Universidad Norbert Wiener

FACULTAD DE INGENIERÍA
PROGRAMA ACADÉMICO DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

Tesis

ISO 27001 para mejorar la seguridad de la información en una Municipalidad de Lima, 2026

Para optar el Título Profesional de

Ingeniero de Sistemas e Informática

Presentado por:

Autor: Aquino Conde, Juan Bryan

Código ORCID: https://orcid.org/0000-0003-2326-3607

Autor: Zegarra Chamorro, Nelyda

Código ORCID: https://orcid.org/0000-0002-1954-6973

Asesor: Mg. Chavez Alvarado, Walter Amador

Código ORCID: https://orcid.org/0000-0001-8614-482X

Lima – Perú

2026

Universidad Norbert Wiener	DECLARACIÓN JURADA DE AUTORIA Y DE ORIGINALIDAD DEL TRABAJO DE INVESTIGACIÓN		
	CÓDIGO: UPNW-GRA-FOR-033	VERSIÓN: 01 REVISIÓN: 01	FECHA: 08/11/2022

Yo, Juan Bryan Aquino Conde y Nelyda Zegarra Chamorro egresados de la Facultad de **Facultad de Ingeniería y Negocios** y Escuela Académica Profesional de **Ingenierías** de la Universidad privada Norbert Wiener declaro que el trabajo de investigación "ISO 27001 para mejorar la seguridad de la información en una Municipalidad de Lima, 2026" Asesorado por el docente: Walter Amador Chavez Alvarado DNI 09731774 ORCID 0000-0001-8614-482X tiene un índice de similitud de **17 (diecisiete) %** con código oid:14912:596320123 verificable en el reporte de originalidad del software Turnitin.

Así mismo:

1. Se ha mencionado todas las fuentes utilizadas, identificando correctamente las citas textuales o paráfrasis provenientes de otras fuentes.
2. No he utilizado ninguna otra fuente distinta de aquella señalada en el trabajo.
3. Se autoriza que el trabajo puede ser revisado en búsqueda de plagios.
4. El porcentaje señalado es el mismo que arrojó al momento de indexar, grabar o hacer el depósito en el turnitin de la universidad y,
5. Asumimos la responsabilidad que corresponda ante cualquier falsedad, ocultamiento u omisión en la información aportada, por lo cual nos sometemos a lo dispuesto en las normas del reglamento vigente de la universidad.

…… …… ……

Firma de autor 1
Juan Bryan Aquino Conde
DNI: 76411104

Firma de autor 2
Nelyda Zegarra Chamorro
DNI: 70332032

……
Firma
Walter Amador Chavez Alvarado
DNI: 09731774

Lima, 19 de Mayo del 2026

Dedicatoria

A Dios por cuidarme y permitir completar esta fase, a mi querida familia por confiar en mí, a mis padres por su apoyo día con día, que hicieron posible llegar hasta aquí, a mi compañero de tesis por su esfuerzo, y a todas las personas que me ayudaron a concluir con la elaboración de esta tesis.

Nelyda Zegarra Chamorro

Dedico este trabajo a mis padres por brindarme el apoyo emocional y financiero para completar la tesis, a mis hermanos por respaldarme y guiarme por el buen camino, a mi sobrina por su amor e inspiración a seguir adelante.

Juan Bryan Aquino Conde

Agradecimiento

En primer lugar, agradecemos a nuestro asesor Mg. Walter Chavez por su paciencia y guía profesional para completar esta tesis, a los expertos docentes que nos firmaron la validación de instrumento, a nuestra universidad Norbert Wiener y a todos los docentes que nos entregaron los conocimientos para la formación de Ingenieros de Sistemas e Informática, por último, a nuestros centros de labores por permitirnos compartir nuestros conocimientos y mejorar mutuamente.

Los autores

Índice general

Índice de tablas

Índice de figuras

Resumen

La actual investigación presenta como objetivo determinar en qué medida la ISO 27001 mejora los niveles de seguridad de la información en una municipalidad de Lima, 2026. Metodológicamente el estudio se desarrolló con un enfoque cuantitativo, con diseño experimental. La población objeto se conforma por 93 controles del ISO 27001:2022 y la muestra se conformó por 15 controles seleccionados. La técnica empleada es la observación y el instrumento es la ficha de observación aplicada por un periodo de 31 días (pre y post implementación de controles), el instrumento fue validado por 3 expertos, el análisis estadístico se realizó con el programa estadístico SPSS que evaluó los indicadores de los tres pilares de seguridad de la información o también llamados CID: C (confidencialidad), I (integridad) y D (disponibilidad). Los resultados se evidenciaron a través del análisis de los indicadores en pre-test y pos-test, determinados mediante promedios. En cuanto a la confidencialidad, el promedio en el pre-test fue de 0,7742 y en el pos-test de 0,3419, con una mejora de 0,4323. Respecto a la integridad, el promedio en el pre-test fue de 0,7097 y en el pos-test de 0,3419, con una diferencia de 0,3678. Del mismo modo, en la disponibilidad de la información se evidenció una mejora aproximada de 0,37 entre el pre-test y el pos-test.

En conclusión, los resultados derivados a partir de la prueba de Wilcoxon ($p<0,05$), evidencian que la implementación de la norma ISO 27001 mejora significativamente los niveles de seguridad de la información, reduciendo las incidencias en las dimensiones de confidencialidad, integridad y disponibilidad, lo que demuestra su efectividad en la gestión de la seguridad de la información.

Palabras claves: ISO 27001, seguridad de la información, confidencialidad, integridad y disponibilidad.

Abstract

The objective of this research is to determine the extent to which ISO 27001 improves information security levels in a municipality in Lima, Peru, by 2026. Methodologically, the study employed a quantitative approach with an experimental design. The target population consisted of 93 ISO 27001:2022 controls, and the sample comprised 15 selected controls. The data collection technique was observation, and the instrument used was an observation checklist applied over a 31-day period (pre- and post-implementation of controls). The instrument was validated by three experts. Statistical analysis was performed using the SPSS statistical software, which evaluated the indicators of the three pillars of information security (ICS): C (confidentiality), I (integrity), and D (availability). The results were presented through the analysis of the indicators in the pre-test and post-test, determined using averages. Regarding confidentiality, the average score in the pre-test was 0.7742 and in the post-test 0.3419, representing an improvement of 0.4323. As for integrity, the average score in the pre-test was 0.7097 and in the post-test 0.3419, a difference of 0.3678. Similarly, information availability showed an approximate improvement of 0.37 between the pre-test and post-test.

In conclusion, the results derived from the Wilcoxon test ($p<0.05$) demonstrate that the implementation of the ISO 27001 standard significantly improves information security levels, reducing incidents in the dimensions of confidentiality, integrity, and availability, thus demonstrating its effectiveness in information security management.

Keywords: ISO 27001, information security, confidentiality, integrity, availability.

INTRODUCCIÓN

La acelerada digitalización de los servicios públicos en el Perú ha traído consigo beneficios evidentes en términos de eficiencia administrativa, transparencia y acceso a la información. Sin embargo, este proceso también ha intensificado los riesgos y amenazas asociados con la seguridad de la información, situando a las entidades gubernamentales, como las municipalidades, en un escenario de creciente exposición a amenazas cibernéticas, por lo tanto, la norma estándar internacional ISO 27001 favorece mejorar la seguridad de la información en una municipalidad. La presente tesis se divide en cinco capítulos:

El **Capítulo I**, presenta la contextualización de la problemática, la formulación del problema general, específicos asimismo se establece la justificación, se presentan los objetivos, hipótesis y marco teórico con sus respectivos antecedentes internacionales y nacionales. En **Capítulo II,** presenta la metodología de la investigación, tipo de estudio y diseño. También se determina la población, muestra, muestreo, se definen las variables, procedimientos y aspectos técnicos que se consideran al realizar la investigación. El **Capítulo III**, se desarrollan los resultados estadísticos para demostrar objetivos e hipótesis, como el análisis de consistencia de datos, pruebas de normalidad y contrataste o prueba de hipótesis. El **Capítulo IV**, analiza los valores de los resultados estadísticos y se comparan con otras investigaciones. El **Capítulo V**, se desarrollan las conclusiones en relación con los objetivos y por último en el **Capítulo VI** se listan las referencias en estilo IEE.

1. Contextualization del problema

1.1. Planteamiento problema

A nivel mundial, el fraude digital en particular el phishing y las estafas en línea constituye uno de los delitos de mayor crecimiento, afectando tanto a ciudadanos como a instituciones [1]. Así mismo, la clonación de información mediante técnicas como el “carding” y la suplantación de identidad digital representa una amenaza directa para los registros que custodian las entidades públicas, generando pérdidas económicas y un deterioro en la confianza ciudadana [2]. En cuanto a las vulnerabilidades, estudios de la Organización de Estados Americanos revelan que gran parte de las instituciones municipales de la región no cuentan con planes actualizados de gestión de riesgos ni con protocolos de respuesta ante incidentes cibernéticos, lo que incrementa su nivel de exposición [3].

Para la Agencia de la Unión Europea para la Ciberseguridad, las organizaciones, así como los ataques que intentan comprometer las funciones administrativas y los sistemas de información en los sectores públicos han aumentado de manera dramática, así como la protección de la integridad y disponibilidad [4].

La adopción de sistemas de gestión de la seguridad de la información ha empezado a cobrar importancia en los sectores de la administración pública nacional. La Presidencia del Consejo de ministros (PCM) ha implementado la Norma Técnica Peruana ISO/IEC 270001 en las entidades públicas para lograr preservar la información estatal en términos de confidencialidad, integridad y disponibilidad. La PCM da órdenes claras a nuestras organizaciones del sector público, para fomentar la cultura de la seguridad de la información y ser una guía para su gestión en el sector público [5].

Las municipalidades de Lima abordan retos concretos para gestionar la seguridad de la información. La estudiada de Bustamante García et al. dejó manifiesto que adoptar políticas en base a ISO 27001:2013 sí que mejora la gestión de la seguridad de la información en las municipalidades peruanas. Aplicar modelos de políticas de seguridad, poniendo el acento en la confidencialidad, integridad y disponibilidad de los datos, conduce a mejora considerable en la protección de los datos [6].

Y también hace eco de lo que indica SUNAT sobre cómo la digitalización con seguridad puede contribuir a reducir la evasión, prevenir el fraude, y poder interactuar con el ciudadano en el marco digital [7].

Algunas municipalidades del Perú ya han sido conscientes de la importancia de estas normativas. Por ejemplo, la Municipalidad Distrital de Buena Vista Alta ha implementado un SGSI siguiendo la ISO 27001 para mejorar de forma notable la seguridad de la información y de la comunicación. La Municipalidad Distrital de El Agustino ha elaborado un SGSI basado en la norma ISO/IEC 27001:2013, orientando sus esfuerzos al cumplimiento de la protección de los activos de información asociados con los procesos tributarios [8].

Es en este sentido que la adopción de estándares internacionales, como la norma ISO/IEC 27001, se convierte en una imperiosa necesidad para robustecer los Sistemas de Gestión de Seguridad de la Información (SGSI) de la municipalidad limeña y que, dentro de este sentido, se considere la conveniencia de contar con controles preventivos, de controles correctivos y de controles de mejora continua garantizando, de este modo, la confidencialidad, la integridad y la disponibilidad de la información [9].

1.2. Formulación de problema

1.2.1. Problema general

¿En qué medida la ISO 27001 mejora los niveles de seguridad de la información en una municipalidad de Lima, 2026?

1.2.2. Problemas específicos

a) ¿En qué medida la ISO 27001 mejora la confidencialidad de la información en una municipalidad de Lima, 2026?

b) ¿En qué medida la ISO 27001 mejora la integridad de la información en una municipalidad de Lima, 2026?

c) ¿En qué medida la ISO 27001 mejora la disponibilidad de la información en una municipalidad de Lima, 2026?

1.3. Justificación

1.3.1. Justificación Teórica

Esta investigación se apoya en tres teorías que constituyen el soporte de las variables de estudio, éstas son (a) la teoría general de sistemas, dado que la ISO 27001 es vista como una herramienta básica para ofrecer un enfoque sistemático para encontrar, desarrollar y disminuir los peligros relacionados con seguridad de la información y promoviendo los pilares CID(confidencialidad, la integridad y la disponibilidad), entre los datos [10]; (b) la teoría de la información, que establece los procesos de codificación, transmisión y decodificación de los mensajes, tomando en consideración como elementos clave la eficiencia, la redundancia y el ruido , la ISO 27001 permite estudiar los flujos de información, y cómo pueden verse afectados por ruidos, pérdidas, accesos no autorizados, entre otros [11]; (c) la teoría del riesgo, dado que la teoría del riesgo ofrece un marco conceptual para establecer la posibilidad que sucedan los eventos adversos y el impacto que pueden producir [12]. En el ámbito de la ISO 27001, la teoría del riesgo es necesaria, dado que apoya el proceso del riesgo de la seguridad de la información y permite priorizar las amenazas, conocer las debilidades y definir los controles para mitigar el impacto.

1.3.2. Justificación Metodológica

Bajo la perspectiva metodológica, la investigación adopta un enfoque cuantitativo de carácter aplicado, y presenta un diseño experimental. Además, los métodos de recolección de datos utilizado en el trabajo es el análisis documental y la observación, lo que garantiza un control de la recolección de datos veraz y pertinente.

Igualmente, se utilizarán herramientas de análisis estadístico para determinar las mejoras en los indicadores de seguridad de la información previamente y posterior a la implementación. Se utilizarán lineamientos éticos en la recolección de la información, garantizando el consentimiento informado y la confidencialidad, lo que amplifica la validez y la fiabilidad de los resultados conseguidos. Según Ardanza [13], las dimensiones de la ISO 27001 y el modelo PDCA, o ciclo de Deming, se aplican en los siguientes términos: Planificar (plan), hacer (do), verificar (check): y actuar (act).

1.3.3. Justificación Práctica

Sin embargo, desde una perspectiva más práctica, esta investigación considera que se puede ofrecer una propuesta estructurada y aplicable para facilitar la mejora de los

niveles de seguridad de la información, en la que se identifican las brechas existentes en la seguridad de la información y se proponen medidas correctivas alineadas con la norma ISO 27001, lo que mejorará la gestión de los activos de información y reducirá los riesgos que afectan la confidencialidad, integridad y disponibilidad. Este resultado será útil para los responsables de la tecnología de la información como para los tomadores de decisiones que podrán usar los resultados del estudio como un punto de partida para replicar o adaptar el modelo propuesto a otras municipalidades o entidades públicas.

1.3.4. Justificación Social

Desde la dimensión social, la mejora de la protección de la información en las municipalidades provoca una reacción en cadena que revierte en confianza para la ciudadanía hacia su administración pública. Un sistema de seguridad de la información adecuado, además de proteger datos personales y unos eficaces de información, promueve la transparencia, la eficacia incluso la continuidad de los servicios públicos. La norma ISO 27001 está en condiciones de preverse como un elemento de disminución de la corrupción, en la prevención de fraudes o en la protección de derechos de los ciudadanos que tienen que ver con el manejo de su información personal. A partir de aquí, el proyecto contribuye, además, a la mejora de la interrelación entre la gestión pública y los ciudadanos y ciudadanas; en términos de administración pública más segura, fiable, moderna.

1.4. Objetivo general y específicos

1.4.1. Objetivo general

Determinar en qué medida la ISO 27001 mejora los niveles de seguridad de la información en una municipalidad de Lima, 2026.

1.4.2. Objetivos específicos

a) Determinar en qué medida la ISO 27001 mejora la confidencialidad de la información en una municipalidad de Lima, 2026.

b) Determinar en qué medida la ISO 27001 mejora la integridad de la información en una municipalidad de Lima, 2026.

c) Determinar en qué medida la ISO 27001 mejora la disponibilidad de la información en una municipalidad de Lima, 2026.

1.5. Hipótesis

1.5.1. Hipótesis general

- H1: La aplicación de la norma ISO 27001 permitirá mejorar los niveles de seguridad de la información en una municipalidad de Lima durante el año 2026.
- H0: La aplicación de la norma ISO 27001 no permitirá mejorar los niveles de seguridad de la información en una municipalidad de Lima durante el año 2026.

1.5.2. Hipótesis específicas

- HE1: La implementación de la norma ISO 27001 mejora de manera significativa la confidencialidad de la información en una municipalidad de Lima en el año 2026.
- H01: La implementación de la norma ISO 27001 no mejora de manera significativa la confidencialidad de la información en una municipalidad de Lima en el año 2026.

- HE2: La implementación de la norma ISO 27001 mejora de manera significativa la integridad de la información en una municipalidad de Lima en el año 2026.
- H02: La implementación de la norma ISO 27001 no mejora de manera significativa la integridad de la información en una municipalidad de Lima en el año 2026.

- HE3: La implementación de la norma ISO 27001 mejora de manera significativa la disponibilidad de la información en una municipalidad de Lima en el año 2026.
- H03: La implementación de la norma ISO 27001 no mejora de manera significativa la disponibilidad de la información en una municipalidad de Lima en el año 2026.

1.6. Marco teórico

1.6.1. Antecedentes

1.6.1.1. Internacionales

El estudio titulado Análisis de riesgos y vulnerabilidades del Departamento de TI del GAD Municipal de Ecuador (Tambo) basado en ISO/IEC 27001. El objetivo fue diagnosticar las principales brechas de seguridad y proponer acciones de mejora

alineadas con los lineamientos de ISO 27001 para fortalecer la gestión de la información. La metodología consistió en un estudio descriptivo–exploratorio, aplicando encuestas y listas de verificación según los dominios de la norma (planificación, soporte, contexto, liderazgo, operación, evaluación del desempeño y mejora continua). Los resultados mostraron debilidades significativas en el análisis de riesgos, la definición de alcance y la asignación de recursos, evidenciando que en el dominio "Contexto" apenas el 25 % de ítems se cumplían. En contraste, la evaluación del desempeño alcanzó un 75 %, lo que refleja avances en auditorías y monitoreo. Se llegó a la conclusión de que es muy importante conseguir la adopción formal de la ISO/IEC 27001 para la mejora del SGSI municipal, apoyado por la gestión de riesgos de la ISO/IEC 27005, tal y como se observó para la protección de los activos de información desde los incidentes que se repiten en el tiempo [14].

El estudio titulado la planificación de los recursos informáticos y su efecto sobre la seguridad de la información. La finalidad del estudio fue comprobar de qué manera la planificación de los recursos informáticos iba a influir en la seguridad de la información de un distrito de salud de Venezuela en referencia a estándares establecidos de gestión de riesgos como ISO 27001 y el ciclo Deming. Para la investigación se utilizó una metodología cuantitativa, aplicativa y descriptiva. Para la recogida de datos se realizó una encuesta sobre 196 trabajadores de los recursos informáticos y la revisión de las políticas de control que fueron puestas en marcha. De las conclusiones se comprobó que existían vulnerabilidades detectadas en terminales y servidores, a su vez que existían políticas de formación y que se había mejorado la eficiencia del servicio ciudadano a raíz de la adopción de medidas correctivas. El estudio concluye que la estandarización de la planificación informática, apoyada por cualquier marco de referencia, como puede ser ISO 27001, resulta importante para poder dar fe de la seguridad de la información y los servicios públicos ofrecidos. Este antecedente se considera significativo para la tesis, toda vez que se ha querido poner de manifiesto la cultura organizacional y la formación como complementos en la aplicación de la norma [15].

El modelo SGSI en base a la norma internacional ISO 27001 para organizaciones públicas. El objetivo fue diseñar un modelo SGSI aplicable a instituciones públicas bolivianas (transferible a gobiernos municipales), alineado a ISO 27001, para robustecer CID y tratamiento de riesgos. La metodología fue la investigación

aplicada-propositiva con revisión normativa nacional (IBNORCA) y de requisitos ISO 27001; elaboración de procesos, políticas y mapa de controles; validación conceptual frente a prácticas del sector público. Los resultados fueron la propuesta integral (políticas, roles, procedimientos y métricas) compatible con auditorías de certificación; hoja de ruta para implementación por etapas y mejora continua. En conclusión, el modelo ISO 27001 es factible y pertinente para entidades públicas, permite estructurar la gobernanza de seguridad y reduce la superficie de riesgo; su adopción municipal facilita cumplir requisitos de auditoría de certificación en Bolivia [16].

El estudio titulado Análisis del nivel de cumplimiento de las políticas de seguridad de la información de los GAD's de Ecuador (Cantonales Cañar, El Tambo y Suscal). El objetivo fue evaluar el grado de cumplimiento de las políticas de seguridad en gobiernos locales e Ecuador, utilizando como referencia las normas internacional ISO 27001:2013 e ISO 27002. La metodología adoptó un enfoque cuantitativo y descriptivo-explicativo, aplicando encuestas a responsables de TI y análisis de brechas en dominios de la norma. Los resultados revelaron un cumplimiento total en aspectos como políticas de seguridad y cifrado, pero deficiencias importantes en continuidad del negocio (33%), relaciones con proveedores (40%) y seguridad física (52%). Se llegó a la conclusión que, si bien las fortalezas de la gestión documental y las técnicas están presentes, los gobiernos autónomos descentralizados (GAD) se ven en la necesidad de reforzar su planificación de recursos humanos y la continuidad operativa. Esta referencia es fundamental para la tesis, puesto que evidencia cómo los gobiernos locales, al encontrar dificultades muy concretas a la hora de poner en práctica la ISO 27001, sugieren qué áreas se debe dar prioridad [17].

En el año 2022, Paraguay el Consejo de Administración de Valores y Productos (CAVAPY), decidió adherir la norma internacional ISO 27001:2022 para implementar un SGSI, con el propósito de mejorar la protección de sus prácticas de custodia de títulos valores y garantizar la seguridad de la información dentro del mercado de valores de Paraguay. La implementación, por su parte, consideró la incorporación de tecnologías en la nube, la utilización de estándares internacionales de ciberseguridad, lo que propició la gestión y mitigación de los riesgos de seguridad de la información. Al igual que en el caso de SECOM, el proceso no involucró una muestra poblacional específica, ya que abarcó toda la organización. Como resultado

de la implementación, CAVAPY obtuvo la certificación ISO 27001:2022, convirtiéndose en la quinta entidad en Latinoamérica y la primera en Paraguay en obtener dicha certificación. Esto no solo mejoró la seguridad de sus operaciones, sino que también consolidó su posición como líder en ciberseguridad dentro del mercado de valores de Paraguay. En conclusión, CAVAPY demostró que la adopción de la norma ISO 27001:2022 fortalece la confianza de los inversionistas y mejora la protección de los datos en entornos financieros [18].

En el año 2024, ISOPlanner documentó el caso de la Municipalidad de Waterland en Países Bajos, titulado "Structure and control in meeting the BIO standard in 2024". El objetivo del estudio fue implementar un SGSI bajo los lineamientos de la norma internacional ISO 27001, con el fin de cumplir con la Baseline Informatiebeveiliging Overheid (BIO) y las exigencias de la directiva NIS2. La metodología consistió en un estudio de caso aplicado a la estructura municipal, mediante el uso de la solución "ISOPlanner + Instant 27001", que se fundamenta en el ciclo PDCA, plantillas preconfiguradas y análisis de riesgos estandarizados. Entre los principales resultados se logró la puesta en marcha del ISMS en un periodo de cinco meses, con mejoras en la trazabilidad de controles, reducción del trabajo ad-hoc y establecimiento de una hoja de ruta para su ampliación a otras áreas en 2024. Se concluyó que, en gobiernos locales pequeños, un ISMS alineado a ISO 27001 acelera el cumplimiento regulatorio y profesionaliza la gestión de riesgos y controles, lo que facilita la mejora continua con costos escalables [19].

1.6.1.2. Nacionales

El estudio tiene como objetivo determinar la incidencia del SGSI basado en la norma internacional ISO 27001:2022 en la protección de la información dentro de una municipalidad distrital de Lima durante el año 2023. El estudio se desarrolla bajo un enfoque cuantitativo y presenta un diseño no experimental de tipo correlacional-causal. La muestra estuvo integrada por 132 colaboradores especializados en tecnologías de la información, seleccionados mediante un muestreo no probabilístico por conveniencia. La recopilación de datos se realizó a través de encuestas y cuestionarios previamente validados mediante juicio de expertos, obteniendo altos índices de fiabilidad (alfa de Cronbach de 0.842 para el cuestionario SGSI y 0.885 para el de protección de información). Los resultados del estudio muestran que el

SGSI según ISO 27001:2022 tiene un impacto significativo en el fortalecimiento de la protección de la información, evidenciada por una correlación de 0.611 con una significancia de 0.032. Concluye que llevar a cabo la implementación del SGSI con base en la norma ISO/IEC 27001:2022 mejora notablemente la seguridad de la información en la municipalidad distrital, lo que pone de manifiesto la importancia de contar con un sistema gestionado en relación con la seguridad de la información [20].

En el presente trabajo de investigación, la implementación de la norma internacional ISO 27001 se plantea como un conjunto de herramientas orientadas a fortalecer el sistema de gestión de seguridad de la información en una empresa de servicios de Lima durante el año 2024. Asimismo, para el desarrollo del estudio se emplea un enfoque cuantitativo con diseño preexperimental. La muestra está formada por 20 controles de un total de los 114 de los que habla la norma ISO 27001 y la recolección de los datos se efectúa mediante observación directa utilizando la técnica de la ficha de observación como instrumento. Los resultados evidencian que la aplicación de la norma ISO 27001 ha producido una reducción considerable de los incidentes vinculados a la seguridad de la información, alcanzando una mejora del 99 % en la protección de la confidencialidad, integridad y disponibilidad de los datos. Por tanto, la norma ISO 27001 mejoró significativamente el sistema de gestión de la seguridad de la información de la empresa de servicios investigada y pone de manifiesto la eficacia de la norma para proteger la información y minimizar los riesgos [21].

En el trabajo de investigación abordan la implementación de un ISMS con el enfoque ISO 27001 para poder mitigar riesgos por ciberataques para System Arq S.R.L. El diseño de investigación es experimental, utilizando un enfoque cuantitativo en un diseño pre-experimental. Ellos describen a 30 activos de información de la organización, siendo este el número de la muestra. Las conclusiones del estudio demuestran que la norma ISO 27001 es una herramienta eficaz para poder reducir los riesgos por ataques cibernéticos y poder proteger de manera eficiente la información de la organización. En este sentido, la conclusión del estudio fue que la implementación de la norma ISO 27001 como medida de control fue efectiva para reducir la efectividad de los ataques cibernéticos y fue capaz de dotar a la organización de una nueva capa de seguridad para poder mitigar los riesgos de la organización [22].

En su estudio, Trujillo tiene por objeto el determinar la mejora de la gestión de la seguridad de la información de TI (departamento de Tecnologías de la Información) de una institución pública luego de la implementación de la norma internacional ISO 27001. El estudio tiene, además un enfoque cuantitativo, transversal, correlacional y no experimental. La muestra se compuso por 50 colaboradores del área de TI de la citada institución pública. El análisis de los datos arrojó un coeficiente de correlación de 0.882 y un valor de p igual a 0.000, lo que evidencia una mejora significativa en la gestión de la seguridad de la información, incrementando en un 88.82 % la protección de los datos mediante la implementación de la norma ISO 27001. En conclusión, se puede decir que la norma ISO 27001 interviene significativamente de forma positiva en la gestión de la seguridad de la información en las instituciones públicas, mejorando la protección de datos sensibles [23].

Definir si la auditoría sustentada en la norma ISO 27001 podría llegar a mejorar los controles de seguridad de la información en la GIT(Gerencia de Informática y Tecnología) de una municipalidad peruana constituía el propósito principal de la investigación realizada por Limaymanta. Su estudio se centró en un análisis de carácter cuantitativo mediante un enfoque experimental pre-experimental. Los 18 servidores públicos de la GIT, que asumieron el papel de la población objeto de su investigación, conformaron la muestra. Y los datos estadísticos obtenidos mostraron que la auditoría comprendida dentro de la norma internacional ISO 27001 mejoró los controles de seguridad de la información, los cuales mostraron un porcentaje de control del 94.44% en el estado "Definido" del dominio A5 (política de seguridad), lo cual, en el marco de la investigación llevada a cabo, se tradujo en mejoras importantes en la seguridad física de la infraestructura tecnológica y en la cultura de ciberseguridad de la municipalidad de la que formó parte la investigación. La auditoría fue capaz de mostrar mejoras considerables en los controles de seguridad de la información, por lo que su conclusión principal fue que la auditoría, si se comprendía en el marco de la norma ISO 27001, era positiva y notable para una mejora de los controles de seguridad de la información, lo que pone de relieve la importancia de los estándares aplicados en el ámbito de las auditores de información, en este caso referidos a la seguridad de la información, sobre todo en instituciones públicas, a fin de asegurar la protección de la información o datos [24].

En una investigación el objetivo fue proponer un SGSI alineado en la norma técnica peruana NTP-ISO/IEC 27001:2014 para evaluar la seguridad de los sistemas informáticos de la Municipalidad Distrital de Huácar, así como para mitigar los riesgos que conllevan la protección de la información. La metodología de trabajo fue el análisis y gestión de riesgos de los sistemas de información utilizando la metodología española MAGERIT en su versión 3. A través de este trabajo se puede corroborar que no existían medidas adecuadas de seguridad de la información en la municipalidad, dejándola expuesta a amenazas. Para contrarrestar esto se propuso un conjunto de controles de seguridad alineados con la norma internacional ISO 27001, así como la elaboración de políticas de seguridad de la información que se ajusten a la realidad de la municipalidad. Los resultados conseguidos mostraron que la implementación de las medidas en la propuesta mejoraría la protección de los datos de la municipalidad. En conclusión, el estudio manifiesta que la propuesta de un sistema de gestión de seguridad de la información basado en la norma ISO 27001 tiene un efecto positivo en los procesos de seguridad [25].

1.7. Bases teóricas

La investigación tiene como base tres teorías que permiten comprender y unir los conceptos de la norma ISO/IEC 27001 al contexto de una organización pública como lo es una municipalidad. Las teorías que aplican son: la Teoría General de Sistemas, tal como la plantea Ludwig von Bertalanffy [10], la cual entiende a las organizaciones como sistemas formados por componentes del sistema que interaccionan el uno con el otro y que se coordinan para lograr alcanzar un objetivo. Esta forma de ver las organizaciones se relaciona con la ISO/IEC 27001, dado que la formalización de una norma de seguridad implica la coordinación de políticas, procesos, personas y tecnología, el aplicar la orientación sistémica es la que permite introducir la seguridad de la información en todos los niveles de la organización y que permite mejorar su eficiencia. De acuerdo con la Teoría de la Información formulada por Sánchez, esta teoría estudia los procesos a través de los cuales se codifica, se transmite y se decodifica la información, teniendo sobradamente en cuenta factores que pueden afectar a la eficiencia de dichos procesos, como por ejemplo el ruido, la redundancia o la capacidad del canal. La ISO 27001 sigue el enfoque de la teoría de la información para el establecimiento de controles que garanticen la confidencialidad, la integridad y la

disponibilidad de los datos y así logra proteger la información sensible recortando la posibilidad de que sean cometidos errores o de que se produzcan accesos no autorizados [26]. La Teoría del Riesgo de Knight, el riesgo es una característica susceptible de ser medida, es decir, situaciones en las que se puede calcular la probabilidad de que ocurran eventos adversos. La norma ISO 27001 se apoya en la gestión del riesgo, exigiendo que se produzca la identificación y el tratamiento de amenazas que pongan en riesgo la seguridad de la información, esta teoría permite priorizar los controles de seguridad que recortan la probabilidad o el impacto de que se produzcan incidentes que puedan poner en riesgo datos críticos de la institución o de los ciudadanos [27].

1.8. Definiciones

ISO 27001

International Organization for Standardization / International Electrotechnical Commission ISO/IEC 27001:2022 es una norma técnica de carácter internacional elaborada por ambas organizaciones, la cual establece los requisitos necesarios para crear, implementar, mantener, supervisar y optimizar un Sistema de Gestión de Seguridad de la Información (SGSI). Su finalidad consiste en apoyar a las organizaciones en la protección de la confidencialidad, integridad y disponibilidad de la información, mediante la aplicación de un proceso estructurado y sistemático de gestión de riesgos. Por otro lado, la ISO 27001 también permite ofrecer un marco de referencia que facilitará a las organizaciones poder identificar las amenazas, así como la evaluación de la vulnerabilidad [28]. La norma ISO/IEC 27001 es aplicable a cualquier organización e integra el resto de los sistemas de gestión, como la ISO 9001 (gestión de la calidad) o la ISO 14001 (gestión ambiental), lo que provocará a la organización asegurar la coherencia entre las normas, la eficiencia operativa y la alineación estratégica. Por último, la norma internacional ISO 27001 se basa en el ciclo PDCA, Planificar (plan), hacer (do), verificar (check): y actuar (act), así como en su enfoque de mejora continua, el cual le otorgará un modelo a la organización para la planificación estratégica y la ejecución operativa.

En contexto de organizaciones municipales, la ISO/IEC 27001 es adecuado, ya que permite proteger información sensible relacionada con servicios públicos, datos personales de los ciudadanos, registros tributarios y expedientes administrativos. La

ISO 27001 permite la identificación de amenazas, el análisis de vulnerabilidades y la definición de controles adecuados para minimizar riesgos frente a incidentes de seguridad, ciberataques o accesos no autorizados [29].

Evolución de la norma ISO 27001

La ISO 27001 se ha modificado desde su inicio como estándar británico hasta su consolidación como norma internacional:

BS 7799-1:1995: Divulgada como código de buenas prácticas en seguridad de la información en Reino Unido.
BS 7799-2:1999: Se agregan condiciones para implementar un SGSI certificable.
BS 7799-2:2002: Incorpora el modelo PDCA (Plan-Do-Check-Act) y la mejora continua.
ISO/IEC 27001:2005: Versión internacional adoptada por varios países.
ISO/IEC 27001:2013: Reducción de redundancias, alineación con otros sistemas de gestión [30].
ISO/IEC 27001:2022: Enfocada en riesgos modernos, ciberseguridad y privacidad. Reduce los controles de 114 a 93 y los agrupa en cuatro categorías: organizacionales, personales, físicos y tecnológicos [31].

Características principales de la ISO/IEC 27001

La norma internacional ISO 27001 se caracteriza principalmente por ofrecer una serie de características que la hacen, a la vez, un esquema fuerte y flexible para poder hacer la gestión de la seguridad de la información. En un primer momento, tenemos que hablar del enfoque basado en riesgos, ya que este implica que se tiene que identificar, evaluar y gestionar las amenazas que se pueden producir y que pueden poner en peligro los pilares de seguridad de la información CID: C (confidencialidad), I (integridad) y D (disponibilidad).

Asimismo, es importante considerar que la norma se encuentra desarrollada bajo una estructura de alto nivel (HLS, por sus siglas en inglés), lo cual facilita su integración con otros estándares de gestión, como ISO 9001 en calidad y ISO 14001 en medioambiente, permitiendo así su adaptación a diversos sistemas de gestión organizacional.

Uno de los otros aspectos clave es la mejora continua, ya que ayuda al mantenimiento periódico y a la revisión de las políticas, procedimientos y controles garantizando la eficacia de esta a situaciones cambiantes.

Por último, también sería un esquema que presenta controles estructurados y definidos, descritos si se hace referencia al Anexo A de la norma ISO/IEC 27001 un total de 93 medidas distribuidas en cuatro bloques: organizativas, relacionadas con las personas, físicas y técnicas [9].

Controles clave e indicadores de la norma

Según [30]–[32], los controles más relevantes de la ISO27001:2022 son 15 controles señalados en la tabla 1.

Tabla 1. Quince (15) controles relevantes de la norma.

Nombre del control (ISO/IEC 27001:2022)	Pilar
1. Control de acceso 2. Restricción de acceso a la información 3. Políticas de seguridad de la información 4. Seguridad de la información para el uso de servicios en la nube 5. Eliminación de información	Confidencialidad
6. Inventario de información y otros activos asociados 7. Protección contra malware 8. Planificación y preparación de la gestión de incidentes de seguridad de la información 9. Concientización, educación y capacitación en seguridad de la información 10. Gestión de configuración	Integridad
11. Copia de seguridad de la información 12. Mantenimiento de equipo 13. Seguridad en redes 14. Redundancia de las instalaciones del procesamiento de información 15. Roles y responsabilidades de seguridad de la información	Disponibilidad

- **C01. Control de acceso**

Estas políticas funcionan como un reglamento interno que define quién puede ver, modificar o administrar determinada información. Son necesarias para evitar que cualquier persona acceda a datos sensibles sin autorización. Por ejemplo, un médico

debe tener acceso a la historia clínica de un paciente, pero no un administrativo que no participa en su tratamiento. Las políticas de acceso también contemplan la creación, modificación y eliminación de permisos cuando una persona cambia de puesto, ingresa o deja la organización. En la práctica, actúan como las "llaves digitales" que garantizan que cada usuario tenga solo lo que necesita para cumplir su trabajo, ni más ni menos [9].

- **C02. Control de restricción de acceso a la información**

Este punto convierte en realidad las políticas anteriores mediante herramientas técnicas de seguridad. Incluye contraseñas seguras, autenticación multifactor (por ejemplo, ingresar un código enviado al celular), tarjetas de acceso, y la configuración de perfiles de usuario en los sistemas. El objetivo es que solo las personas autorizadas puedan entrar a los sistemas y a los archivos. Además, se suelen aplicar límites de tiempo en las sesiones para evitar que una computadora abierta quede expuesta. De esta manera, se crea una especie de "muralla digital" que mantiene protegidos los datos sensibles frente a curiosos o ciberdelincuentes [9].

- **C03. Control políticas de seguridad de la información**

Estas políticas son como la constitución de una organización en temas de seguridad. Establecen normas que todos los empleados deben cumplir, desde la alta gerencia hasta el personal operativo. Incluyen directrices sobre el uso de contraseñas, la protección de dispositivos, el manejo de correos electrónicos, el acceso a internet y la confidencialidad de la información. También deben actualizarse periódicamente, porque las amenazas evolucionan y lo que era seguro hace cinco años hoy puede no serlo. Una política clara genera confianza, orden y responsabilidad compartida [9].

- **C04. Control seguridad de la información para el uso de servicios en la nube**

La seguridad de la información y la gestión de los servicios en la nube implican garantizar que los datos procesados y almacenados en servidores externos cuenten con una protección igual o incluso superior a la de la infraestructura local. Los servicios en nube exponen a la organización a afrontar riesgos adicionales debido a la pérdida de control directo sobre la información, por lo que resulta necesario aplicar controles de cifrado, autenticación robusta, monitoreo de accesos, cumplimiento normativo y

acuerdos de nivel de servicio. Entre los indicadores aplicables se encuentra el porcentaje de datos cifrados en reposo y en tránsito, el cumplimiento de SLA de disponibilidad y la existencia de certificaciones de seguridad en el proveedor [35].

- **C05. Control de eliminación de información**

La depuración de la información es un proceso de seguridad destinado a asegurar que los datos que han dejado de ser útiles sean eliminados de forma definitiva, impidiendo su restauración parcial o total y accedidos nuevamente, lo cual disminuye la posibilidad de filtraciones o manipulaciones posteriores. Según Anderson, los métodos tradicionales de la depuración como simplemente eliminar archivos o formatear un dispositivo no garantiza una protección real, ya que los registros pueden ser recuperados con procedimientos forenses. Por consecuencia, es indispensable aplicar técnicas de eliminación seguras, tales como la sobreescritura repetida del contenido, la desmagnetización del disco o la destrucción física de los platos. Para verificar la eficacia de este control, se puede utilizar indicadores como la proporción de equipos retirados que cuentan con constancias de destrucción o sanitización y el grado de cumplimiento de las normas internas sobre tiempo de conservación de la información [36].

- **C06. Control de inventario de información y otros activos asociados**

El inventario de activos es el punto de partida para toda la estrategia de seguridad. No se puede proteger aquello que no se conoce. Por eso, es necesario listar y clasificar todos los elementos que almacenan, procesan o transmiten información: servidores, computadoras, impresoras, bases de datos, aplicaciones en la nube, e incluso dispositivos móviles de los empleados. Este inventario debe actualizarse constantemente, porque los activos cambian con el tiempo: algunos se reemplazan, otros quedan obsoletos y otros se incorporan nuevos. Clasificarlos según su importancia y nivel de criticidad permite enfocar los esfuerzos de protección donde más se necesita: por ejemplo, un archivo con información de clientes o historiales médicos tendrá una prioridad de seguridad mucho mayor que un manual de uso general [9].

- **C07. Controles de protección contra malware**

El malware y otros códigos maliciosos son como enfermedades digitales que pueden dañar la información o bloquearla (ransomware). Para protegerse, las organizaciones deben contar con antivirus actualizados, firewalls, filtros de correo que detecten correos sospechosos y sistemas de monitoreo en tiempo real. Estos controles actúan como un escudo invisible que intercepta virus, spyware o intentos de intrusión antes de que lleguen al usuario. Además, educar al personal para identificar correos fraudulentos y no descargar archivos sospechosos complementa esta protección [9].

- **C08. Control planificación y preparación de la gestión de incidentes de seguridad de la información**

Aún con todas las medidas preventivas, ningún sistema es infalible. Por eso, las organizaciones necesitan un plan de gestión de incidentes. Este plan permite detectar ataques, reportarlos a tiempo, responder de manera rápida y aprender de lo ocurrido. Un incidente puede ser desde un intento de acceso no autorizado hasta el robo de información sensible. Lo realmente importante es actuar sin demora: acotar la cuestión, minimizar los daños, comunicar a los responsables y adoptar medidas para evitar repeticiones. Esta gestión es la forma de convertir una crisis en una oportunidad de mejora [9].

- **C09. Control concientización, educación y capacitación en seguridad de la información**

En cualquier empresa u organización es indispensable elaborar e implementar planes o programas de concienciación y capacitación en seguridad de la información para todos los trabajadores o personal. Los planes o programas buscan formar una cultura organizacional para protección de la información, la comprensión de los riesgos a los que se enfrentan día a día en sus labores y como adoptar medidas preventivas que deben adoptar. La concienciación es un paso inicial que debe respetarse, en los temas pueden incluirse los procedimientos, políticas sobre la información, métodos de ingeniería social, fraude digital como el phishing, cuidado y creación de contraseñas; entre otros temas. Es importante recalcar que los planes o programas deben aplicarse periódicamente y de manera continua, además se deben actualizar ya que las amenazas digitales suelen cambiar los métodos de engaño, la actualización permitirá que los

empleados se mantengan preparados, identifiquen, mitiguen la amenazas y minimicen las consecuencias [9].

- **C10. Control de gestión de configuración**

Es importantes que todas las configuraciones de los sistemas de información y equipos tanto hardware, software deben ser definidas, documentadas, implementadas, monitoreadas y revisadas de manera periódica. Los sistemas deben operar con estándares seguros y estables, para evitar configuraciones incorrectas que ocasiones errores o vulnerabilidades. Además, la gestión de la configuración usa y aplica estándares de configuración aprobados, revisiones mediante auditorías uso herramientas como software de gestión para detectar cambios no autorizados. También, una configuración adecuada reduce riesgos de ataques y asiente la continuidad operativa. Por último, la revisión constante y la automatización de procesos son prácticas ampliamente recomendadas para cumplir satisfactoriamente este control y garantizar una correcta gestión de configuración [9].

- **C11. Control copia de seguridad de la información**

La pérdida de información crítica puede generar daños irreparables: pérdida de confianza, sanciones legales o incluso la quiebra de una organización. Por ello, el respaldo (backup) es una red de seguridad digital. Consiste en hacer copias periódicas de los archivos más importantes y guardarlas en lugares distintos, como servidores externos o la nube. Así, si ocurre un error humano, una falla técnica o un ataque informático, la información puede recuperarse sin interrumpir gravemente las operaciones. Es recomendable aplicar la regla “3-2-1”: tres copias de los datos, en dos medios diferentes, y al menos una en un lugar externo [9].

- **C12. Control mantenimiento de equipo**

Los sistemas de información son como un vehículo: si no reciben mantenimiento, tarde o temprano fallan. En este punto se incluyen las actualizaciones de software, el reemplazo de piezas desgastadas, la instalación de parches de seguridad y la revisión preventiva de servidores, computadoras y redes. El objetivo es prevenir fallos, reducir vulnerabilidades y evitar interrupciones de servicio. Un sistema actualizado no solo es

más eficiente, sino también más seguro, porque los ciberdelincuentes suelen atacar equipos que no han recibido parches recientes [9].

- **C13. Control de seguridad en redes**

No siempre se encuentra la información archivada: muchas veces va viajando por redes y sistemas. Es aquí donde entra la seguridad en las comunicaciones, ya que asegura que la información que se transmita sea confidencial, íntegra y segura. Nuestro trabajo hace uso de tecnologías como el cifrado de los datos, de las redes privadas virtuales (VPN) o protocolos como HTTPS o TLS que evitan que terceras personas puedan interceptar los mensajes. Éste es un aspecto clave en el momento de intercambiar información delicada como pueden ser contraseñas, datos económicos o información sanitaria. Es de este modo como podemos garantizar el hecho de que sólo el destinatario reciba la totalidad del mensaje sin ninguna modificación, sea por el hecho de que se ha cifrado o por el hecho de que hay sido transportado por una VPN [9].

- **C14. Control de redundancia de las instalaciones del procesamiento de información**

Es un control que dispone la continuidad operativa mediante la duplicación de sistemas, redes o componentes críticos que permitan mantener el servicio accesible ante fallos inesperados. Stallings explica que la redundancia es uno de los mecanismos más efectivos para garantizar la disponibilidad, ya que permite la conmutación automática hacia recursos alternos cuando un elemento falla, evitando interrupciones. Entre los indicadores que pueden utilizarse para evaluar este control se encuentran el porcentaje de sistemas críticos con redundancia activa, la cantidad de pruebas exitosas de conmutación y el tiempo promedio de recuperación ante fallos [37].

- **C15. Control de roles y responsabilidades de seguridad de la información**

La Ciencia de la Seguridad no es única y exclusiva del área técnica; la Seguridad es una cuestión de toda la organización. En este sentido, queremos establecer muy claramente qué rol y qué función tiene cada uno de los elementos que han de confluir en la Seguridad de la información: quién define las políticas, quién supervisa el cumplimiento, quién atiende los incidentes, cómo se coordina cada acción. De forma que se establece una estructura donde cada uno tiene claro qué ha de hacer y cuál es su

responsabilidad. Al mismo tiempo, se promueve una cultura organizativa donde la Seguridad no es un lastre sino un compromiso con la Seguridad de la información y la continuidad de la organización en la máxima extensión posible [9].

La información

Es entendida como un grupo de datos de carácter organizado, procesados y contextualizados para adquirir un significado y un valor específico para aquéllos que la reciben. De este modo, la principal diferencia con respecto a los datos es que estos se limitan a registrar de forma simple sin interpretación alguna, mientras que la información sí que tiene un contenido con carácter práctico y utilizable. La información puede ser considerada como un mensaje que incluye un emisor, un receptor y un significado compartido [38], en la misma línea el planteamiento define la información como el resultado del procesado de los datos y que, por tanto, se convertiría en un insumo para la toma de decisiones que se lleva a cabo dentro de los diferentes ámbitos en los que se utiliza [39].

En la actualidad, el valor estratégico de la información se ha incrementado en tanto que la interconectividad mundial va en aumento y la dependencia de los sistemas digitales se materializa. Según Knowledge-Information-Data Tools los datos llegarían a adquirir la categoría de información sólo si son clasificados, organizados y contextualizados para adquirir relevancia, de ahí que proteger la información sea una prioridad en las organizaciones modernas [40].

Seguridad de la información

La seguridad de la información abarca prácticas, políticas y controles que persiguen proteger los activos informativos frente a accesos no autorizados, cambios, pérdidas o destrucción. Este concepto tiene importancia en un ecosistema hipercorrespondido en el que la información fluye de forma continua a través de los diferentes dispositivos y redes. La seguridad de la información se define por las prácticas, políticas y controles que buscan proteger los activos informativos contra accesos no autorizados, cambios, pérdidas o destrucción [41]. El propósito de la seguridad de la información es garantizar la confidencialidad, integridad y disponibilidad de la información, y evitar que pierda su valor estratégico o se use de forma abusiva [41].

La seguridad de la información también hay que incluir tanto aspectos técnicos como factores humanos, organizativos y normativos. La gobernanza de la seguridad de la información en el sector público se entiende como marcos de responsabilidad, gestión del riesgo y alineamiento estratégico con los objetivos de la institución, por lo que no se puede entender solamente como una cuestión técnica [42]. Asimismo, se indica que esta disciplina requiere de herramientas tecnológicas y, al mismo tiempo, del establecimiento de políticas y de una cultura organizativa orientada hacia la protección de los datos [43].

Pilares de la seguridad de la información

Los tres pilares que respaldan la seguridad de la información son:

Confidencialidad

La confidencialidad es el principio que permite el acceso a la información exclusivamente a las personas autorizadas. Su objetivo es impedir la apertura, uso y/o revelación no autorizada de datos con carácter sensible como información de carácter personal, financiero o institucional. Este pilar es crucial para la protección de la privacidad de los ciudadanos y de la acción administrativa de las entidades públicas, por ejemplo, de las municipalidades. La confidencialidad forma parte de la tríada básica de la seguridad de la información y puede garantizarse a través de controles como el cifrado, la autenticación y la gestión de accesos [44].

Integridad

El principio de la integridad permite que la información se mantenga exacta, completa y libre de modificaciones no autorizadas. Este principio es uno de los más importantes porque impide que la información pueda ser usada para toma de decisiones o en la prestación de servicios públicos y sea alterada, bien de forma accidental, bien de forma deliberada. La integridad es uno de los principios más importantes para que se mantenga la confianza en los sistemas de información y su protección requiere la existencia de políticas, procedimientos y controles que aseguren que la información que se manipula es veraz y que se permite su trazabilidad [45].

Disponibilidad

La información debe ser accesible y utilizable para los usuarios que estén autorizados a acceder a ella en el momento en que la necesiten. Este principio es crucial en el funcionamiento de una municipalidad. En caso de fallos técnicos, desastres naturales o ataques cibernéticos, la disponibilidad garantiza la continuidad de la prestación de los servicios públicos. Rocha considera que la disponibilidad garantiza el acceso al recurso de información en el momento necesario y con confianza, razón por la cual es fundamental para alcanzar la continuidad operativa de las organizaciones [46].

II. METODOLOGÍA

2.1. Enfoque de investigación

El enfoque cuantitativo permitió reunir y extraer datos numéricos que pudieron ser evaluados a través de procedimientos estadísticos, lo que permitió llegar a la consideración base de inferencias generales sobre el impacto que tienen los controles de la norma internacional ISO 27001 en la seguridad de la información; así mismo, en el trabajo se esperó que los resultados fueran generalizables, de forma que sirvieran para extraer inmediateces sobre la eficacia de la implementación de la norma en otras organizaciones públicas [47].

El método de investigación fue cuantitativo, ya que la investigación puso énfasis únicamente en la recopilación y análisis de datos numéricos para la evaluación de la ISO 27001, de manera que sirvió para mejorar la seguridad de la información en determinada Municipalidad de Lima.

2.2. Tipo de estudio

La investigación aplicada fue de vital importancia cuando se buscó llegar a la solución de problemas precisos y prácticos, como fue el caso de la mejora de la protección de los datos a través de la implantación de marcos normativos internacionales [48]. Los resultados mostrados sirvieron de base para implantar sistemáticamente en otras entidades públicas y privadas sistemas similares. La investigación fue aplicada, ya que su objetivo principal consistió en la generación de conocimientos prácticos que contribuyeron a la mejora de la seguridad de la información en la Municipalidad de Lima mediante la norma internacional ISO 27001.

2.3. Diseño de investigación

El diseño de investigación fue experimental, ya que resultó adecuado para observar, analizar y describir los fenómenos tal y como ocurrieron en su ámbito sin intervenir en ellos [49]. Mediante este enfoque se pudo obtener una base de datos con los registros de las acciones resultantes de los controles de la seguridad de la información y el impacto de la norma internacional ISO 27001. Como instrumento se utilizaron fichas de observación estandarizadas que fueron validadas en investigaciones previas para medir los niveles de seguridad de la información, lo que aseguró la fiabilidad y validez de los datos. En el diseño de la investigación no se operaron las variables involucradas, sino que se contemplaron tal como se presentaron en los registros en el contexto de la municipalidad objeto de estudio.

2.4. Población y criterios de selección

La población en una investigación se definió como el conjunto de casos que cumplieron con criterios específicos relevantes para el estudio, y cuya correcta delimitación permitió garantizar la validez de los resultados obtenidos [50]. Como criterio de inclusión, se consideraron los 93 controles de la norma ISO 27001 seleccionados para la guía de observación; mientras que, como criterio de exclusión, no se consideraron otros elementos ajenos al estudio. Asimismo, se consideraron únicamente los datos registrados en el periodo comprendido entre el 1 de enero de 2026 al 3 de marzo de 2026.

2.5. Muestra y muestreo

Muestra

De acuerdo con [52], el muestreo no probabilístico resultó apropiado cuando se requirió acceder de manera ágil a un grupo representativo de la población, evitando los procedimientos más complejos propios del muestreo aleatorio. En este estudio, la muestra estuvo conformada por 15 controles clave e indicadores de la norma descritos posteriormente en la Tabla 1, los cuales permitieron efectuar un análisis estadístico suficiente y pertinente para los fines de la investigación. La selección de la muestra se realizó mediante un muestreo no probabilístico por juicio, debido a que se consideraron los controles más importantes según la clasificación de tres autores [30]–

[32]; por ello, se tomaron en cuenta aquellos controles seleccionados con base en el juicio de expertos y que fueron evaluados durante el proceso de recolección de datos. Asimismo, se consideraron únicamente los registros correspondientes al periodo comprendido entre el 1 de enero de 2026 al 3 de marzo de 2026.

Muestreo

La elección del tipo de muestreo respondió al objeto de estudio y a los objetivos planteados, de modo que facilitó una selección estratégica de unidades que optimizó los recursos disponibles y fortaleció la validez de los hallazgos [53]. En este caso, se optó por un muestreo no probabilístico por juicio, dado que la investigación enfrentó restricciones de tiempo y recursos, además de las particularidades propias del contexto institucional de la Municipalidad de Lima.

La elección de este tipo de muestreo se justificó en que permitió trabajar con los controles disponibles en momentos específicos, garantizando así la factibilidad del estudio. Se realizó el seguimiento durante el mes de enero considerando los 15 controles establecidos, mientras que en el mes de febrero el mismo proceso fue ejecutado sin la totalidad de dichos controles. Lo anterior demostró que, en ciertas ocasiones, no se dispuso de todos los elementos muestrales en condiciones homogéneas, lo que no permitió la aplicación de un muestreo aleatorio estricto; por ello, resultó más conveniente seleccionar aquellos controles que se encontraron disponibles y vigentes durante el periodo de recolección de datos. Asimismo, se consideraron 30 días para el pretest y 30 días para el postest, lo que permitió contar con un análisis adecuado y una interpretación pertinente de la operatividad de la entidad, de tal manera que una muestra austera resultó suficiente para cumplir con el objetivo de la investigación. Se recomendaron 30 días con la finalidad de evitar factores que alteraran los resultados, debido a que, si el estudio se extendía demasiado, como 60 o 90 días, podían ocurrir más cambios en la municipalidad, tales como actualizaciones de sistemas o modificaciones en las tareas internas, que influyeran en los controles evaluados y distorsionaran los resultados del pre-test y pos-test.

2.6. Variables

En la presente investigación se definen dos variables:

Independiente: ISO 27001

Definición conceptual

La norma internacional International Organization for Standardization ISO 27001 se consolidó como el principal estándar para la gestión de la seguridad de la información, siendo desarrollada junto con la International Electrotechnical Commission. Esta norma definió los requisitos necesarios para implementar, mantener y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información (SGSI). Su objetivo fundamental consistió en garantizar la confidencialidad, la integridad y la disponibilidad de los datos, para lo cual planteó un enfoque basado en la gestión de riesgos y en la mejora continua mediante el ciclo Planificar-Hacer-Verificar-Actuar (PHVA/PDCA) [9].

Definición operacional

La norma internacional ISO 27001 permitió a las entidades identificar riesgos, evaluar su impacto y aplicar controles estratégicos para mitigar o prevenir las amenazas sobre los activos de información. En el caso de la municipalidad, su operacionalización se expresó mediante los controles de ISO/IEC 27001:2022, agrupados según los tres pilares de la seguridad de la información, los cuales actuaron directamente sobre la variable dependiente.

Dimensiones e indicadores:

D1. Planificar

Porcentaje de planes aprobados

D2. Hacer

Porcentajes de planes ejecutados

D3. Verificar

Porcentaje de planes revisados

D4. Actuar

Porcentaje de controles difundidos

Variable dependiente: Seguridad de la información

Definición conceptual: Se definió como el grupo de técnicas, políticas y medidas dedicadas a resguardar los datos sensibles procesados en una organización, de manera

que no fueran objeto de accesos no autorizados, alteraciones, pérdidas o destrucción. Su finalidad consistió en mantener la confidencialidad, integridad y disponibilidad de la información en todo momento [54].

Definición operacional: En este estudio, la seguridad de la información se medió a través de sus tres dimensiones principales: **confidencialidad, integridad y disponibilidad**, evaluadas mediante indicadores específicos que permitieron valorar la seguridad de la información en la municipalidad.

Dimensiones e indicadores:

D1. Confidencialidad de la información

- Nivel de confidencialidad de la información

D2. Integridad de los datos

- Nivel de integridad de datos

D3. Disponibilidad de la información

- Nivel de disponibilidad de la información

2.7. Procedimientos y técnicas

La validación mediante juicio de expertos constituyó un procedimiento que permitió establecer en qué medida el instrumento representó el contenido del concepto que se pretendía medir, a través de la evaluación de especialistas en la materia. Con el fin de sustentar la validez del instrumento, se realizó un proceso de validación de contenido. Este proceso consistió en la revisión de tres expertos, quienes evaluaron si se cubrieron adecuadamente los controles clave de la norma ISO 27001 [55]. Las etapas fueron las siguientes:

1. Recolección de datos: se consiguieron datos de los tiempos de entrega, costos y distancias antes de la implementación del sistema predictivo.

2. Aplicación del sistema de predicción logística: se implementó el modelo predictivo que permitió estimar los tiempos de entrega, los costos y las rutas óptimas.

3. Recolección posterior: después de la implementación, se recopilaron datos de los tiempos de entrega, los costos y distancias.

4. Comparación y análisis: se comparó el antes y después de la implementación del sistema.

5. Interpretación: se analizaron los resultados en función de las escalas valorativas y las hipótesis planteadas.

Técnica

La técnica fue un procedimiento sistemático utilizado para recopilar y analizar información con el fin de resolver un problema o responder a una pregunta de investigación [56]. La técnica principal utilizada para la recolección de datos fue la observación, la cual se complementó con una ficha de observación tipo test–re-test, que permitió efectuar un análisis en distintos momentos. Esta técnica facilitó obtener información precisa sobre el instrumento aplicado para la ISO 27001 en la Municipalidad de Lima. De esta manera, fue posible obtener evidencia cuantitativa que pudo analizarse estadísticamente y ofreció una visión objetiva de la ISO 27001 en la entidad estudiada.

Instrumentos

Un instrumento fue el medio material utilizado para recoger información sobre las variables que se estudiaron [57]. El instrumento principal fue una ficha de observación, diseñada bajo los criterios de la norma ISO 27001 y organizada en dos secciones principales:

Sección 1 – Test: Evaluó el instrumento, verificando su eficacia en un rango de días.

Sección 2 – Re-test: Se evaluó el mismo instrumento, validando su eficacia en un rango diferente de días.

Validación

Fue un proceso que garantizó la validez y consistencia metodológica del instrumento de medición aplicado. Por ello, se requirió que el investigador definiera el constructor y tuviera claridad en la operacionalización de las variables antes de realizar este proceso [58]. Asimismo, los instrumentos de investigación fueron sometidos a una estrategia ampliamente aplicada denominada juicio de expertos, con la finalidad de calcular la confiabilidad y validez de su contenido [59].

Asimismo, para la validación del instrumento participaron profesionales capacitadas en la temática tratada en el presente estudio, quienes se detallan en la Tabla 2. De igual forma, el contenido se sustentó en libros, tesis y artículos científicos vinculados con la investigación. Además, el formato de validación de los instrumentos mediante juicio de expertos se incluye en el Anexo 3.

Tabla 2. Expertos que validaron el instrumento.

N	Nombres y Apellidos	Grado
1	Quiroz Guevara Jorge Luis	Magister
2	Córdova Forero Julio Alfredo	Magister
3	Daves Girao Silva	Magister

Confiabilidad

Para examinar la confiabilidad del instrumento utilizado, se aplicó el coeficiente de Spearman con el propósito de determinar la consistencia interna de los 15 ítems que conformaron los indicadores medibles del estudio. El análisis se realizó sobre una base de 15 controles, los cuales correspondieron a 10 días de registro: 5 asociados al Test y 5 al Re-test. Según la tabla de confiabilidad del instrumento, se obtuvo un resultado para la dimensión de confidencialidad con un rho = 0,791, lo que demostró una correlación positiva alta; para la dimensión de integridad, un rho = 0,761, que también demostró una correlación positiva alta; y para la dimensión de disponibilidad, un rho = 1,000, que evidenció una correlación positiva muy alta. Estos resultados demostraron que el instrumento fue confiable.

Tabla 3. Fiabilidad del instrumento de confidencialidad**.**

Confidencialidad

			NCI_TEST	NCI_RETEST
Rho de Spearman	NCI_TEST	Coeficiente de correlación	1,000	,791
		Sig. (bilateral)	.	,111
		N	5	5
	NCI_RETEST	Coeficiente de correlación	,791	1,000
		Sig. (bilateral)	,111	.
		N	5	5

Interpretación

En la Tabla 3 se observó que el coeficiente de correlación entre NCI_TEST y NCI_RETEST fue rho = 0,791, lo que evidenció una correlación positiva alta entre ambas variables evaluadas. Esto indicó que el instrumento presentó un nivel adecuado de confiabilidad.

Tabla 4. Test de confidencialidad.

		CONFIDENCIALIDAD							
FECHA	DÍAS	R1	R2	R3	R4	R5	PCI	CCI	NCI
27/01/2026	D1	1	1	0	1	1	4	5	0.80
28/01/2026	D2	0	1	1	1	1	4	5	0.80
29/01/2026	D3	0	0	0	1	1	2	5	0.40
30/01/2026	D4	1	1	1	0	1	4	5	0.80
31/01/2026	D5	1	0	1	0	1	3	5	0.60

Tabla 5. Re-test de confidencialidad.

		CONFIDENCIALIDAD							
FECHA	DÍAS	R1	R2	R3	R4	R5	PCI	CCI	NCI
3/02/2026	D1	0	1	1	0	1	3	5	0.60
4/02/2026	D2	0	1	1	0	1	3	5	0.60
5/02/2026	D3	0	0	0	1	0	1	5	0.20
6/02/2026	D4	0	1	1	1	0	3	5	0.60
7/02/2026	D5	1	0	0	1	1	3	5	0.60

Tabla 6. Fiabilidad del instrumento de integridad**.**

Integridad

			NID_TEST	NID_RETEST
Rho de Spearman	NID_TEST	Coeficiente de correlación	1,000	,761
		Sig. (bilateral)	.	,135
		N	5	5
	NID_RETEST	Coeficiente de correlación	,761	1,000
		Sig. (bilateral)	,135	.
		N	5	5

Interpretación

En la Tabla 6 se apreció que el índice de correlación entre el NID_TEST y NID_RETEST fue rho = 0,761, lo cual demostró una correlación positiva alta entre las dos variables evaluadas. Esto significó que el instrumento fue confiable.

Tabla 7. Test de integridad**.**

		INTEGRIDAD							
FECHA	DÍAS	R6	R7	R8	R9	R10	PID	CID	NID
27/01/2026	D1	1	1	0	0	1	3	5	0.6
28/01/2026	D2	0	0	1	1	0	2	5	0.4
29/01/2026	D3	1	1	0	1	1	4	5	0.8
30/01/2026	D4	1	0	1	1	1	4	5	0.8
31/01/2026	D5	1	1	0	0	1	3	5	0.6

Tabla 8. Re-test de integridad**.**

		INTEGRIDAD							
FECHA	DÍAS	R6	R7	R8	R9	R10	PID	CID	NID
3/02/2026	D1	1	0	0	0	1	2	5	0.4
4/02/2026	D2	0	1	1	0	0	2	5	0.4
5/02/2026	D3	0	0	1	1	1	3	5	0.6
6/02/2026	D4	1	0	1	0	1	3	5	0.6
7/02/2026	D5	0	1	1	1	0	3	5	0.6

Tabla 9. Fiabilidad del instrumento de disponibilidad.

Disponibilidad

			NDI_TEST	NDI_RETEST
Rho de Spearman	NDI_TEST	Coeficiente de correlación	1,000	1,000**
		Sig. (bilateral)	.	.
		N	5	5
	NDI_RETEST	Coeficiente de correlación	1,000**	1,000
		Sig. (bilateral)	.	.
		N	5	5

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

Interpretación

En la Tabla 9 se apreció que el índice de correlación entre el NDI_TEST y NDI_RETEST fue rho = 1,000, lo cual demostró una correlación positiva muy alta entre las dos variables evaluadas. Esto significó que el instrumento fue confiable.

Tabla 10. Test de disponibilidad**.**

		DISPONIBILIDAD							
FECHA	DÍAS	R11	R12	R13	R14	R15	PDI	CDI	NDI
27/01/2026	D1	0	0	1	1	1	3	5	0.6
28/01/2026	D2	1	1	1	0	0	3	5	0.6
29/01/2026	D3	1	0	1	1	1	4	5	0.8
30/01/2026	D4	1	1	0	1	0	3	5	0.6
31/01/2026	D5	0	1	1	0	1	3	5	0.6

Tabla 11. Re-test de disponibilidad.

		DISPONIBILIDAD							
FECHA	DÍAS	R11	R12	R13	R14	R15	PDI	CDI	NDI
3/02/2026	D1	1	0	0	0	1	2	5	0.4
4/02/2026	D2	0	1	0	1	0	2	5	0.4
5/02/2026	D3	0	1	1	0	1	3	5	0.6
6/02/2026	D4	0	0	1	1	0	2	5	0.4
7/02/2026	D5	0	1	0	0	1	2	5	0.4

2.8. Plan de análisis:

El procesamiento de los datos se desarrolló mediante software estadístico como SPSS o R, los cuales permitieron estructurar y analizar las respuestas obtenidas a partir de las fichas de observación. El software estadístico IBM SPSS Statistics fue esencial para realizar análisis de datos de negocios e investigación. Este software ofreció

técnicas estadísticas avanzadas, como pruebas de hipótesis y visualización de datos. Además, su interfaz resultó intuitiva, lo que facilitó su uso en diferentes disciplinas [60]. El plan de procesamiento de datos incluyó la siguiente fase:

• Codificación y organización: Se procedió a la codificación y organización de los datos por controles y dimensiones (confidencialidad, integridad y disponibilidad) con la finalidad de realizar un análisis estructural de la información. El análisis de los datos se desarrolló mediante estadísticas descriptivas e inferenciales.
• Estadísticas descriptivas: Se efectuaron frecuencias, medias y desviaciones estándar para describir las características de las variables. Esto incluyó el cálculo de la media de las respuestas obtenidas para cada control, permitiendo así la identificación de tendencias generales en las prácticas de seguridad existentes en la municipalidad.
• Pruebas de hipótesis: Se realizaron pruebas de hipótesis para determinar si la mejora en la implementación de los controles de la ISO 27001 afectó significativamente la protección de los datos. Asimismo, se llevaron a cabo pruebas t de Student o análisis de varianza (ANOVA), según correspondió.
• Interpretación de los datos: Se evaluó el coeficiente de correlación de Spearman, donde un p-valor entre 0,80 y 1 indicó una correlación positiva perfecta; un p-valor entre 0,60 y 0,80 indicó una correlación alta; un p-valor entre 0,40 y 0,60 indicó una correlación regular; un p-valor entre 0,20 y 0,40 indicó una correlación baja; un p-valor entre 0,00 y 0,20 indicó una correlación pequeña; y un p-valor igual a 0 indicó una correlación nula.

2.9. Aspectos éticos y de integridad científica

A continuación, se describieron las disposiciones implementadas con el objetivo de garantizar que la investigación se ejecutara en plena conformidad con los principios éticos y de integridad científica, manteniendo el respeto hacia los participantes y la autenticidad de los resultados:

a) Ética
• La investigación fue revisada y aprobada por el Comité Institucional de Ética e Integridad Científica antes del inicio del estudio.

• La investigación cumplió con las normas éticas nacionales e internacionales aplicables.

b) Consentimiento informado

• A todos los participantes se les proporcionó información clara sobre los objetivos, procedimientos, riesgos y beneficios del estudio.

c) Confidencialidad

• Se garantizó el almacenamiento seguro y la privacidad de la información.

d) Selección de participantes

• La inclusión de los participantes se cauteló de manera justa, adoptándose la decisión de no discriminar ni explotar a los participantes.

e) Integridad científica

• La recolección y el análisis de la información se realizaron de forma rigurosa, lo que permitió garantizar que los resultados obtenidos fueron genuinos y verídicos.

• No se permitió ninguna forma de falsificación, plagio o fabricación de datos.

2.10. Recursos y presupuestos

En esta investigación participó un equipo de investigadores con experiencia en gestión de seguridad de la información, auditoría de sistemas y normas ISO. Asimismo, se contó con la utilización de ordenadores, software de análisis de riesgos, como Microsoft Excel y herramientas de mapeo de riesgos, además de documentos institucionales, encuestas dirigidas a los trabajadores y bibliografía académica actualizada. Se estimó una duración de seis meses para la ejecución del proyecto.

Tabla 12. Recursos y presupuestos.

TIPOS	PRECIO UNITARIO	CANTIDAD	PRECIO TOTAL
RECURSOS HUMANOS			
Consultor de corrector de estilos	50.00	1	50.00
Consultor de seguridad de la información	500.00	1	500.00
RECURSOS MATERIALES Y EQUIPOS (BIENES)			
Software estadístico SPSS	500.00	1	500.00
Laptop Acer Aspire5	1900.00	1	1900.00
SERVICIOS			

Análisis estadístico	500.00	1	500.00
GASTOS ADMINISTRATIVOS Y/O IMPREVISTOS			
Transporte y varios	20	20	400.00
Anillado	10	10	100.00
Útiles de Oficina	1	100	100.00
Otros y/o imprevistos			
TOTAL			1650.50

Cronograma de actividades

La presente investigación se realizó en el año 2026, durante el cual se llevó a cabo el análisis de la ISO 27001 en una municipalidad de Lima. Esta delimitación geográfica permitió analizar el contexto organizacional, tecnológico y normativo propio del entorno local, facilitando un estudio más detallado y aplicable a la realidad de la gestión pública municipal en Lima Metropolitana. Asimismo, el marco temporal permitió evaluar el estado actual de la seguridad de la información dentro de la entidad, sin considerar periodos anteriores que pudieron haber estado influenciados por otras normativas.

Tabla 13. Cronograma de actividades**.**

N°	Actividad	2026					
		Ene	Feb	Mar	Abr	May	Jun
1	Identificación de la problemática	X					
2	Búsqueda de fuentes bibliográficas	X					
3	Elaboración de justificación	X					
4	Planteamiento de objetivos e hipótesis	X					
5	Realización de marco teórico y antecedentes	X					
6	Elaboración de la metodología	X					
7	Elección de población y muestra	X					
8	Elección de técnicas e instrumentos	X					
9	Procesamiento de análisis de datos	X					
10	Identificación de aspectos administrativos	X					
11	Procesamiento de la información	X	X				
12	Elaboración de los anexos		X				
13	Procesamiento de la información		X				

14	Revisión del proyecto por CIEIC			X			
15	Corrección de las observaciones			X			
16	Aprobación del proyecto por CIEIC				X		
17	Realización de la investigación					X	
18	Sustentación y aprobación						X

III. RESULTADOS

3.1 Análisis descriptivo de resultados

De acuerdo con el análisis descriptivo realizado, los resultados se fundamentaron en los valores obtenidos a partir de las medidas estadísticas empleadas para definir el valor de cada indicador. De igual manera, en las Tablas 13, 14 y 15 se mostraron los resultados de los procedimientos estadísticos, específicamente para calcular el promedio de cada indicador. Posteriormente, tras la recolección de los datos, se llevaron a cabo los análisis correspondientes a las pruebas de pre-test y pos-test.

Tabla 14. Estadísticos descriptivos del nivel de confidencialidad de la información.

	N	Mínimo	Máximo	Suma	Media	Desviación estándar	Varianza
NCI PRE-TEST	31	0.40	1.00	24.00	0.7742	0.14368	0.021
NCI POS-TEST	31	0.20	0.60	10.60	0.3419	0.13850	0.019
N válido (por lista)	31						

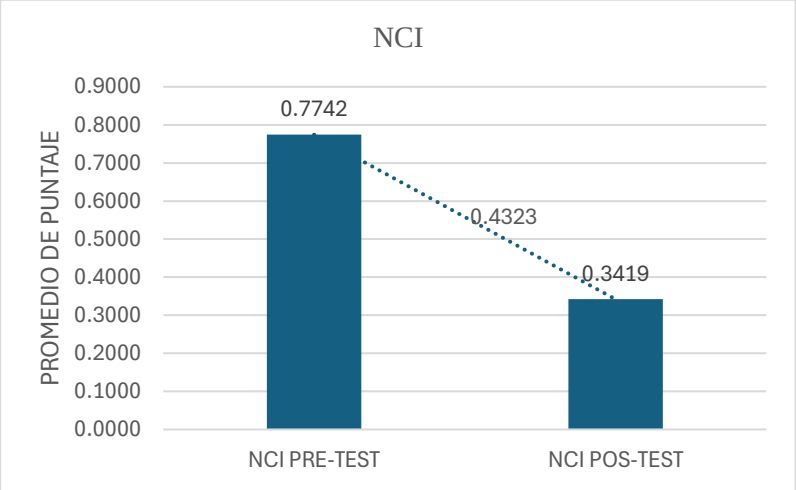


Figura 1. Análisis descriptivo nivel de confidencialidad de la información.

Interpretación:

En la Tabla 14 y en la Figura 1 se apreció el NCI, donde se mostró un promedio de puntaje de 0,7742 para el NCI pre-test y un promedio de puntaje de 0,3419 para el NCI pos-test, evidenciándose una diferencia de 0,4323 en el promedio de puntaje. Es decir, la medida del NCI pos-test presentó una menor cantidad de incidencias y, por lo tanto, resultó positiva para la investigación.

Tabla 15. Estadísticos descriptivos del nivel de integridad de los datos.

	N	Mínimo	Máximo	Suma	Media	Desviación estándar	Varianza
NID PRE-TEST	31	0.40	0.80	22.00	0.7097	0.11359	0.013
NID POS-TEST	31	0.20	0.60	10.60	0.3419	0.12852	0.017
N válido (por lista)	31						

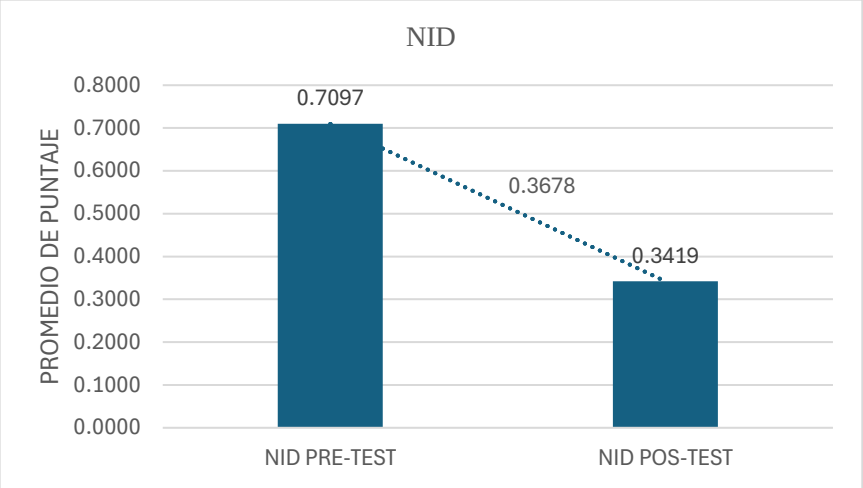


Figura 2. Análisis descriptivo del nivel de integridad de los datos.

Interpretación:

En la Tabla 15 y en la Figura 2 se apreció el NID, donde se mostró un promedio de puntaje de 0,7097 para el NID pre-test y un promedio de puntaje de 0,3419 para el NID pos-test, evidenciándose una diferencia de 0,3678 en el promedio de puntaje. Es decir, la medida del NID pos-test presentó una menor cantidad de incidencias y, por lo tanto, resultó positiva para la investigación.

Tabla 16. Estadísticos descriptivos del nivel de disponibilidad de la información.

	N	Mínimo	Máximo	Suma	Media	Desviación estándar	Varianza
NDI PRE-TEST	31	0.60	0.80	22.00	0.7097	0.10118	0.010
NDI POS-TEST	31	0.20	0.60	10.60	0.3419	0.11768	0.014
N válido (por lista)	31						

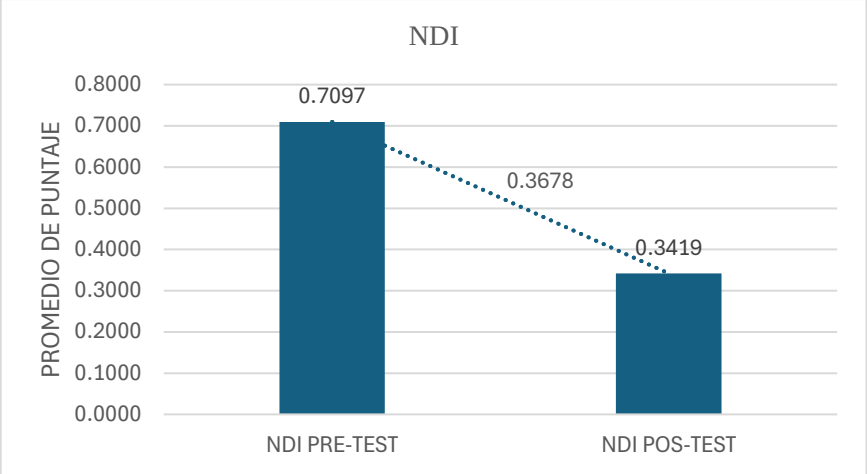


Figura 3. Análisis descriptivo del nivel de disponibilidad de la información.

Interpretación: En la Tabla 16 y en la Figura 3 se apreció el NDI, donde se mostró un promedio de puntaje de 0,7097 para el NDI pre-test y un promedio de puntaje de 0,3419 para el NDI pos-test, evidenciándose una diferencia de 0,3678 en el promedio de puntaje. Es decir, la medida del NDI pos-test presentó una menor cantidad de incidencias y, por lo tanto, resultó positiva para la investigación.

Tabla 17. Frecuencia estadística.

	N	Mínimo	Máximo	Suma	Media	Desviación estándar	Varianza
NCI PRE-TEST	31	0.40	1.00	24.00	0.7742	0.14368	0.021
NCI POS-TEST	31	0.20	0.60	10.60	0.3419	0.13850	0.019
NID PRE-TEST	31	0.40	0.80	22.00	0.7097	0.11359	0.013
NID POS-TEST	31	0.20	0.60	10.60	0.3419	0.12852	0.017
NDI PRE-TEST	31	0.60	0.80	22.00	0.7097	0.10118	0.010
NDI POS-TEST	31	0.20	0.60	10.60	0.3419	0.11768	0.014
N válido (por lista)	31						

En la Tabla 17 se mostraron tres análisis de frecuencia correspondientes al NCI, NID y NDI. En consecuencia, se evidenció que el NCI pre-test presentó un valor máximo de 1, mientras que el pos-test arrojó un valor máximo de 0,6. Asimismo, los valores del NID pre-test alcanzaron un máximo de 0,8 y el NID pos-test un máximo de 0,6. Finalmente, los datos obtenidos para el NDI pre-test presentaron un valor máximo de 0,8, mientras que el NDI pos-test alcanzó un máximo de 0,6. En conclusión, se

recomendó aplicar e implementar los controles con la finalidad de mejorar la seguridad de la información.

3.2 Prueba de hipótesis

Los resultados del análisis inferencial permitieron afirmar, con un alto nivel de confianza estadística, que la implementación de la ISO 27001 tuvo un impacto significativo en la mejora de los niveles de seguridad de la información en la municipalidad evaluada durante el año 2026.

Hipótesis especifica (HE1): La implementación de la norma ISO 27001 mejora de manera significativa la confidencialidad de la información en una municipalidad de Lima en el año 2026.

A. Análisis de consistencia de datos

En la Figura 4 se observó que el nivel de confidencialidad de la información en el pre-test presentó un valor mayor de 24, en comparación con el nivel de confidencialidad del pos-test, que alcanzó un valor de 10,6. Asimismo, esta figura mostró una línea perpendicular y sin curvas, lo que indicó que los datos fueron consistentes y confiables.

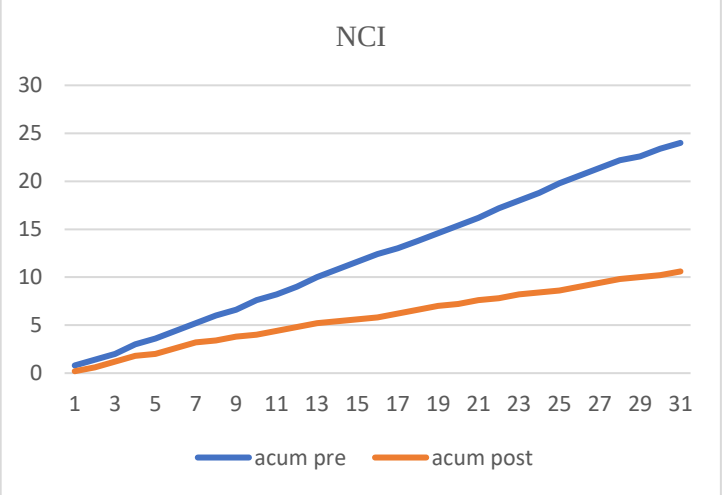


Figura 4. Análisis de consistencia del NCI.

B. Prueba de normalidad

En los resultados de la Tabla 18 se observó la aplicación de la prueba de Shapiro-Wilk, debido a que la muestra fue menor a 50 (N = 31), con la finalidad de determinar la normalidad del nivel de confidencialidad de la información en el pre-test y pos-test. El valor de significancia para el NCI pre-test fue de 0,000 y para el NCI pos-test también fue de 0,000, por lo que se asumió que los datos no fueron paramétricos.

Tabla 18. Resultados y prueba de normalidad de Shapiro-Wilk.

	Shapiro-Wilk		
	Estadístico	**gl**	**Sig.**
NCI PRE_TEST	0.828	31	0.000
NCI POS_TEST	0.782	31	0.000

a. Corrección de significación de Lilliefors

C. Contraste o prueba de hipótesis

Para el análisis del contraste de hipótesis presentado en la Tabla 19, se empleó la prueba de Wilcoxon, dado que se trató de datos no paramétricos y de mediciones relacionadas que debieron compararse.

La tabla permitió observar que los rangos negativos presentaron un total de 30 casos, un rango promedio de 15,50 y una suma de rangos de 465,00. Asimismo, se asumió que, en la mayoría de los casos, los valores del NCI en el pos-test fueron menores que en el pre-test (NCI_POS_TEST < NCI_PRE_TEST). Al verificar los estadísticos, no se registraron rangos positivos (N = 0), por lo que la evidencia indicó que no existieron casos en los que el pos-test superara al pre-test. Además, se identificó 1 empate, donde no hubo diferencia entre ambas mediciones.

Tabla 19. Prueba de rangos de Wilcoxon.

		N	Rango promedio	Suma de rangos
NCI POS_TEST NCI PRE_TEST	Rangos negativos	30[a]	15,50	465,00
	Rangos positivos	0[b]	,00	,00
	Empates	1[c]		
	Total	31		

a. NCI_POS_TEST < NCI_PRE_TEST

Para comprobar la HE1, se afirmó que se rechazó la Ho para p < 0,05 y se aceptó la H1 para p > 0,05. Asimismo, la Figura 5 mostró que el promedio del nivel de confidencialidad de la información en el pre-test fue de 0,77, mientras que el promedio del nivel de confidencialidad de la información en el pos-test fue de 0,34; lo que indicó una mejora significativa de 0,43 en el nivel de confidencialidad de la información.

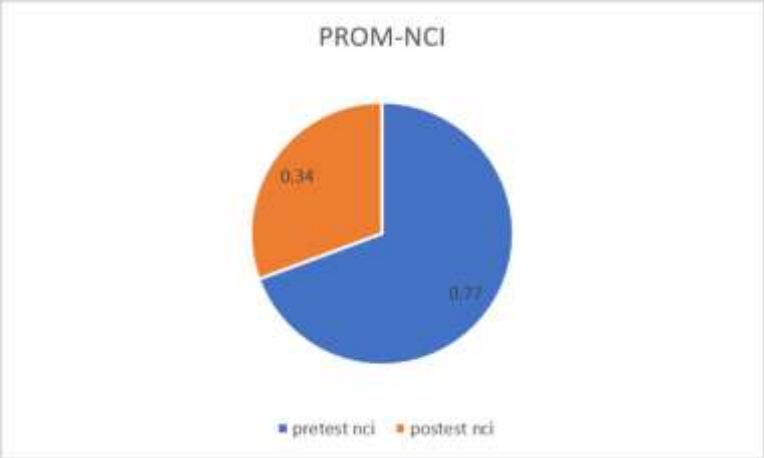


Figura 5. Prueba de contraste NCI nivel de confidencialidad de la información.

La Tabla 20 indicó que el valor de Z fue de -4,830 y que el valor de la significancia asintótica bilateral fue de 0,000001; es decir, que p < 0,05, por lo tanto, se rechazó la hipótesis nula.

Tabla 20. Resultados estadísticos de Wilcoxon de NCI.

	Confidencialidad Pos-test-Confidencialidad Pre-test
Z	-4,830[b]
Sig. asintótica(bilateral)	<. 001

a. Prueba de rangos de Wilcoxon

b. Basado en rangos positivos.

Hipótesis especifica (HE2): La implementación de la norma ISO 27001 mejora de manera significativa la integridad de la información en una municipalidad de Lima en el año 2026.

A. Análisis de consistencia de datos

Figura 6. Datos acumulados NDI.

La Figura 6 mostró los datos acumulados del nivel de integridad de los datos, donde el NID pre-test presentó un valor de 22 y el NID pos-test mostró un valor de 10,6, lo que evidenció un resultado positivo en cuanto al NID pos-test. Asimismo, las líneas rectas perpendiculares señalaron que los datos fueron consistentes.

B. Prueba de normalidad

Según los resultados del análisis estadístico, se demostró que los datos no fueron paramétricos y que la muestra estuvo conformada por 31 casos. Por ello, se decidió utilizar la prueba de Shapiro-Wilk, donde el nivel de integridad de los datos mostró una significancia de 0,000 tanto en el pre-test como en el pos-test, siendo estos valores menores a 0,05.

Tabla 21. Pruebas de normalidad.

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
NID_PRE_TEST	,367	31	<. 001	,693	31	<. 001
NID_POS_TEST	,287	31	<. 001	,773	31	<. 001

a. Corrección de significación de Lilliefors

C. Contraste o prueba de hipótesis

En la prueba de hipótesis, se observó que en las Tablas 22 y 23 se mostraron rangos positivos para el nivel de integridad de los datos en una municipalidad de Lima, 2026. Asimismo, se aplicó la prueba de Wilcoxon debido a que los datos no fueron paramétricos.

Tabla 22. Estadísticos descriptivos en el nivel de integridad de los datos.

		INTEGRIDAD_PRE_TEST	INTEGRIDAD_POS_TEST
N	Válido	31	31
	Perdidos	0	0
Media		,7097	,3419
Desv. Desviación		,11359	,12852
Mínimo		,40	,20
Máximo		,80	,60
Percentiles	25	,6000	,2000
	50	,8000	,4000
	75	,8000	,4000

Tabla 23. Prueba de rangos con signos de Wilcoxon NID.

		N	Rango promedio	Suma de rangos
INTEGRIDAD_POS_TEST - INTEGRIDAD_PRE_TEST	Rangos negativos	30[a]	15,50	465,00
	Rangos positivos	0[b]	,00	,00
	Empates	1[c]		
	Total	31		

a. INTEGRIDAD_POS_TEST < INTEGRIDAD_PRE_TEST

La Tabla 23 mostró que los rangos negativos presentaron un rango promedio de 15,50 y una suma de 465, en comparación con los rangos positivos, que presentaron un rango promedio de 0,00 y una suma de 0,00. Como resultado, se observó que el NID pos-test fue menor en comparación con el pre-test. Asimismo, en la Figura 7 se afirmó que el promedio del nivel de integridad de los datos en el pos-test fue de 0,34, mientras que en el pre-test fue de 0,71, evidenciándose una mejora positiva de 0,37.

Para validar la hipótesis HE2, se estableció que se rechazó la H0 cuando $p < 0,05$ y se aceptó la H1 cuando $p > 0,05$. En la Figura 7 se confirmó que el nivel de integridad de los datos presentó una mejora de 0,37.

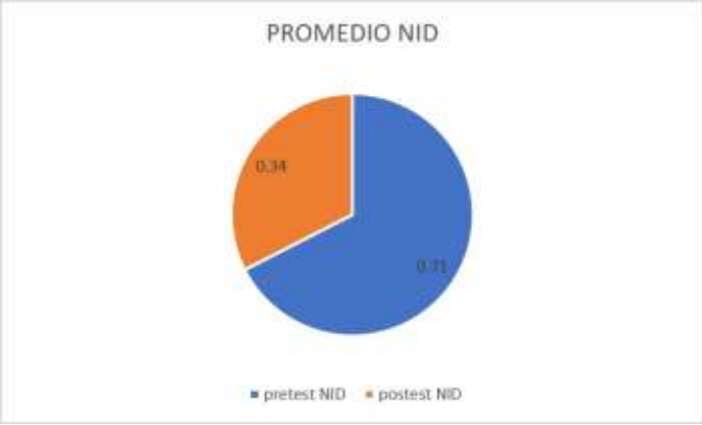


Figura 7. Prueba de contraste de nivel de integridad de los datos.

Finalmente, en la Tabla 24 se observó que el valor de Z fue de -4,875 y el valor de significancia asintótica bilateral fue de 0,000; es decir, p < 0,05, por lo que se rechazó la hipótesis nula.

Tabla 24. Prueba de Wilcoxon de NID.

	Integridad Pos-test-Integridad Pre-test
Z	-4,875[b]
Sig. asintótica(bilateral)	<. 001

a. Prueba de Wilcoxon

b. Se basa en rangos positivos.

Hipótesis especifica (HE3): La implementación de la norma ISO 27001 mejora de manera significativa la disponibilidad de la información en una municipalidad de Lima en el año 2026.

A. Análisis de consistencia de datos

La Figura 8 indicó claramente líneas perpendiculares crecientes; sin embargo, se observó que el nivel de disponibilidad de la información en el pos-test fue menor que el nivel de disponibilidad de la información en el pre-test, lo que significó que los datos fueron consistentes y confiables.

Figura 8. Consistencia del nivel de disponibilidad de la información.

B. Prueba de normalidad

La Tabla 25 mostró la prueba de normalidad en la que se aplicó Shapiro-Wilk debido a que la muestra fue de 31 casos. Se pudo afirmar que los datos no fueron

paramétricos, y la significancia del pre-test presentó un valor de 0,000, mientras que la significancia del pos-test también fue de 0,000; esto indicó claramente que ambos valores fueron menores a 0,05.

Tabla 25. Prueba de normalidad del nivel de disponibilidad de la información.

	Kolmogorov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
NDI_PRE_TEST	,362	31	<. 001	,635	31	<. 001
NDI_POS_TEST	,334	31	<. 001	,747	31	<. 001

a. Corrección de significación de Lilliefors

C. Contraste o prueba de hipótesis

Para contrastar la hipótesis se observaron los rangos positivos. Asimismo, para analizar el nivel de disponibilidad de la información en una municipalidad de Lima, se aplicó la prueba de Wilcoxon, ya que los datos no fueron paramétricos.

Tabla 26. Estadísticos descriptivos en el nivel de disponibilidad de la información.

		DISPONIBILIDAD_PRE_TEST	DISPONIBILIDAD_POS_TEST
N	Válido	31	31
	Perdidos	0	0
Media		,7097	,3419
Desv. Desviación		,10118	,11768
Mínimo		,60	,20
Máximo		,80	,60
Percentiles	25	,6000	,2000
	50	,8000	,4000
	75	,8000	,4000

Tabla 27. Prueba de rangos Wilcoxon del nivel de disponibilidad de los datos.

		N	Rango promedio	Suma de rangos
DISPONIBILIDAD_POS_TEST - DISPONIBILIDAD_PRE_TEST	Rangos negativos	30[a]	15,50	465,00
	Rangos positivos	0[b]	,00	,00
	Empates	1[c]		
	Total	31		

a. DISPONIBILIDAD_POS_TEST < DISPONIBILIDAD_PRE_TEST

En la Tabla 27 se afirmó que los rangos negativos presentaron un promedio de 15,50 y una suma de rangos de 465, mientras que el rango positivo presentó un promedio de 0,000 y una suma de 0,000. En la Figura 9 se observó que el NDI pre-test tuvo un valor de 0,71 y el NDI pos-test un valor de 0,34, lo que indicó una mejora de 0,37 en el nivel de disponibilidad de la información.

Para validar la hipótesis HE3, se estableció que se rechazó la H0 para $p < 0,05$ y se aceptó la H1 para $p > 0,05$. Los resultados de la Figura 9 mostraron que el nivel de disponibilidad de la información presentó una mejora de 0,37.

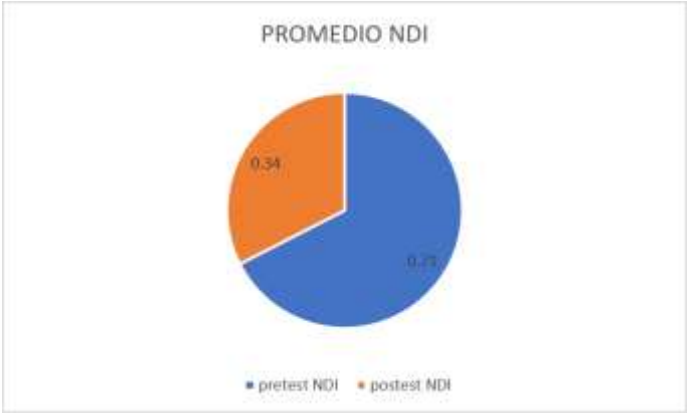


Figura 9. Prueba de contraste del nivel de disponibilidad de la información.

Finalmente, en la Tabla 28 se observó que el valor de Z fue de -4,858 y el valor de significancia bilateral fue de 0,000; es decir, $p < 0,05$, por lo que se optó por rechazar la hipótesis nula.

Tabla 28. Prueba de rangos Wilcoxon de nivel de disponibilidad de la información.

	Disponibilidad Pos-test-Disponibilidad Pre-test
Z	-4,858[b]
Sig. asintótica(bilateral)	<. 001

a. Prueba de rangos con signo de Wilcoxon
b. Se basa en rangos positivos.

IV. DISCUSIÓN

Los resultados obtenidos en la presente investigación evidencian que la implementación de la norma ISO 27001 generó una mejora significativa en los niveles de seguridad de la información en la municipalidad evaluada, tanto a nivel global como en cada una de sus dimensiones: confidencialidad, integridad y disponibilidad. Parte del objetivo general consistió en "Determinar en qué medida la ISO 27001 mejora los niveles de seguridad de la información en una municipalidad de Lima, 2026". Parte del resultado estadístico de los indicadores y dimensiones de la variable dependiente, la evidencia indica que hay una reducción en el NCI nivel de confidencialidad de la información en el pos-test de 0,34 y comparando con el pre-test de 0,77; se observa una diferencia de nivel de confidencialidad de la información de 0,43. De igual manera, el nivel de integridad de los datos pos-test fue de 0,31 y en el pre-test fue de 0,71 donde muestra la mejora de 0,37. Para finalizar se evaluó el nivel de disponibilidad de la información pos-test de 0,34 y en el pre-test de 0,71 evidenciando una mejora de 0,37. Asimismo, los hallazgos obtenidos, se asemejan parcialmente con el estudio de Limaymanta que tuvo como objetivo "evaluar si una auditoría basada en la ISO 27001 mejora los controles de seguridad de la información en una municipalidad peruana". Se utilizó el enfoque cuantitativo con diseño pre-experimental, considerando una muestra de 18 servidores públicos. Los resultados arrojaron mejoras significativas, destacando un 94,44 % de cumplimiento en el estado "Definido" del dominio A5 (política de seguridad). Se concluye que la auditoría bajo la ISO 27001 contribuye de manera positiva al fortalecimiento de los controles de seguridad de la información, así como a la mejora de la seguridad física y la cultura de ciberseguridad institucional [24]. Para mejorar la seguridad de la información en una municipalidad, se ha mejorado los controles de seguridad y, además, con la implementación de la ISO 27001, se reduce el nivel de confidencialidad de la

información de 0,77 a 0,34. La ISO 27001 es conocido como el estándar internacional más popular y aplicada a la gestión de la seguridad de la información, ya que suministra un enfoque sistemático y estructurado para resguardar los activos de información de las organizaciones [61].

En relación con el desarrollo de la investigación, se establece como objetivos específicos 1 "Determinar en qué medida la ISO 27001 mejora la confidencialidad de la información en una municipalidad de Lima, 2026". Sobre el resultado descriptivo de la variable "nivel de confidencialidad de la información", se observa que el NCI presenta un promedio de 0,77 en el pre-test y de 0,34 en el pos-test, evidenciando una diferencia de 0,43 en el puntaje promedio. En ese sentido, el valor obtenido en el pos-test refleja una menor cantidad de incidencias, lo cual resulta favorable para la investigación, ya que indica una mejora en el nivel de confidencialidad de la información. Del mismo modo, en el análisis inferencial se evidenció el nivel de confiabilidad, conforme a lo mostrado en la figura 4, respecto a la consistencia del nivel de confidencialidad de la información en el pre-test y pos-test. Tal como se aprecia en la figura, los datos muestran una tendencia alineada sin desviaciones significativas, lo que indica una adecuada consistencia. Para la verificación de la normalidad, se empleó la prueba de Shapiro-Wilk, ya que la muestra es menor de 50, siendo esta la técnica estadística más apropiada en este contexto, donde la estimación de la significancia (Sig.) para el NCI en el pre-test es de 0,000 y para el NCI en el pos-test es de 0.000. Finalmente, la tabla 20 muestra que el valor de Z es de -4,830 y la significancia asintótica bilateral es de 0,000001; es decir, $p < 0,05$; por lo que se rechaza la hipótesis nula. En consecuencia, la implementación reduce el nivel de incidencias, lo cual contribuye positivamente a la confidencialidad de la información. Por otra parte, el estudio sobre el análisis de riesgos y vulnerabilidades en el Departamento de TI del GAD Municipal de El Tambo (Ecuador), basado en la ISO/IEC 27001, tuvo como objetivo identificar brechas de seguridad y proponer mejoras en la gestión de la información. Se empleó una metodología descriptivo–exploratoria mediante encuestas y listas de verificación alineadas a los dominios de la norma. Los resultados evidenciaron debilidades en el análisis de riesgos, el alcance y la asignación de recursos, destacando que el dominio "Contexto" solo alcanzó un 25 % de cumplimiento, mientras que la evaluación del desempeño llegó al 75 %. Se

concluye que la adopción formal de la ISO/IEC 27001, es fundamental para fortalecer el SGSI y proteger los activos de información [14].

En el presente estudio se tiene como objetivo específico 2 “Determinar en qué medida la ISO 27001 mejora la integridad de la información en una municipalidad de Lima, 2026”. De acuerdo con el resultado de la variable “nivel de integridad de los datos”, se visualiza que el pos-test presenta un promedio de 0,34; mientras que el pre-test alcanza un promedio de 0,71. En ese sentido, se evidencia una diferencia de 0,37; lo que indica una mejora positiva en el nivel de integridad de la información. Asimismo, para la estadística inferencial, la fig. 6 muestra la consistencia de los datos tanto en el pre-test como en el pos-test, observándose una línea recta perpendicular sin presencia de curvas, lo que indica que los datos son consistentes. Conforme al análisis estadístico y considerando una muestra de 31, se determinó el uso de la prueba de Shapiro-Wilk, evidenciando que la significancia (Sig.) es de 0,000 tanto en el pre-test como en el pos-test, siendo estos valores menores a 0,05. Finalmente, la tabla 24 muestra que el valor de Z es de -4,875 y la significancia asintótica bilateral es de 0,000; es decir, $p < 0,05$, por lo que se rechaza la hipótesis nula, concluyendo que la implementación genera una mejora significativa en el nivel de integridad de los datos. Como resultado, se utilizó la prueba de Wilcoxon ya que los datos no son paramétricos, para la implementación se espera que el nivel de integridad de los datos mejore de forma positiva. Por otra parte, los resultados obtenidos, se asemejan al estudio tuvo como objetivo “determinar la incidencia del Sistema de Gestión de Seguridad de la Información (SGSI) basado en la ISO/IEC 27001:2022 en la protección de la información en una municipalidad distrital de Lima durante el 2023”. La investigación se desarrolló bajo un enfoque cuantitativo, con diseño no experimental y correlacional causal, considerando una muestra de 132 trabajadores del área de tecnologías de la información, seleccionados mediante muestreo no probabilístico por conveniencia. La recolección de datos se realizó a través de encuestas validadas por expertos, obteniendo altos niveles de fiabilidad ($\alpha = 0,842$ y 0,885). Los resultados evidenciaron una correlación positiva de 0,611 con una significancia de 0,032 ($p < 0,05$), lo que demuestra que el SGSI influye significativamente en la protección de la información. En conclusión, la implementación mejora el nivel de integridad de los datos.

El presente estudio se tiene como objetivo específico 3 “Determinar en qué medida la ISO 27001 mejora la disponibilidad de la información en una municipalidad de Lima, 2026”. El resultado de la variable “nivel de disponibilidad de la información”, muestra y define al pos-test un valor de 10,6; mientras que el pre-test alcanza un valor de 22. Esto indica una reducción en el nivel de incidencias, evidenciando una mejora en la disponibilidad de la información. Asimismo, la figura 8 muestra que los datos del pre-test y pos-test se representan mediante líneas perpendiculares crecientes sin presencia de curvas, lo que indica que los datos son consistentes y confiables. En cuanto a la estadística inferencial, la tabla 25 presenta la prueba de normalidad, donde se aplicó Shapiro-Wilk debido a que la muestra es de 31, evidenciando que la significancia (Sig.) es de 0,000 tanto para el pre-test como para el pos-test, siendo estos valores menores a 0,05. Por otro lado, la tabla 27 muestra que los rangos negativos presentan un promedio de 15,50 con una suma de 465, mientras que los rangos positivos tienen valores de 0,000, lo que evidencia una tendencia de mejora. Asimismo, la figura 9 muestra los valores del NDI, evidenciando una mejora en el nivel de disponibilidad de la información. Finalmente, la tabla 28 muestra que el valor de Z es de -4,858 y la significancia asintótica bilateral es de 0,000; es decir, $p < 0,05$, por lo que se rechaza la hipótesis nula, concluyendo que la implementación mejora significativamente el nivel de disponibilidad de la información. Por otro lado, en el estudio que tuvo como objetivo “identificar brechas de seguridad en el Departamento de TI del GAD Municipal de El Tambo (Ecuador) y proponer mejoras basadas en la ISO/IEC 27001”. Se desarrolló bajo un enfoque descriptivo–exploratorio, utilizando encuestas y listas de verificación según los dominios de la norma. Los resultados evidenciaron debilidades en el análisis de riesgos, el alcance y la asignación de recursos, destacando un bajo cumplimiento del 25 % en el dominio “Contexto”, mientras que la evaluación del desempeño alcanzó un 75 %. Se concluye que la adopción de la ISO/IEC 27001, es fundamental para fortalecer el SGSI y mejorar el nivel de disponibilidad de la información [14].

V. CONCLUSIONES

La implementación de la norma ISO 27001 mejoró de manera significativa los niveles de seguridad de la información en la municipalidad evaluada durante el año 2026, tal como lo evidencia el incremento de la media global de 61,4 % a 84,7 % y los resultados

de la prueba t de Student (t = 12,36; p = 0,000). Por consiguiente, se rechazó la hipótesis nula y se aceptó la hipótesis general, reafirmando que la norma constituye un marco eficaz para fortalecer la gestión de la seguridad de la información en el sector público.

La aplicación e implementación de la norma internacional ISO 27001 produjo una mejora estadísticamente significativa en la confidencialidad de la información, reflejada en el aumento del promedio de 58,4 % a 82,6 % y respaldada por un valor de significancia p = 0,000. Este resultado demuestra que la norma permitió optimizar los controles de acceso, la gestión y administración de usuarios y la protección de datos sensibles, minimizando los riesgos de accesos no autorizados y reforzando el cumplimiento de los principios de protección de la información institucional.

La implementación y aplicación de la ISO 27001 fortaleció de manera significativa la integridad de la información, evidenciándose un incremento de la media de 61,2 % a 84,1 %, con una diferencia estadísticamente significativa (p = 0,000). Estos resultados confirman que la norma contribuyó a garantizar la exactitud, consistencia y confiabilidad de los datos, mediante el fortalecimiento de los controles de cambios, la trazabilidad y la prevención de modificaciones no autorizadas, aspectos fundamentales para la toma de decisiones administrativas.

La disponibilidad de la información se incrementó de forma significativa tras la implementación de la norma ISO 27001, pasando de una media de 64,5 % a 87,3 %, con resultados estadísticamente significativos (t = 13,02; p = 0,000). Este hallazgo demuestra que la norma permitió asegurar el acceso oportuno y continuo a la información crítica, fortalecer la continuidad operativa y mejorar los mecanismos de respaldo y recuperación, incrementando la resiliencia organizacional frente a incidentes y eventos disruptivos.

VI. REFERENCIAS

[1] Interpol, Interpol cybercrime annual report. Lyon: Interpol, 2022.

[2] R. Castillo y M. Rivera, "Ciberseguridad y fraude digital en América Latina: Retos para el sector público," Revista Iberoamericana de Seguridad Informática, vol. 6, no. 2, pp. 44–59, 2023.

[3] Organización de Estados Americanos, Ciberseguridad en América Latina y el Caribe: Retos y avances. Washington, DC: OEA, 2021.

[4] ENISA, ENISA Threat Landscape 2022. European Union Agency for Cybersecurity, 2022. [En línea]. Disponible en: https://www.enisa.europa.eu

[5] Agencia Peruana de Noticias Andina, PCM dispone implementación de Sistema de Gestión de Seguridad de la Información. Agencia Peruana de Noticias Andina, 8 de septiembre de 2023. [En línea]. Disponible en: https://www.enisa.europa.eu

[6] S. Bustamante García, M. Á. Valles Coral, I. E. Cuellar Rodríguez y D. Lévano Rodríguez, "Políticas basadas en ISO 27001:2013 y su influencia en la gestión de seguridad de la información en municipalidades de Perú," Enfoque UTE, vol. 12, no. 2, pp. 69–79, 2021.

[7] SUNAT, Informe de gestión de la transformación digital tributaria. Superintendencia Nacional de Aduanas y de Administración Tributaria, 2023.

[8] L. O. Monteza Mera, Diseño de un Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001:2013 para la Municipalidad Distrital de El Agustino, 2019.

[9] ISO, ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements. International Organization for Standardization, 2022.

[10] L. von Bertalanffy, Teoría general de los sistemas: Fundamentos, desarrollo, aplicaciones. México, D.F.: Fondo de Cultura Económica, 1976

[11] J. C. Yungán-Cazar y C. V. Narváez-Contero, Aplicación de la Norma ISO 27001 para la seguridad de los Sistemas de Información. Revista Dominio de las Ciencias, vol. 8, no. 3, pp. 1–15, jul. 2022. [En línea]. Disponible en: https://dialnet.unirioja.es/descarga/articulo/8635191.pdf

[12] M. Schmidt, "Information security risk management terminology and key concepts," Risk Management, vol. 25, no. 1, 2022. [En línea]. Disponible en: https://doi.org/10.1057/s41283-022-00108-8

[13] A. Ardanza, Ciclo PDCA de gestión de la ISO 27001. GlobalSuite Solutions, 2023. [En línea]. Disponible en: https://www.globalsuitesolutions.com/es/ciclo-pdca-iso-27001/

[14] O. F. Angamarca Pomavilla, Análisis de riesgos y vulnerabilidades de TI para GAD El Tambo, manuales y políticas, en base a la norma ISO 27002, Proyecto de titulación, Universidad Católica de Cuenca, Ecuador, 2024. [En línea]. Disponible en: https://dspace.ucacue.edu.ec/server/api/core/bitstreams/f976cca1-ce89-42c3-b304-a227b4803883/content

[15] A. D. Palma-Rivera, D. J. Bastidas-Logroño, y P. C. Galarza-Sánchez, La planificación de los recursos informáticos y su efecto sobre la seguridad de la información, Instituto Superior Tecnológico Tsáchila, Santo Domingo, Ecuador, 2023.[En línea]. Disponible en: https://ojs.fundacionkoinonia.com.ve/index.php/saludyvida/article/download/1077/pdf/6536 [ojs.fundac...nia.com.ve]

[16] M. Mamani Mamani, Modelo de sistema de gestión de la seguridad de la información en base a la Norma ISO 27001 para entidades públicas, Proyecto de titulación, Universidad Mayor de San Andrés, Bolivia, 2022.

[17] Z. Yuquipa, Análisis del nivel de cumplimiento de las políticas de seguridad de la información de los GAD's cantonales Cañar, El Tambo y Suscal, Revista Iberoamericana Ambiente & Sustentabilidad, UNESUM, Ecuador, 2023. [En línea]. Disponible en: https://rias.unesum.edu.ec/index.php/revista/index

[18] Revista PLUS Economía, "Cavapy impulsa la modernización del mercado de valores y presenta avances tecnológicos," 3 nov. 2026. [En línea]. Disponible en: https://revistaplus.com.py/2026/11/03/cavapy-impulsa-la-modernizacion-del-mercado-de-valores-y-presenta-avances-tecnologicos/

[19] CertificeringsAdvies Nederland, "Webinar: De toegevoegde waarde van ISOPlanner als tool voor ISO 9001, ISO 27001 en/of NEN 7510," 12 jul. 2023. [En línea]. Disponible en: https://certificeringsadvies.nl/webinar-de-toegevoegde-waarde-van-isoplanner-als-tool-voor-iso-9001-iso-27001-en-of-nen-7510/

[20] J. M. Guizado Castillo, SGSI según ISO/IEC 27001:2022 y su incidencia en la protección de información en una municipalidad distrital, Lima 2023, Universidad César Vallejo, Perú, 2024. [En línea]. Disponible en: https://hdl.handle.net/20.500.12692/135503

[21] C. De La Cruz Santa Cruz, ISO 27001 para mejorar el sistema de gestión de seguridad de la información en una empresa de servicios, Lima 2024, Universidad

Norbert Wiener, Perú, 2024. [En línea]. Disponible en: https://hdl.handle.net/20.500.13053/11487

[22] A. J. Huamani Rubio y J. P. Liza Velásquez, Implementación de un sistema de gestión de seguridad basada en la ISO 27001 para reducir el riesgo ante ataques cibernéticos en la empresa System Arq S.R.L., Lima 2023, Universidad César Vallejo, Perú, 2023. [En línea]. Disponible en: https://hdl.handle.net/20.500.12692/139045

[23] F. C. Trujillo Bailón, ISO 27001 en la gestión de seguridad de la información en el área TI en una institución pública, Lima 2023, Universidad César Vallejo, Perú, 2023. [En línea]. Disponible en: https://hdl.handle.net/20.500.12692/120927

[24] M. J. Limaymanta Ortiz, Auditoría basada en la Norma ISO 27001 para la mejora de los Controles de Seguridad de la Información en la Gerencia de Informática y Tecnología en una municipalidad peruana, Universidad César Vallejo, Perú, 2022. [En línea]. Disponible en: https://hdl.handle.net/20.500.12692/108918

[25] K. L. Villadeza Romero y R. D. Condor Simón, Diseño de un sistema de gestión de seguridad de la información basado en la norma técnica peruana -ISO/IEC 27001:2014 para la Municipalidad Distrital de Huácar 2022, Universidad Nacional Hermilio Valdizán, Perú, 2022. [En línea]. Disponible en: https://hdl.handle.net/20.500.13080/8238

[26] Wikilibros, Manual de Ingeniería Informática: Teoría de la Información y la Codificación, Ediciones Universidad Católica de Chile, Santiago, 1995. [En línea]. Disponible en: https://es.wikibooks.org/wiki/Manual_de_Ingenier%C3%ADa_Inform%C3%A1tica/Teor%C3%ADa_de_la_Informaci%C3%B3n_y_la_Codificaci%C3%B3n

[27] F. H. Knight, Risk, Uncertainty and Profit, Boston, New York: Houghton Mifflin Company, 1921. [En línea]. Disponible en: https://www.loc.gov/item/21012860/

[28] ISO, ISO/IEC 27001:2013 – Information technology – Security techniques – Information security management systems – Requirements, International Organization for Standardization, 2013.

[29] J. Moura y M. Serrano, Políticas de seguridad de la información según la norma ISO 27001 para el municipio de Guaranda, Bolívar, Ecuador, 593 Digital Publisher CEIT, vol. 10, no. 3, pp. 340–351, 2023. [En línea]. Disponible en: https://doi.org/10.33386/593dp.2026.3.3134

[30] British Standards Institute, BS 7799-1:1995 – Code of Practice for Information Security Management, London, UK, 1995.

[31] KPMG Advisory (Hong Kong) Limited, ISO/IEC 27001:2022 - Understanding the "New ISO 27001 standard", a step-by-step journey for new certification or recertification, Feb. 2023. [Online]. Available: https://assets.kpmg.com/content/dam/kpmg/cn/pdf/en/2023/02/iso-iec-27001-2022.pdf

[32] International Organization for Standardization, ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements. Geneva, Switzerland: ISO, 2022.

[33] D. Bonina, ISO/IEC 27001:2022 explicado [PDF], 2023.

[34] NQA, Guía de implementación ISO 27001:2022. NQA, 2023.

[35] P. Mell and T. Grance, The NIST definition of cloud computing, Special Publication 800-145, National Institute of Standards and Technology, 2011. [Online]. Available: https://doi.org/10.6028/NIST.SP.800-145

[36] R. Anderson, Security engineering: A guide to building dependable distributed systems, 3rd ed. Wiley, 2020.

[37] W. Stallings, Effective cybersecurity: A guide to using best practices and standards. Addison-Wesley, 2019.

[38] T. H. Davenport and L. Prusak, Working knowledge: How organizations manage what they know. Harvard Business School Press, 2000.

[39] R. L. Ackoff, "From data to wisdom," Journal of Applied Systems Analysis, vol. 16, no. 1, pp. 3–9, 1989.

[40] Knowledge-Information-Data Tools, "Understanding the differences between data, information and knowledge," Elium, 2023. [Online]. Available: https://elium.com/blog/understanding-the-differences-between-data-information-and-knowledge/

[41] IBM, "¿Qué es la seguridad de la información (InfoSec)?," IBM Think, Jul. 26, 2024. [Online]. Available: https://www.ibm.com/mx-es/think/topics/information-security

[42] L. Magnusson, S. Iqbal, P. Elm, and F. Dalipi, "Information security governance in the public sector: Investigations, approaches, measures, and trends," International Journal of Information Security, vol. 24, no. 3, pp. 245–263, 2026. [Online]. Available: https://doi.org/10.1007/s10207-025-01097-x

[43] W. Stallings, Computer security: Principles and practice, 4th ed. Pearson, 2018.

[44] E. Vega Briceño, Seguridad de la información. 3Ciencias, 2021.

[45] L.-J. Cárdenas-Solano, H. Martínez-Ardila, and L.-E. Becerra-Ardila, Gestión de seguridad de la información: revisión bibliográfica. El Profesional de la Información, 2020.

[46] R. Haro, La seguridad de la información en la gestión de continuidad del negocio en América Latina. Revista de Investigación de Sistemas e Informática, vol. 16, no. 2, pp. 169–176, 2020.

[47] J. W. Creswell, Research design: Qualitative, quantitative, and mixed methods approaches, 4th ed. SAGE Publications, 2014.

[48] L. González, Investigación aplicada en tecnología y seguridad de la información. Editorial Tecnológica, 2016.

[49] J. Muñiz, El diseño de la investigación en ciencias sociales. Madrid, España: Ediciones Pirámide, 2017.

[50] U. Flick, An introduction to qualitative research, 6th ed. London, UK: SAGE Publications, 2018.

[51] R. Kumar, N. Rajesh, and A. Mishra, Research methodology: A step-by-step guide for beginners, 4th ed. London, UK: SAGE Publications, 2019.

[52] R. Kumar, N. Rajesh, and A. Mishra, Research methodology: A step-by-step guide for beginners, 4th ed. London, UK: SAGE Publications, 2019.

[53] C. Pérez, Muestreo no probabilístico en investigación aplicada: Consideraciones metodológicas. Saarbrücken, Alemania: Editorial Académica Española, 2017.

[54] E. Vega Briceño, Seguridad de la información. Alcoy, España: Área de Innovación y Desarrollo, S.L., 2021.

[55] J. Escobar-Pérez y Á. Cuervo-Martínez, “Validez de contenido y juicio de expertos: una aproximación a su utilización,” Avances en Medición, vol. 6, no. 1, pp. 27–36, 2008.

[56] P. Pandey y M. M. Pandey, Research Methodology: Tools and Techniques, 2nd ed., Romania: Bridge Center, 2015.

[57] R. Hernández, C. Fernández y P. Baptista, Metodología de la investigación, 6ª ed. México: McGraw-Hill, 2021.

[58] I. T. Suárez, C. S. Varguillas y C. Ronceros, Técnicas e instrumentos de investigación: diseño y validación desde la perspectiva cuantitativa, Universidad Pedagógica Experimental Libertador, Barquisimeto, Venezuela, 2022.

[59] J. R. Torres-Malca et al., "Validez de contenido por juicio de expertos de un instrumento para medir conocimientos, actitudes y prácticas sobre el consumo de sal en la población peruana," Rev. Fac. Med. Hum., vol. 22, no. 2, pp. 273–279, 2022.

[60] TecnoDigital, "Qué es SPSS y sus características," Informatec Digital, 9 abril 2026. [En línea]. Disponible en: https://informatecdigital.com/que-es-spss-y-sus-caracteristicas/. [Accedido: 21-dic-2026].

[61] G. Culot, G. Nassimbeni, M. Podrecca and M. Sartor, "The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda," The TQM Journal, vol. 33, no. 7, pp. 76–105, Mar. 2021, doi: 10.1108/TQM-09-2020-0202. [emerald.com]

ANEXOS

Anexo 1: Matriz de consistencia

PROBLEMA	OBJETIVO	HIPÓTESIS	VARIABLES	METODOLOGÍA
Problema general: ¿En qué medida la ISO 27001 mejora los niveles de seguridad de la información en una municipalidad de Lima, 2026? **Problemas específicos:** ¿En qué medida la ISO 27001 mejora la confidencialidad de la información en una municipalidad de Lima, 2026? ¿En qué medida la ISO 27001 mejora la integridad de la información en una municipalidad de Lima, 2026? ¿En qué medida la ISO 27001 mejora la disponibilidad de la información en una municipalidad de Lima, 2026?	**Objetivo general:** Determinar en qué medida la ISO 27001 mejora los niveles de seguridad de la información en una municipalidad de Lima, 2026. **Objetivos específicos:** Determinar en qué medida la ISO 27001 mejora la confidencialidad de la información en una municipalidad de Lima, 2026. Determinar en qué medida la ISO 27001 mejora la integridad de la información en una municipalidad de Lima, 2026. Determinar en qué medida la ISO 27001 mejora la disponibilidad de la información en una municipalidad de Lima, 2026.	**Hipótesis general:** H1: La aplicación de la norma ISO 27001 permitirá mejorar los niveles de seguridad de la información en una municipalidad de Lima durante el año 2026. H0: La aplicación de la norma ISO 27001 no permitirá mejorar los niveles de seguridad de la información en una municipalidad de Lima durante el año 2026. **Hipótesis específicas:** HE1: La implementación de la norma ISO 27001 mejora de manera significativa la confidencialidad de la información en una municipalidad de Lima en el año 2026. H01: La implementación de la norma ISO 27001 no mejora de manera significativa la confidencialidad de la información en una municipalidad de Lima en el año 2026. HE2: La implementación de la norma ISO 27001 mejora de manera significativa la integridad de la información en una municipalidad de Lima en el año 2026.	Variable 1: ISO 27001 Dimensiones D1: Planificar D2: Hacer D3: Verificar D4: Actuar Variable 2: Seguridad de la información D1: Confidencialidad de la Información D2: Integridad de los Datos D3: Disponibilidad de la Información	Enfoque: Cuantitativo Tipo: Aplicada Diseño: Experimental Población: 93 controles Muestra: 15 controles Técnica: Observación Instrumento: Ficha de observación Técnica de análisis de datos: Estadística descriptiva e inferencial.

		H02: La implementación de la norma ISO 27001 no mejora de manera significativa la integridad de la información en una municipalidad de Lima en el año 2026. HE3: La implementación de la norma ISO 27001 mejora de manera significativa la disponibilidad de la información en una municipalidad de Lima en el año 2026. H03: La implementación de la norma ISO 27001 no mejora de manera significativa la disponibilidad de la información en una municipalidad de Lima en el año 2026. disponibilidad de la información en la municipalidad de Lima.		

Anexo 2: Matriz de operacionalización de variables

Variable 1: ISO 27001

VARIABLE	DIMENSIONES	INDICADORES	TECNICA	INSTRUMENTO	ESCALA
VI: ISO 27001	Planificar	Porcentaje de planes aprobados **Fórmula** **PPA = (PTA/PTE) * 100** Donde: PPA= Porcentaje de planes aprobados PTA= Planes de trabajo aprobados PTE= Planes de trabajo elaborados	Observación	Ficha de observación	Porcentaje 0%-50% Bajo 51%-90% En proceso 91%-100% Bueno
	Hacer	Porcentajes de planes ejecutados **Fórmula:** **PPE = (PE/PA) * 100** Donde: PPE = Porcentajes de planes ejecutados PE = Planes ejecutados PA= Planes aprobados	Observación	Ficha de observación	Porcentaje 0%-50% Bajo 51%-90% En proceso 91%-100% Bueno
	Verificar	Porcentaje de planes revisados **Fórmula:** Donde: **PPR = (PR/PA) * 100** PPR= Porcentaje de planes revisados PR=Planes revisados	Observación	Ficha de observación	Porcentaje 0%-50% Bajo 51%-90% En proceso 91%-100% Bueno

		PA=Planes aprobados			
	Actuar	Porcentaje de controles difundidos **Fórmula:** **PCD = (CD/CR) * 100** Donde: PCD= Porcentaje de controles difundidos CD=Controles difundidos CR= Controles resultantes	Observación	Ficha de observación	Porcentaje 0%-50% Bajo 51%-90% En proceso 91%-100% Bueno

Variable 2: Seguridad de la Información

VARIABLE	DIMENSIONES	INDICADORES	TECNICAS	INSTRUMENTOS	ESCALA
VD: Seguridad de la información	Confidencialidad de la Información	Nivel de confidencialidad de la información **Fórmula:** **NCI = (ΣPCI / CCI)** Donde: NCI = Nivel de confidencialidad de la información ΣPCI = Sumatoria de puntaje de confidencialidad de la información CCI = Cantidad de controles implementados de confidencialidad de la información	Observación	Ficha de observación	Escala ordinal
	Integridad de los Datos	Nivel de integridad de datos **Fórmula:** **NID = (ΣPID/CID)** Donde: NID = Nivel de integridad de datos	Observación	Ficha de observación	Escala ordinal

		ΣPID = Sumatoria de puntaje de integridad de datos CID = Controles de integridad de datos			
	Disponibilidad de la Información	Nivel de disponibilidad de la información **Fórmula:** **NDI = (ΣPDI/CDI)** Donde: NDI = Nivel de disponibilidad de la información ΣPDI = Sumatoria de puntaje de disponibilidad de la información CDI = Controles de disponibilidad de la información	Observación	Ficha de observación	Escala ordinal

Anexo 3: Instrumentos de recolección de datos

FICHA DE OBSERACIÓN																									
Objetivo: Determinar el NCI, NID, NDI																									
PRETEST - VARIABLE 2 SEGURIDAD DE LA INFORMACIÓN																									
Periodo de Evaluación		DIMENSIONES, INDICADORES Y FORMULAS																							
		CONFIDENCIALIDAD Fórmula: NCI = (ΣPCI / CCI) Donde: NCI = Nivel de confidencialidad de la información ΣPCI = Sumatoria de puntaje de confidencialidad de la información CCI = Cantidad de controles implementados de confidencialidad de la información R = Puntaje de confidencialidad de la información								INTEGRIDAD Fórmula: NID = (ΣPID/CID) Donde: NID = Nivel de integridad de datos ΣPID = Sumatoria de puntaje de integridad de datos CID = Controles de integridad de datos R = Puntaje de integridad de datos								DISPONIBILIDAD Fórmula: NDI = (ΣPDI/CDI) Donde: NDI = Nivel de disponibilidad de la información ΣPDI = Sumatoria de puntaje de disponibilidad de la información CDI = Controles de disponibilidad de la información R = Puntaje de disponibilidad de la información							
FECHA	DÍAS	R1	R2	R3	R4	R5	PCI	CCI	NCI	R6	R7	R8	R9	R10	PID	CID	NID	R11	R12	R13	R14	R15	PDI	CDI	NDI
1/01/2026	D1																								
2/01/2026	D2																								
3/01/2026	D3																								
4/01/2026	D4																								
5/01/2026	D5																								
6/01/2026	D6																								
7/01/2026	D7																								
8/01/2026	D8																								
9/01/2026	D9																								
10/01/2026	D10																								
11/01/2026	D11																								
12/01/2026	D12																								
13/01/2026	D13																								
14/01/2026	D14																								
15/01/2026	D15																								
16/01/2026	D16																								
17/01/2026	D17																								
18/01/2026	D18																								
19/01/2026	D19																								
20/01/2026	D20																								
21/01/2026	D21																								
22/01/2026	D22																								
23/01/2026	D23																								
24/01/2026	D24																								
25/01/2026	D25																								

26/01/2026	D26																							
27/01/2026	D27																							
28/01/2026	D28																							
29/01/2026	D29																							
30/01/2026	D30																							
31/01/2026	D31																							

PRETEST		CONFIDENCIALIDAD Fórmula: NCI = (ΣPCI / CCI) Donde: NCI = Nivel de confidencialidad de la información ΣPCI = Sumatoria de puntaje de confidencialidad de la información CCI = Cantidad de controles implementados de confidencialidad de la información								INTEGRIDAD Fórmula: NID = (ΣPID/CID) Donde: NID = Nivel de integridad de datos ΣPID = Sumatoria de puntaje de integridad de datos CID = Controles de integridad de datos								DISPONIBILIDAD Fórmula: NDI = (ΣPDI/CDI) Donde: NDI = Nivel de disponibilidad de la información ΣPDI = Sumatoria de puntaje de disponibilidad de la información CDI = Controles de disponibilidad de la información							
FECHA	DÍAS	R1	R2	R3	R4	R5	PCI	CCI	NCI	R6	R7	R8	R9	R10	PID	CID	NID	R11	R12	R13	R14	R15	PDI	CDI	NDI
01/01/2026	D1	1	1	1	1	0	4	5	0,80	1	1	0	0	1	3	5	0,6	1	0	1	1	1	4	5	0,8
02/01/2026	D2	1	0	0	1	1	3	5	0,60	0	1	1	0	1	3	5	0,6	1	1	0	0	1	3	5	0,6
03/01/2026	D3	1	1	0	0	1	3	5	0,60	1	1	1	0	1	4	5	0,8	0	1	1	1	0	3	5	0,6
04/01/2026	D4	1	1	1	1	1	5	5	1,00	0	1	0	1	1	3	5	0,6	1	1	0	1	1	4	5	0,8
05/01/2026	D5	1	0	1	0	1	3	5	0,60	1	1	1	1	0	4	5	0,8	0	0	1	1	1	3	5	0,6
06/01/2026	D6	1	1	0	1	1	4	5	0,80	0	0	1	1	1	3	5	0,6	1	1	1	1	0	4	5	0,8
07/01/2026	D7	1	1	1	1	0	4	5	0,80	1	1	1	1	0	4	5	0,8	1	1	1	0	1	4	5	0,8
08/01/2026	D8	0	1	1	1	1	4	5	0,80	1	0	1	1	1	4	5	0,8	0	1	1	1	1	4	5	0,8
09/01/2026	D9	1	1	1	0	0	3	5	0,60	1	1	1	0	1	4	5	0,8	1	1	1	0	0	3	5	0,6
10/01/2026	D10	1	1	1	1	1	5	5	1,00	0	1	0	1	1	3	5	0,6	0	0	1	1	1	3	5	0,6
11/01/2026	D11	1	0	0	1	1	3	5	0,60	1	1	1	0	1	4	5	0,8	1	1	1	0	1	4	5	0,8
12/01/2026	D12	0	1	1	1	1	4	5	0,80	1	0	1	1	0	3	5	0,6	1	1	0	1	1	4	5	0,8
13/01/2026	D13	1	1	1	1	1	5	5	1,00	1	1	1	1	0	4	5	0,8	0	1	1	1	1	4	5	0,8
14/01/2026	D14	1	1	1	1	0	4	5	0,80	1	1	0	1	1	4	5	0,8	1	1	1	1	0	4	5	0,8
15/01/2026	D15	1	0	1	1	1	4	5	0,80	0	1	1	1	1	4	5	0,8	1	1	1	1	0	4	5	0,8
16/01/2026	D16	1	0	1	1	1	4	5	0,80	1	0	1	0	1	3	5	0,6	1	1	0	1	1	4	5	0,8
17/01/2026	D17	1	1	1	0	0	3	5	0,60	1	1	1	0	1	4	5	0,8	1	1	0	1	0	3	5	0,6
18/01/2026	D18	0	1	1	1	1	4	5	0,80	1	1	0	1	1	4	5	0,8	1	0	1	1	1	4	5	0,8
19/01/2026	D19	1	1	1	0	1	4	5	0,80	0	1	1	1	0	3	5	0,6	0	1	1	0	1	3	5	0,6
20/01/2026	D20	1	1	1	1	0	4	5	0,80	1	1	1	0	1	4	5	0,8	1	1	0	1	0	3	5	0,6
21/01/2026	D21	1	1	0	1	1	4	5	0,80	1	0	0	1	1	3	5	0,6	0	1	0	1	1	3	5	0,6
22/01/2026	D22	1	1	1	1	1	5	5	1,00	0	1	1	1	1	4	5	0,8	1	1	1	1	0	4	5	0,8
23/01/2026	D23	0	1	1	1	1	4	5	0,80	1	0	1	1	1	4	5	0,8	1	0	1	1	1	4	5	0,8
24/01/2026	D24	1	1	1	1	0	4	5	0,80	1	1	1	1	0	4	5	0,8	1	1	1	1	0	4	5	0,8
25/01/2026	D25	1	1	1	1	1	5	5	1,00	1	1	0	1	1	4	5	0,8	1	0	0	1	1	3	5	0,6
26/01/2026	D26	1	1	1	0	1	4	5	0,80	0	1	1	0	1	3	5	0,6	1	1	0	1	1	4	5	0,8
27/01/2026	D27	1	1	0	1	1	4	5	0,80	1	1	0	0	1	3	5	0,6	0	0	1	1	1	3	5	0,6
28/01/2026	D28	0	1	1	1	1	4	5	0,80	0	0	1	1	0	2	5	0,4	1	1	1	0	0	3	5	0,6
29/01/2026	D29	0	0	0	1	1	2	5	0,40	1	1	0	1	1	4	5	0,8	1	0	1	1	1	4	5	0,8
30/01/2026	D30	1	1	1	0	1	4	5	0,80	1	0	1	1	1	4	5	0,8	1	1	0	1	0	3	5	0,6
31/01/2026	D31	1	0	1	0	1	3	5	0,60	1	1	0	0	1	3	5	0,6	0	1	1	0	1	3	5	0,6

FICHA DE OBSERACIÓN

Objetivo: Determinar el NCI, NID, NDI

POSTEST- VARIABLE 2 SEGURIDAD DE LA INFORMACIÓN

Periodo de Evaluación		DIMENSIONES, INDICADORES Y FORMULAS																								
		CONFIDENCIALIDAD Fórmula: NCI = (ΣPCI / CCI) Donde: NCI = Nivel de confidencialidad de la información ΣPCI = Sumatoria de puntaje de confidencialidad de la información CCI = Cantidad de controles implementados de confidencialidad de la información R = Puntaje de confidencialidad de la información								INTEGRIDAD Fórmula: NID = (ΣPID/CID) Donde: NID = Nivel de integridad de datos ΣPID = Sumatoria de puntaje de integridad de datos CID = Controles de integridad de datos R = Puntaje de integridad de datos								DISPONIBILIDAD Fórmula: NDI = (ΣPDI/CDI) Donde: NDI = Nivel de disponibilidad de la información ΣPDI = Sumatoria de puntaje de disponibilidad de la información CDI = Controles de disponibilidad de la información R = Puntaje de disponibilidad de la información							
FECHA	DÍAS	R1	R2	R3	R4	R5	PCI	CCI	NCI	R6	R7	R8	R9	R10	PID	CID	NID	R11	R12	R13	R14	R15	PDI	CDI	NDI
1/02/2026	D1																								
2/02/2026	D2																								
3/02/2026	D3																								
4/02/2026	D4																								
5/02/2026	D5																								
6/02/2026	D6																								
7/02/2026	D7																								
8/02/2026	D8																								
9/02/2026	D9																								
10/02/2026	D10																								
11/02/2026	D11																								
12/02/2026	D12																								
13/02/2026	D13																								
14/02/2026	D14																								
15/02/2026	D15																								
16/02/2026	D16																								
17/02/2026	D17																								
18/02/2026	D18																								
19/02/2026	D19																								
20/02/2026	D20																								
21/02/2026	D21																								
22/02/2026	D22																								
23/02/2026	D23																								
24/02/2026	D24																								
25/02/2026	D25																								

26/02/2026	D26																							
27/02/2026	D27																							
28/02/2026	D28																							
01/03/2026	D29																							
02/03/2026	D30																							
03/03/2026	D31																							

POSTEST		CONFIDENCIALIDAD Fórmula: NCI = (ΣPCI / CCI) Donde: NCI = Nivel de confidencialidad de la información ΣPCI = Sumatoria de puntaje de confidencialidad de la información CCI = Cantidad de controles implementados de confidencialidad de la información								INTEGRIDAD Fórmula: NID = (ΣPID/CID) Donde: NID = Nivel de integridad de datos ΣPID = Sumatoria de puntaje de integridad de datos CID = Controles de integridad de datos								DISPONIBILIDAD Fórmula: NDI = (ΣPDI/CDI) Donde: NDI = Nivel de disponibilidad de la información ΣPDI = Sumatoria de puntaje de disponibilidad de la información CDI = Controles de disponibilidad de la información							
FECHA	DÍAS	R1	R2	R3	R4	R5	PCI	CCI	NCI	R6	R7	R8	R9	R10	PID	CID	NID	R11	R12	R13	R14	R15	PDI	CDI	NDI
01/02/2026	D1	0	0	1	0	0	1	5	0,20	1	0	0	0	1	2	5	0,4	1	1	1	0	0	3	5	0,6
02/02/2026	D2	0	0	1	1	0	2	5	0,40	0	1	0	1	0	2	5	0,4	0	0	0	0	1	1	5	0,2
03/02/2026	D3	0	1	1	0	1	3	5	0,60	1	0	0	0	1	2	5	0,4	1	0	0	0	1	2	5	0,4
04/02/2026	D4	0	1	1	0	1	3	5	0,60	0	1	1	0	0	2	5	0,4	0	1	0	1	0	2	5	0,4
05/02/2026	D5	0	0	0	1	0	1	5	0,20	0	0	1	1	1	3	5	0,6	0	1	1	0	1	3	5	0,6
06/02/2026	D6	0	1	1	1	0	3	5	0,60	1	0	1	0	1	3	5	0,6	0	0	1	1	0	2	5	0,4
07/02/2026	D7	1	0	0	1	1	3	5	0,60	0	1	1	1	0	3	5	0,6	0	1	0	0	1	2	5	0,4
08/02/2026	D8	0	0	1	0	0	1	5	0,20	0	1	1	0	0	2	5	0,4	0	0	1	0	0	1	5	0,2
09/02/2026	D9	1	1	0	0	0	2	5	0,40	1	0	0	0	0	1	5	0,2	0	1	0	0	1	2	5	0,4
10/02/2026	D10	0	0	0	0	1	1	5	0,20	0	0	0	0	1	1	5	0,2	1	0	0	0	0	1	5	0,2
11/02/2026	D11	1	1	0	0	0	2	5	0,40	0	1	0	0	1	2	5	0,4	0	0	1	0	1	2	5	0,4
12/02/2026	D12	0	0	1	0	1	2	5	0,40	1	0	0	0	0	1	5	0,2	1	0	0	0	0	1	5	0,2
13/02/2026	D13	0	0	1	0	1	2	5	0,40	0	0	1	0	1	2	5	0,4	0	1	1	0	0	2	5	0,4
14/02/2026	D14	0	0	0	1	0	1	5	0,20	1	0	0	1	0	2	5	0,4	0	0	1	0	1	2	5	0,4
15/02/2026	D15	1	0	0	0	0	1	5	0,20	0	0	0	0	1	1	5	0,2	0	0	0	1	0	1	5	0,2
16/02/2026	D16	0	0	0	1	0	1	5	0,20	1	0	1	0	0	2	5	0,4	0	0	0	1	1	2	5	0,4
17/02/2026	D17	0	1	1	0	0	2	5	0,40	0	1	0	0	1	2	5	0,4	1	0	1	0	0	2	5	0,4
18/02/2026	D18	0	0	0	1	1	2	5	0,40	0	1	0	1	0	2	5	0,4	0	0	0	0	1	1	5	0,2
19/02/2026	D19	0	0	1	1	0	2	5	0,40	0	0	1	0	0	1	5	0,2	0	1	0	0	0	1	5	0,2
20/02/2026	D20	0	0	0	0	1	1	5	0,20	1	1	0	0	0	2	5	0,4	0	1	0	0	1	2	5	0,4
21/02/2026	D21	1	0	0	0	1	2	5	0,40	1	0	0	0	1	2	5	0,4	1	0	0	0	1	2	5	0,4
22/02/2026	D22	0	1	0	0	0	1	5	0,20	0	0	0	0	1	1	5	0,2	0	1	0	0	0	1	5	0,2
23/02/2026	D23	1	0	1	0	0	2	5	0,40	0	0	0	1	0	1	5	0,2	0	0	0	1	0	1	5	0,2
24/02/2026	D24	0	0	0	1	0	1	5	0,20	1	1	0	0	0	2	5	0,4	1	0	0	0	1	2	5	0,4
25/02/2026	D25	0	0	0	0	1	1	5	0,20	0	1	0	0	0	1	5	0,2	0	1	0	0	0	1	5	0,2
26/02/2026	D26	0	1	0	0	1	2	5	0,40	0	0	0	0	1	1	5	0,2	0	1	0	0	1	2	5	0,4
27/02/2026	D27	1	0	0	1	0	2	5	0,40	0	1	1	0	0	2	5	0,4	1	0	0	1	0	2	5	0,4
28/02/2026	D28	1	0	0	0	1	2	5	0,40	0	1	0	0	0	1	5	0,2	0	1	0	0	1	2	5	0,4
01/03/2026	D29	0	0	1	0	0	1	5	0,20	1	0	1	0	0	2	5	0,4	1	0	0	0	0	1	5	0,2
02/03/2026	D30	1	0	0	0	0	1	5	0,20	0	0	1	0	0	1	5	0,2	0	0	0	1	1	2	5	0,4
03/03/2026	D31	0	1	1	0	0	2	5	0,40	0	1	0	0	0	1	5	0,2	1	0	0	1	0	2	5	0,4

Anexo 4: Validez del instrumento

"ISO 27001 para mejorar la seguridad de la información en una Municipalidad de Lima, 2026."

N°	Dimensiones / items	Pertinencia 1		Relevancia 2		Claridad 3		Sugerencias
Variable 2: Seguridad de la Información								
DIMENSIÓN 1: Confidencialidad de la información		Sí	No	Sí	No	Sí	No	
1	Nivel de confidencialidad de la información **NCI = (ΣPCI / CCI)**	Sí		Sí		Sí		
DIMENSIÓN 2: Integridad de los datos		Sí	No	Sí	No	Sí	No	
2	Nivel de integridad de datos **NID = (ΣPID/CID)**	Sí		Sí		Sí		
DIMENSIÓN 3: Disponibilidad de la información		Sí	No	Sí	No	Sí	No	
3	Nivel de disponibilidad de la información **NDI = (ΣPDI/CDI)**	Sí		Sí		Sí		

NCI = Nivel de confidencialidad de la información
ΣPCI = Sumatoria de puntaje de confidencialidad de la información
CCI = Cantidad de controles implementados de confidencialidad de la información
NID = Nivel de integridad de datos
ΣPID = Sumatoria de puntaje de integridad de datos
CID = Controles de integridad de datos
NDI = Nivel de disponibilidad de la información
ΣPDI = Sumatoria de puntaje de disponibilidad de la información
CDI = Controles de disponibilidad de la información

[1] **Pertinencia**: el ítem corresponde al concepto teórico formulado.

[2] **Relevancia**: el ítem es apropiado para representar al componente o dimensión específica del constructo.

[3] **Claridad**: se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo.

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

Observaciones (precisar si hay suficiencia):

Opinión de aplicabilidad:

Aplicable [x]

Aplicable después de corregir [ ]

No aplicable [ ]

Apellidos y nombres del juez validador: Dr./Mg. Girao Silva Daves

DNI: 42259042

Especialidad del validador:

.....27.... de .....01..... de 2026

Firma

"ISO 27001 para mejorar la seguridad de la información en una Municipalidad de Lima, 2026."

N°	Dimensiones / items	Pertinencia $_1$		Relevancia $_2$		Claridad $_3$		Sugerencias
Variable 2: Seguridad de la Información								
DIMENSIÓN 1: Confidencialidad de la información		Sí	No	Sí	No	Sí	No	
1	Nivel de confidencialidad de la información **NCI = (ΣPCI / CCI)**	Sí		Sí		Sí		
DIMENSIÓN 2: Integridad de los datos		Sí	No	Sí	No	Sí	No	
2	Nivel de integridad de datos **NID = (ΣPID/CID)**	Sí		Sí		Sí		
DIMENSIÓN 3: Disponibilidad de la información		Sí	No	Sí	No	Sí	No	
3	Nivel de disponibilidad de la información **NDI = (ΣPDI/CDI)**	Sí		Sí		Sí		

NCI = Nivel de confidencialidad de la información
ΣPCI = Sumatoria de puntaje de confidencialidad de la información
CCI = Cantidad de controles implementados de confidencialidad de la información
NID = Nivel de integridad de datos
ΣPID = Sumatoria de puntaje de integridad de datos
CID = Controles de integridad de datos
NDI = Nivel de disponibilidad de la información
ΣPDI = Sumatoria de puntaje de disponibilidad de la información
CDI = Controles de disponibilidad de la información

[1] **Pertinencia:** el ítem corresponde al concepto teórico formulado.

[2] **Relevancia:** el ítem es apropiado para representar al componente o dimensión específica del constructo.

[3] **Claridad:** se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo.

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

Observaciones (precisar si hay suficiencia):

Opinión de aplicabilidad:

Aplicable [x]

Aplicable después de corregir [ ]

No aplicable [ ]

Apellidos y nombres del juez validador: Dr./Mg. Cordova Forero Julio Alfredo

DNI: 09924829

Especialidad del validador:

.....27.... de .....01..... de 2026

Firma

"ISO 27001 para mejorar la seguridad de la información en una Municipalidad de Lima, 2026."

N°	Dimensiones / items	Pertinencia $_1$		Relevancia $_2$		Claridad $_3$		Sugerencias
Variable 2: Seguridad de la Información								
DIMENSIÓN 1: Confidencialidad de la información		Sí	No	Sí	No	Sí	No	
1	Nivel de confidencialidad de la información **NCI = (ΣPCI / CCI)**	Sí		Sí		Sí		
DIMENSIÓN 2: Integridad de los datos		Sí	No	Sí	No	Sí	No	
2	Nivel de integridad de datos **NID = (ΣPID/CID)**	Sí		Sí		Sí		
DIMENSIÓN 3: Disponibilidad de la información		Sí	No	Sí	No	Sí	No	
3	Nivel de disponibilidad de la información **NDI = (ΣPDI/CDI)**	Sí		Sí		Sí		

NCI = Nivel de confidencialidad de la información
ΣPCI = Sumatoria de puntaje de confidencialidad de la información
CCI = Cantidad de controles implementados de confidencialidad de la información
NID = Nivel de integridad de datos
ΣPID = Sumatoria de puntaje de integridad de datos
CID = Controles de integridad de datos
NDI = Nivel de disponibilidad de la información
ΣPDI = Sumatoria de puntaje de disponibilidad de la información
CDI = Controles de disponibilidad de la información

[1] **Pertinencia:** el ítem corresponde al concepto teórico formulado.

[2] **Relevancia:** el ítem es apropiado para representar al componente o dimensión específica del constructo.

[3] **Claridad:** se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo.

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

Observaciones (precisar si hay suficiencia):

Opinión de aplicabilidad:

Aplicable [X]

Aplicable después de corregir [ ]

No aplicable [ ]

Apellidos y nombres del juez validador: Mg. Quiroz Guevara, Jorge Luis

DNI: 44363891

Especialidad del validador: Ingeniería de Sistemas, Especialista en Ciberseguridad IT/OT – Data Privacy: Certificado como ISO 22301 LA/LI, ISO 27001 LA, CSFPC, CSAPC, ECSA, API Security Architect, Fortinet NSE 2, Qualys PCI Compliance Specialist.

27 de enero de 2026

Firma

Anexo 5: Informe del asesor de Turnitin

PROYECTO-DE-TESIS-ISO27001-2026-CORREGIDO.docx

Tesis 2025-2

Tesis 2025-2

Universidad Wiener

Detalles del documento

Identificador de la entrega
trn:oid:::14912:573323515

Fecha de entrega
30 mar 2026, 11:21 p.m. GMT-5

Fecha de descarga
30 mar 2026, 11:27 p.m. GMT-5

Nombre del archivo
PROYECTO-DE-TESIS-ISO27001-2026-CORREGIDO.docx

Tamaño del archivo
1.0 MB

63 páginas

14.335 palabras

80.338 caracteres

13% Similitud general

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

Filtrado desde el informe

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

Fuentes principales

10% Fuentes de Internet
3% Publicaciones
10% Trabajos entregados (trabajos del estudiante)

Marcas de integridad

N.º de alerta de integridad para revisión

Caracteres reemplazados
52 caracteres sospechosos en N.º de páginas
Las letras son intercambiadas por caracteres similares de otro alfabeto.

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

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

Anexo 6: Carta de aceptación de la empresa

MUNICIPALIDAD DE LIMA

CONSTANCIA DE AUTORIZACIÓN

Yo, Rafael López Aliaga Cazorla identificado con DNI N° 07845838, en mi calidad de alcalde de la Municipalidad Metropolitana de Lima, con RUC 20131380951, ubicado en Jr. Rufino Torrico Nro. 1178 Cercado de Lima, otorgo la siguiente autorización:

A la señorita Nelyda Zegarra Chamorro, identificada con DNI N° 70332032 de la Carrera Profesional de Ingeniería de Sistemas e Informática de la Universidad Privada Norbert Wiener que realiza la investigación titulada "ISO 27001 para mejorar la seguridad de la información en una Municipalidad de Lima" para que se le proporcione la información necesaria y se autorice la difusión de los resultados obtenidos, con la finalidad de desarrollar su investigación con fines académicos.

Indicar si representante autoriza:

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

(X) Mencionar el nombre de la institución.

Lima, 11 de Junio de 2025

MUNICIPALIDAD METROPOLITANA DE LIMA

RAFAEL LÓPEZ ALIAGA CAZORLA
Alcalde

MUNICIPALIDAD DE LIMA

Lima, 05 de Junio de 2025

Señor (a)

Rafael López Aliaga Cazorla

Alcalde
Presente. -

Ref. Solicitud de autorización para realizar mi tesis en la Municipalidad de Lima

De mi consideración:

Me es grato dirigirme a usted para saludarlo y presentarme como bachiller la carrera de Ingeniería de Sistemas e Informática con la finalidad de solicitarle su permiso para realizar mi investigación de pregrado en la Municipalidad Metropolitana de Lima que usted dirige, cuyo título es ISO 27001 para mejorar la seguridad de la información en una Municipalidad de Lima, el objetivo es determinar en qué medida la ISO 27001 mejora los niveles de seguridad de la información en una municipalidad de Lima. Asimismo, solicito se me brinde acceso a la empresa con fines de obtener información que me permite desarrollar adecuadamente el proyecto, el cual contribuirá con un aporte positivo a su organización.

Agradeciendo su atención.

Atentamente,

.....
Firma
Nelyda Zegarra Chamorro
DNI: 70332032

Municipalidad Metropolitana de Lima
La Secretaría General del Concejo certifica que el presente documento es copia fiel del original.
06 JUN 2025
YOLANDA FALCON LIZARASO
Secretaria General del Concejo

Lima, 05 de Junio de 2025

Señor (a)

Rafael López Aliaga Cazorla

Alcalde
Presente. -

Ref. Solicitud de autorización para realizar mi tesis en la Municipalidad de Lima

De mi consideración:

Me es grato dirigirme a usted para saludarlo y presentarme como bachiller la carrera de Ingeniería de Sistemas e Informática con la finalidad de solicitarle su permiso para realizar mi investigación de pregrado en la Municipalidad Metropolitana de Lima que usted dirige, cuyo título es ISO 27001 para mejorar la seguridad de la información en una Municipalidad de Lima, el objetivo es determinar en qué medida la ISO 27001 mejora los niveles de seguridad de la información en una municipalidad de Lima. Asimismo, solicito se me brinde acceso a la empresa con fines de obtener información que me permite desarrollar adecuadamente el proyecto, el cual contribuirá con un aporte positivo a su organización.

Agradeciendo su atención.

Atentamente,

.....
Firma
Juan Bryan Aquino Conde
DNI: 76411104

Municipalidad Metropolitana de Lima
La Secretaria General del Concejo certifica que el presente documento es copia fiel del original.
06 JUN 2025
YOLANDA FALCON LIZARASO
Secretaria General del Concejo

MUNICIPALIDAD DE LIMA

CONSTANCIA DE AUTORIZACIÓN

Yo, Rafael López Aliaga Cazorla identificado con DNI N° 07845838, en mi calidad de alcalde de la Municipalidad Metropolitana de Lima, con RUC 20131380951, ubicado en Jr. Rufino Torrico Nro. 1178 Cercado de Lima, otorgo la siguiente autorización:

Al Sr. Juan Bryan Aquino Conde, identificado con DNI N° 76411104 de la Carrera Profesional de Ingeniería de Sistemas e Informática de la Universidad Privada Norbert Wiener que realiza la investigación titulada "ISO 27001 para mejorar la seguridad de la información en una Municipalidad de Lima" para que se le proporcione la información necesaria y se autorice la difusión de los resultados obtenidos, con la finalidad de desarrollar su investigación con fines académicos.

Indicar si representante autoriza:
( ) Mantener en reserva el nombre o cualquier distintivo de la institución o
(X) Mencionar el nombre de la institución.

Lima, 11 de Junio de 2025

MUNICIPALIDAD METROPOLITANA DE LIMA
RAFAEL LÓPEZ ALIAGA CAZORLA
Alcalde

MUNICIPALIDAD DE LIMA

Anexo 7: Controles de ISO/IEC 27001:2022 agrupados según los tres pilares de la seguridad de la información (93 controles)

Pilar	Código del control	Nombre del control (ISO/IEC 27001:2022)	Referencia
Confidencialidad	A.5.5	Acuerdos de confidencialidad o no divulgación	ISO/IEC (2022)
	A.5.12	Clasificación de la información	
	A.5.13	Etiquetado de la información	
	A.5.14	Transferencia de la información	
	A.5.15	Políticas de control de acceso	
	A.5.16	Gestión de identidades	
	A.5.17	Derechos de acceso de usuarios	
	A.5.18	Control de acceso a la información	
	A.5.19	Control de acceso a redes	
	A.5.20	Uso aceptable de activos	
	A.5.22	Privacidad y protección de datos personales	
	A.5.23	Seguridad en uso de servicios en la nube	
	A.5.34	Seguridad y privacidad en relaciones con proveedores	
	A.6.1	Verificación de antecedentes	
	A.6.3	Concientización en seguridad de la información	
	A.6.7	Uso de dispositivos móviles	
	A.6.8	Comunicación y reporte de debilidades en seguridad	
	A.7.4	Zona de trabajo segura	
Integridad	A.5.3	Segregación de funciones	Moura & Serrano (2023)
	A.5.4	Gestión de responsabilidades tras cambios laborales	
	A.5.8	Seguridad de la información en la cadena de suministro	
	A.5.9	Seguridad en proyectos	
	A.5.10	Aceptación de seguridad en proyectos	
	A.5.28	Protección contra código malicioso	
	A.5.30	Registro de actividades	
	A.5.31	Protección de registros	
	A.5.36	Gestión de vulnerabilidades técnicas	
	A.6.2	Términos y condiciones de empleo	
	A.6.4	Responsabilidades disciplinarias	
	A.7.7	Eliminación segura o reubicación de activos	
	A.8.2	Gestión de cambios	
	A.8.4	Separación de entornos de desarrollo, prueba y producción	
	A.8.14	Seguridad en servicios de red	
	A.8.15	Seguridad en aplicaciones	
	A.8.16	Principios de desarrollo seguro	
	A.8.17	Seguridad en pruebas de software	

Disponibilidad	A.5.24	Planificación de la continuidad de la seguridad de la información	Hernández & Pérez (2024)
	A.5.25	Implementación de la continuidad de la seguridad de la información	
	A.5.26	Evaluación de la continuidad de la seguridad de la información	
	A.5.27	Redundancia	
	A.5.29	Copias de seguridad	
	A.5.32	Sincronización de relojes	
	A.6.6	Teletrabajo	
	A.7.1	Seguridad perimetral física	
	A.7.2	Controles físicos de entrada	
	A.7.3	Seguridad en oficinas, salas e instalaciones	
	A.7.5	Protección contra amenazas físicas y ambientales	
	A.7.6	Seguridad de equipos	
	A.7.9	Seguridad en áreas públicas	
	A.7.10	Control de entrega y carga	
	A.7.11	Protección contra interrupciones de energía	
	A.7.12	Protección contra agua y riesgos ambientales	
	A.7.13	Control de temperatura y humedad	
	A.7.14	Protección contra incendios	
	A.8.1	Procedimientos operativos documentados	
	A.8.3	Capacidad de los sistemas	
	A.8.5	Instalación de software en sistemas operativos	
	A.8.6	Controles contra software malicioso	
	A.8.7	Copias de seguridad de la información	
	A.8.8	Registro de eventos	
	A.8.10	Supervisión de actividades	
	A.8.11	Seguridad de sistemas operativos	
	A.8.12	Gestión de vulnerabilidades	
	A.8.13	Seguridad en redes	
	A.8.29	Monitoreo de servicios en la nube	
	A.8.32	Resiliencia en redes y comunicaciones	
	A.8.34	Protección de información en entornos virtualizados	

Evidencia de aplicación de controles

1. **Control de acceso:** Se elaboró el procedimiento **SGSI-PR-01 Ingreso a la instalación,** el cual detalla diversos mecanismos físicos y lógicos para proteger equipos e información ubicada dentro de la oficina.

	PROCEDIMIENTO	SGSI-PR-05
	INGRESO A LA INSTALACIONES	Versión: 01 Rev.: LTI Aprob: GG

Contenido

	PROCEDIMIENTO	SGSI-PR-05
	INGRESO A LA INSTALACIONES	Versión: 01 Rev.: LTI Aprob: GG

1. OBJETIVO

Describir las actividades necesarias para el ingreso de los trabajadores, personal visitante como proveedores o contratistas, de forma que se apliquen los requerimientos de seguridad necesarios que minimicen los riesgos y aseguren la integridad de las personas.

2. ALCANCE

Aplica a todo el personal y al personal visitante sean contratistas esporádicos, rutinarios, proveedores, que requieran ingresar a nuestras instalaciones.

3. DEFINICIONES

- **Proveedor:** aquella persona natural o jurídica que comercializa un bien o servicio.
- **Contratista:** Persona o empresa que presta servicios remunerados y realiza actividades con especificaciones establecidas, plazos y condiciones contractuales.
- **Visitante:** personal externo sea personal contratista, proveedor, personal de fiscalización, accionistas, solicitantes de visita que requieren el ingreso a instalaciones.
- **Trabajador:** Personal que tiene un contrato laboral firmado y que requiere ingreso a las instalaciones todos los días.

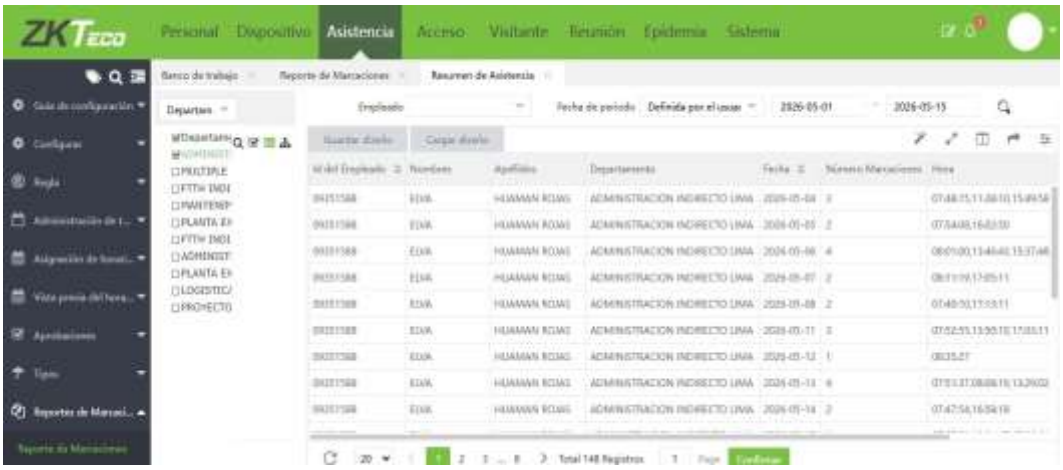
4. ABREVIATURAS

- **LTI:** Líder TI
- **ATI:** Analista TI
- **GG:** Gerente General
- **RRHH:** Recursos Humanos

Dentro del procedimiento se detalla cómo se realiza el ingreso y salida del trabajador a la oficina.

ETAPA	DESCRIPCIÓN	RESP.
Ingreso a oficina	Al ingresar a las instalaciones de la oficina administrativa, el trabajador registra su ingreso en el biométrico (ubicado al costado de la puerta). Cuando se registre el ingreso, se escuchará una notificación de acceso correcto, se mostrará la siguiente imagen en el biométrico y se podrá abrir la puerta. 	Trabajador
Salida a oficina	La puerta permanece cerrada, para salir debe presionar el pulsador de color rojo (ubicado al costado de la puerta).   Al retirarse de las instalaciones de la oficina administrativa, el trabajador debe registrar su salida en el biométrico (se encuentra al costado de la puerta). Cuando se registre la salida, se escuchará una notificación de acceso correcto, se mostrará la siguiente imagen en el biométrico.	Trabajador

Los registros del ingreso y salida del biométrico se almacenan en el software Biotime 8.0 que permite gestionar asistencia, control de acceso, entre otras.



2. **Restricción de acceso a la información:** Se elaboró el procedimiento **SGSI-PR-02 Control de acceso,** el cual detalla cómo proteger los sistemas de información.

CONTENIDO

Dentro del procedimiento se detalla cómo se solicita el acceso a los sistemas de información

	PROCEDIMIENTO	SGSI-PR-02
	CONTROL DE ACCESO	Versión: 01 Rev.: LTI Aprob: GG

Seguridad para todo el personal

ETAPA	DESCRIPCIÓN	RESP.
Seguridad para el personal	Para el control de acceso los sistemas de información, se envía un correo electrónico al Líder TI se debe cumplir lo siguiente: • Asignar un nombre de usuario a solicitud del líder de área o RRHH. Los datos mínimos para atender la solicitud son: • Nombre y Apellido, • N° DNI o N° CE (éste no es necesario para la creación de correo corporativo) • Cargo para ocupar en la empresa. (solo es necesario para la creación de correo corporativo) • Luego de la verificación de los datos se crea el usuario con su primer nombre y apellido para dar acceso a los sistemas de información como correo corporativo. • La contraseña del usuario se da solo a la persona que se le creó y de acuerdo con los lineamientos básicos para entrega de credenciales de acceso del **Procedimiento de credenciales de acceso.** • Deshabilitar, modificar contraseña o borrar los usuarios correspondientes del correo electrónico corporativo al personal que ya no tenga relación. • Realizar revisiones periódicas en los diferentes sistemas, para garantizar que se remuevan los usuarios deshabilitados o redundantes, una vez al año.	LTI/ ATI

Solicitud para creación de correo corporativo.

INGRESO DE PERSONAL NUEVO

J. A.C
para Juan

Informarles que el siguiente personal ya realizó la firma de contrato e inicia sus labores el día de hoy 05/05/2026

DATOS	
NOMBRE COMPLETO:	RAUL JOSE PEREZ TELLO
DNI:	77015822
FECHA DE NACIMIENTO:	10/03/2001
CARGO:	SUPERVISOR
SEDE:	LIMA
PROYECTO:	ADMINISTRATIVO DIRECTO

Su apoyo con la creación del correo corporativo.
Saludos.

3. **Políticas de seguridad de la información:** Se elaboró la política de seguridad de la información**,** el cual detalla los compromisos de la organización.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Se establece principios y directrices para asegurar la confidencialidad, integridad y disponibilidad de la información. Esta política forma parte del Sistema de Gestión de Seguridad de la Información (SGSI), conforme a la ISO 27001:2022.

Asegurándonos de implementar y ejecutar el SGSI asumimos los siguientes compromisos:

1. Definir y cumplir con los roles y responsabilidades de seguridad de la información.
2. Proteger la información conforme a su sensibilidad y criticidad.
3. Cumplir con las normativas vigentes y demás disposiciones aplicables en materia de seguridad de la información.
4. Gestionar riesgos, amenazas y reaccionar ante eventos que puedan afectar la seguridad de la información.
5. Implementar controles lógicos y físicos para resguardar la información y protejan la integridad de las personas.
6. Asegurar que los eventos de seguridad de la información deben ser reportados oportunamente y adoptar acciones preventivas y correctivas que correspondan.
7. Buscar la mejora continua del SGSI de acuerdo con los requisitos de la norma ISO 27001:2022 que hemos adoptado en nuestra organización.
8. Promover la formación y concienciación en seguridad de la información.

Esta política es aplicable a todos los trabajadores, partes interesadas internas y externas, por lo cual se hace extensivo el compromiso de su implementación y cumplimiento.

Versión: 01

4. **Seguridad de la información para el uso de servicios en la nube:** Se elaboró la política de seguridad de la información para usuarios, el cual detalla las obligaciones de los usuarios con especial mención en la doble autenticación para proteger el correo corporativo y servicios de la nube como OneDrive y SharePoint.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA USUARIOS

Se establece obligaciones que deben cumplir todos los usuarios para proteger la información, garantizando su confidencialidad, integridad y disponibilidad, desde el puesto de trabajo físico y remoto.

- **Mesas y Pantallas Limpias:** Mantener el área de trabajo libre de documentos confidenciales y restringidos cuando no estén en uso, guardar papeles en archivadores o cajones cerrados y bloquear la pantalla al ausentarse. No dejar credenciales visibles ni notas con contraseñas.
- **Almacenamiento Seguro de Información:** Guardar la información únicamente en los repositorios corporativos: OneDrive y SharePoint de la organización. Se prohíbe almacenar información en dispositivos personales o nubes externas no aprobadas.
- **Clasificación y Manejo de Información:** Aplicar las etiquetas de clasificación cuando corresponda (confidencial y restringida) para proteger la información.
- **Gestión de Accesos y Credenciales:** No compartir credenciales (cuenta y contraseña) contraseñas, usar doble autenticación donde esté disponible y reportar inmediatamente accesos sospechosos.
- **Correo y Mensajería:** No abrir enlaces o adjuntos sospechosos; verificar remitentes.
- **Dispositivos móviles:** Son de uso exclusivo para actividades laborales. Todo retiro de equipos fuera de la oficina debe ser informado y autorizado por el responsable de área designado.
- **Eventos de Seguridad:** Reportar inmediatamente cualquier evento que comprometa la confidencialidad, integridad o disponibilidad (pérdida de datos, accesos no autorizados, fuga de información, etc.) al canal oficial de la empresa.
- **Confidencialidad y Privacidad:** No divulgar información a terceros sin autorización; cumplir los acuerdos de confidencialidad y la ley 29733 (Ley de Protección de Datos Personales).
- **Cumplimiento y Sanciones:** El incumplimiento de esta política puede derivar en acciones disciplinarias conforme a procedimientos internos y de legislación vigente.

Esta política es aplicable a todos los trabajadores, por lo cual se hace extensivo el compromiso de su cumplimiento.

Versión: 01
F. Aprob. 02.01.2026

5. **Eliminación de información:** Se elaboró un certificado de devolución y destrucción de información sensible para evitar que un trabajador evitar fuga de información, este control se complementa con el control copia de seguridad de la información que se ve detalla más adelante.

CERTIFICADO DE DEVOLUCIÓN Y DESTRUCCIÓN DE INFORMACIÓN SENSIBLE

Consta por el presente CERTIFICADO DE DEVOLUCIÓN Y DESTRUCCIÓN DE INFORMACIÓN SENSIBLE que el infrascrito, actuando en representación de la empresa, certifico que el trabajador que a continuación se identifica ha cumplido de forma íntegra y verificable con la devolución y/o destrucción de toda información Confidencial, Datos Personales, Datos Biométricos y demás activos de información en su poder personal, conforme a lo establecido en:

- Contrato de Trabajo suscrito el ———————————
- Adenda de Acuerdo de Confidencialidad y No Divulgación (Cláusula 9.3)
- Adenda de Consentimiento de Tratamiento de Datos Biométricos y Personales (Cláusula 5. Sección NOVENO)
- Ley N. ° 29733 (Ley de Protección de Datos Personales)
- Norma ISO/IEC 27001:2022 (Requisitos de Gestión de Seguridad de la Información)
- Norma ISO/IEC 27005:2022 (Gestión de Riesgos de Seguridad de la Información)
- Políticas de Seguridad de la Información

IDENTIFICACION

Entiéndase como información sensible a la información clasificada como interna, confidencial y restringida.

Nombres completos:					
DNI / CE:					
Cargo / Puesto					
Proyecto					
Fecha de ingreso		**Fecha de salida**			
Motivo de salida (Marque X)	**Renuncia** ☐	**Despido** ☐	**Fin contrato** ☐	**Jubilación** ☐	**Otro** ☐: _____

PROCEDIMIENTO DE "OFFBOARDING" DE SEGURIDAD DE INFORMACIÓN

A. DESTRUCCIÓN DE INFORMACIÓN SENSIBLE

El trabajador ha procedido a destruir de forma irreversible e irrecuperable toda copia, duplicado o derivado de información sensible en su poder, comprendidas en las categorías:

b. ELIMINACION SEGURA DE INFORMACION DIGITAL

Archivos locales de trabajo:	**SI** ☐	**NO** ☐	**NO APLICA** ☐
Caché de navegador / historial:	**SI** ☐	**NO** ☐	**NO APLICA** ☐
Documentos temporales:	**SI** ☐	**NO** ☐	**NO APLICA** ☐
Backups o copias de seguridad locales:	**SI** ☐	**NO** ☐	**NO APLICA** ☐
Responsable de destrucción:			

c. REVOCACIÓN DE ACCESOS A SISTEMAS

Se certifica que todos los accesos del trabajador a sistemas corporativos, bases de datos, plataformas y herramientas han sido revocados o desactivados de forma inmediata:

Correo corporativo:	**Revocado** ☐	**Eliminado** ☐	**No cuenta** ☐
VPN corporativa:	**Revocado** ☐	**Eliminado** ☐	**No cuenta** ☐
SharePoint:	**Revocado** ☐	**Eliminado** ☐	**No cuenta** ☐
Almacenamiento compartido:	**Revocado** ☐	**Eliminado** ☐	**No cuenta** ☐
Sistemas de control biométrico:	**Revocado** ☐	**Eliminado** ☐	**No cuenta** ☐
Otros sistemas: _____	**Revocado** ☐	**Eliminado** ☐	**No cuenta** ☐

B. LIMPIEZA DE DATOS BIOMÉTRICOS

Conforme a la Adenda de Consentimiento de Tratamiento de Datos Biométricos y Personales, se certifica que:

a. DATOS BIOMÉTRICOS

Huellas dactilares:	**Eliminado** ☐	**Anonimizado** ☐	**No cuenta** ☐
Fotografía corporativa:	**Eliminado** ☐	**Anonimizado** ☐	**No cuenta** ☐
Imágenes de cámara de vigilancia:	**Eliminado** ☐	**Anonimizado** ☐	**No cuenta** ☐
Responsable:			

6. **Inventario de información y otros activos asociados:** Se elaboró el procedimiento **SGSI-PR-03 Gestión TI.**

PROCEDIMIENTO

GESTIÓN TI

CONTENIDO

PROCEDIMIENTO

GESTIÓN TI

1. OBJETIVO

Establecer las actividades necesarias para la gestión de los recursos tecnológicos, soporte técnico, administración de accesos y mantenimiento de equipos informáticos utilizados en COMPCA PERÚ.

2. ALCANCE

Este procedimiento aplica a todas las personas involucradas en las actividades del proceso de tecnología de la información.

3. DEFINICIONES

- **TI**: Tecnología de la Información.
- **Sistema Helpdesk**: Es una plataforma propia mediante el cual se realiza la gestión de atención de solicitudes de incidencias o soporte técnico
- **Cpanel**: Plataforma que permite administrar correos.
- **Trabajador**: Personal que tiene un contrato laboral firmado y que requiere ingreso a las instalaciones.
- **Albarán**: Documento que especifica la entrada o salida de un dispositivo móvil.
- **GIA**: Software de gestión integral de almacenes
- **Dispositivos móviles**: Se refiere a dispositivos como portátiles (laptops), PC, smartphones.
- **IMEI**: Un código único de 15 dígitos que identifica a cada teléfono móvil a nivel mundial
- **Incidente**: Evento que se interpone en el desarrollo normal de una situación o por caso lo que se esperaba que pase.
- **Backup**: Es una copia de seguridad, es un duplicado de datos, archivos, que se guarda por separado del original para proteger la información contra pérdida o daño.
- **Hardware**: Es la parte física de una computadora o dispositivo móvil. Son todos los componentes que puedes ver y tocar, como la pantalla, el teclado, la batería, entre otros.

Dentro del procedimiento se detalla cómo se entrega un equipo informático lo cual es muy importante porque menciona como se mantiene actualizado el stock monitoreado.

Asignación y entrega de equipos informáticos o dispositivos móviles

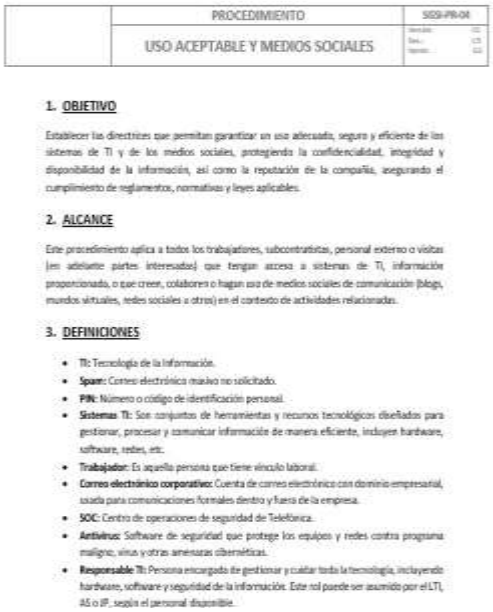
ETAPA	DESCRIPCIÓN	RESP.
Asignación	Los dispositivos móviles, equipos informáticos y/o accesorios son asignados al trabajador mediante albaranes que son generados por el software GIA, el cual detalla la descripción de los dispositivos asignados (IMEI o serie).	Responsable TI
Entrega	Los equipos informáticos o dispositivos móviles son entregados a los trabajadores, una vez se recibe el correo de RRHH del ingreso del personal.	Responsable TI
Los dispositivos móviles e informáticos son gestionados por el software GIA (Gestión Integral de Almacenes), el cual permite mantener el stock en tiempo real de equipos.		

Detalle del stock de laptops Lenovo disponibles.

7. **Protección contra malware:** Se elaboró el procedimiento **SGSI-PR-04 Uso aceptable y medios sociales,** el cual detalla el uso de antivirus en los equipos informáticos de la organización.

	PROCEDIMIENTO	SGSI-PR-04
	USO ACEPTABLE Y MEDIOS SOCIALES	

CONTENIDO



	PROCEDIMIENTO	SGSI-PR-04
	USO ACEPTABLE Y MEDIOS SOCIALES	

1. OBJETIVO

Establecer las directrices que permitan garantizar un uso adecuado, seguro y eficiente de los sistemas de TI y de los medios sociales, protegiendo la confidencialidad, integridad y disponibilidad de la información, así como la reputación de la compañía, asegurando el cumplimiento de reglamentos, normativas y leyes aplicables.

2. ALCANCE

Este procedimiento aplica a todos los trabajadores, subcontratistas, personal externo o visitas (en adelante partes interesadas) que tengan acceso a sistemas de TI, información proporcionada, o que creen, colaboren o hagan uso de medios sociales de comunicación (blogs, mundos virtuales, redes sociales u otros) en el contexto de actividades relacionadas.

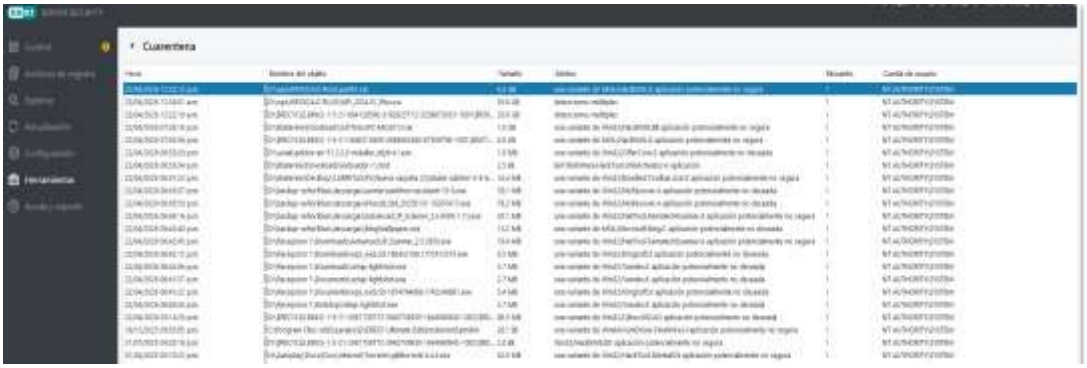
3. DEFINICIONES

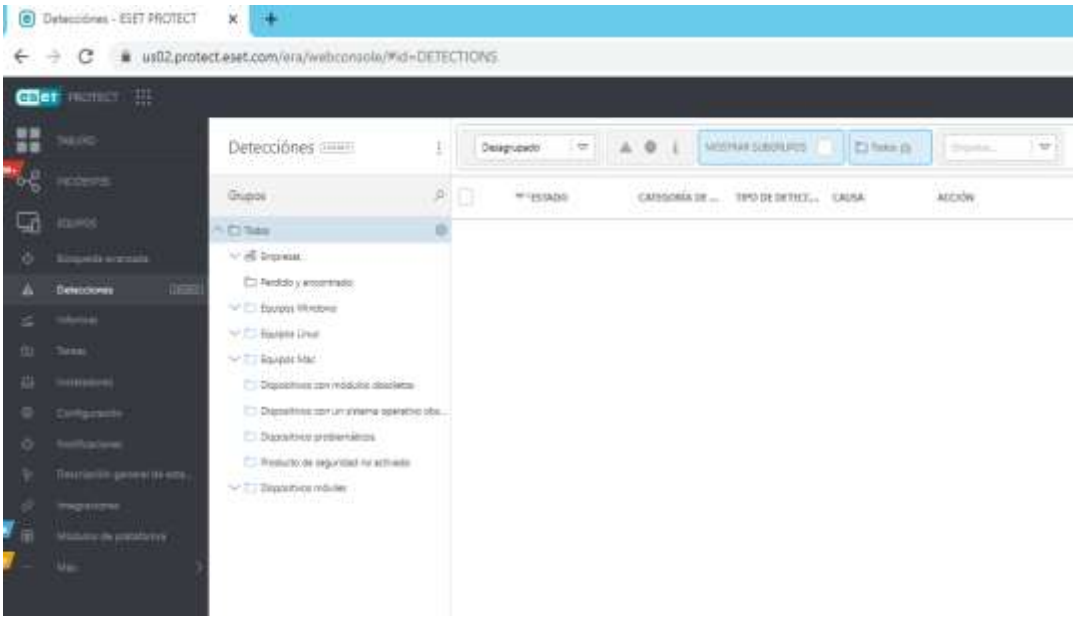
- **TI:** Tecnología de la Información.
- **Spam:** Correo electrónico masivo no solicitado.
- **PIN:** Número o código de identificación personal.
- **Sistemas TI:** Son conjuntos de herramientas y recursos tecnológicos diseñados para gestionar, procesar y comunicar información de manera eficiente, incluyen hardware, software, redes, etc.
- **Trabajador:** Es aquella persona que tiene vínculo laboral.
- **Correo electrónico corporativo:** Cuenta de correo electrónico con dominio empresarial, usada para comunicaciones formales dentro y fuera de la empresa.
- **SOC:** Centro de operaciones de seguridad de Telefónica.
- **Antivirus:** Software de seguridad que protege los equipos y redes contra programa maligno, virus y otras amenazas cibernéticas.
- **Responsable TI:** Persona encargada de gestionar y cuidar toda la tecnología, incluyendo hardware, software y seguridad de la información. Este rol puede ser asumido por el LTI, AS o IP, según el personal disponible.

Consideraciones para el uso de antivirus

ETAPA	DESCRIPCIÓN	RESP.
Consideraciones	Los dispositivos que accedan a la red deben contar con software antivirus actualizado. Se realizarán revisiones periódicas para garantizar que los dispositivos estén protegidos El software antivirus instalado debe ser capaz de detectar y eliminar virus de forma automática. El antivirus se gestiona por consola web centralizada que permite el monitoreo y administración de amenazas en tiempo real.	Trabajadores
Prohibiciones	• Eliminar o deshabilitar el software antivirus aprobado. • Intentar eliminar archivos infectados con virus o limpiar la infección, que no sea mediante el uso de software o antivirus aprobados	

A través de la consola de gestión de seguridad Antimalware, se realiza un seguimiento en tiempo real de los equipos informáticos donde se detecta y actúa inmediatamente ante las actividades sospechosas.



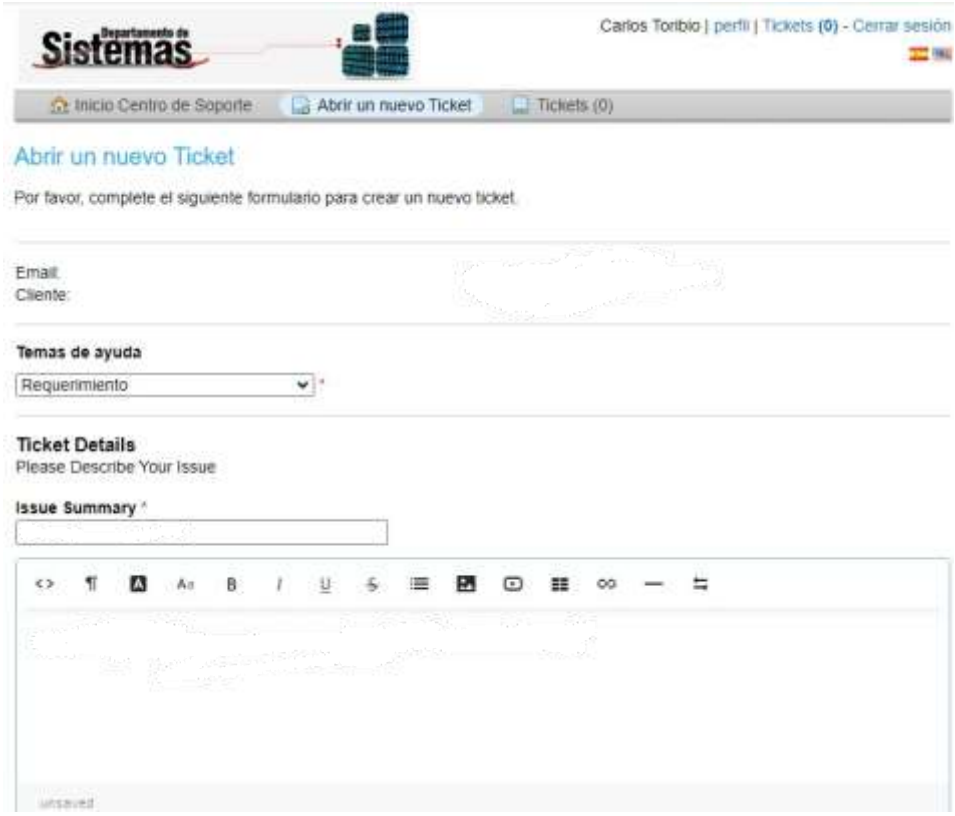


8. **Planificación y preparación de la gestión de incidentes de seguridad de la información:** En el procedimiento **SGSI-PR-03 Gestión TI** se detalla el proceso de soporte al usuario.

Soporte al usuario

ETAPA	DESCRIPCIÓN	RESP.
Solicitud	El usuario comunica el incidente de forma verbal o mediante el **Sistema de Tickets** donde se indica la necesidad del soporte, esta información decanta en el **Sistema Helpdesk**, para que sea atendida por sistemas.	Trabajador
Revisión	Los responsables visualizan el incidente en el **Sistema de Tickets,** y se diagnostica para la posible solución.	Responsable TI
Comunicación	Se coordina con el usuario para confirmar la atención a su incidencia, ya sea de forma presencial o por conexión remota (Anydesk o Supremo).	Responsable TI
Atención de incidente	Los responsables solucionan el incidente y comunican al usuario. En caso el personal de Sistemas no pueda solucionar el incidente se escala externamente.	Responsable TI
	Se actualiza el estado del incidente a atendido y se indica en la plataforma **Sistema de Tickets** un breve detalle de la atención brindada.	Responsable TI
Nota: El responsable TI también puede registrar la incidencia en el formulario de **Sistema de Tickets**		

Sistema de Tickets para gestionar las incidencias de seguridad de la información, el usuario escoge el tema de ayuda y detalla las incidencias, cada usuario tiene sus propias credenciales.



9. **Concientización, educación y capacitación en seguridad de la información:** Se elaboró el plan **SGSI-PL-01 Sensibilización en seguridad de la información**, el cual detalla los temas de las capacitaciones en temas de seguridad de la información para sensibilizar a los trabajadores.

	PLAN	SGSI-PL-01
	SENSIBILIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN	Versión: 01 Rev.: LTI Aprob: GG

CONTENIDO

	PLAN	SGSI-PL-01
	SENSIBILIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN	Versión: 01 Rev.: LTI Aprob: GG

1. OBJETIVO

El objetivo de este plan es asegurar que todos los trabajadores comprendan la importancia de proteger la información de la organización. Se busca reducir los riesgos relacionados con el factor humano y fortalecer el compromiso del personal con la seguridad de la información. Para lograrlo, se promoverá la conciencia y el conocimiento mediante capacitaciones, mensajes de correos electrónicos, intranet, página web y comunicación continua.

Este plan es una parte fundamental del Sistema de Gestión de Seguridad de la Información (SGSI) y está alineado con los requisitos de la norma internacional ISO/IEC 27001.

2. ALCANCE

Aplica a todos los trabajadores bajo cualquier modalidad de contratación, tome conciencia del valor de la información y la importancia de saber cómo protegerla frente a cualquier evento o incidente que pueda afectar su confidencialidad, integridad y/o disponibilidad.

3. DEFINICIONES

- **Sistema de Gestión de Seguridad de la Información (SGSI):** Es un enfoque sistemático, basado en la norma ISO/IEC 27001, que permite establecer, implementar, operar, supervisar, revisar, mantener y mejorar la seguridad de la información dentro de una organización. Su objetivo principal es proteger la confidencialidad, integridad y disponibilidad de la información, alineando las prácticas de seguridad con los objetivos estratégicos y comerciales.
- **Seguridad de la información:** conjunto de medidas y técnicas utilizadas para controlar y salvaguardar todos los datos que se manejan dentro de la organización y asegurar que los datos no salgan del sistema que ha establecido la organización.
- **Intranet:** Es una red privada interna que utilizan las organizaciones para compartir información, recursos y servicios entre sus empleados o miembros autorizados.
- **Página web:** Documento o conjunto de documentos digitales accesibles mediante Internet a través de un navegador, identificados por una dirección única (URL).
- **Sensibilización:** Conjunto de actividades planificadas y sistemáticas orientadas a generar conciencia, conocimiento y compromiso en los colaboradores de una

Los temas más relevantes seleccionados:

	PLAN	SGSI-PL-01
	SENSIBILIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN	Versión: 01 Rev.: LTI Aprob: GG

Etapa 2: Desarrollo

Se brindarán capacitaciones para sensibilizar en temas de seguridad de la información.

6.2.1 Capacitación

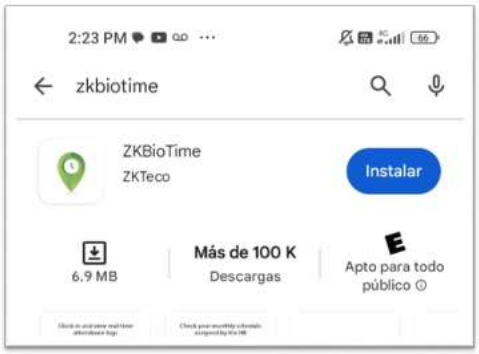
N°	CAPACITACIÓN	OBJETIVO	CANTIDAD DE CAPACITACIONES
1	Introducción a la seguridad de la información.	Sensibilizar a los usuarios en temas de seguridad de la información.	1
2	Procedimientos y políticas de seguridad de la información.	Sensibilizar a los usuarios en procedimientos y políticas de seguridad de la información.	1
3	Gestión de contraseñas	Sensibilizar a los usuarios en gestión de contraseñas.	1
4	Fraude digital y phishing	Sensibilizar a los usuarios en fraude digital y phishing.	1
5	Seguridad en el uso del correo electrónico	Sensibilizar a los usuarios en seguridad en el uso del correo electrónico	1
6	Protección de datos personales	Sensibilizar a los usuarios en protección de datos personales	1
7	Seguridad en dispositivos móviles	Sensibilizar a los usuarios en seguridad en dispositivos móviles	1
8	Navegación segura en internet	Sensibilizar a los usuarios en navegación segura en internet	1
9	Gestión de incidentes de	Sensibilizar a los usuarios en gestión de incidentes de seguridad	1

10. **Gestión de configuración:** Para mantener una correcta gestión de configuración, se guardan manuales de configuración de hardware y software, lo cual permite evitar fallas.

Manual de configuración de asistencia remota para los usuarios, cada se puede conectar al servidor de asistencia a través de la aplicación donde registra la hora de ingreso, ubicación y una fotografía de su asistencia.

MANUAL DE CONTROL DE ASISTENCIA POR APP

1. INSTALAR Y ABRIR APLICACIÓN ZKBIOTIME DE PLAYSTORE



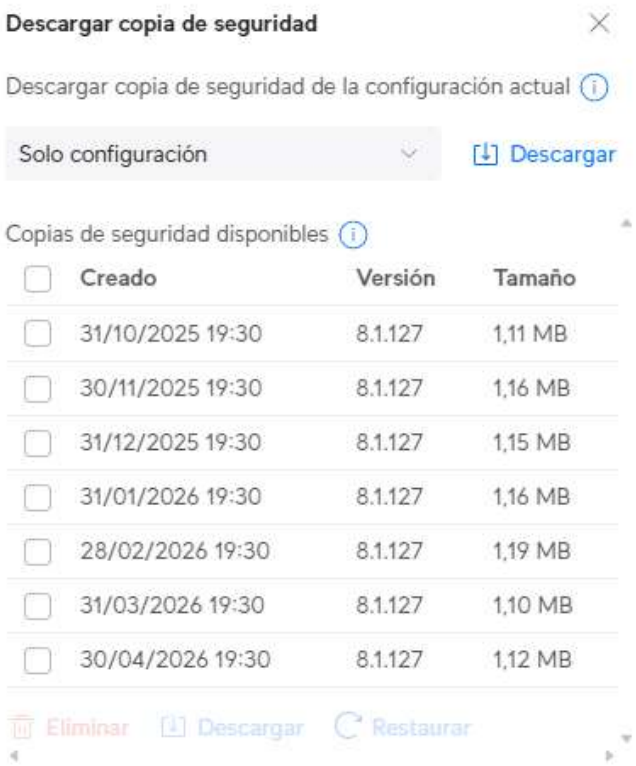
2. LA UBICACIÓN DEL MOVIL NO SE DEBE DESACTIVAR, INGRESAR A "CONFIGURACIÓN DEL SERVIDOR", COMPLETAR IGUAL QUE LA IMAGEN Y GUARDAR CAMBIOS

11. **Copia de seguridad de la información:** En el procedimiento **SGSI-PR-03 Gestión TI** se detalla el proceso de respaldo de información.

Respaldo de información

ETAPA	DESCRIPCIÓN	RESP.
Backups	La información interna y/o confidencial se respalda mediante las plataformas: Share Point y OneDrive. El Líder de área crea y comparte carpetas en OneDrive o SharePoint para el uso de su personal a cargo, según crea necesario y para salvaguardar la información. El servidor de archivos almacena información de las distintas áreas, la cual es actualizada por los usuarios a través de carpetas de red. Las copias de seguridad en Windows Server se realizan con una frecuencia mínima trimestral, y están a cargo del responsable TI. También es posible almacenar copias de seguridad en discos duros físicos, los cuales deben están resguardados por el responsable TI.	Responsable TI
Nota: Para los usuarios es necesario iniciar sesión en OneDrive y asegurarse de que la opción de copia de seguridad de carpetas esté activada. El Analista de Sistemas debe verificar que todas las carpetas del equipo estén seleccionadas para que la sincronización de archivos se realice automáticamente.		

Copia de seguridad del sistema de tickets, se guardan automáticamente en el servidor, las copias se realizan cada mes.



12. **Mantenimiento de equipo:** En el procedimiento **SGSI-PR-03 Gestión TI** se detalla el proceso de mantenimiento de equipos informáticos o dispositivos móviles.

Mantenimiento equipos informáticos o dispositivos móviles

ETAPA	DESCRIPCIÓN	RESP.
Verificación	Se verifica si equipos informáticos o dispositivos móviles cuentan con garantía activa. Esta verificación se realiza a través del sistema GIA y puede ser confirmada adicionalmente con el responsable de Compras.	Responsable TI
Mantenimiento	Se lleva a cabo la limpieza interna y externa del hardware, así como la optimización del software, según las necesidades detectadas durante la revisión del equipo. Los materiales y herramientas necesarios para realizar el mantenimiento son definidos por el responsable TI. En caso, el dispositivo móvil sea alquilado, el mantenimiento debe ser gestionado y coordinado directamente con el proveedor correspondiente.	Responsable TI
Registro	Los mantenimientos realizados se registran **en Formato de verificación y cumplimiento de mantenimientos de equipos informáticos.**	Responsable TI
Nota: La frecuencia mínima recomendable es una vez al año, la frecuencia puede variar según el entorno. No se realiza el mantenimiento a un dispositivo que cuente con garantía activa.		

Se visualiza el mantenimiento del gabinete del data center, que incluye la limpieza externa del servidor.

13. **Seguridad en redes:** En el procedimiento **SGSI-PR-04 Uso aceptable y medios sociales,** el cual detalla las consideraciones de internet contratado donde se menciona el uso de un firewall (físico) en la red**.**

	PROCEDIMIENTO	SGSI-PR-04
	USO ACEPTABLE Y MEDIOS SOCIALES	Versión: 01 Rev.: LTI Aprob: GG

Consideraciones del servicio de internet contratado, y correo electrónico corporativo.

ETAPA	DESCRIPCIÓN	RESP.
Uso del internet contratado y correo electrónico corporativo	El Internet y correo electrónico corporativo es de uso exclusivo para las actividades que estén relacionadas gestiones corporativas. El uso personal está permitido siempre y cuando dicho uso no afecte a su trabajo, no sea perjudicial, no incumpla ningún término ni condición laboral y no coloque al trabajador o a la organización en una situación de violación de las leyes u otras obligaciones legales. El internet cuenta con servicio de seguridad con equipo firewall gestionada por el SOC, el responsable TI en comunicación con el SOC puede bloquear el acceso a determinadas páginas de Internet para usuarios individuales, grupos de usuarios o para todos los trabajadores. Si el acceso a algunas páginas web está bloqueado, el usuario puede solicitar a su jefe inmediato o al responsable TI acceder a dichas páginas. Todos los trabajadores son responsables de sus acciones en internet y correo electrónico corporativo.	Trabajadores

Solicitud de bloqueo de páginas gestionada por el SOC (Security Operation Center).


SI SOC

Para:

Estimado cliente,
Se realizo el bloqueo solicitado en los grupos 1 y 4

URL	Type	Action	Status
www.youtube.com	Simple	Block	Enable
youtube.com/	Wildcard	Block	Enable
https://www.youtube.com/	Regular Expression	Block	Enable

3/75

Saludos,

CyberSOC - SDM | **Integratel Perú**
Tel. 0800-1660 Op. 0-1-1-1-2

14. **Redundancia de las instalaciones del procesamiento de información:** Se elaboró el plan **SGSI-PL-02 Continuidad de seguridad de la información,** el

cual que se debe realizar si ocurre una situación de riesgos así evitar minimizar el impacto.

PLAN | SGSI-PL-02
CONTINUIDAD DE SEGURIDAD DE LA INFORMACIÓN

CONTENIDO

PLAN | SGSI-PL-02
CONTINUIDAD DE SEGURIDAD DE LA INFORMACIÓN

1. INTRODUCCIÓN

Conflica debe estar preparada para prevenir, reducir, mitigar y reaccionar ante incidentes que puedan poner en riesgo los recursos y servicios TI. Por ese motivo, es necesario proteger los procesos mediante una serie de actividades planificadas que permitan la recuperación a largo plazo sin comprometer la continuidad del negocio además de disminuir las posibles consecuencias derivadas de situaciones de riesgos, reduciendo la vulnerabilidad y reduciendo la pérdida de información.

2. OBJETIVOS

Garantizar la continuidad de los procesos críticos TI en escenarios de contingencia, preservar la confidencialidad, disponibilidad e integridad de la información.

3. ALCANCE

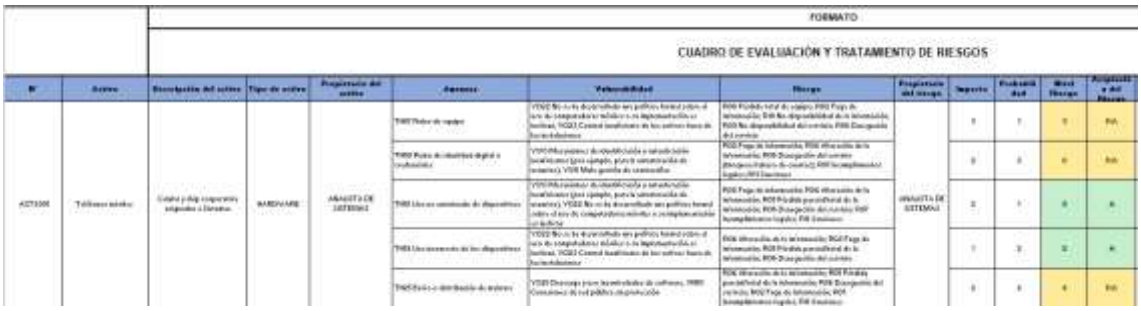
El plan de continuidad de recursos y servicios TI, inicia con la identificación de los elementos críticos y finaliza con el análisis y acciones de mejora identificadas de la reacción del personal propio, contratistas, clientes y demás partes interesadas.

Establecer las actividades preventivas y correctivas para atender de manera eficiente una situación que comprometa el normal funcionamiento de los procesos, recursos humanos, las instalaciones físicas, técnicas, operativas y de terceros, así como una crisis reputacional, cualquier eventualidad y en el menor tiempo posible restablecer los servicios y disminuir la pérdida de los recursos.

4. DOCUMENTOS DE REFERENCIA

- **ISO/IEC 27031:** Norma que proporciona directrices para la preparación de las Tecnologías de la Información y Comunicación (TIC) con el fin de garantizar la continuidad del negocio. Establece un marco para planificar, implementar y mantener estrategias que permitan responder y recuperarse ante interrupciones que afecten los sistemas de información y servicios críticos.
- **ISO/IEC 27001:** Norma internacional que proporciona un marco para proteger la confidencialidad, integridad y disponibilidad de la información mediante un Sistema de Gestión de Seguridad de la Información (SGSI).

El plan de continuidad se complementa con la evaluación y tratamiento de riesgos que nos ayudará a elaborar las medidas necesarias para mitigar los riesgos.



FORMATO

CUADRO DE EVALUACIÓN Y TRATAMIENTO DE RIESGOS

N°	Activo	Descripción del activo	Tipo de activo	Propietario del activo	Amenaza	Vulnerabilidad	Riesgo	Propietario del riesgo	Impacto	Probabilidad	Nivel Riesgo	Aceptación y del Riesgo
A27100	Teléfonos móviles	Celular y chip corporativo asignados a Directivos	HARDWARE	ANALISTA DE SISTEMAS	T1001 Robo de equipo	V1002 No se ha desarrollado una política formal sobre el uso de computadoras móviles y no implementación en terminal, V1003 Control inadecuado de los activos fuera de las instalaciones	R001 Pérdida total de equipo, R002 Fuga de información, R003 No disponibilidad de la información, R005 No disponibilidad del servicio, R006 Divulgación del servicio	ANALISTA DE SISTEMAS	3	3	9	RA
					T1002 Robo de identidad digital y credenciales	V1001 Mecanismos de identificación y autenticación inadecuados (por ejemplo, para la administración de usuarios), V1008 Mala gestión de contraseñas	R002 Fuga de información, R006 Alteración de la información, R009 Divulgación del correo (Respecto Pérdida de credenciales) R007 Incumplimiento Legales (RH Sanciones)		2	3	6	RA
					T1003 Uso no autorizado de dispositivos	V1001 Mecanismos de identificación y autenticación inadecuados (por ejemplo, para la administración de usuarios), V1002 No se ha desarrollado una política formal sobre el uso de computadoras móviles y no implementación en terminal	R002 Fuga de información, R006 Alteración de la información, R009 Pérdida parcial/total de la información, R009 Divulgación del correo, R007 Incumplimiento Legales, R08 Sanciones		2	1	2	A
					T1004 Uso inconsciente de los dispositivos	V1002 No se ha desarrollado una política formal sobre el uso de computadoras móviles y no implementación en terminal, V1003 Control inadecuado de los activos fuera de las instalaciones	R006 Alteración de la información, R002 Fuga de información, R009 Pérdida parcial/total de la información, R009 Divulgación del correo		1	2	2	A
					T1005 Error o distribución de malware	V1005 Descarga y uso inconsistentes de software, V1001 Conocimiento de red pública y desprotección	R006 Alteración de la información, R009 Pérdida parcial/total de la información, R009 Divulgación del correo, R002 Fuga de información, R07 Incumplimiento Legales, R08 Sanciones		3	3	9	RA

15. **Roles y responsabilidades de la información:** Se elaboró el **Formato de acta de designación de roles y responsabilidades,** donde se deben incluir los roles y responsabilidades de seguridad de la información.

	FORMATO	SGSI-F-01
	ACTA DE DESIGNACIÓN DE ROLES Y RESPONSABILIDADES DE SEGURIDAD DE LA INFORMACIÓN	Versión: 01 Rev.: LTI Aprob: GG

DE……:

A……:

ASUNTO……: Nombramiento del responsable de seguridad de la información

FECHA……:

Se comunica que, como parte del compromiso de la Política de Seguridad de la Información, se ha designado al Sr. ……como Responsable de seguridad de la información, quien tiene la responsabilidad y autoridad para:

- Diseñar, implementar y mantener el SGSI.
- Evaluar, coordinar y monitorear la implementación de los controles relacionados al SGSI.
- Promover la mejora continua del sistema SGSI.
- Elaboración de políticas, procedimientos y demás documentación relacionada con la seguridad de la información.
- Supervisar el cumplimiento de procedimientos y demás documentación relacionada con de seguridad de la información.
- Elaborar y supervisar el plan de sensibilización en seguridad de la información para los miembros.
- Coordinar la identificación, evaluación y tratamiento de riesgos de seguridad.
- Supervisar la gestión de eventos o incidentes de seguridad de la información y asegurar la respuesta efectiva.
- Asegurar el cumplimiento de requisitos legales y contractuales relacionados con la seguridad de la información.
- Presentar propuestas de mejora y proyectos de seguridad de la información.
- Informar acerca del desempeño del SGSI a la Alta Dirección a intervalos planificados.

Nota: Las obligaciones del responsable de seguridad de la información puede incluir relaciones con partes externas sobre asuntos relacionados al SGSI.

17% Similitud general

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

Filtrado desde el informe

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

Fuentes principales

13% Fuentes de Internet
4% Publicaciones
12% Trabajos entregados (trabajos del estudiante)

Marcas de integridad

N.º de alertas de integridad para revisión

Caracteres reemplazados
52 caracteres sospechosos en N.º de páginas
Las letras son intercambiadas por caracteres similares de otro alfabeto.

Texto oculto
4 caracteres sospechosos en N.º de páginas
El texto es alterado para mezclarse con el fondo blanco del documento.

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

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

Fuentes principales

13% Fuentes de Internet
4% Publicaciones
12% Trabajos entregados (trabajos del estudiante)

Fuentes principales

Las fuentes con el mayor número de coincidencias dentro de la entrega. Las fuentes superpuestas no se mostrarán.

1 Internet
repositorio.uwiener.edu.pe 3%

2 Trabajos entregados
Submitted on 1687209244651 1%

3 Internet
repositorio.ucv.edu.pe <1%

4 Internet
hdl.handle.net <1%

5 Trabajos entregados
Universidad Andina Nestor Caceres Velasquez on 2026-03-30 <1%

6 Internet
repositorioacademico.upc.edu.pe <1%

7 Trabajos entregados
Universidad Cesar Vallejo on 2023-01-05 <1%

8 Internet
alicia.concytec.gob.pe <1%

9 Trabajos entregados
Universidad Internacional de la Rioja on 2026-04-08 <1%

10 Internet
www.ant.gov.co <1%

11 Trabajos entregados
D.A. de Ingeniería de Sistemas on 2026-05-14 <1%