	4	4	

CUESTIONARIO N.º 02						
Autor	Keymer Alexis Bustamante Campos					
Objetivo	Recopilar información para llevar a cabo un análisis de la seguridad de la información en la Empresa Municipal de Servicios Eléctricos Utcubamba S.A.C.					
Dimensión 1: Integridad						
Indicadores	Ítem	Idoneidad	Claridad	Coherencia	Relevancia	Observaciones
Exactitud	01	4	4	4	4	
	02	4	4	4	4	
	03	4	3	4	4	
Consistencia	04	4	4	4	4	
	05	4	4	4	4	
	06	4	4	4	4	
Complejidad	07	4	4	4	4	
	08	4	4	4	4	
	09	4	3	4	4	
Dimensión 2: Confidencialidad						
Indicadores	Ítem	Idoneidad	Claridad	Coherencia	Relevancia	Observaciones
Control de acceso	10	4	4	4	4	
	11	4	3	4	4	
	12	4	4	4	4	
	13	4	4	4	4	
Protección de datos	14	4	4	4	4	
	15	4	4	4	4	
	16	4	4	4	4	
	17	4	4	4	4	
Dimensión 3: Disponibilidad						
Indicadores	Ítem	Idoneidad	Claridad	Coherencia	Relevancia	Observaciones
Rendimiento	18	4	4	4	4	
	19	4	4	4	4	
	20	4	4	4	4	
Capacidad de respuesta	21	4	4	4	4	
	22	4	4	4	4	
	23	4	4	4	4	
Capacidad de recuperación	24	4	4	4	4	
	25	4	4	4	4	

EVALUACIÓN GENERAL

Marque con una 'X' en la casilla correspondiente.



	Excelente	Bueno	Regular	Deficiente
Contenido del cuestionario N.º 01	x			
Contenido del cuestionario N.º 02	x			

DECISIÓN

	Aplicable	Aplicable después de corregir	No aplicable
Opinión de aplicabilidad	x		

DATOS GENERALES DEL EXPERTO

Nombre y apellidos	Elvis Eduardo Otiniano Amambal
Grado académico	Ingeniero de Sistemas
Especialidad	Ingeniería de Sistemas
Cargo	Jefe de Tecnologías de la Información
Institución	Empresa Municipal de Servicios Eléctricos Utcubamba S.A.C.

Fecha de la validación	18/04/2024
Firma	 Elvis Eduardo Otiniano Amambal JEFE TECNOLOGÍAS DE LA INFORMACIÓN 

¡Gracias por su participación y valiosa contribución con el estudio!

CUESTIONARIO N.º 01						
Autor	Keymer Alexis Bustamante Campos					
Objetivo	Recopilar información para llevar a cabo un análisis de la implementación del estándar internacional ISO/ IEC 27001:2022 en la Empresa Municipal de Servicios Eléctricos Utcubamba S.A.C.					
Dimensión 1: Planificación						
Indicadores	Ítem	Idoneidad	Claridad	Coherencia	Relevancia	Observaciones
Liderazgo	01	4	4	4	4	
	02	4	4	4	4	
	03	4	4	4	4	
	04	4	4	4	4	
	05	4	4	4	4	
Planificación	06	4	4	4	4	
	07	4	4	4	4	
	08	4	4	4	4	
Soporte	09	4	4	4	4	
	10	4	4	4	4	
	11	4	4	4	4	
	12	4	4	4	4	
Dimensión 2: Ejecución						
Indicadores	Ítem	Idoneidad	Claridad	Coherencia	Relevancia	Observaciones
Operación	13	4	4	4	4	
	14	4	4	4	4	
	15	4	4	4	4	
	16	4	4	4	4	
	17	4	4	4	4	
Dimensión 3: Verificación						
Indicadores	Ítem	Idoneidad	Claridad	Coherencia	Relevancia	Observaciones
Desempeño	18	4	4	4	4	
	19	4	4	4	4	
	20	4	4	4	4	
	21	4	4	4	4	
	22	4	4	4	4	
Dimensión 4: Mejoramiento						
Indicadores	Ítem	Idoneidad	Claridad	Coherencia	Relevancia	Observaciones
Mejora	23	4	4	4	4	
	24	4	4	4	4	
	25	4	4	4	4	

CUESTIONARIO N.º 02						
Autor	Keymer Alexis Bustamante Campos					
Objetivo	Recopilar información para llevar a cabo un análisis de la seguridad de la información en la Empresa Municipal de Servicios Eléctricos Utcubamba S.A.C.					
Dimensión 1: Integridad						
Indicadores	Ítem	Idoneidad	Claridad	Coherencia	Relevancia	Observaciones
Exactitud	01	4	4	4	4	
	02	4	4	4	4	
	03	4	4	4	4	
Consistencia	04	4	4	4	4	
	05	4	4	4	4	
	06	4	4	4	4	
Complejidad	07	4	4	4	4	
	08	4	4	4	4	
	09	4	4	4	4	
Dimensión 2: Confidencialidad						
Indicadores	Ítem	Idoneidad	Claridad	Coherencia	Relevancia	Observaciones
Control de acceso	10	4	4	4	4	
	11	4	4	4	4	
	12	4	4	4	4	
	13	4	4	4	4	
Protección de datos	14	4	4	4	4	
	15	4	4	4	4	
	16	4	4	4	4	
	17	4	4	4	4	
Dimensión 3: Disponibilidad						
Indicadores	Ítem	Idoneidad	Claridad	Coherencia	Relevancia	Observaciones
Rendimiento	18	4	4	4	4	
	19	4	4	4	4	
	20	4	4	4	4	
Capacidad de respuesta	21	4	4	4	4	
	22	4	4	4	4	
	23	4	4	4	4	
Capacidad de recuperación	24	4	4	4	4	
	25	4	4	4	4	

EVALUACIÓN GENERAL

Marque con una 'X' en la casilla correspondiente.

	Excelente	Bueno	Regular	Deficiente
Contenido del cuestionario N.º 01	x			
Contenido del cuestionario N.º 02	x			

DECISIÓN

	Aplicable	Aplicable después de corregir	No aplicable
Opinión de aplicabilidad	x		

DATOS GENERALES DEL EXPERTO

Nombre y apellidos	Kenett Ronald Serrano Carranza
Grado académico	Ingeniero de Sistemas
Especialidad	Ingeniería de Sistemas
Cargo	Jefe de la Unidad de Tecnología de la Información
Institución	Red Integrada de Salud Bagua

Fecha de la validación	19/04/2023
Firma	 <p>GOBIERNO REGIONAL AMAZONAS DIRECCIÓN REGIONAL DE SALUD AMAZONAS DIRECCIÓN DE RED DE SALUD BAGUA</p> <p>..... ING. SIST. KENETT RONALD SERRANO CARRANZA C.P. 103635 JEFE DE LA UNIDAD DE TECNOLOGÍA DE LA INFORMACIÓN</p>

¡Gracias por su participación y valiosa contribución con el estudio!

CUESTIONARIO N.º 01						
Autor	Keymer Alexis Bustamante Campos					
Objetivo	Recopilar información para llevar a cabo un análisis de la implementación del estándar internacional ISO/ IEC 27001:2022 en la Empresa Municipal de Servicios Eléctricos Utcubamba S.A.C.					
Dimensión 1: Planificación						
Indicadores	Ítem	Idoneidad	Claridad	Coherencia	Relevancia	Observaciones
Liderazgo	01	4	4	4	4	
	02	4	4	4	4	
	03	4	4	4	4	
	04	4	4	4	4	
	05	4	4	4	4	
Planificación	06	4	4	4	4	
	07	4	4	4	4	
	08	4	4	4	4	
Soporte	09	4	4	4	4	
	10	4	4	4	4	
	11	4	4	4	4	
	12	4	4	4	4	
Dimensión 2: Ejecución						
Indicadores	Ítem	Idoneidad	Claridad	Coherencia	Relevancia	Observaciones
Operación	13	4	4	4	4	
	14	4	4	4	4	
	15	4	4	4	4	
	16	4	4	4	4	
	17	4	4	4	4	
Dimensión 3: Verificación						
Indicadores	Ítem	Idoneidad	Claridad	Coherencia	Relevancia	Observaciones
Desempeño	18	4	4	4	4	
	19	4	4	4	4	
	20	4	4	4	4	
	21	4	4	4	4	
	22	4	4	4	4	
Dimensión 4: Mejoramiento						
Indicadores	Ítem	Idoneidad	Claridad	Coherencia	Relevancia	Observaciones
Mejora	23	4	4	4	4	
	24	4	4	4	4	
	25	4	4	4	4	

CUESTIONARIO N.º 02						
Autor	Keymer Alexis Bustamante Campos					
Objetivo	Recopilar información para llevar a cabo un análisis de la seguridad de la información en la Empresa Municipal de Servicios Eléctricos Utcubamba S.A.C.					
Dimensión 1: Integridad						
Indicadores	Ítem	Idoneidad	Claridad	Coherencia	Relevancia	Observaciones
Exactitud	01	4	4	4	4	
	02	4	4	4	4	
	03	4	4	4	4	
Consistencia	04	4	4	4	4	
	05	4	4	4	4	
	06	4	4	4	4	
Complejidad	07	4	4	4	4	
	08	4	4	4	4	
	09	4	4	4	4	
Dimensión 2: Confidencialidad						
Indicadores	Ítem	Idoneidad	Claridad	Coherencia	Relevancia	Observaciones
Control de acceso	10	4	4	4	4	
	11	4	4	4	4	
	12	4	4	4	4	
	13	4	4	4	4	
Protección de datos	14	4	4	4	4	
	15	4	4	4	4	
	16	4	4	4	4	
	17	4	4	4	4	
Dimensión 3: Disponibilidad						
Indicadores	Ítem	Idoneidad	Claridad	Coherencia	Relevancia	Observaciones
Rendimiento	18	4	4	4	4	
	19	4	4	4	4	
	20	4	4	4	4	
Capacidad de respuesta	21	4	4	4	4	
	22	4	4	4	4	
	23	4	4	4	4	
Capacidad de recuperación	24	4	4	4	4	
	25	4	4	4	4	

EVALUACIÓN GENERAL

Marque con una 'X' en la casilla correspondiente.


	Excelente	Buena	Regular	Deficiente
Contenido del cuestionario N.º 01	x			
Contenido del cuestionario N.º 02	x			

DECISIÓN

	Aplicable	Aplicable después de corregir	No aplicable
Opinión de aplicabilidad	x		

DATOS GENERALES DEL EXPERTO

Nombre y apellidos	Luis Manuel Sánchez Fernández
Grado académico	Magister en Docencia Universitaria
Especialidad	Ingeniera en Computación y Sistemas
Cargo	Coordinador del Área de Informática
Institución	Hospital Bicentenario de Chota

Fecha de la validación	20/04/2023
Firma	

¡Gracias por su participación y valiosa contribución con el estudio!

CUESTIONARIO N.º 01						
Autor	Keymer Alexis Bustamante Campos					
Objetivo	Recopilar información para llevar a cabo un análisis de la implementación del estándar internacional ISO/ IEC 27001:2022 en la Empresa Municipal de Servicios Eléctricos Utcubamba S.A.C.					
Dimensión 1: Planificación						
Indicadores	Ítem	Idoneidad	Claridad	Coherencia	Relevancia	Observaciones
Liderazgo	01	4	4	3	4	La pregunta debe referirse a los procedimientos de identificación y clasificación de activos.
	02	4	4	4	4	
	03	4	4	4	4	
	04	4	4	4	4	
	05	4	4	4	4	
Planificación	06	4	4	4	4	
	07	4	4	4	4	
	08	4	4	4	4	
Soporte	09	4	4	4	4	
	10	4	4	4	4	
	11	4	4	4	4	
	12	4	4	4	4	
Dimensión 2: Ejecución						
Indicadores	Ítem	Idoneidad	Claridad	Coherencia	Relevancia	Observaciones
Operación	13	4	4	4	4	
	14	4	4	4	4	
	15	4	4	4	4	
	16	4	4	4	4	
	17	4	4	4	4	
Dimensión 3: Verificación						
Indicadores	Ítem	Idoneidad	Claridad	Coherencia	Relevancia	Observaciones
Desempeño	18	4	4	4	4	
	19	4	4	4	4	
	20	4	4	4	4	
	21	4	4	4	4	
	22	4	4	4	4	
Dimensión 4: Mejoramiento						
Indicadores	Ítem	Idoneidad	Claridad	Coherencia	Relevancia	Observaciones
Mejora	23	4	4	4	4	
	24	4	4	4	4	
	25	4	4	4	4	

CUESTIONARIO N.º 02						
Autor	Keymer Alexis Bustamante Campos					
Objetivo	Recopilar información para llevar a cabo un análisis de la seguridad de la información en la Empresa Municipal de Servicios Eléctricos Utcubamba S.A.C.					
Dimensión 1: Integridad						
Indicadores	Ítem	Idoneidad	Claridad	Coherencia	Relevancia	Observaciones
Exactitud	01	4	4	4	4	
	02	4	4	4	4	
	03	4	4	4	4	
Consistencia	04	4	4	4	4	
	05	4	4	4	4	
	06	4	4	4	4	
Compleitud	07	4	4	4	4	
	08	4	4	4	4	
	09	4	4	4	4	
Dimensión 2: Confidencialidad						
Indicadores	Ítem	Idoneidad	Claridad	Coherencia	Relevancia	Observaciones
Control de acceso	10	4	4	4	4	
	11	4	4	4	4	
	12	4	4	4	4	
	13	4	4	4	4	
Protección de datos	14	4	4	4	4	
	15	4	4	4	4	
	16	4	4	4	4	
	17	4	4	4	4	
Dimensión 3: Disponibilidad						
Indicadores	Ítem	Idoneidad	Claridad	Coherencia	Relevancia	Observaciones
Rendimiento	18	4	4	4	4	
	19	4	4	4	4	
	20	4	4	4	4	
Capacidad de respuesta	21	4	4	4	4	
	22	4	4	4	4	
	23	4	4	4	4	
Capacidad de recuperación	24	4	4	4	4	
	25	4	4	4	4	

EVALUACIÓN GENERAL

Marque con una 'X' en la casilla correspondiente.


	Excelente	Bueno	Regular	Deficiente
Contenido del cuestionario N.º 01	x			
Contenido del cuestionario N.º 02	x			

DECISIÓN

	Aplicable	Aplicable después de corregir	No aplicable
Opinión de aplicabilidad	x		

DATOS GENERALES DEL EXPERTO

Nombre y apellidos	Juliana del Pilar Alva Zapata
Grado académico	Maestro en Ingeniería de Sistemas y Computación con Mención en Dirección Estratégica de Tecnologías de Información
Especialidad	Ingeniera en Computación e Informática
Cargo	Auditor Interno de TI
Institución	Edpyme Alternativa S.A.

Fecha de la validación	22/04/2023
Firma	

¡Gracias por su participación y valiosa contribución con el estudio!

CUESTIONARIO N.º 01						
Autor	Keymer Alexis Bustamante Campos					
Objetivo	Recopilar información para llevar a cabo un análisis de la implementación del estándar internacional ISO/ IEC 27001:2022 en la Empresa Municipal de Servicios Eléctricos Utcubamba S.A.C.					
Dimensión 1: Planificación						
Indicadores	Ítem	Idoneidad	Claridad	Coherencia	Relevancia	Observaciones
Liderazgo	01	4	4	3	4	Considerar preguntar sobre un documento que evidencie el compromiso de la alta dirección con el SGSI.
	02	4	4	3	4	
	03	4	4	3	4	
	04	4	4	3	4	
	05	4	4	3	4	
Planificación	06	4	4	4	4	Considerar preguntar sobre la frecuencia que se planifica el SGSI.
	07	4	4	4	4	
	08	4	4	4	4	
Soporte	09	4	4	4	4	
	10	4	4	4	4	
	11	4	4	4	4	
	12	4	4	4	4	
Dimensión 2: Ejecución						
Indicadores	Ítem	Idoneidad	Claridad	Coherencia	Relevancia	Observaciones
Operación	13	4	4	4	4	
	14	4	4	4	4	
	15	4	4	4	4	
	16	4	4	4	4	
	17	4	4	4	4	
Dimensión 3: Verificación						
Indicadores	Ítem	Idoneidad	Claridad	Coherencia	Relevancia	Observaciones
Desempeño	18	4	4	4	4	
	19	4	4	4	4	
	20	4	4	4	4	
	21	4	4	4	4	
	22	4	4	4	4	
Dimensión 4: Mejoramiento						
Indicadores	Ítem	Idoneidad	Claridad	Coherencia	Relevancia	Observaciones
Mejora	23	4	4	4	4	
	24	4	4	4	4	
	25	4	4	4	4	

CUESTIONARIO N.º 02						
Autor	Keymer Alexis Bustamante Campos					
Objetivo	Recopilar información para llevar a cabo un análisis de la seguridad de la información en la Empresa Municipal de Servicios Eléctricos Utcubamba S.A.C.					
Dimensión 1: Integridad						
Indicadores	Ítem	Idoneidad	Claridad	Coherencia	Relevancia	Observaciones
Exactitud	01	4	4	4	4	
	02	4	4	4	4	
	03	4	4	4	4	
Consistencia	04	4	4	4	4	
	05	4	4	4	4	
	06	4	4	4	4	
Compleitud	07	4	4	4	4	
	08	4	4	4	4	
	09	4	4	4	4	
Dimensión 2: Confidencialidad						
Indicadores	Ítem	Idoneidad	Claridad	Coherencia	Relevancia	Observaciones
Control de acceso	10	4	4	4	4	
	11	4	4	4	4	
	12	4	4	4	4	
	13	4	4	4	4	
Protección de datos	14	4	4	4	4	
	15	4	4	4	4	
	16	4	4	4	4	
	17	4	4	4	4	
Dimensión 3: Disponibilidad						
Indicadores	Ítem	Idoneidad	Claridad	Coherencia	Relevancia	Observaciones
Rendimiento	18	4	4	4	4	
	19	4	4	4	4	
	20	4	4	4	4	
Capacidad de respuesta	21	4	4	4	4	
	22	4	4	4	4	
	23	4	4	4	4	
Capacidad de recuperación	24	4	4	4	4	
	25	4	4	4	4	

EVALUACIÓN GENERAL

Marque con una 'X' en la casilla correspondiente.


	Excelente	Buena	Regular	Deficiente
Contenido del cuestionario N.º 01	x			
Contenido del cuestionario N.º 02	x			

DECISIÓN

	Aplicable	Aplicable después de corregir	No aplicable
Opinión de aplicabilidad	x		

DATOS GENERALES DEL EXPERTO

Nombre y apellidos	Junior Eugenio Cachay Maco
Grado académico	Maestro en Ingeniería de Sistemas
Especialidad	Ingeniería en Computación e Informática
Cargo	Gerente General
Institución	Audit and Control of Information Systems S.A.C.

Fecha de la validación	24/04/2023
Firma	

¡Gracias por su participación y valiosa contribución con el estudio!

Anexo 5. Confiabilidad de instrumentos

CUESTIONARIO N.º 01																											
Encuestados	ítem 01	ítem 02	ítem 03	ítem 04	ítem 05	ítem 06	ítem 07	ítem 08	ítem 09	ítem 10	ítem 11	ítem 12	ítem 13	ítem 14	ítem 15	ítem 16	ítem 17	ítem 18	ítem 19	ítem 20	ítem 21	ítem 22	ítem 23	ítem 24	ítem 25	Suma	
E1	4	4	4	5	5	4	5	4	4	4	5	4	4	5	4	5	4	5	4	5	4	4	4	5	4	109	
E2	5	5	5	5	5	4	5	5	5	5	4	5	4	4	4	5	5	4	4	4	4	4	5	5	5	4	115
E3	4	5	4	4	5	5	5	4	5	4	5	4	5	4	5	4	4	5	4	4	4	4	5	5	5	5	112
E4	5	5	5	4	5	4	4	4	3	5	4	3	4	4	3	4	5	4	4	4	5	5	4	4	4	4	105
E5	5	5	3	4	5	5	5	4	5	5	5	3	5	4	3	5	5	3	3	5	5	5	4	4	4	5	110
E6	4	3	4	4	4	3	4	4	3	4	3	4	3	3	4	4	4	4	4	4	3	3	4	4	3	3	90
E7	4	3	3	4	4	3	4	4	4	4	4	3	4	3	3	4	4	3	3	4	4	4	4	3	4	4	91
E8	4	4	5	4	4	5	5	4	4	5	4	5	4	5	4	5	4	5	4	5	4	4	5	5	4	5	111
E9	4	4	5	4	5	3	5	4	3	4	3	5	4	4	4	4	5	3	4	5	5	5	3	4	4	3	102
E10	5	3	3	5	5	3	4	4	3	4	3	4	3	5	3	5	4	4	5	3	3	4	3	5	5	5	98
E11	5	3	5	4	4	4	4	5	3	4	4	5	4	3	3	4	5	4	4	3	3	4	3	4	4	3	97
E12	4	4	5	5	5	4	4	5	4	5	4	5	4	4	4	4	4	5	4	5	4	5	4	4	4	5	110
E13	4	5	3	4	4	3	4	4	5	4	4	3	4	3	4	5	4	3	4	4	3	4	3	4	3	4	95
E14	4	5	3	5	4	4	4	5	4	5	3	4	5	4	4	4	4	4	4	4	3	4	5	4	5	4	104
E15	5	4	5	5	5	5	5	4	4	4	4	5	5	4	5	4	4	5	5	4	5	5	4	4	4	4	114
E16	4	5	4	4	5	4	4	4	5	4	4	4	4	4	5	5	4	4	4	4	4	4	5	4	5	4	107
E17	5	4	4	4	5	5	4	4	4	4	4	4	5	5	4	4	4	4	4	5	5	5	5	5	4	5	111
E18	5	3	3	4	5	4	4	5	3	5	3	3	4	3	3	4	5	4	4	3	4	5	3	4	4	3	96
E19	4	4	3	5	4	3	4	5	4	4	3	3	4	5	3	4	4	4	4	3	4	4	4	4	4	3	96
E20	4	3	4	4	4	4	5	4	3	5	3	4	5	5	3	4	4	5	5	3	4	4	3	5	4	101	
E21	4	4	3	4	4	3	5	4	4	4	4	3	4	4	4	5	4	5	4	3	5	4	5	3	4	100	
E22	5	4	4	5	4	5	4	4	4	4	4	4	5	4	5	5	5	4	4	5	4	5	5	4	4	4	109
E23	5	4	5	5	5	4	5	5	5	5	5	5	4	4	4	5	4	4	5	5	4	5	5	5	4	4	116
E24	5	5	4	4	4	5	5	4	4	5	5	4	5	4	5	5	5	5	4	5	4	5	4	5	4	4	114
E25	4	4	3	4	4	4	4	4	3	4	3	3	4	3	4	4	4	4	4	4	3	4	4	4	4	3	93
E26	4	5	3	5	4	3	4	5	4	5	4	4	3	3	4	4	5	3	5	4	4	5	3	4	4	4	101
E27	5	4	3	4	5	3	4	4	5	4	5	4	3	4	4	5	4	4	3	4	3	4	3	4	3	4	99
E28	5	3	4	4	5	4	5	5	3	4	4	4	5	4	4	5	4	4	3	4	4	4	4	5	5	5	105
E29	5	4	5	5	4	5	5	5	4	5	4	5	4	4	5	5	4	5	4	5	4	4	5	5	4	4	113
E30	4	3	4	5	5	4	5	5	5	4	4	4	5	4	5	4	5	4	5	5	4	5	4	4	4	5	111
E31	5	4	5	5	4	4	5	4	5	4	5	4	4	5	5	4	5	5	4	4	4	4	5	4	5	5	113
E32	4	4	5	4	5	4	5	5	4	5	3	4	4	4	3	4	5	4	4	3	3	5	3	4	5	5	103
E33	4	3	4	4	4	4	4	5	5	5	4	3	4	5	3	5	5	3	3	4	5	5	5	4	4	3	103
E34	4	3	5	5	4	3	5	5	4	5	4	4	4	4	4	4	4	4	5	5	5	5	4	5	5	5	109
E35	5	4	4	5	5	3	5	5	4	4	3	4	3	4	4	5	4	5	4	4	5	4	4	5	3	105	
Varianza	0.248	0.542	0.656	0.245	0.250	0.536	0.250	0.248	0.542	0.245	0.478	0.454	0.387	0.454	0.478	0.240	0.248	0.444	0.389	0.511	0.501	0.245	0.485	0.420	0.536		

Alfa de Cronbach		Análisis General		Rango	Confiabilidad	
Coeficiente que sirve para medir la fiabilidad de una escala de medida.	$\alpha = \frac{K}{K-1} \left[1 - \frac{\sum S_i^2}{S^2} \right]$	k:	Número de ítems del instrumento	25	< 0.5	Inaceptable
		$\sum_{i=1}^k S_i^2$:	Sumatoria de las varianzas de los ítems	10.03	0.50 - 0.59	Pobre
		S_f^2 :	Varianza total del instrumento	51.99	0.60 - 0.69	Débil
		α :	Coeficiente de confiabilidad	0.841	0.70 - 0.79	Aceptable
CONFIABILIDAD ÓPTIMA						
				0.80 - 0.89	Óptima	
				> 0.9	Excelente	

CUESTIONARIO N.º 02

Encuestados	ítem 01	ítem 02	ítem 03	ítem 04	ítem 05	ítem 06	ítem 07	ítem 08	ítem 09	ítem 10	ítem 11	ítem 12	ítem 13	ítem 14	ítem 15	ítem 16	ítem 17	ítem 18	ítem 19	ítem 20	ítem 21	ítem 22	ítem 23	ítem 24	ítem 25	Suma
E1	5	5	5	4	4	4	4	5	5	5	4	5	5	5	5	4	4	4	5	4	5	5	5	4	5	115
E2	5	4	4	5	4	4	5	5	4	5	5	4	5	4	5	4	4	5	4	3	4	5	4	5	4	110
E3	4	5	4	5	4	4	3	4	4	4	4	4	4	4	4	4	4	5	4	3	4	4	4	4	4	101
E4	4	4	4	4	4	4	4	5	4	4	4	4	4	4	4	4	4	4	5	4	5	5	5	5	4	106
E5	4	4	4	5	4	4	3	5	4	5	4	4	4	4	4	4	3	4	5	4	5	4	4	4	3	102
E6	4	4	4	4	3	4	4	5	4	4	4	4	3	3	4	4	3	4	4	4	4	4	5	4	4	98
E7	4	4	4	4	4	3	4	4	4	4	4	4	5	4	3	4	4	4	4	4	4	4	3	4	3	97
E8	4	5	4	5	4	4	3	5	4	4	4	4	4	4	5	4	4	5	5	4	4	4	5	4	4	106
E9	5	4	5	4	4	4	5	5	4	5	4	4	4	4	4	4	4	3	5	3	4	4	5	5	3	105
E10	4	4	4	3	3	4	5	5	4	5	4	4	4	4	4	4	4	4	3	4	4	4	3	4	3	98
E11	5	4	4	4	4	4	5	5	4	5	5	4	3	3	5	3	3	4	4	4	4	4	4	4	3	101
E12	4	4	3	5	4	4	3	5	4	5	4	4	4	4	4	4	4	3	4	3	5	5	4	4	4	101
E13	5	4	4	4	4	4	4	4	4	5	5	4	3	4	4	4	4	5	4	4	4	5	3	5	4	104
E14	4	5	4	5	4	3	5	5	5	4	5	4	4	4	4	4	4	4	5	4	5	4	5	4	4	107
E15	4	4	5	4	4	3	4	5	4	4	4	4	5	4	4	3	3	4	5	4	5	5	5	5	3	104
E16	4	4	4	4	4	3	4	5	5	5	4	3	4	4	5	4	4	3	4	3	4	4	4	4	4	100
E17	4	4	5	4	4	3	4	5	4	4	4	4	4	4	4	4	4	5	5	4	5	4	3	4	4	103
E18	5	4	4	5	4	4	5	5	5	5	5	4	5	4	4	4	4	4	4	4	5	5	5	5	4	112
E19	4	4	4	3	4	3	4	4	4	4	4	4	3	4	4	4	4	3	4	4	4	4	3	4	4	95
E20	4	5	5	4	4	4	4	5	4	4	4	4	4	4	4	4	4	5	5	3	5	4	4	5	4	106
E21	4	4	4	5	4	3	4	4	5	5	4	4	5	4	4	4	4	4	5	4	4	4	4	4	3	104
E22	4	4	3	4	3	4	3	4	4	4	4	3	4	4	4	3	3	4	4	3	4	4	4	4	4	93
E23	5	5	4	5	4	4	5	5	5	4	5	4	3	4	4	4	3	5	5	4	5	4	5	4	4	109
E24	4	4	4	4	4	3	3	5	4	5	4	4	4	4	5	4	4	4	4	5	4	4	5	4	5	104
E25	4	4	4	4	4	3	4	5	4	4	4	3	3	4	3	4	3	3	4	3	4	3	3	4	4	92
E26	5	5	5	4	4	4	5	5	5	5	5	4	4	5	4	4	4	4	4	5	4	5	4	5	4	112
E27	4	4	4	4	4	4	4	4	4	4	4	3	4	4	4	4	3	4	4	3	4	4	4	4	4	97
E28	4	4	3	4	3	4	4	5	4	4	5	4	3	4	4	3	4	3	4	4	4	4	3	4	4	96
E29	4	4	5	4	4	4	4	5	4	5	4	5	5	5	4	4	4	4	4	4	5	5	4	5	4	107
E30	4	5	4	5	4	4	4	5	4	5	5	4	4	4	5	4	4	5	4	5	4	5	4	5	4	110
E31	5	4	4	4	4	3	3	4	5	4	4	4	4	4	4	4	4	4	5	4	4	4	3	4	4	100
E32	4	4	4	5	4	4	4	5	4	4	5	4	5	4	4	4	4	3	5	4	5	4	4	5	4	106
E33	4	4	4	4	3	3	3	4	4	4	4	3	3	4	4	3	4	4	4	3	4	4	3	4	3	91
E34	5	4	4	5	4	4	4	4	5	5	5	4	5	4	4	4	3	4	4	4	4	4	4	5	4	107
E35	5	5	5	4	4	4	4	5	4	5	5	4	4	5	4	4	4	4	5	4	5	4	5	5	5	112
Varianza	0.216	0.191	0.294	0.318	0.122	0.216	0.457	0.204	0.191	0.250	0.233	0.225	0.397	0.237	0.237	0.122	0.191	0.428	0.233	0.348	0.225	0.248	0.568	0.233	0.313	

Alfa de Cronbach

Coefficiente que sirve para medir la fiabilidad de una escala de medida.


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

Análisis General		
k:	Número de ítems del instrumento	25
$\sum_{i=1}^k S_i^2$:	Sumatoria de las varianzas de los ítems	6.70
S^2 :	Varianza total del instrumento	35.51
α :	Coefficiente de confiabilidad	0.845

CONFIABILIDAD ÓPTIMA

Rango	Confiabilidad
< 0.5	Inaceptable
0.50 - 0.59	Pobre
0.60 - 0.69	Débil
0.70 - 0.79	Aceptable
0.80 - 0.89	Óptima
> 0.9	Excelente

Anexo 6. Autorización de la empresa



EMSEU S.A.C.
con mas energía

EMPRESA MUNICIPAL DE SERVICIOS ELÉCTRICOS UTCUBAMBA

"AÑO DE LA UNIDAD, LA PAZ Y EL DESARROLLO"

Bagua Grande, 22 de mayo del 2023.

CARTA N° 159-2023-EMSEU/GG

SEÑOR
KEYMER ALEXIS BUSTAMANTE CAMPOS
BAGUA GRANDE.

ASUNTO : ALCANZA AUTORIZACIÓN PARA REALIZAR TRABAJO DE INVESTIGACIÓN

REFERENCIA : SOLICITUD DE FECHA 03 DE MAYO. Exp. N° 683-23


De mi especial consideración,

Me es grato dirigirme a Usted, para saludarle y así mismo en respuesta a la solicitud mencionada en la referencia, en la cual solicita autorización para uso de la información de la Empresa Municipal de Servicios Eléctricos Utcubamba, para realizar el proyecto de tesis "INFLUENCIA DE LA ISO/IEC 27001:2022 EN LA SEGURIDAD DE LA INFORMACIÓN DE EMPRESA ELÉCTRICA"

Por lo tanto, **SE AUTORIZA** al Bachiller en Ingeniería de Sistemas de la UNTRM el señor **KEYMER ALEXIS BUSTAMANTE CAMPOS**, identificado con DNI N° 71976964, el **USD DE INFORMACIÓN** de la Empresa Municipal de Servicios Eléctricos Utcubamba, para fines **NETAMENTE ACADÉMICOS**.

Sin otro particular, hago propicia la oportunidad para expresarle las muestras de mi especial consideración y estima personal.

Atentamente,



Ing. Alexander Jucvara Bustamante
GERENTE GENERAL
EMSEU

AG/kefv
GG/sec
C.c. Archivo

Jr. Angamos N° 731 - Teléfono 041- 474220
Web Site: www.emseu.com - E-mail: gerencia@emseu.com
Bagua Grande - Amazonas - Perú

Anexo 7. Implementación la ISO/IEC 27001:2022

Empresa Municipal de Servicios Eléctricos Utcubamba S.A.C.

Implementación de la ISO/IEC 27001:2022

Sección	Requisito ISO/IEC 27001	Estado
4	Contexto de la organización	
4.1	Conocimiento de la organización y de su contexto	
4.1	Determinar los objetivos del SGSI de la organización y cualquier cuestión que pueda comprometer su efectividad.	Gestionado
4.2	Comprensión de las necesidades y expectativas de las partes interesadas	
4.2 (a)	Identificar las partes interesadas, incluyendo leyes aplicables, regulaciones, contratos, etc.	Gestionado
4.2 (b)	Determinar sus requisitos relevantes al respecto de la seguridad de la información y sus obligaciones.	Gestionado
4.3	Determinación del alcance del SGSI	
4.3	Determinar y documentar el alcance del SGSI.	Gestionado
4.4	SGSI	
4.4	Establecer, implementar, mantener y mejorar continuamente un SGSI de conformidad con la norma.	Gestionado
5	Liderazgo	
5.1	Liderazgo y compromiso	
5.1	La alta dirección debe demostrar liderazgo y compromiso en relación con el SGSI.	Definido
5.2	Política	
5.2	Establecer la política de seguridad de la información.	Gestionado
5.3	Roles, responsabilidades y autoridades en la organización	
5.3	Asignar y comunicar los roles y responsabilidades de la seguridad de la información.	Definido
6	Planificación	
6.1	Acciones para tratar riesgos y oportunidades	
6.1.1	Diseñar / planificar el SGSI para satisfacer los requisitos, tratando con los riesgos y oportunidades.	Gestionado
6.1.2	Definir y aplicar un proceso de apreciación de riesgos de seguridad de la información.	Gestionado
6.1.3	Documentar y aplicar un proceso de tratamiento de riesgos de seguridad de la información.	Gestionado
6.2	Objetivos de seguridad de la información y planes para lograrlos	
6.2	Establecer y documentar los objetivos y planes de seguridad de la información.	Gestionado
6.3	Planificación de cambios	
6.3	Los cambios sustanciales al SGSI deben ser llevados a cabo de manera planificada.	No Aplica
7	SopORTE	
7.1	Recursos	
7.1	Determinar y proporcionar los recursos necesarios para el SGSI.	Limitado

Sección	Requisito ISO/IEC 27001	Estado
7.2	Competencias	
7.2	Determinar, documentar y poner a disposición las competencias necesarias.	Definido
7.3	Toma de conciencia	
7.3	Establecer un programa de concientización en seguridad.	Definido
7.4	Comunicación	
7.4	Determinar la necesidad para las comunicaciones internas y externas relevantes al SGSI.	Gestionado
7.5	Información documentada	
7.5.1	Proveer la documentación requerida por la norma, así como la requerida por la organización.	Gestionado
7.5.2	Proveer títulos, autores, etc. para la documentación, adecuar el formato consistentemente, revisarlos y aprobarlos.	Definido
7.5.3	Controlar la documentación adecuadamente.	Limitado
8	Operación	
8.1	Planificación y control operacional	
8.1	Planificar, implementar, controlar y documentar el proceso del SGSI para gestionar los riesgos (i.e. un plan de tratamiento de riesgos).	Gestionado
8.2	Valoración de riesgos de la seguridad de la información	
8.2	(Re)hacer la apreciación y documentar los riesgos de seguridad de la información en forma regular ante cambios o modificaciones.	Gestionado
8.3	Tratamiento del riesgo de seguridad de la información	
8.3	Implementar el plan de tratamiento de riesgos (tratar los riesgos) y documentar los resultados.	Gestionado
9	Evaluación del desempeño	
9.1	Seguimiento, medición, análisis y evaluación	
9.1	Hacer seguimiento, medir, analizar y evaluar el SGSI y los controles.	Gestionado
9.2	Auditoría interna	
9.2	Planificar y llevar a cabo auditorías internas del SGSI.	Definido
9.3	Revisión por la dirección	
9.3	Emprender revisiones por la dirección del SGSI regularmente.	Limitado
10	Mejora	
10.1	Mejora continua	
10.1	Mejorar continuamente el SGSI.	Definido
10.2	No conformidad y acciones correctivas	
10.2	Identificar, corregir y llevar a cabo acciones para prevenir la recurrencia de no conformidades, documentando las acciones.	Definido

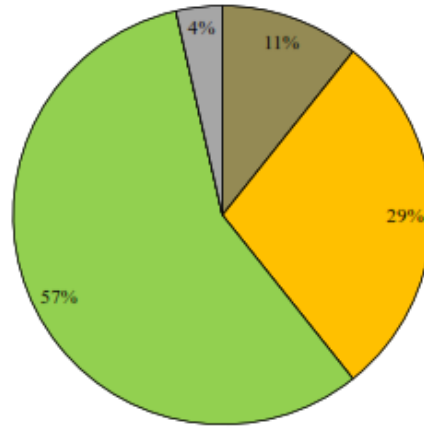
Sección	Control de seguridad de la Información	Estado
A5	Controles organizacionales	
A.5.1	Políticas para la seguridad de la información	Gestionado
A.5.2	Roles y responsabilidades en la seguridad de la información	Definido
A.5.3	Segregación de tareas	Definido
A.5.4	Responsabilidades de gestión	Gestionado
A.5.5	Contacto con las autoridades	Definido
A.5.6	Contacto con grupos de interés especial	Definido
A.5.7	Inteligencia de amenazas	Limitado
A.5.8	Seguridad de la información en la gestión de proyectos	Limitado
A.5.9	Inventario de activos de información y otros asociados a la misma	Gestionado
A.5.10	Uso aceptable de activos de información y otros asociados a la misma	Gestionado
A.5.11	Devolución de activos	Limitado
A.5.12	Clasificación de la información	Definido
A.5.13	Etiquetado de la información	Definido
A.5.14	Intercambio de la información	Gestionado
A.5.15	Control de Acceso	Gestionado
A.5.16	Gestión de la identidad	Gestionado
A.5.17	Información de autenticación	Gestionado
A.5.18	Derechos de acceso	Definido
A.5.19	Seguridad de la información en la relación con proveedores	Definido
A.5.20	Requisitos de seguridad de la información en contratos con terceros	Definido
A.5.21	Gestión de la seguridad de la información en la cadena de suministro de las TIC (Tecnologías de Información y Comunicación)	Limitado
A.5.22	Gestión del cambio, revisión y monitoreo de los servicios del proveedor o suministrador	Definido
A.5.23	Seguridad de la información para el uso de servicios en la nube (cloud)	Gestionado
A.5.24	Planeamiento y preparación de la gestión de incidentes de seguridad de la información	Gestionado
A.5.25	Evaluación y decisión en los eventos de seguridad de la información	Definido
A.5.26	Respuesta a los incidentes de seguridad de la información	Gestionado
A.5.27	Aprendizaje sobre los incidentes de seguridad de la información	Definido
A.5.28	Recolección de evidencia	Limitado
A.5.29	Seguridad de la información durante interrupciones	Gestionado
A.5.30	Preparación de las TIC para la continuidad de negocio	Gestionado
A.5.31	Requisitos legales, estatutarios, regulatorios y contractuales	Limitado
A.5.32	Derechos de propiedad intelectual	No Aplica

Sección	Control de seguridad de la Información	Estado
A.5.33	Protección de registros	Limitado
A.5.34	Privacidad y protección de la PII (Información Identificable Personal)	Definido
A.5.35	Revisión independiente de la seguridad de la información	Definido
A.5.36	Cumplimiento con las políticas, reglas y normas de la seguridad de la información	Gestionado
A.5.37	Procedimientos operacionales documentados	Definido
A6	Controles personales	
A.6.1	Revisión de antecedentes	No Aplica
A.6.2	Términos y condiciones de empleo	Definido
A.6.3	Concientización, educación y entrenamiento en seguridad de la información	Gestionado
A.6.4	Proceso disciplinario	Limitado
A.6.5	Responsabilidades luego de la finalización o cambio de empleo	Limitado
A.6.6	Acuerdos de confidencialidad o no revelación	Gestionado
A.6.7	Trabajo remoto	Gestionado
A.6.8	Reportes de eventos de seguridad de la información	No Aplica
A7	Controles físicos	
A.7.1	Perímetros de seguridad física	Optimizado
A.7.2	Entrada física	Optimizado
A.7.3	Seguridad de oficinas, despachos e instalaciones	Optimizado
A.7.4	Supervisión de la seguridad física	Optimizado
A.7.5	Protección contra amenazas físicas y ambientales	Optimizado
A.7.6	Trabajo en áreas seguras	Gestionado
A.7.7	Escritorio y pantalla limpios	Optimizado
A.7.8	Emplazamiento y protección de equipos	Gestionado
A.7.9	Seguridad de activos fuera de las instalaciones	No Aplica
A.7.10	Medios de almacenamiento	Optimizado
A.7.11	Servicios de suministro	Definido
A.7.12	Seguridad del cableado	Optimizado
A.7.13	Mantenimiento de equipos	Gestionado
A.7.14	Eliminación o reutilización segura de equipos	Gestionado
A8	Controles tecnológicos	
A.8.1	Dispositivos terminales de usuario	Gestionado
A.8.2	Derechos de acceso privilegiado	Gestionado
A.8.3	Restricción de acceso a la información	Gestionado

Sección	Control de seguridad de la Información	Estado
A.8.4	Acceso al código fuente	Gestionado
A.8.5	Autenticación segura	Gestionado
A.8.6	Gestión de la capacidad	Limitado
A.8.7	Protección contra código malicioso (malware)	Gestionado
A.8.8	Gestión de vulnerabilidades técnicas	Gestionado
A.8.9	Gestión de la configuración	Gestionado
A.8.10	Borrado de información	Gestionado
A.8.11	Enmascaramiento de datos	Definido
A.8.12	Prevención de filtración de datos	Definido
A.8.13	Respaldo de información	Gestionado
A.8.14	Redundancia de las instalaciones de procesamiento de información	Optimizado
A.8.15	Registración	Limitado
A.8.16	Actividades de supervisión	Limitado
A.8.17	Sincronización de reloj (clock)	Optimizado
A.8.18	Uso de programas utilitarios privilegiados	Gestionado
A.8.19	Instalación de software en sistemas operacionales	Gestionado
A.8.20	Seguridad en redes	Gestionado
A.8.21	Seguridad de servicios de red	Gestionado
A.8.22	Segregación de redes	Definido
A.8.23	Filtrado web	Gestionado
A.8.24	Uso de criptografía	Definido
A.8.25	Desarrollo seguro del ciclo de vida	Limitado
A.8.26	Requerimientos de seguridad en aplicaciones	Definido
A.8.27	Principios de arquitectura de sistemas e ingeniería segura	Limitado
A.8.28	Generación de código seguro	Gestionado
A.8.29	Prueba segura en el desarrollo y aceptación	Limitado
A.8.30	Desarrollo tercerizado	No Aplica
A.8.31	Separación de entornos de desarrollo, prueba y producción	Gestionado
A.8.32	Gestión de cambios	Gestionado
A.8.33	Información de prueba	Definido
A.8.34	Protección de sistemas de información durante pruebas de auditoría	Limitado
Total		93

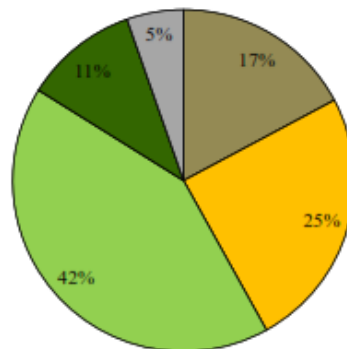
Estado	Significado	Proporción de requisitos del SGSI	Proporción de controles de seguridad de la información
Desconocido	No ha sido siquiera revisado aún.	0%	0%
Inexistente	Ausencia completa de una política, procedimiento, control, etc legibles.	0%	0%
Inicial	El desarrollo apenas ha comenzado y requerirá un trabajo significativo para satisfacer los requisitos.	0%	0%
Limitado	Progresando bien pero no completado aún.	11%	17%
Definido	El desarrollo está más o menos completo aunque con ausencia de detalles y/o no está aún implementado, en cumplimiento vigente ni activamente avalado por la alta dirección.	29%	25%
Gestionado	El desarrollo está completo, el proceso / control ha sido implementado y recientemente comenzó a operar.	57%	42%
Optimizado	El requisito está plenamente conforme, está plenamente operativo como se espera, está siendo activamente supervisado y mejorado, y hay evidencia sustancial para demostrar todo lo antedicho a los auditores.	0%	11%
No Aplica	TODOS los requerimientos en el cuerpo principal de la norma ISO/IEC 27001 son obligatorios SI su SGSI va a ser certificado. Caso contrario, la gerencia a cargo, puede ignorarlos.	4%	5%
Total		100%	100%

Implementación SGSI



■ Limitado ■ Definido ■ Gestionado ■ No Aplica

Controles SGSI



■ Limitado ■ Definido ■ Gestionado ■ Optimizado ■ No Aplica

Anexo 8. Evidencias fotográficas

