UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

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

Norma internacional ISO/IEC 27001:2022 para la gestión de activos de TI en una institución pública, Ica 2023

TESIS PARA OBTENER EL GRADO ACADÉMICO DE:

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

AUTOR:

Reyes Ramirez, Ronald Enrique (orcid.org/0000-0002-5112-7023)

ASESORES:

Dra. Alza Salvatierra, Silvia Del Pilar (orcid.org/0000-0002-7075-6167)

Dr. Vargas Huamán, Jhonatan Isaac (orcid.org/0000-0002-1433-7494)

LÍNEA DE INVESTIGACIÓN:

Auditoría de Sistemas y Seguridad de la Información

LÍNEA DE ACCIÓN DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:

Desarrollo económico, empleo y emprendimiento

LIMA - PERÚ

2023

DEDICATORIA

Dedico esta tesis a mis padres Sara Ramirez y a mi padre Jovo Reyes y en especial a mi esposa Cecilia Duffaut por su apoyo, ánimos y motivarme a perseguir mis sueños.

AGRADECIMIENTO

Agradecemos en primer lugar a Dios por la guía y sabiduría en cada decisión tomada, a nuestros padres y familia por ser las bases en nuestra formación y a los profesores que nos ayudaron en nuestra carrera universitaria.

DECLARATORIA DE AUTENTICIDAD DEL ASESOR

UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

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

Declaratoria de Autenticidad del Asesor

Yo, ALZA SALVATIERRA SILVIA DEL PILAR, docente de la ESCUELA DE POSGRADO MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA NORTE, asesor de Tesis titulada: "Norma Internacional ISO/IEC 27001:2022 para la Gestión de Activos de TI en una Institución Pública, Ica 2023", cuyo autor es REYES RAMIREZ RONALD ENRIQUE, constato que la investigación tiene un índice de similitud de 20.00%, verificable en el reporte de originalidad del programa Turnitin, el cual ha sido realizado sin filtros, ni exclusiones.

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

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

LIMA, 06 de Enero del 2024

Apellidos y Nombres del Asesor:	Firma
ALZA SALVATIERRA SILVIA DEL PILAR **DNI:** 18110381 **ORCID:** 0000-0002-7075-6167	Firmado electrónicamente por: SALZAS el 14-01-2024 11:53:02

Código documento Trilce: TRI - 0722961

INVESTIGA UCV

DECLARATORIA DE ORIGINALIDAD DEL AUTOR

UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

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

Declaratoria de Originalidad del Autor

Yo, REYES RAMIREZ RONALD ENRIQUE estudiante de la ESCUELA DE POSGRADO MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA NORTE, declaro bajo juramento que todos los datos e información que acompañan la Tesis titulada: "Norma Internacional ISO/IEC 27001:2022 para la Gestión de Activos de TI en una Institución Pública, Ica 2023", es de mi autoría, por lo tanto, declaro que la Tesis:

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

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

Nombres y Apellidos	Firma
RONALD ENRIQUE REYES RAMIREZ **DNI:** 44888957 **ORCID:** 0000-0002-5112-7023	Firmado electrónicamente por: RREYESRA01 el 06-01-2024 17:43:49

Código documento Trilce: TRI - 0722960

INVESTIGA UCV

Índice de contenidos

Índice de tablas

Página

RESUMEN

El objetivo general fue determinar la influencia de la Norma Internacional ISO/IEC 27001:2022 para la Gestión de Activos de TI en una Institución Pública, Ica - 2023. Contiene el análisis, implementación y busca solucionar el problema a través de la aplicabilidad de la norma Internacional.

El método utilizado en este estudio se base en un diseño experimental - Pre experimental, con muestra relacionadas y método cuantitativo. La muestra consta de 11 trabajadores de TI. Los datos fueron recolectados utilizando un instrumento técnico tipo encuesta para medir la variable Gestión de Activos de TI. La herramienta ha sido aprobada por 3 expertos para garantizar su eficacia y fiabilidad. Los resultados se analizaron utilizando el software SPSS.

En resultados se concluyó y demostró el impacto significativo de la norma internacional ISO/IEC 27001:2022, que indican una mejora significativa en la gestión de activos de hardware, software e información, y son refrendados por un valor de $p=0.001<0.005$. Esto no solo confirma el rechazo de la hipótesis nula (H0) sino que también subraya la eficacia de la norma ISO/IEC 27001:2022 en fortalecer la gestión de activos de TI.

Palabras Clave: Gestión de activos de TI, ITAM, Sistema de seguridad de la información SGSI, ISO 27001.

ABSTRACT

The general objective was to determine the influence of the International Standard ISO/IEC 27001:2022 for IT Asset Management in a Public Institution, Ica - 2023. It contains the analysis, implementation and seeks to solve the problem through the applicability of the International standard.

The method used in this study is based on an experimental design - Pre-experimental, with related samples and quantitative method. The sample consists of 11 IT workers. The data were collected using a survey-type technical instrument to measure the IT Asset Management variable. The tool has been approved by 3 experts to ensure its effectiveness and reliability. The results were analyzed using SPSS software.

The results concluded and demonstrated the significant impact of the international standard ISO/IEC 27001:2022, which indicate a significant improvement in the management of hardware, software and information assets, and are endorsed by a value of $p=0.001<0.005$. This not only confirms the rejection of the null hypothesis (H0) but also underlines the effectiveness of ISO/IEC 27001:2022 in strengthening IT asset management.

Keywords: IT asset management, ITAM, ISMS information security system, ISO 27001.

I. INTRODUCCIÓN

Gestión de activos de TI (ITAM) es un proceso estructurado, se enfoca en controlar los activos de TI de una organización. Esta gestión ayuda a obtener una visibilidad clara de los activos y a comprender el valor que cada uno de ellos proporciona.

En el ámbito Internacional, en su investigación Stone et al., 2018, indica que las organizaciones emplean decenas o cientos de miles de empleados que garanticen el funcionamiento de todas las operaciones (incluyendo computadoras, dispositivos móviles, sistemas operativos, aplicaciones, datos y recursos de red). Para administrar, utilizar y garantizar de manera efectiva cada uno de esos activos, es esencial tener un conocimiento detallado de sus ubicaciones y funciones. Aunque los activos físicos pueden etiquetarse con códigos de barras y ser rastreados en una base de datos, este enfoque no aborda preguntas más específicas, como ¿Cuáles son los sistemas operativos actualmente en uso en nuestros laptops? y ¿Qué dispositivos se encuentran susceptibles a la amenaza más reciente?. Profesionales de seguridad informática se enfrentan a la gran diversidad de hardware y software que intentan rastrear, así como a la falta de control centralizado. Esta complejidad dificulta evaluar las vulnerabilidades o responder rápidamente a las amenazas, así como evaluar con precisión el riesgo en primer lugar, al identificarse los activos más esenciales para el negocio.

En el ámbito nacional, Resolución Directoral N° 022-2022-INACAL/DN, el 29 de diciembre del 2022 el Comité Permanente de Normalización aprueban la Normas Técnica Peruana (NTP) ISO/IEC 27001:2022 “SGSI”. Requisitos. 3ª Edición. Con la finalidad de mejorar la gestión pública, aplicando procedimientos, controles y buenas prácticas para sus diferentes procesos siendo uno de ellos ITAM. Otro desafío que deberá afrontar el gobierno peruano es el fomento de la seguridad y confianza digital. Según un informe de FortiGuard Labs, Perú fue objetivo de más de 3.000 millones de ciberataques durante la primera mitad del 2023. Dado que el sector público maneja una cantidad considerable de datos sensibles, resultará crucial implementar medidas de seguridad para resguardar esta información. Para abordar esta problemática, se requiere trabajar en la seguridad de la información mediante la puesta en marcha de sólidas medidas de

seguridad destinadas a proteger y gestionar los activos de tecnologías de la información (ITAM) donde residen los datos.

La organización de estudio, a nivel nacional es una institución con derecho público y personería jurídica, con autonomía funcional y patrimonio propio, brinda como ente estatal, servicios al ciudadano a nivel nacional y tiene como principal misión otorgar seguridad jurídica. actualmente cuenta con su Sede Central en Lima y 14 sedes distribuidas en los principales departamentos del Perú, cada sede tiene a su cargo oficinas principales y receptoras haciendo un total de 252 oficinas a nivel nacional, asimismo cada Sede gestiona sus activos de TI forma independiente, pero trabajan de forma colaborativa ya que varios servicios están desplegados a nivel nacional, y gestionar los activos de TI de cada Sede o en forma conjunta es decir a nivel nacional, se vuelve todo un reto por las importantes inversiones y cambios que viene pasando la infraestructura de TI en los últimos años.

En el ámbito local, la institución de estudio en su sede de Ica, tiene a su cargo 12 oficinas entre principales y receptoras distribuidas en el departamento de Ica. Las entrevistas realizadas con el personal de TI, han indicado que poseen información imprescindible que deben proteger ante cualquier eventualidad o amenazas, y deben ser correctamente gestionadas, esta información se encuentra en los principales activos de la unidad de TI. Lamentablemente no cuentan: con un control adecuado de inventarios de activos críticos de TI, clasificación de los activos de TI según su grado de importancia, impacto de cada activo o tiempos de respuesta en caso de falla, tampoco saben la dependencia que existen entre los propios activos, asimismo no cuentan con un plan de contingencia o recuperación ante desastres de los activos críticos de TI, ni con procedimientos y/o manuales estandarizados u homologados para gestionar los activos de TI y de esta forma garantizar la continuidad operativa de los servicios incluyendo la integridad, disponibilidad, confidencialidad de la información en la institución pública.

En este sentido la institución pública ha considerado aceptar el apoyo de una investigación donde la Norma Internacional ISO/IEC 27001:2022 influya en ITAM, con intención de evaluar una posible solución a los problemas antes descritos, por lo consiguiente, se formula la siguiente interrogante como problema general:

¿Cómo influye la norma internacional ISO/IEC 27001:2022 en la Gestión de Activos de TI en una institución pública, Ica 2023?

Así mismo, se plantean las siguientes interrogantes como problemáticas específicas: (a) ¿De qué manera la norma internacional ISO/IEC 27001:2022 influye en la gestión de activos de hardware en una institución pública, Ica 2023?; (b) ¿De qué manera la norma internacional ISO/IEC 27001:2022 influye en la gestión de activos de software en una institución pública, Ica 2023?; (c) ¿De qué manera la norma internacional ISO/IEC 27001:2022 influye en la gestión de activos de información en una institución pública, Ica 2023?

Por otro lado, la presente investigación es justificada desde muchas perspectivas académicas. En los siguientes enunciados indicaremos las principales justificaciones:

La justificación epistemológica, es sustentado por el conocimiento científico con base al observación y análisis de información con el fin de explicar la realidad de las condiciones actuales de la Gestión de Activos de TI dentro de la institución pública, por este motivo lo que se busca es la influencia de la norma internacional ISO/IEC 27001:2022 en la mejora de la Gestión de Activos de TI. Adicionalmente, se ampara las evidencias recolectadas del presente estudio de investigación, así mismo se obtendrá la veracidad a las hipótesis indicadas, en función a criterios razonables y se prevalecerá la verdad científica.

La justificación teórica, que tiene por finalidad brindar conocimiento de la utilización de norma internacional ISO/IEC 27001:2022 en la Gestión de Activos de TI, plantea cómo se podría controlar varias tareas y saber cómo actuar ante alguna eventualidad o contingencia. Adicionalmente, lo que busca la presente investigación es brindar una metodología para guiar en la adopción de norma internacional ISO/IEC 27001:2022.

La justificación práctica, que busca fundamentar desde las dimensiones de norma internacional ISO/IEC 27001:2022 puede lograr relevancia e incidencia en la Gestión de Activos de TI, vinculados a sus respectivas dimensiones como gestión de activos de hardware, activos de software y activos de información.

Por último, la justificación metodológica, se sustenta por el diseño preexperimental, buscando sustentar y mejorar ITAM. Con el propósito de obtener resultados fidedignos recopilados mediante instrumentos metodológicos fiables y válidos por expertos.

Así mismo, El propósito u objetivo general es: Determinar la influencia de la norma internacional ISO/IEC 27001:2022 en la Gestión de Activos de TI en una institución pública, Ica 2023.

El objetivo específico de la presente investigación define las siguientes interrogantes: (a) Determinar la influencia de la norma internacional ISO/IEC 27001:2022 en los activos de hardware de la Gestión de Activos de TI en una institución pública, Ica 2023; (b) Determinar la influencia de la norma internacional ISO/IEC 27001:2022 en los activos de software de la Gestión de Activos de TI en una institución pública, Ica 2023; (c) Determinar la influencia de la norma internacional ISO/IEC 27001:2022 en los activos de información de la Gestión de Activos de TI en una institución pública, Ica 2023

Ante los objetivos la hipótesis general es la siguiente: la norma internacional ISO/IEC 27001:2022 influye significativamente en la Gestión de Activos de TI en una institución pública, Ica 2023

hipótesis específicas: (a) Norma internacional ISO/IEC 27001:2022 influye en los activos de hardware de la Gestión de Activos de TI en una institución pública, Ica 2023; (b) Norma internacional ISO/IEC 27001:2022 influye en los activos de software de la Gestión de Activos de TI en una institución pública, Ica 2023; (c) Norma internacional ISO/IEC 27001:2022 influye en los activos de información de la Gestión de Activos de TI en una institución pública, Ica 2023.

II. MARCO TEÓRICO

Como fundamentos teóricos que respaldan la presente investigación se presentara los siguientes antecedentes:

Como antecedentes Internacionales, Razikin & Soewito (2022) cuya investigación tiene el objetivo de mitigar las amenazas de seguridad basados en el SGSI ISO/IEC 27001. El estudio finaliza mediante una evaluación estadística del sistema desarrollado, señalando un incremento en el promedio de la evaluación de conformidad con ISO/IEC 27001, que aumenta de 36.27 a 82.37. El valor p de la prueba T pareada es de 0.002138, siendo inferior a 0.05. Además, en 12 tipos de muestras de amenazas, se tiene una criticidad pasando de 8.75 a 4.00, con un valor de p en chi cuadrado de 0.0006605 < 0.05 y un valor de p de la prueba de Fisher de 0.000008284 < 0.05, lo que significa que existe una relación de asociación entre las amenazas a los sistemas de seguridad de TI que aplican y no aplican las recomendaciones de nivel de criticidad de las amenazas TI. A medida que se evaluaron los resultados de la relación entre la implementación de las recomendaciones del sistema de seguridad y la mitigación de ataques cibernéticos, se evidenció un incremento en la efectividad de dicha mitigación. Esto se reflejó en un aumento en la calificación promedio, partiendo desde. 18.32 a 40.74, con un valor de p de la prueba de 0.000005221 < 0.05 y un valor de p de la prueba de Fisher de 0.00000005658 < 0.05, lo que significa que existe una relación de asociación entre los sistemas que implementan y no implementan recomendaciones basadas en ISO/IEC 27001 para la mitigación de ataques cibernéticos.

De igual forma Kurnianto et al. (2018) cuya investigación fue “Evaluación del SGSI ISO/IEC 27001:2013 En Subdirección de Data Center y Centro de recuperación de datos en el Ministerio del Interior”, por la Universidad Diponegoro, La seguridad de la información es un problema que concierne a todos los procesos empresariales de una organización, es buena y cumple con los estándares internacionales, se realiza utilizando el SGSI - ISO/IEC 27001:2013. se llevó una evaluación de nivel elevado para analizar la robustez de la SI en el Ministerio de Asuntos Internos. La investigación detalla la construcción de la evaluación, la cual se implementó mediante PHP. Los datos de entrada se basan en información

primaria y secundaria recopilada a través de observaciones. El proceso adquiere madurez a través de la evaluación conforme a la ISO/IEC 27001:2013. El Análisis de Brechas observa situaciones actuales y luego proporciona recomendaciones y un plan de acción. El resultado de esta investigación identifica que todos los procesos de información en el Ministerio de Asuntos Internos aún no son lo suficientemente buenos, y brinda recomendaciones y un plan de acción para mejorar parte de todos los sistemas de información que se están ejecutando. Esto indica que ISO/IEC 27001:2013 evalúa la madurez de la gestión de SI. Como siguiente análisis, esta investigación utiliza las Cláusulas y Anexos de ISO/IEC 27001:2013 que son adecuados para las condiciones del Centro de Datos y el Centro de Recuperación de Datos.

Del mismo modo Valencia & Orozco (2017) La metodología que propone para la aplicacion de un SGSI está basada en la ISO/IEC 27000, destacando la interrelación de cuatro normas fundamentales que abarcan las actividades necesarias para cumplir ISO 27001, los controles ISO 27002, el esquema de la norma ISO 27005 y todos los pasos que se recomiendan en la norma ISO 27003. Como resultado, se ha desarrollado una metodología que proporciona orientación sobre cómo abordar un proyecto. El proceso metodológico representa una contribución para todos los profesionales encargados en esta labor y están buscando un enfoque para lograr un SGSI implementado de forma exitosa.

Asimismo, Park & Lee (2014) indicando que las organizaciones utilizan información importante en su negocio diario. La salvaguarda de información confidencial es crucial y requiere una gestión adecuada. Empresas en diversas partes del mundo resguardan información confidencial mediante la implementación del estándar internacional conocido como SGSI (ISMS por sus siglas en inglés). La serie ISO 27000 constituye el estándar internacional de ISMS utilizado para preservar la integridad, disponibilidad y confidencialidad de información sensible. Aunque un ISMS basado en la serie ISO 27000 no presenta defectos específicos para los sistemas de información en general, no resulta adecuado para administrar información sensible (ICS por sus siglas en inglés). Esto se debe a que la principal prioridad del control industrial es la seguridad del sistema. Por lo tanto, se requiere un nuevo SGSI basado en la integridad, confidencialidad, disponibilidad y seguridad

para los ICS.

También. Latsou et al. (2016) en cuya investigación Modelado de redes de Petri para activos de TI mejorados Soluciones de reciclaje por la universidad de Loughborough, que tienen como objetivo el diseño preliminar hasta el mantenimiento del producto en los sistemas de ingeniería. Diversas metodologías de modelado matemático están disponibles para evaluar el rendimiento de sistemas y diseños de procesos. La técnica de Redes de Petri se destaca por su capacidad para representar y simular situaciones complejas, con la perspectiva de generar de forma automática un modelo a partir de la descripción del sistema o proceso. La generación automatizada de modelos facilita la exploración de cambios, permitiendo así la evaluación de diversos diseños. En el curso de esta investigación, se ha desarrollado un modelo de Redes de Petri específicamente aplicado a un proceso de reciclaje de activos de Tecnologías de la Información (TI). El modelo resultante se empleará en futuros estudios para validar la efectividad del proceso de automatización. La implementación y simulación de este modelo se lleva a cabo utilizando la plataforma Matlab. El modelo posibilita la simulación de distintos flujos de trabajo a lo largo del proceso de reciclaje, brindando una comprensión detallada de los actuales factores limitantes en dicho proceso. A partir de estas observaciones, se pueden identificar oportunidades para mejorar la eficiencia del reciclaje y optimizar la estrategia de gestión de activos de TI vigente. La meta a futuro de este proyecto de investigación consiste en lograr la generación automática de modelos de sistemas aplicados a sistemas y procesos industriales complejos, mediante la conversión de especificaciones fundamentadas en SysML a Redes de Petri.

De igual forma, Rose et al. (2016) cuya investigación indicando que a medida que el negocio crece, las tareas que antes eran tolerables se vuelven pesadas. Esto es especialmente evidente en un negocio donde los compartimentos estancos impiden una visión completa de principio a fin de los flujos de trabajo y los procesos. La gestión de configuración y de activos son dos puntos problemáticos en los que participan múltiples unidades de negocio, pero que constantemente enfrentan obstáculos debido a su antigüedad, falta de automatización y falta de interacciones con otras aplicaciones vitales. La sugerencia de introducir un nuevo sistema de

Gestión (ITALM) y Gestión de Configuraciones (CM) mediante el empleo de Arquitecturas de Referencia (RAs) actualizadas, como ISO 55000-2 para la gestión de activos y ANSI/EIA 649B para CM, contribuirá a la adopción de las mejores prácticas durante su implementación. La integración de tecnologías de seguimiento de activos inalámbricos también puede desempeñar un papel crucial al establecer un método continuo y automatizado para monitorear los ciclos de vida de los activos desde su inicio hasta el final de su utilidad. Aunque comúnmente se asocian los activos con hardware, es esencial reconocer que el software constituye un activo fundamental que debe ser rastreado. Dado que el software que opera en los activos físicos está sujeto a cambios debido a defectos constantes y vulnerabilidades recién descubiertas, contar con un mecanismo para rastrear y evaluar las versiones de software que se ejecutan en los activos físicos puede ser clave para la aplicación proactiva de parches y actualizaciones, evitando así posibles problemas críticos de software. Aunque el negocio no promueve ni instituye activamente un programa de Arquitectura Empresarial, se recomienda practicar sus principios a lo largo de este proceso utilizando arquitecturas de referencia, como TOGAF y su Método de Desarrollo de Arquitectura (ADM), métodos ágiles scrum de scrum y reuniendo al equipo adecuado para dar un paso atrás y observar la imagen de toda la empresa.

Iluore et al. (2020), Cuya investigación fue Desarrollo de modelo de gestión de activos usando monitoreo de equipos en tiempo real (RTEM): estudio de caso de una empresa industrial, por la universidad de Covenant, indicando que a nivel mundial, la implementación ha sido un desafío en la mayoría de las empresas, Particularmente, aquellas organizaciones que operan en la industria del gas y petróleo enfrentan desafíos significativos debido a la complejidad inherente de sus operaciones. En los últimos años, el escenario del mercado se ha vuelto extremadamente competitivo, atribuible en parte a la disminución de los precios del petróleo., al punto que incluso unos pocos minutos de inactividad de los equipos podrían resultar en pérdidas económicas sustanciales. Se han identificado brechas notables en las prácticas actuales, y hasta el momento, la empresa no ha aprovechado plenamente las herramientas tecnológicas avanzadas para la gestión de sus activos. Específicamente, la empresa no cuenta actualmente con un sistema adecuado para ubicar, monitorear, rastrear sus activos, a pesar de que los activos se desplazan de un lugar a otro para satisfacer toda necesidad solicitada por los

clientes. Se desarrolla un sistema de monitoreo de equipos en tiempo real para la empresa industrial utilizando GPS, códigos de barras y RFID.

Por último, Idowu et al. (2022) cuya investigación fue Gestión de activos en aprendizaje automático: estado de la investigación y estado de la práctica por la universidad de Gothenburg, donde indica que los componentes de aprendizaje automático son esenciales para los sistemas de software actuales, lo que genera la necesidad de adaptar las prácticas tradicionales de ingeniería de software al desarrollar sistemas basados en aprendizaje automático. La necesidad de abordar numerosos desafíos asociados al desarrollo de componentes de aprendizaje automático, como la gestión de activos, experimentos y dependencias, es evidente. En respuesta a estos desafíos, han surgido diversas herramientas de gestión de activos que desempeñan un papel crucial. Comprender el respaldo proporcionado por estas herramientas resulta fundamental para facilitar tanto la investigación como la implementación, con un enfoque nativo en activos de aprendizaje automático e ingeniería de software. Este artículo sitúa la gestión de activos de aprendizaje automático como una disciplina que ofrece métodos y herramientas mejoradas para llevar a cabo operaciones en el ámbito de los activos de aprendizaje automático. Se presenta una encuesta basada en características de 18 herramientas de estado de la práctica y 12 herramientas de estado de la investigación que respaldan la gestión de activos de aprendizaje automático. Se resumen sus características, las cuales abordan la gestión de diversos tipos de activos utilizados en experimentos de aprendizaje automático. En términos generales, la mayoría de las herramientas de estado de la investigación se enfocan en el seguimiento, exploración y recuperación de activos para abordar preocupaciones de desarrollo, como la reproducibilidad. En contraste, las herramientas de estado de la práctica también ofrecen funcionalidades de colaboración y operaciones relacionadas con la ejecución de flujos de trabajo. Además, los activos se rastrean predominantemente de manera intrusiva desde el código fuente mediante API, gestionándose a través de paneles web o interfaces de línea de comandos (CLI). Se identifican la colaboración asincrónica y la reutilización de activos como áreas de enfoque para nuevas herramientas y técnicas.

Asimismo, Hayllami (2020) En su investigación que trata de la Gestión de Riesgos con enfoque en el SGSI para el Ministerio de Salud, el principal objetivo fue evaluar el impacto de la implementación de un SGSI en la administración del riesgo. Se adoptó un enfoque metodológico hipotético-deductivo, con un diseño cuantitativo aplicado y una estructura longitudinal correlacional. La población bajo estudio comprendió a 145 empleados. La recopilación de datos se llevó a cabo mediante dos herramientas diseñadas para medir las variables pertinentes. El análisis de los resultados se basó en el coeficiente estadístico de Rho de Spearman, que facilitó la validación de las hipótesis a través de los datos recopilados con las herramientas aplicadas. Los resultados revelaron la existencia de una relación positiva y significativa entre las variables SGSI y Gestión del Riesgo

De la misma manera, citamos a, Huerta (2020), Esta investigación evaluó el impacto de implementar un SGSI en Coopsol Consultoría durante 2019. Se utilizó la metodología ISO 27001:2013 y un enfoque de investigación aplicada con un diseño preexperimental. La muestra consistió en 24 activos críticos de información, considerados como la población objetivo debido a su tamaño reducido. Se recopilaron datos utilizando fichas de observación como instrumentos. Realizando un análisis de información que incluyó la evaluación de la normalidad mediante los estadísticos de Shapiro-Wilks y Kolmogorov-Smirnov, La investigación incluyó la comparación entre los resultados previos y posteriores para dos indicadores, evidenciando de manera concluyente, que la implementación del (SGSI) tuvo un impacto positivo en el proceso de gestión de riesgos en Coopsol Consultoría en 2019. Este impacto se verifica mediante los resultados de la prueba t de Student, que reveló un valor de 4.614 en la comparación de medias entre el pretest y postest, con un nivel de significancia (p-valor) de 0.000 para el indicador de nivel de riesgo. Asimismo, la prueba de Wilcoxon indicó un valor de -9.644 en el pretest y postest, con un nivel de significancia (p-valor) de 0.000 para el indicador de número de controles. Estos resultados respaldaron la negación de la hipótesis nula y la aceptación de las hipótesis planteadas en la investigación ($p < 0.05$).

También, citamos a, Ponte (2022), Impacto de la implementación de medidas de SI (ISO 27001) en el teletrabajo durante la pandemia de Covid-19 en la empresa OSIR E.I.R.L. en Ancash en 2022. Para lograr esto, se llevó a cabo un enfoque de

investigación preexperimental. Durante el estudio, se manipuló la variable de SI para evaluar su efecto en el teletrabajo. Se realizó un análisis longitudinal al llevar a cabo dos mediciones, una antes y otra después, y se trabajó con una muestra de 45 empleados. Además, el cuestionario fue revisado por 3 ingenieros con maestría y doctorado, y se evaluó su confiabilidad, obteniendo un valor de 0.874. Los resultados del estudio revelaron de manera significativa (to=13.857 > tc=1.680; sig. 0.00 < 0.05) que la incorporación de medidas de SI (ISO27001) influye en el teletrabajo durante la pandemia de Covid-19 en la empresa OSIR E.I.R.L. en Ancash en 2022. El análisis descriptivo mostró una reducción del 44.4% en el nivel deficiente, una mejora del 22.2% en el nivel regular y un aumento del 66.7% en el nivel eficiente, lo cual evidencia la eficacia lograda en la empresa. En resumen, en conclusión, la implementación de medidas de SI (ISO27001) tiene un efecto significativo en el teletrabajo durante la pandemia de Covid-19 en la empresa OSIR E.I.R.L. en Ancash en 2022. Estos resultados se respaldan con la disminución en el nivel deficiente, la optimización en el nivel regular y el aumento en el nivel eficiente, lo cual demuestra el desarrollo de eficiencia en la empresa.

Del mismo modo, citamos a, Gonzales (2021), una organización dedicada al sector de microfinanzas que enfrentaba dificultades en el monitoreo de sus activos de TI. Debido a la falta de conocimiento sobre los recursos disponibles, los acuerdos no eran eficientes. Para abordar esta situación, se implementaron buenas prácticas de ITIL4 en los procesos con el objetivo de monitorear y controlar los activos de TI. Permitiendo conocer su ciclo de vida y nivel de detalle. Los resultados obtenidos fueron altamente satisfactorios, hasta la fecha se han mantenido los procesos implementados, los cuales aseguran la continuidad de los recursos. Gracias a estos procesos, se obtiene información en tiempo real sobre los activos de TI, lo que facilita que los colaboradores cuenten con los recursos necesarios. Esto evita complicaciones, Particularmente en el actual contexto, donde se da prioridad al trabajo remoto. En resumen, el proyecto se centró en solucionar el déficit en el monitoreo de los activos de TI en el Banco de la Microempresa. A través de la implementación de procesos basados en ITIL4, se logró un control efectivo y un monitoreo adecuado de los activos, brindando información actualizada y permitiendo a los colaboradores disponer de los recursos necesarios. Esto ha asegurado la continuidad de los recursos y ha evitado problemas durante el trabajo

remoto.

Citamos a, Banda (2019), El modelo propuesto fue validado mediante la evaluación de expertos, utilizando medidas de confiabilidad como el coeficiente basado en Kendall. Además. Durante este proceso, se identificaron escenarios de riesgo, se realizaron cálculos y se clasificó el nivel de riesgo de acuerdo con los criterios de aceptación establecidos, el cual fue validado y aplicado en una empresa como estudio de caso. Esto permitió la identificación y clasificación de los riesgos, así como la propuesta de proyectos de mitigación para aquellos riesgos que no cumplían con los criterios de aceptación establecidos.

Por último, Madueño (2022) El enfoque utilizado fue cuantitativo y de tipo aplicado, con un diseño preexperimental y un método hipotético-deductivo. Para recopilar los datos, se empleó la técnica de observación y Se empleó una ficha de observación como herramienta para documentar y registrar los activos TI. Se aplicó la escala de razón en el análisis de los registros de activos de TI, y la población de estudio consistió en 5000 registros de la BD del área de informática. Se implementó la metodología Kaizen, específicamente el enfoque de las 5'S. Después de llevar a cabo la investigación y aplicar los instrumentos, Se utilizó la prueba estadística de Wilcoxon a través del software estadístico SPSS, obteniendo un valor de W = -4.690 y un valor p = 0.00.

Como fundamentos teóricos que respaldan la presente investigación, se han consideran los siguientes:

La Teoría General de Sistemas (TGS), se enfoca en el estudio de diferentes disciplinas y en cualquier nivel de los sistemas y en todos los campos de la investigación, con el propósito de entender los principios aplicables a éstos. Según Gómez (2013) la TGS es un método de análisis que se centra en la realidad y el desarrollo de modelos. De la Peña y Velázquez (2018) menciona que la TGS es una herramienta para analizar los sistemas, yendo de lo complejo a lo simple, del todo a las partes, e infiriendo en sistemas que van de lo simple a lo complejo, de las partes al todo. Por otro lado, Becerra (2020) describe la TGS como una ciencia transdisciplinaria, donde la transdisciplinariedad se logra cuando cada disciplina colabora en la construcción de una base común de métodos y conceptos, que pueden entenderse como una especie de ejemplificación de sus propios métodos

y conceptos. Por lo tanto, la transdisciplinariedad no implica la eliminación del conocimiento disciplinario, sino la búsqueda de una perspectiva más amplia. Según García (2020), Se señala que una TGS se fundamenta en la perspectiva de aprendizaje. El autor detalla su intención, el procedimiento utilizado y los alcances de su teoría de la actividad, así como la teoría de estructura que se desprende de ella. Estas teorías se revelan más beneficiosas para su aplicación práctica en comparación con la antropología filosófica y la filosofía social. Además, sobrepasan a los modelos que consideran a organizaciones e individuos desde la óptica de sistemas extremadamente estables. Finalmente, Stoica et al. (2015) resalta que en la ingeniería de software, la TGS introduce el concepto de sistema-modelo, fusionando el proceso de diseño de ingeniería de software en una teoría de toma de decisiones y un enfoque basado en valores de bajo riesgo. El sistema-modelo se define como una agrupación de componentes interconectados y coherentes que colaboran para conceptualizar, desarrollar y entregar un sistema de software. Dentro de esta teoría general de sistemas, este concepto se emplea para representar diversas dimensiones de un proyecto, tales como los interesados, los modelos relacionados con el dominio o entorno, el éxito, las decisiones, el producto, el proceso y la propiedad.

Por otro lado, La Teoría de la Administración aborda propuestas formuladas a partir del estudio de factores, ya sea de manera indirecta o directa, que influyen en el rendimiento tanto de las organizaciones como el personal que las integran. A lo largo de los años, ha habido diferentes enfoques y no existe una teoría definitiva, según Peñaloza (2010), referido en la situación que se presenta en nuestra vida diaria en la que debemos elegir entre diferentes opciones, desde levantarnos de la cama hasta tomar decisiones más complejas con mayores implicaciones. En cuanto a la Teoría de la Complejidad Computacional, según Zapata (2004), se enfoca en estudiar los recursos necesarios, como el tiempo y el espacio, para resolver un problema en particular. Por otro lado, la Teoría de la Computabilidad se expresar los problemas algorítmicos, sin considerar la información de los recursos necesarios para hacerlo. Finalmente, la Teoría Crítica de la Tecnología, según Lorena y Mirabal (2017), ofrece elementos analíticos valiosos para estudiar en el diseño, Entendido como el proceso de concebir y diseñar artefactos y sistemas técnicos, adaptándolos a sus objetivos, especificaciones y restricciones.

En el siguiente punto abordaremos las definiciones de las variables.

En relación a la variable independiente el (SGSI), Según ISO/CEI 27001:2022 Tercera edición, Ofrece a compañías de variadas magnitudes y en todas las áreas un manual que les permite ejecutar, instaurar, conservar y perfeccionar de forma constante un SGSI, siguiendo los tres principios fundamentales Confidencialidad, Integridad y disponibilidad de la información. Asimismo, Tonysé (2021), Constituye el componente central de la normativa ISO 27001, que establece los estándares para valorar los riesgos vinculados a la gestión de la información corporativa. El SGSI busca preservar la confidencialidad, accesibilidad e integridad de los datos. Y por último Bolek (2023), Asegura la preservación de la confidencialidad, integridad y accesibilidad de la información a través de la instauración de un proceso de gestión de riesgos, lo que inspira confianza en las partes involucradas respecto a una gestión efectiva de los riesgos. Asimismo según Raggad. (2010), La confidencialidad de la información, tiene como objetivo evitar la fuga de información a destinatarios no autorizados. La Integridad de la información tiene el objetivo prevenir la corrupción de la información. La corrupción es la modificación no autorizada de la información por parte de un agente. Este agente puede ser una persona, un virus o un sistema. La Disponibilidad de la información tiene como propósito garantizar que la información esté accesible para los usuarios de acuerdo con lo estipulado en la política de seguridad del recurso de información en el que se encuentra almacenada.

Los estudios de investigación identificados en la revisión resaltan principalmente la aplicación de metodologías sistemáticas para detectar y analizar activos críticos, junto con sus posibles vulnerabilidades, amenazas y riesgos. Esto cobra relevancia debido al aumento en la implementación de diversas tecnologías en las empresas, que van desde la computación en la nube hasta el Internet de las cosas (IoT), generando cambios significativos y subrayando la importancia de la gestión de riesgos indicaron Kure & Islam (2019) y Haji et al (2019). Asimismo Mackita et al., (2019), se hace hincapié en la evaluación y gestión de riesgos de seguridad de la información, destacando la necesidad de esta práctica. Además, se mencionan algunos marcos generales para llevar a cabo evaluaciones y se analizan sus características comunes, abarcando la identificación de activos, amenazas y

vulnerabilidades, así como el impacto y la probabilidad asociados.

En una teoría conexa, de acuerdo con Ambit (2020), la finalidad de un SGSI es la capacidad de evaluar los riesgos vinculados a los activos de información gestionados dentro de una organización. El SGSI representa un componente crucial dentro de los lineamientos de la norma ISO 27001. El propósito subyacente del SGSI consiste en respaldar tres aspectos fundamentales la disponibilidad, confidencialidad e integridad y la de la información.

El Anexo A de la norma incluye objetivos de control de seguridad, los cuales están distribuidos en 93 controles, agrupados 4 dominios, de los cuales 37 controles son organizacionales, 8 de personas, 14 físicos y 34 tecnológicos.

Según la afirmación de Rodríguez (2013), MAGERIT Se refiere a una metodología empleada para llevar a cabo el análisis y la gestión de riesgos, permitiendo la evaluación de los riesgos asociados a los SI. Esta metodología propone realizar un análisis de riesgos que involucre la evaluación del impacto de posibles vulnerabilidades de seguridad en la organización. Además, enfatiza la identificación de amenazas y la determinación de la vulnerabilidad del sistema frente a dichas amenazas, con el propósito de obtener resultados concretos. Estos resultados permiten que la gestión de riesgos proponga las medidas apropiadas para prevenir, reducir, contener, identificar y controlar las amenazas identificadas, con el fin de minimizar su posible impacto negativo.

La Gestión de Riesgos engloba 2 actividades fundamentales a) Facilita la identificación y evaluación de posibles eventualidades. b) Adopta una postura proactiva que le permite organizar una fuerza de defensa vigilante y diligente, con el propósito de resguardarse ante posibles eventualidades, estar preparado para cualquier situación de emergencia, resolver problemas de manera efectiva y continuar las operaciones en las mejores condiciones posibles.

En el proceso de análisis de riesgos, se llevan a cabo varios pasos a) Identificación de Activos Relevantes, Se procede a identificar los activos significativos de la empresa, sus interrelaciones y valor, evaluando el daño potencial en términos de costos que podría acarrear su deterioro. b) identificación de Amenazas, se identifican las posibles amenazas a las que podría estar expuesto el activo. c) Identificación de Salvaguardas, se determinan las salvaguardas que se

pueden implementar y se evalúa su efectividad para mitigar un riesgo. d) Estimación de Impacto, se realiza una estimación del impacto, entendido como el daño causado a la propiedad como consecuencia de una amenaza. e) Estimación de Riesgo, se calcula el riesgo, que es la estimación del impacto ponderado por la probabilidad de ocurrencia del peligro. Estos pasos proporcionan un marco integral para comprender y gestionar los riesgos de manera efectiva.

Siguiendo con la definición de la variable dependiente de la presente investigación, Gestión de Activos de TI, según Axelos Limited (2019) Cualquier elemento de sustancial valía financiera que aporta de manera significativa a la entrega de un producto o servicio de Tecnologías de la Información (TI), englobando tanto software, hardware, redes, servicios en la nube y dispositivos cliente, e incluso considerando activos no directamente relacionados con TI, como edificaciones o información. De acuerdo con Piedra et al. (2018), ITAM tiene la capacidad de integrar tanto activos físicos como virtuales, ofreciendo a la gestión una visión completa de la ubicación y el modo en que se utilizan dichos activos. ITAM contribuye a mejorar la visibilidad para los analistas de seguridad, lo cual resulta en una utilización y seguridad mejoradas de los activos. Por último, el Centro de Seguridad Cibernética de Canadá (2023) ITAM es un proceso continuo que implica mantener un registro actualizado de todos los activos relacionados con la tecnología de la información, tanto los físicos como los virtuales. Consiste en un conjunto de políticas y procedimientos diseñados para asistir a las organizaciones en llevar un control y seguimiento de sus activos a lo largo de su ciclo de vida. ITAM desempeña un papel fundamental en el éxito y desarrollo de cualquier entidad, ya sea a través del seguimiento en tiempo real de los activos de TI o de la mejora de su visibilidad, garantiza la rápida detección, respuesta y resolución de incidentes, lo que a su vez minimiza las posibles pérdidas para la organización. De acuerdo con Marulanda et al. (2017), se señala que la gestión de activos de TI, tiene la responsabilidad de suministrar de manera eficaz los servicios y productos necesarios para el continuidad eficiente de las operaciones de TI. Esta responsabilidad recae en los ejecutivos y la alta dirección. Además, dicha gestión posibilita a la organización tomar decisiones orientadas a sostener el crecimiento empresarial. También Haldane (2014), la gestión de activos de TI ha experimentado una evolución significativa en la industria y en las organizaciones, convirtiéndose

en una agencia que abarca diversas actividades. Además, los activos están bajo la gestión de la industria (AUM) y se estima que actualmente ascienden a alrededor de $87 billones a nivel mundial. Por último, Wang et al. argumentan que los activos de Tecnologías de la Información (TI) en sí mismos no influyen directamente en el desarrollo de las empresas. En cambio, sostienen que la gestión de estos activos se presenta como un recurso estratégico capaz de potenciar la ventaja competitiva y el crecimiento de una organización.

Primera dimensión, Gestión de Activos de Hardware, según Axelos Limited (2019), es una subpráctica y se refiere a la disciplina que se encarga de gestionar de manera efectiva todos los componentes de hardware utilizados en una organización, con el objetivo de optimizar su ciclo de vida y su valor, garantizando que los activos de hardware estén disponibles y operativos cuando se necesiten. De la misma forma la para NIST IR 8011 (2017), la capacidad de gestionar activos de hardware brinda a la organización una visibilidad integral de los dispositivos que operan en sus redes, permitiendo una gestión efectiva y una defensa adecuada. Asimismo, ofrece una perspectiva clara de la responsabilidad en la gestión de dispositivos, posibilitando la presentación de defectos prioritarios a la parte correspondiente para la implementación de acciones de toma de decisiones y mitigación respecto a la aceptación de riesgos. El sistema HWAM (Hardware Asset Management) identifica los dispositivos, incluyendo las máquinas virtuales, que están físicamente presentes en la red y los compara con el inventario que refleja el estado deseado para determinar si están autorizados. En este proceso, se consideran tanto los dispositivos direccionables por red como los extraíbles, que presumiblemente están conectados a dispositivos direccionables. La metodología para identificar estos dispositivos reales puede variar, dependiendo de las capacidades automatizadas disponibles y del tipo de dispositivo en cuestión. El proceso de Gestión Integral y Continua de la Seguridad de la Información (ISCM), adaptado a las necesidades específicas de cada agencia, suministrará información acerca de qué proporción de los activos de hardware reales están alineados con el estado deseado. Además, revelará cuántos de estos activos identifican a un administrador asignado, proporcionando así una visión detallada de la gestión y asignación de responsabilidades en relación con los activos de hardware.

Segunda dimensión, Gestión de Activos de Software, según Axelos Limited (2019), Su enfoque está especialmente diseñado para administrar de manera específica la obtención, creación, introducción, implementación, mantenimiento y posterior retirada de activos de software. Según Albert et al. (2013) sugieren que la Gestión de Activos de Software (SAM) es una metodología para rastrear los activos de software, permitiendo a las organizaciones mantener y optimizar su utilización del software. La meta principal es alinear el uso del software con los derechos de licencia adecuados proporcionados por los proveedores de software, con el fin de mitigar los riesgos de tecnologías de la información asociados con posibles incumplimientos de licencias. Asimismo La Gestión de Activos de Software (SAM), según Varela et al. (2018), brinda a las organizaciones las herramientas y procesos necesarios para identificar no solo sus activos de software, sino también para entender su utilización, ubicación y configuración. Este enfoque asegura que las organizaciones cumplan con los requisitos de licencia y aborda la asimetría de la información al registrar de manera integral todos los activos de software desplegados en sus redes, como señala la Organización Internacional de Normalización (2015).

Tercera dimensión, Gestión de activos de Información, según el centro de Seguridad Cibernética de Canadá (2023), es la categoría que incluye datos confidenciales y valiosos que deben considerarse un activo de TI clave. Estos datos deben rastrearse, gestionarse, mantenerse y eliminarse de forma segura siguiendo el ciclo de vida de la información. Por otro lado, Según Alonge et al. (2020), la clasificación de activos de información enfrenta un desafío significativo relacionado con la falta de directrices genéricas. Esto se debe a la ausencia de una adaptación universal en la clasificación de activos de información para todas las organizaciones. Como resultado, cada organización puede tener su propio esquema de clasificación, generando diversidad en los enfoques utilizados asimismo Angraini et al. (2018) subrayan la importancia de priorizar los activos de información más críticos para la organización, ya que estos desempeñarán un papel fundamental en la mitigación de riesgos identificados. En este sentido, la elaboración de un plan de riesgos específico para los activos de información se vuelve esencial. Establecer y mejorar un plan de SI efectivo se convierte en un elemento crucial en este contexto. Por ende, la detección, clasificación y

priorización de los activos de información se consideran elementos integrales en este proceso.

La gestión de activos de TI (ITAM) engloba el conjunto de sistema, procesos y tecnología empleados para identificar, rastrear, administrar y optimizar los activos de TI a lo largo de todas las fases de su ciclo de vida. Se consideran activos de TI a cualquier hardware, software, suscripciones o servicios relacionados con TI que la organización posea, esté pagando o utilice directa o indirectamente. Esta definición abarca no solo servidores, equipos de escritorio y dispositivos móviles, sino también dispositivos IoT, de red y almacenamiento, así como servicios en la nube como Software como Servicio (SaaS), Infraestructura como Servicio (IaaS) y Plataforma como Servicio (PaaS), entre otros.

ITAM es clave para la mitigación de riesgos de TI. Un tipo de riesgo exclusivo de ITAM es el cumplimiento de la licencia de software. La industria del software es reconocida por llevar a cabo auditorías de cumplimiento de licencias de software. Sin una gestión de activos de TI (ITAM) efectiva, incluso una organización bien intencionada podría implementar software más allá de los límites de sus derechos de licencia. Esto expone a la organización a riesgos legales, financieros y repetitivos, destacando la importancia crítica de una gestión precisa y completa de los activos de software. Esto se debe a múltiples factores, incluidos los siguientes (a) Complejidad de las reglas de licencia en constante cambio (b) Nuevas tecnologías que impactan en las licencias (p. ej., virtualización, nube y edge computing) (c) La cantidad de diferentes proveedores de software bajo administración (que puede exceder los 1000 para una organización grande) (d) Fusiones y adquisiciones tanto del lado de la organización como del lado del editor de software (e) Limitaciones inherentes de las herramientas disponibles para ayudar en el proceso (f) Incapacidad para controlar las acciones no autorizadas del usuario final, por nombrar solo algunos desafíos.

La gestión de activos de TI (ITAM) desempeña un papel fundamental en el ahorro de costos en el ámbito de TI. La carencia de información completa y precisa de ITAM puede llevar a las organizaciones a incurrir en gastos excesivos en activos de TI, especialmente en software, que cada vez representa una parte más significativa de los presupuestos de TI. Ejemplos de esta situación incluyen: (a)

Shelf-ware se refiere a la situación en la que la organización paga por software o renovación de mantenimiento que no está en uso y no es necesario. Este problema es más común en el caso de Software como Servicio (SaaS) en comparación con el software local tradicional. Un adecuado ITAM contribuye a evitar este tipo de gastos innecesarios, optimizando así los recursos financieros de la organización. ITAM eficaz evita que se produzcan estanterías (b) Recolección es cuando se retira el hardware, las licencias de software consumidas por ese hardware deberían estar disponibles para volver a implementarse dentro de la organización; sin embargo, esto solo es posible con un ITAM efectivo (c) Optimización de la arquitectura, sin un ITAM eficaz, las organizaciones pueden configurar sus entornos de forma no optimizada desde el punto de vista de las licencias, lo que hace que se necesiten más licencias sin ningún beneficio funcional u operativo para la organización (d) Negociación desde una posición de conocimiento, sin un ITAM efectivo, las organizaciones carecen de información sobre sus necesidades y están a merced de los editores de software cuando negocian contratos de software.

El ciclo de vida de los activos de TI puede variar según los diferentes sectores de la industria. Por ejemplo, la publicación especial NIST 1800-5 del gobierno de EE. UU., Gestión de activos de TI, divide el ciclo de vida de los activos de TI en ocho etapas: estrategia, planificación, diseño, adquisición, operación, mantenimiento, modificación y eliminación. Otros grupos las dividen de manera diferente, generalmente con solo tres a cinco etapas. En última instancia, la organización es responsable de determinar tanto el número como los nombres de los activos de acuerdo con sus políticas operativas.

Las etapas del ciclo de vida de los activos de TI son cinco, son bastante convencionales e incluyen todas las etapas anteriores designadas por el NIST, pero en un nivel superior.

Al abordar la gestión de activos de TI, ya sean unidades, computadoras u otros dispositivos de almacenamiento de datos, los administradores de activos de TI deben tener en cuenta cómo los datos se ven afectados en cada una de las cinco etapas del ciclo de vida. Este enfoque no solo contribuirá a la protección de los datos almacenados o procesados, sino que también permitirá maximizar la eficiencia en el uso de los presupuestos de TI.

La Planificación es la etapa donde las organizaciones desarrollan sus requisitos para nuevos activos. Esto implica una evaluación minuciosa de los activos existentes y su historial de uso. Las organizaciones pueden tomar en consideración la posibilidad de reutilizar los activos que ya poseen. Incluso si los activos que en su momento fueron de vanguardia ya no son adecuados para ciertos usos, aún conservan valor si se destinan a propósitos distintos. En la fase de Adquisición se busca identificar la fuente más adecuada para obtener los activos de Tecnologías de la Información necesarios. Aprovechando tanto los recursos internos como los externos, se procede al desarrollo, recuperación, obtención y compra de computadoras, servidores, laptops o tabletas apropiadas, con el objetivo de realizar un uso más eficiente del presupuesto disponible para TI. En la etapa de Despliegue, los activos son serializados y puestos en uso activo. Estos pueden ser implementados en departamentos que manejan y procesan datos con diferentes niveles de confidencialidad. La implementación puede ocurrir de forma remota o en las instalaciones, en dispositivos de punto final destinados al personal o clientes, ya sea de forma centralizada o distribuida, y también pueden estar alojados en diversos centros de datos. La etapa de Gestión constituye la fase operativa diaria en el ciclo de vida de los activos de Tecnologías de la Información, abarcando el seguimiento y mantenimiento de unidades y dispositivos. El mantenimiento planificado se realiza para prolongar la vida útil de los activos de TI, asegurar operaciones más eficientes, preservar la disponibilidad adecuada de los datos y prevenir la pérdida de información. La fase de Desecho generalmente ocurre cuando los activos se vuelven obsoletos o se considera que tienen un alto riesgo de falla. Los servidores, unidades o computadoras que experimentan fallos inesperados también atraviesan un proceso de eliminación. Los activos se pueden destruir físicamente o se pueden desinfectar todos los datos a un nivel de Purga utilizando un software de borrado de datos certificado.

Por otro lado, el procedimiento operativo del ITAM implica registrar un activo al recibirlo, asignar y documentar un número de serie, cargar una imagen base de TI con un listado de software aprobado, incluyendo agentes de gestión de configuración y de activos que comienzan a supervisar e informar sobre los activos una vez registrados. Estos agentes recopilan información previamente establecida por los administradores.

Los agentes de gestión de configuración aplican una línea base de seguridad y configuración, mientras que los agentes de gestión de activos de software capturan los detalles del software instalado. Ambas categorías de agentes envían informes a sus respectivos servidores, que funcionan como almacenes de datos. Los servidores formatean los datos antes de enviar informes periódicos al motor de análisis. A través de la capacidad de visualización de este motor, un analista o gerente puede acceder a un informe visual con un nivel específico de detalle. Los cambios que afectan los atributos de los activos se registran en estos informes enviados al motor de análisis.

Aunque el sistema ITAM incorpora alguna detección automatizada de anomalías, los analistas deben revisar periódicamente los informes para identificar posibles irregularidades o cambios relevantes. Se definen vistas con información específica sobre los activos en el motor de análisis, lo que permite a los analistas detectar violaciones de políticas o anomalías que puedan requerir una mayor investigación. Las alertas provenientes de otras fuentes de información de seguridad también desencadenan investigaciones más detalladas por parte de los analistas.

La detección de violaciones de políticas activa la aplicación o corrección de políticas si se identifica una alerta negativa relevante. Estas alertas podrían incluir, por ejemplo, vulnerabilidades recientemente descubiertas o la identificación de software incluido en la lista negra. La función de gestión de configuración se utilizaría para exigir la eliminación de dicho software o para parchear la vulnerabilidad en cualquier número de hosts, llevando a la empresa a un estado más acorde con la política empresarial definida.

III. METODOLOGÍA

3.1. Tipo y diseño de investigación

3.1.1. Tipo de investigación. La investigación que se lleva a cabo es de carácter aplicado, según la definición de Hernández et al. (2014). Esta implica la utilización de conocimientos teóricos existentes con el propósito de abordar y resolver problemas específicos o mejorar la práctica profesional. Se basa en la búsqueda de soluciones prácticas y concretas, mediante la implementación de estrategias y técnicas que permitan abordar situaciones reales.

3.1.2. Diseño de investigación. Diseño fue experimental, de tipo pre-experimental con variables de escala ordinal, con lo cual según Hernández y Mendoza (2018), enfoque de pre prueba y pos prueba con solo 1 grupo de control, aplicando la prueba previa al experimento después se aplica el tratamiento y al final se aplica nuevamente la prueba posteriormente del estímulo.

Para el presente trabajo se muestra la siguiente esquematización:

G01- X02

G: Es la parte representativa de la población

01: La muestra antes de la norma internacional

X: Es la implementación de la norma internacional

02: La muestra después de la norma internacional

En la presente investigación con un diseño pre-experimental, por lo tanto, se efectuó una medición al grupo de estudio antes y después de la influencia del fenómeno o intervención en estudio. SGSI según ISO/IEC 27001:2022 para la Gestión de Activos de TI en una Institución Pública.

3.2. Variables y operacionalización

Variable independiente. Normal Internacional ISO/CEI 27001:2022

Definición conceptual

Según ISO/CEI 27001:2022 Tercera edición, El objetivo de esta guía es brindar a las empresas, fuese el tamaño o sector, un marco de referencia para establecer, implementar, mantener y mejorar de manera constante un SGSI. Aplicando los tres principios Confidencialidad, Integridad de la información y disponibilidad de los datos.

Variable dependiente. Gestión de Activos de TI

Definición conceptual

Axelos Limited (2019) es cualquier componente de valor financiero que pueda contribuir a la entrega de un producto o servicio de TI. Incluye todo el software, hardware, redes, servicios en la nube y dispositivos cliente; también puede incluir activos que no son de TI como edificios o información.

Definición operacional

La Gestión de Activos de TI es una variable categórica con medida ordinal (tres niveles de medición), compuesta por tres dimensiones: activos de hardware, software e información, las cuales serán medidas por un cuestionario conformado por 30 ítems. Ver Anexo 4.

3.3. Población, muestra, muestreo, unidad de análisis

3.3.1. Población

Robles (2019), la población se caracteriza como el conjunto de entidades, usualmente personas, objetos o eventos, que son seleccionados para ser investigados en un estudio en particular. La población estuvo conformada por 180 trabajadores de la entidad. En la investigación, se tomó 11 trabajadores de la unidad de TI de la institución pública, conforme a los criterios de inclusión.

Criterios de inclusión:

- Trabajadores de la unidad de TI de la sede de Ica con experiencia dentro del área de TI mínima de 6 meses.

Criterios de exclusión:

- Trabajadores que no pertenezcas a la Unidad de TI, no cuenten con 6 meses de trabajo en el área, y no tengan permiso o licencia mayores a 3 meses.

3.3.2. Muestra

Hernández et al (2018), La muestra, es un subconjunto específico de la población de interés sobre la cual se recopilarán información, debe ser delimitada y definida con precisión de antemano. Es imperativo que esta muestra sea representativa de la totalidad de la población para garantizar la validez y la generalización de los resultados obtenidos; Alcanzando en la presente investigación la cantidad de 11 trabajadores del área de TI.

3.3.3. Muestreo

Según Hernández et al (2018), muestro por conveniencia es una técnica no probabilística donde las muestras de la población se seleccionan a conveniencia del investigador.

3.3.4. Unidad de análisis

Se determinó llevar a cabo el estudio con la totalidad de la población compuesta por 11 trabajadores de la unidad de TI de la institución pública. Estos trabajadores están directamente vinculados con la variable de estudio.

3.4. Técnicas e instrumentos de recolección de datos

Técnica:

Se utilizará la encuesta como método de recolección de datos. Según Hernández et al (2018), la encuesta es una técnica utilizada para obtener información a través de la formulación de preguntas.

Instrumentos:

En este estudio, se empleará el cuestionario como herramienta de recolección de datos. Conforme a Hernández et al. (2018), el cuestionario se define como un instrumento compuesto por una serie de preguntas relativas a una o más variables,

las cuales serán objeto de medición. En este estudio, se utilizó un cuestionario conformado por 30 ítems para evaluar la variable dependiente.

Validez: Gestión de Activos de TI

Instrumento: Cuestionario de Gestión de activos de TI.

Escala de medición: Ordinal

Extensión: 30 ítems. (Ver Anexo 4)

Ámbito de Aplicación: trabajadores de la unidad de TI

Duración: 20 minutos.

Puntuación: Escala Likert

1 = No se ha practicado ni documentado

2 = Se ha practicado, pero no documentado o se ha documentado, pero no practicado

3 = Se ha practicado y documentado

4 = Se ha practicado, documentado y revisado en el último año

5 = Se ha practicado, documentado, revisado y armonizado según la estrategia empresarial o de TI

Validez

La validez se define como un procedimiento que evalúa la idoneidad de un instrumento. En el marco de la presente investigación, se utilizaron cuestionarios validados, cuya validez se evidenció a través de la coherencia interna entre los ítems y las dimensiones, según lo descrito en el estudio de Larsen et al. (2020). Para obtener información detallada se puede consultar el Anexo 6.

Confiabilidad

Consiste en determinar si, al aplicar un instrumento en poblaciones similares, se obtienen resultados que son comparables a los registrados durante su fase de desarrollo. (Hernández & Mendoza, 2018).

La confiabilidad del cuestionario de madures de la Gestión de activos de TI se realizó un piloto que involucró a diez trabajadores del área de TI. La evaluación se llevó a cabo mediante el coeficiente Alfa de Cronbach, Considerando los valores policotómicos de las opciones de respuesta de los instrumentos empleados, los resultados indicaron que los cuestionarios exhibieron una fiabilidad excelente. Para más detalles, consultar el Anexo 7.

3.5. Procedimientos

Se realizaron reuniones con la unidad de TI, para conocer los detalles de la realidad problemática y definir los alcances de la investigación. El levantamiento de la información física y digital de forma confidencial nos brindó las debilidades en la gestión de activos de TI; construyendo así un cuestionario para utilizarlo como instrumento de recolección de datos que servía para medir la persección y aplicabilidad de SGSI en la unidad de TI por parte de todos sus integrantes (11 trabajadores). El cuestionario fue evaluado por expertos en la materia y pudo reunir información necesaria para medir el antes y después de la aplicación de la norma internacional.

Con los datos obtenidos de forma confidencial por medio del cuestionario nos llevó a realizar diferentes planes, procedimientos, instructivos, charlas, entre otras actividades para formalizar, concientizar, y divulgar las medidas correctivas y las buenas prácticas aplicadas por la norma internacional. Finalizando estas acciones se procedió con la toma de postest para medir el grado de madures y aplicabilidad de la norma internacional, aplicada en las 3 dimensiones de ITAM. Finalizando con la construcción de las conclusiones y recomendación de la presente investigación.

3.6. Métodos de análisis de datos

En el análisis descriptivo los datos recogidos corresponden a variables categóricas, cualitativas, que corresponden a una escala ordinal. En consecuencia, el uso de la prueba no paramétrica de rangos de Wilcoxon es apropiada para analizar la comparación

En la realización de este análisis, se utilizará el software SPSS, una herramienta ampliamente empleada en el campo de la investigación estadística, con el fin de llevar a cabo los cálculos necesarios y generar los resultados relevantes.

En el análisis inferencial En esta instancia, los datos corresponden a variables categóricas de naturaleza cualitativa y están asociados con una escala ordinal. Por lo tanto, se considera apropiado emplear la prueba no paramétrica de rangos de Wilcoxon para llevar a cabo la comparación y análisis correspondiente. Esta prueba es especialmente adecuada cuando se trabaja con variables no distribuidas normalmente y permite evaluar diferencias entre dos conjuntos relacionados sin asumir distribuciones particulares en los datos.

3.7. Aspectos éticos

La presente indagación se llevó a cabo con un enfoque ético y responsable, asegurando rigurosamente la preservación del anonimato de los participantes involucrados en el estudio. Se rigieron las directrices de citación de la séptima edición de la norma APA de la American Psychological Association para las citas y referencias, garantizando así la integridad académica del trabajo. La originalidad del documento fue evaluada a través del empleo del programa Turnitin, que generó un informe detallado sobre la autenticidad del contenido. La recopilación de datos se efectuó mediante el uso de encuestas, lo cual proporcionó un marco sistemático para la obtención de información.

En esta investigación se inscribe dentro de la línea de Auditoría de Sistemas y SI, según lo dispuesto en la Resolución N° 0200-2018/UCV del Consejo Universitario. La confidencialidad de los hallazgos se ha garantizado rigurosamente, asegurando que su uso se restrinja exclusivamente a los fines investigativos. Además, se ha dado especial consideración a los principios de autonomía, ya que cada participante fue debidamente consultado sobre su decisión de participar en el estudio.

IV. RESULTADOS

Resultados descriptivos

El análisis descriptivo realizado es una forma de análisis estadístico que se centra en resumir y describir las características fundamentales de un conjunto de datos. Este tipo de análisis proporciona una visión clara de cómo se distribuyen las observaciones o datos a través de diferentes categorías o valores.

En la distribución de frecuencias, los datos se organizan de manera que se pueda ver el número de veces (frecuencia) que cada valor o categoría particular ocurre en el conjunto de datos, ofreciendo una manera clara de comparar frecuencias entre diferentes grupos.

Tabla 1

Distribución de frecuencias de la Gestión de activos según pre y postest

Variable/ Dimensión	Nivel	Pretest		Postest	
		Recuento	Porcentaje	Recuento	Porcentaje
Gestión de activos	Escasa	11	100%	0	0.0%
	Regular	0	0.0%	0	0.0%
	Adecuada	0	0.0%	11	100.0%
Activos de hardware	Escasa	11	100.0%	0	0.0%
	Regular	0	0.0%	6	54.5%
	Adecuada	0	0.0%	5	45.5%
Activos de software	Escasa	11	100.0%	0	0.0%
	Regular	0	0.0%	0	0.0%
	Adecuada	0	0.0%	11	100.0%
Activos de información	Escasa	11	100.0%	0	0.0%
	Regular	0	0.0%	0	0.0%
	Adecuada	0	0.0%	11	100.0%

La distribución porcentual de la gestión de activos que se muestra en la Tabla 1, dan cuenta de los resultados obtenidos en el pretest y el postest aplicados a los elementos de la muestra. En el pretest, el 100% de las dimensiones de activos de hardware, activos de software y activos de información fueron calificados como 'Escasos'. Sin embargo, en el postest, hubo una mejora significativa. Para los activos de hardware, el 100% pasó a ser calificado como 'Adecuado'. En los activos

de software, el 54.5% se consideró 'Regular' y el 45.5% 'Adecuado'. Finalmente, en los activos de información, el 100% se calificó como 'Adecuado', indicando una mejora general en la gestión de activos de TI tras la intervención.

Resultados inferenciales

El análisis estadístico realizado consideró que los datos corresponden a muestras relacionadas o muestras pareadas donde las observaciones en un conjunto de datos están emparejadas de alguna manera lógica o están relacionadas entre sí. Las muestras relacionadas se encuentran en diseños experimentales donde los mismos sujetos son expuestos a una condición o tratamiento. El análisis estadístico de muestras relacionadas debe tener en cuenta la naturaleza relacionada de los datos. En este caso, los datos corresponden a variables categóricas, cualitativas, que corresponden a una escala ordinal. En consecuencia, el uso de la prueba no paramétrica de rangos de Wilcoxon es apropiada para analizar la comparación.

Prueba de rangos con signo de Wilcoxon para muestras relacionadas:

Esta versión se utiliza para comparar dos muestras relacionadas o pareadas. Es adecuada cuando se desea evaluar si hay una diferencia significativa en las medianas de dos grupos relacionados. Se puede utilizar en estudios de medidas repetidas donde se evalúa el mismo grupo de sujetos en dos momentos diferentes (como antes y después de un tratamiento). La prueba toma las diferencias entre los pares de observaciones, les asigna rangos basados en el valor absoluto de estas diferencias y luego utiliza estos rangos para evaluar la hipótesis de que las medianas de las dos muestras relacionadas son iguales.

La prueba de Wilcoxon es valiosa cuando los datos son ordinales, cuando las muestras son pequeñas, o cuando no se puede asumir una distribución normal. Son herramientas esenciales en el análisis de datos no paramétrico.

La prueba de hipótesis se realizó considerando un valor de significancia (α) de 0.05, un nivel de acierto del 95% y la decisión de rechazo de H_0 cuando el valor calculado sea menor que α.

Prueba de hipótesis general

H_0: La implementación de la norma internacional ISO/IEC 27001:2022 no mejora la gestión de activos de TI

H_G: La implementación de la norma internacional ISO/IEC 27001:2022 mejora la gestión de activos de TI

Tabla 2

Estadísticos de la prueba de rangos con signo de Wilcoxon de la Gestión de activos de TI

	Gestión de activos (Postest) - Gestión de activos (Pretest)
Z	-3.317[b]
Sig. asintótica(bilateral)	0.001

Nota. [b.] Se basa en rangos negativos

Se observa que el valor de significancia obtenido es p=0.001<0.005 lo que refrenda el rechazo de H_0, es decir que implementación de la norma internacional ISO/IEC 27001:2022 mejora significativamente la gestión de activos de TI. Estos resultados se complementan con la prueba de rangos con signo que se muestra a continuación:

Tabla 3

Prueba de rangos con signo de Wilcoxon de la Gestión de activos

		N	Rango promedio	Suma de rangos
Gestión de activos (Postest) - Gestión de activos (Pretest)	Rangos negativos	0[a]	0.00	0.00
	Rangos positivos	11[b]	6.00	66.00
	Empates	0[c]		
	Total	11		

Nota. [a.] Gestión de activos (Postest) < Gestión de activos (Pretest)

[b.] Gestión de activos (Postest) > Gestión de activos (Pretest)

[c.] Gestión de activos (Postest) = Gestión de activos (Pretest)

Los resultados de la Prueba de rangos con signo de Wilcoxon aplicada a la gestión de activos en un pretest y un postest que se muestran en la Tabla 3 permiten

apreciar que no hay rangos negativos, lo que indica que no hubo casos en los que la gestión de activos en el postest fuera inferior al pretest. Por otro lado, hay 11 rangos positivos con un rango promedio de 6.00 y una suma de rangos de 66.00, lo que sugiere una mejora significativa en la gestión de activos de TI en el postest en comparación con el pretest. Esto se interpreta como una mejora general en la gestión de activos de TI después de la intervención realizada entre el pretest y el postest.

Prueba de hipótesis 1

H_0: La implementación de la norma internacional ISO/IEC 27001:2022 no mejora los activos de hardware

H_1: La implementación de la norma internacional ISO/IEC 27001:2022 mejora los activos de hardware

Tabla 4

Estadísticos de la prueba de rangos con signo de Wilcoxon de los activos de hardware

	Activos de hardware (Postest) - Activos de hardware (Pretest)
Z	-3.017[b]
Sig. asintótica(bilateral)	0.003

Nota. [b.] Se basa en rangos negativos

Se observa que el valor de significancia obtenido es p=0.003<0.005 lo que refrenda el rechazo de H_0, es decir que implementación de la norma internacional ISO/IEC 27001:2022 mejora significativamente los activos de hardware. Estos resultados se complementan con la prueba de rangos con signo que se muestra a continuación:

Tabla 5

Prueba de rangos con signo de Wilcoxon de Activos de hardware

		N	Rango promedio	Suma de rangos
Activos de hardware (Postest) - Activos de hardware (Pretest)	Rangos negativos	0[a]	0.00	0.00
	Rangos positivos	11[b]	6.00	66.00
	Empates	0[c]		
	Total	11		

Nota. [a.] Activos de hardware (Postest) < Activos de hardware (Pretest)

[b.] Activos de hardware (Postest) > Activos de hardware (Pretest)

[c.] Activos de hardware (Postest) = Activos de hardware (Pretest)

Los resultados de la Prueba de rangos con signo de Wilcoxon aplicada a los activos de hardware en un pretest y un postest que se muestran en la Tabla 5 permiten apreciar que no hay rangos negativos, lo que indica que no hubo casos en los que los activos de hardware en el postest fueran inferior al pretest. Por otro lado, hay 11 rangos positivos con un rango promedio de 6.00 y una suma de rangos de 66.00, lo que sugiere una mejora significativa en los activos de hardware en el postest en comparación con el pretest. Esto se interpreta como una mejora general en los activos de hardware después de la intervención realizada entre el pretest y el postest.

Prueba de hipótesis 2

H_0: La implementación de la norma internacional ISO/IEC 27001:2022 no mejora los activos de software

H_2: La implementación de la norma internacional ISO/IEC 27001:2022 mejora los activos de software

Tabla 6

Estadísticos de la prueba de rangos con signo de Wilcoxon de los activos de software

	Activos de software (Postest) - Activos de software (Pretest)
Z	-3.317[b]
Sig. asintótica(bilateral)	0.001

Nota. [b.] Se basa en rangos negativos

Se observa que el valor de significancia obtenido es p=0.001<0.005 lo que refrenda el rechazo de H_0, es decir que implementación de la norma internacional ISO/IEC 27001:2022 mejora significativamente los activos de software. Estos resultados se complementan con la prueba de rangos con signo que se muestra a continuación:

Tabla 7

Prueba de rangos con signo de Wilcoxon de Activos de software

		N	Rango promedio	Suma de rangos
Activos de software (Postest) - Activos de software (Pretest)	Rangos negativos	0[a]	0.00	0.00
	Rangos positivos	11[b]	6.00	66.00
	Empates	0[c]		
	Total	11		

Nota. [a.] Activos de software (Postest) < Activos de software (Pretest)

[b.] Activos de software (Postest) > Activos de software (Pretest)

[c.] Activos de software (Postest) = Activos de software (Pretest)

Los resultados de la Prueba de rangos con signo de Wilcoxon aplicada a los activos de software en un pretest y un postest que se muestran en la Tabla 7 permiten apreciar que no hay rangos negativos, lo que indica que no hubo casos en los que los activos de software en el postest fueran inferior al pretest. Por otro lado, hay 11 rangos positivos con un rango promedio de 6.00 y una suma de rangos de 66.00, lo que sugiere una mejora significativa en los activos de software en el postest en comparación con el pretest. Esto se interpreta como una mejora general en los activos de software después de la intervención realizada entre el pretest y el postest.

Prueba de hipótesis 3

H_0: La implementación de la norma internacional ISO/IEC 27001:2022 no mejora los activos de información

H_3: La implementación de la norma internacional ISO/IEC 27001:2022 mejora los activos de información

Tabla 8

Estadísticos de la prueba de rangos con signo de Wilcoxon de los activos de información

	Activos de información (Postest) - Activos de información (Pretest)
Z	-3.317[b]
Sig. asintótica(bilateral)	0.001

Nota. [b.] Se basa en rangos negativos

Se observa que el valor de significancia obtenido es p=0.001<0.005 lo que refrenda el rechazo de H_0, es decir que implementación de la norma internacional ISO/IEC 27001:2022 mejora significativamente los activos de información. Estos resultados se complementan con la prueba de rangos con signo que se muestra a continuación:

Tabla 9

Prueba de rangos con signo de Wilcoxon de Activos de información

		N	Rango promedio	Suma de rangos
Activos de información (Postest) - Activos de información (Pretest)	Rangos negativos	0[a]	0.00	0.00
	Rangos positivos	11[b]	6.00	66.00
	Empates	0[c]		
	Total	11		

Nota. [a.] Activos de información (Postest) < Activos de información (Pretest)

[b.] Activos de información (Postest) > Activos de información (Pretest)

[c.] Activos de información (Postest) = Activos de información (Pretest)

Los resultados de la Prueba de rangos con signo de Wilcoxon aplicada a los activos de información en un pretest y un postest que se muestran en la Tabla 9 permiten apreciar que no hay rangos negativos, lo que indica que no hubo casos en los que los activos de información en el postest fueran inferior al pretest. Por otro lado, hay 11 rangos positivos con un rango promedio de 6.00 y una suma de rangos de 66.00, lo que sugiere una mejora significativa en los activos de información en el postest en comparación con el pretest. Esto se interpreta como una mejora general en los activos de información después de la intervención realizada entre el pretest y el postest.

V. DISCUSIÓN

La discusión de resultados en una investigación es una sección donde se interpretan y analizan los hallazgos obtenidos del estudio. En esta parte, se contextualizan los resultados en relación con las preguntas de investigación o hipótesis, comparándolos con estudios previos y teorías existentes. Se abordan las implicaciones de los hallazgos, se reconocen las limitaciones del estudio y se sugieren áreas para investigaciones futuras.

La discusión de los resultados obtenidos de la implementación de la norma ISO/IEC 27001:2022 en la mejora de la gestión de activos de TI, y su comparación con los hallazgos de diversos autores presentados en este documento, ofrece una perspectiva integral y crítica sobre el impacto de las normativas de seguridad de la información en el ámbito empresarial y tecnológico.

En cuanto al impacto significativo de ISO/IEC 27001:2022, los resultados obtenidos, que indican una mejora significativa en la gestión de activos de hardware, software e información, son refrendados por un valor de $p=0.001<0.005$. Esto no solo confirma el rechazo de la hipótesis nula (H0) sino que también subraya la eficacia de la norma ISO/IEC 27001:2022 en fortalecer la gestión de activos de TI. Estos hallazgos son consistentes con las observaciones de varios autores que destacan la importancia de esta normativa en la mejora de la seguridad y la gestión de activos.

La ausencia de rangos negativos en la Prueba de rangos con signo de Wilcoxon sugiere que no hubo disminuciones en la eficacia de la gestión de activos tras la implementación de la norma. Esto es un indicativo positivo de que la implementación no solo evita el deterioro del rendimiento, sino que contribuye a su mejoramiento.

La presencia de rangos positivos y la mejora en los indicadores de gestión de activos de TI son evidencias concretas del impacto benéfico de la norma. Esto se alinea con estudios de autores como Razikin & Soewito y Kurnianto et al. (2022), quienes también observaron mejoras en la seguridad y la gestión de activos con la adopción de estándares similares.

Si bien los resultados son positivos, es crucial reflexionar sobre los desafíos y las posibles áreas de mejora en la implementación de normas como ISO/IEC 27001. Como se evidencia en la adaptación de la norma a contextos específicos (como discuten Park & Lee (2014)) y la integración continua de nuevas tecnologías y prácticas (como el aprendizaje automático mencionado por Idowu et al. (2022)) son aspectos cruciales para mantener la relevancia y eficacia de la normativa.

La implementación exitosa de normas de seguridad y gestión no debe ser vista como un logro único, sino como parte de un proceso de mejora continua. Esto se alinea con el enfoque de Madueño (2022) en la aplicación de la metodología Kaizen, sugiriendo que la adaptación y el mejoramiento continuos son fundamentales para mantener la eficacia de la gestión de activos de TI.

La implementación de ISO/IEC 27001:2022 ha demostrado ser una estrategia efectiva para mejorar la gestión de activos de TI, según lo evidencian los resultados obtenidos y los estudios comparativos. Sin embargo, es vital abordar esta implementación como un proceso continuo y adaptable, considerando los retos específicos de cada organización y la evolución constante del paisaje tecnológico y de seguridad de la información.

Respecto a la hipótesis 1 que infiere que la implementación de la norma internacional ISO/IEC 27001:2022 mejora los activos de hardware. Los resultados de la Prueba de rangos con signo de Wilcoxon para la gestión de activos en una comparación pre y postest indican una mejora significativa, evidenciada por la ausencia de rangos negativos y la presencia de 11 rangos positivos con un rango promedio de 6.00 y una suma de rangos de 66.00. Esto sugiere que la gestión de activos mejoró significativamente después de la intervención como lo demuestra el valor de significancia de p=0.003

La comparación con los trabajos previos y teorías considerados en este documento en relación con los resultados obtenidos en la comprobación de la hipótesis 1, se pueden establecer las siguientes comparaciones respecto a Razikin & Soewito (2022) se encontraron similitudes dado que los autores también encontraron mejoras significativas tras la implementación de ISO/IEC 27001, con un enfoque en la seguridad y evaluación de amenazas. Como también se encontraron diferencias, dado que los autores se centraron en la seguridad general

y las amenazas, en tanto que en el resultado obtenido en este caso, se enfoca específicamente en la mejora de los activos de hardware.

De igual forma, se encontraron similitudes con el estudio de Kurnianto et al. (2018) sobre el uso de la norma ISO/IEC 27001 para evaluar y mejorar aspectos de la gestión de activos de TI. No obstante, se difiere en que los autores se enfocaron en la evaluación de la seguridad de la información en un contexto específico, mientras que este estudio se centra en la mejora cuantitativa de los activos de hardware.

Por su parte, Valencia-Duque y Orozco-Alzate (2017) coinciden con este estudio en el uso de la norma ISO/IEC 27001 para mejorar la gestión de activos de TI. En cambio desarrollaron una metodología para la implementación de un SGSI, mientras que en este estudio se muestra los efectos directos de la implementación en los activos de hardware.

El trabajo realizado por Park & Lee (2014) es similar en el empleo de la norma ISO/IEC 27001 coincidiendo en que juega un papel crucial en la mejora de la gestión de activos. No obstante, Park & Lee discuten la necesidad de adaptar la norma ISO/IEC 27001 para contextos específicos, en tanto que en este caso se centra en los efectos de su implementación estándar en los activos de hardware.

Por su parte, Latsou et al. (2016) y Rose et al. (2016) se enfocaron en la mejora y gestión de activos de TI, diferenciándose en que los primeros se centran en el modelado y simulación para la gestión de activos, y los segundos proponen un sistema de gestión integral, mientras que en este estudio se muestran resultados prácticos de la implementación de una norma enfocándose en mejoras específicas en activos de hardware post implementación de ISO/IEC 27001.

Cada uno de estos estudios aporta una perspectiva única sobre la importancia y el impacto de la implementación de normas como la ISO/IEC 27001 en la gestión de activos de TI. Mientras que algunos se enfocan en aspectos de seguridad, otros abordan la gestión desde una perspectiva más amplia o específica.

Respecto a la hipótesis 2 que infiere que la implementación de la norma internacional ISO/IEC 27001:2022 mejora los activos de software. Los resultados de la Prueba de rangos con signo de Wilcoxon en una comparación pre y postest

indican una mejora significativa, evidenciada por la ausencia de rangos negativos y la presencia de 11 rangos positivos con un rango promedio de 6.00 y una suma de rangos de 66.00. Esto sugiere que activos de software mejoró significativamente después de la intervención como lo demuestra el valor de significancia de p=0.003

La comparación con los trabajos previos y teorías considerados en este documento en relación con los resultados obtenidos en la comprobación de la hipótesis 2, se pueden establecer las siguientes comparaciones en relación con el resultado sobre la mejora significativa de los activos de software tras la implementación de ISO/IEC 27001:2022. Los resultados obtenidos por Ponte (2022) muestran las similitudes con este estudio, destacando la importancia de la norma ISO/IEC 27001 en la mejora de la gestión de activos de TI, ya sea en hardware o software. Sin embargo, Ponte se enfoca en el impacto de las medidas de seguridad de la información en el teletrabajo, mientras que el resultado presentado se centra en la mejora de activos de software.

El estudio realizado por Huerta (2020) también resalta la influencia positiva de la implementación de un SGSI según ISO/IEC 27001, similar al impacto observado en el resultado para los activos de software. No obstante, el estudio de Huerta se centra en la gestión del riesgo, no directamente en la mejora de los activos de software.

Por su parte, Gonzales (2021) reconoce la eficacia de las prácticas de gestión (como ITIL4 e ISO/IEC 27001) en la mejora de la gestión de activos de TI. Difiriendo con los hallazgos de este estudio, dado que Gonzales aborda el monitoreo de activos de TI en un banco, con un enfoque más amplio que incluye hardware y software, mientras que el resultado presentado se enfoca exclusivamente en los activos de software.

Banda (2019) también se centra en la gestión de activos y la identificación de riesgos, alineándose con la temática general de mejorar la gestión de activos de TI, sin embargo, el enfoque de Banda es en la gestión de riesgos y no se centra específicamente en los activos de software como el resultado presentado.

Los hallazgos de Madueño (2022) mostraron que también utiliza la prueba de Wilcoxon en su metodología, similar al enfoque estadístico empleado en el resultado presentado, no obstante, se enfoca en la aplicación de la metodología

Kaizen para la gestión de activos de TI, mientras que el resultado presentado se centra en los cambios en los activos de software tras la implementación de ISO/IEC 27001.

Cada uno de estos estudios aporta diferentes perspectivas sobre la gestión de activos de TI y la implementación de normativas de seguridad. Mientras que algunos autores se enfocan en aspectos específicos como el riesgo, la gestión del cambio o la eficiencia operativa, el resultado presentado proporciona evidencia concreta del impacto positivo de la implementación de ISO/IEC 27001 en la mejora específica de los activos de software.

Respecto a la hipótesis 3 que infiere que la implementación de la norma internacional ISO/IEC 27001:2022 mejora los activos de información. Los resultados de la Prueba de rangos con signo de Wilcoxon en una comparación pre y postest indican una mejora significativa, evidenciada por la ausencia de rangos negativos y la presencia de 11 rangos positivos con un rango promedio de 6.00 y una suma de rangos de 66.00. Esto sugiere que activos de información mejoró significativamente después de la intervención como lo demuestra el valor de significancia de p=0.001

La comparación con los trabajos previos y teorías considerados en este documento en relación con los resultados obtenidos en la comprobación de la hipótesis 3, se pueden establecer las siguientes comparaciones en relación con el resultado sobre la mejora significativa de los activos de información tras la implementación de ISO/IEC 27001:2022. Los resultados obtenidos por Iloure et al. (2020) mostraron similitudes puesto que tienen un enfoque en la mejora de la gestión de activos mediante tecnologías avanzadas, lo cual se alinea con la mejora en los activos de información observada en el resultado obtenido. Las diferencias encontradas se centran en el monitoreo de equipos en tiempo real en una empresa industrial, mientras que el resultado presentado se enfoca en la mejora de los activos de información en un contexto de seguridad de la información.

En tanto que Idowu et al. (2022) abordan la gestión de activos en el contexto de aprendizaje automático, lo que puede tener paralelismos con la mejora de los activos de información en el resultado presentado. Las diferencias se encuentran en su enfoque, que es más técnico y específico en el aprendizaje automático,

mientras que el resultado presentado se centra en una mejora general de los activos de información bajo la normativa ISO/IEC 27001.

El estudio de Huerta (2020) demuestra el impacto positivo de la implementación del SGSI en la gestión de activos de TI, no obstante se enfoca en la gestión del riesgo en una consultoría, mientras que el resultado presentado muestra mejoras específicas en activos de información.

La investigación de Ponte (2022) subraya la importancia de la norma ISO/IEC 27001 en la seguridad de la información, lo cual es coherente con las mejoras en los activos de información en el resultado presentado. El enfoque de Ponte es en el impacto de estas medidas de seguridad en el teletrabajo durante la pandemia, a diferencia del enfoque en los activos de información del resultado obtenido.

Por su parte, Gonzales (2021) también se enfoca en la mejora de la gestión de activos de TI, un tema que está en línea con el resultado obtenido. El estudio de Gonzales se centra en el monitoreo de activos de TI en un banco, abordando tanto hardware como software, mientras que el resultado presentado se centra en los activos de información.

Mientras que Banda (2019) aborda la identificación y clasificación de riesgos, lo que puede relacionarse con la mejora en la gestión de activos de información en el resultado de este trabajo. Su enfoque es más en la gestión de riesgos en sí misma y no se centra específicamente en los activos de información como el resultado presentado.

La investigación de Madueño (2022) utiliza la prueba de Wilcoxon en su metodología, similar al enfoque estadístico empleado en el resultado de este trabajo. Madueño se enfoca en la aplicación de la metodología Kaizen para la gestión de activos de TI, mientras que el resultado presentado muestra mejoras específicas en activos de información tras la implementación de ISO/IEC 27001.

Cada uno de estos estudios aporta diferentes perspectivas sobre la gestión de activos de TI, la seguridad de la información y la implementación de normativas de seguridad. Mientras algunos autores se enfocan en aspectos generales o específicos como la gestión de riesgos o el monitoreo de equipos, el resultado

presentado proporciona evidencia concreta del impacto positivo de la implementación de ISO/IEC 27001 en la mejora específica de los activos de información.

La comparación con los trabajos previos y teorías considerados en este documento en relación con los resultados obtenidos en la comprobación de la hipótesis general, se pueden establecer las siguientes comparaciones en relación con el resultado sobre la mejora significativa de los activos de información tras la implementación de ISO/IEC 27001:2022.

VI. CONCLUSIONES

Primero, se demostró que la implementación de la norma internacional ISO/IEC 27001:2022 mejora la gestión de activos de TI en una institución pública, Ica – 2023, sustentado en la prueba de rangos con signo de Wilcoxon, donde p=0.001<0.005 lo que sugiere una mejora significativa en la gestión de activos en el postest en comparación con el pretest.

Segundo, se demostró que la implementación de la norma internacional ISO/IEC 27001:2022 mejora la gestión de activos de hardware en una institución pública, Ica – 2023, sustentado en la prueba de rangos con signo de Wilcoxon, donde p=0.003<0.005 lo que sugiere una mejora significativa en la gestión de activos de hardware en el postest en comparación con el pretest.

Tercero, se demostró que la implementación de la norma internacional ISO/IEC 27001:2022 mejora la gestión de activos de software en una institución pública, Ica – 2023, sustentado en la prueba de rangos con signo de Wilcoxon, donde p=0.001<0.005 lo que sugiere una mejora significativa en la gestión de activos de software en el postest en comparación con el pretest.

Cuarto, se demostró que la implementación de la norma internacional ISO/IEC 27001:2022 mejora la gestión de activos de información en una institución pública, Ica – 2023, sustentado en la prueba de rangos con signo de Wilcoxon, donde p=0.001<0.005 lo que sugiere una mejora significativa en la gestión de activos de información en el postest en comparación con el pretest.

VII. RECOMENDACIONES

Primero, se recomienda a la especialista y el personal de TI, la aplicación y actualización periódica de los protocolos, procedimientos e instructivos proporcionados, con la finalidad de mejorar y madurar la gestión de activos de TI que incluye todos los activos de hardware, software e información de la institución.

Segundo, se recomienda a los especialistas en gestión de TI realicen autoevaluación con el mismo cuestionario realizado para medir periódicamente el impacto de la implementación de la norma ISO/IEC 27001:2022. Esto asegurará que las prácticas se mantengan actualizadas con las últimas tendencias en seguridad y gestión de activos de TI.

Tercero, se recomienda a los directivos realizar inversiones en formación y capacitación para los empleados sobre la importancia y aplicación de la normativa ISO/IEC 27001. La efectividad de cualquier norma depende en gran medida del nivel de conocimiento y compromiso del personal.

Cuarto, se sugiere a los directivos consideren la incorporación de tecnologías emergentes, como el aprendizaje automático y la IA, en la gestión de activos de TI, para mejorar la eficiencia y la capacidad de respuesta ante amenazas de seguridad.

Quinto, se recomienda a los directivos adoptar un enfoque de mejora continua, alineado con metodologías como Kaizen, para asegurar que los procesos y prácticas de seguridad y gestión de activos de TI evolucionen constantemente.

Sexto, se recomienda a los investigadores lleven a cabo investigaciones comparativas entre diferentes industrias y contextos organizacionales para entender cómo la adaptabilidad y aplicabilidad de la norma ISO/IEC 27001 influye en su eficacia en distintos entornos.

Séptimo, Se sugiere a los investigadores indagar sobre los desafíos y barreras que enfrentan las organizaciones al implementar la norma ISO/IEC 27001, para desarrollar estrategias que faciliten su adopción y efectividad.

REFERENCIAS

Albert, B. E., Santos, R. P., & Werner, C. M. (2013). Software ecosystems governance to enable IT architecture based on software asset management. 2013 7th IEEE International Conference on Digital Ecosystems and Technologies (DEST). doi:10.1109/dest.2013.6611329 and Virtualization, 115-122. IARIA.

Alonge, C. Y., Arogundade, O. T., Adesemowo, K., Ibrahalu, F. T., Adeniran, O. J., & Mustapha, AM (2020).Modelo de clasificación y etiquetado de activos de información que utiliza un enfoque difuso para una seguridad eficazEvaluación de Riesgos. Conferencia Internacional 2020 en Matemáticas, Ingeniería Informática y Ciencias de la Computación (ICMCECS), 1–7. https://doi.org/10.1109/ICMCECS47690.2020.240911

Ambit. SGSI Controles y Fases https://www.ambit-bst.com/blog/paraqu%C3%A9-sirve-un-sgsi-controles-y-fases"

Angraini, Megawati, & Haris, L. (2018). Risk Assessment on Information Asset an academic Application Using ISO 27001. 2018 6th International Conference on Cyber and IT Service Management (CITSM), 1–4. https://doi.org/10.1109/CITSM.2018.8674294

Banda, J. (2019), Modelo basado en metodologías de gestión de riesgos de TI para contribuir en la mejora de la seguridad de los activos de información en empresas del sector agroindustrial de la región Lambayeque http://hdl.handle.net/20.500.12423/2159

Becerra G. (2020) La Teoría de los Sistemas Complejos y la Teoría de los Sistemas Sociales en las controversias de la complejidad. https://doi.org/10.29101/crcs.v27i83.12148

Bolek (2023) Next generation cloud computing: New trends and research directions https://doi.org/10.1016/j.future.2017.09.020

Calder. (2016). Nine steps to succes : an ISO 27001: 2013 implementation overview (Third edition.). IT Governance Publishing.

Centro de Seguridad Cibernetica de Canada (2023), Uso de la gestion de activos de Tecnologia de la informacion (ITAM) para mejorar la cberseguridad, ISBN 978-0-660-48191-3 CAT D97-4/10-004-2023E-PDF https://www.cyber.gc.ca/sites/default/files/itsm10004-using-information-technology-asset-management-enhance-cyber-security-v2-e.pdf

CONGRESO DE LA REPUBLICA (2022), LEY N°30224 Sistema Nacional para la Calidad y el Instituto Nacional de Calidad Resolución Directoral N° 022-2022-INACAL/DN. https://cdn.www.gob.pe/uploads/document/file/4040804/2022-RD22.pdf?v=1673565693

Davies, R., Dieter, J., & McGrail, T. (2011). The IEEE and asset management: A discussion paper. 2011 IEEE Power and Energy Society General Meeting, 3. https://doi.org/10.1109/pes.2011.6039770

De la Peña G. y Velázquez R. (2018) ÁvilaAlgunas reflexiones sobre la teoría general de sistemas y el enfoque sistémico en las investigaciones científicas versión On-line ISSN 0257-4314 http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S0257-43142018000200003

Diario Oficial del Bicentenario El Peruano (2023) Transformación digital, retos para el 2024 por Ximena Bravo Gerente Comercial Sector Gobierno de CANVIA. https://www.elperuano.pe/noticia/232025-transformacion-digital-retos-para-el-2024

Erick Guerra, Harold Neira, Jorge L. Díaz y Janns Patiño (2021). Desarrollo de un sistema de gestión para la seguridad de la información basado en metodología de identificación y análisis de riesgo en bibliotecas universitarias Vol. 32(5), 145-156 (2021) http://dx.doi.org/10.4067/S0718-07642021000500145

Fuente del texto citado en ITIL® Foundation (edición ITIL® 4), 2019. AXELOS Limited ISBN 9780113316076

García, M. A. (2020). Persons and organizations: Introduction to juan antonio pérez lópez general systems theory | Personas y Organizaciones: Introducción a la Teoría General de Sistemas de Juan Antonio Pérez López. Studia Poliana, 22, 71–100. https://doi.org/10.15581/013.22.71-100

Gómez Guitierrez (2013), Teoria General de Sistemas, Ediciones USTA. ISBN: 978-958-631-850-1

Gonzales, K (2021), Implementación De Procesos Para La Gestión De Activos De Ti Basado En Las Prácticas De Itil4 Como Apoyo A La Toma De Decisiones En Ti En El Banco De La Microempresa https://repositorio.untels.edu.pe/jspui/handle/123456789/751

Haji, Sami, & Tan, Q. S. (2019). A Hybrid Model for Information Security Risk Assessment. International Journal of Advanced Trends in Computer Science and Engineering, 8(1.1), 100 - 1. doi: https://doi.org/10.30534/ijatcse/2019/1981.12019

Haldane, A. (2014). The age of asset management?. Revista Bank of England. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.642.236&rep=rep1&type=pdf

Huayllani, O. (2020), Sistema de gestión de seguridad de la información y la gestión del riesgo en el Ministerio de Salud, 2019. https://hdl.handle.net/20.500.12692/42775

Huerta, C. (2020) Sistema de gestión de seguridad de la información para mejorar el proceso de gestión del riesgo de Coopsol Consultoría, 2019 https://hdl.handle.net/20.500.12692/46037

Idowu, S., Strüber, D., & Berger, T. (2022). Asset Management in Machine Learning: State-of-research and State-of-practice. ACM Computing Surveys, 55(7). https://doi.org/10.1145/3543847

Iluore, O. E., Mamudu Onose, A., & Emetere, M. (2020). Development of asset management model using real-time equipment monitoring (RTEM): case study of an industrial company. Cogent Business and Management, 7(1). https://www.tandfonline.com/doi/full/10.1080/23311975.2020.1763649

ISO/IEC 2022, Sistemas de gestión de la seguridad de la información. Www.iso.org https://www.iso.org/standard/27001#lifecycle

ISO/IEC/IEEE International Standard - Systems and software engineering – Software life cycle processes. (2017). ISO/IEC/IEEE International Standard, 55. https://doi.org/10.1109/ieeestd.2017.8100771

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

Kure, H. I., & Islam, S. (2019). Assets focus risk management framework for critical infrastructure cybersecurity risk management. IET Cyber-Physical Systems: Theory & Applications, 4(4), 332-340. doi: 10.1049/iet-cps.2018.5079

Kurnianto, A., Isnanto, R., & Widodo, A. P. (2018). Assessment of Information Security Management System based on ISO/IEC 27001:2013 On Subdirectorate of Data Center and Data Recovery Center in Ministry of Internal Affairs. E3S Web of Conferences, 31. https://doi.org/10.1051/e3sconf/20183111013

Latsou, C., Dunnett, S. J., & Jackson, L. M. (2016). Petri net modelling for enhanced IT asset recycling solutions. OpenAccess Series in Informatics, 50, 3.1-3.10. https://doi.org/10.4230/OASIcs.SCOR.2016.3

Lorena M. y Mirabal A. (2017) la visión directiva en la toma de decisiones bajo el enfoque de la teoría cognitiva de la organización. 42 (4) 11-28 https://doi.org/10.22206/cys.2017.v42i4.pp11-28

Mackita, M., S. S.-Y., & Choe, T.-Y. (2019). ERMOCTAVE: A risk management framework for IT systems which adopt cloud computing. Future Internet, 11(9). doi:10.3390/fi11090195

Madueño, N (2022) Metodología Kaizen para mejorar la gestión de activos de TI, en el área de informática del MINEDU, Lima 2021 https://hdl.handle.net/20.500.12692/87235

Maquera H & Serpa P (2019), GESTIÓN DE ACTIVOS BASADO EN ISO/IEC 27002 PARA GARANTIZAR SEGURIDAD DE LA INFORMACIÓN. https://doi.org/10.33326/26176033.2017.21.736

Maria P. (2010). Teorìa de las decisiones. ISSN: 1994-3733. https://www.redalyc.org/pdf/4259/425942454012.pdf

Marulanda, C., Trujillo, M. & Valencia, F. (2017). Gobierno y Gestión de TI en las Entidades Públicas. AD-Minister, 31, 74–92. https://doi.org/10.17230/administer.31.5

McCarthy, M. A., & Herger, L. M. (2011). Managing Software Assets in a Global Enterprise. 2011 IEEE International Conference on Services Computing, 1. https://doi.org/10.1109/scc.2011.119

Mercedes A. & Tùa J. (2020) IT assets: a benchmark in the characterization of IT risk management processes INNOVA Vol. 5, No.3.2 pp. 196-213 https://doi.org/10.33890/innova.v5.n3.2.2020.1608

NIST Interagency Report 8011 (2017), Automation Support for Security Control Assessments. Volume 1: Hardware Asset Management. Volume 2 https://doi.org/10.6028/NIST.IR.8011-2

Park, S., & Lee, K. (2014). Advanced approach to information security management system model for industrial control system. Scientific World Journal, 2014. https://doi.org/10.1155/2014/348305

Piedra, M., Irrechukwu, C., Perper, H., Wynne, D., Kauffman, L., (2018) Gestion de Activos de TI (9) http://doi.org/10.6028/NIST.SP.1800-5

Ponte, E. (2022), Seguridad de la información (ISO27001) para el desarrollo de teletrabajo en tiempos de Covid-19. Empresa OSIR E.I.R.L., Ancash – 2022 https://hdl.handle.net/20.500.12692/94036

Raggad. (2010). Information security management : concepts and practice (First edition.). CRC Press, an imprint of Taylor and Francis. https://doi.org/10.1201/9781439882634

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

Rodriguez. M.(2013).Gestión de Riesgos Magerit.ISO/IEC 27001:2013. Obtenido de: SGSI. https://www.normas-iso.com/iso-27001/.

Rose, B., Else, S., Tierney, T. J., & McGuire, M. J. (2016). Evolving Productivity with IT Asset Lifecycle Management and Configuration Management for Master of Science Software Design and Programming. https://eapj.org/wp-content/uploads/2017/01/Evolving-Productivity-with-IT-Asset-Lifecycle-Management-and-Configuration-Management-Brandon-Rose.pdf

Stoica, A. J., Pelckmans, K., & Rowe, W. (2015). System components of a general theory of software engineering. Science of Computer Programming, 101, 42- 65. https://doi.org/10.1016/j.scico.2014.11.008

Stone, M., Irrechukwu, C., Perper, H., Wynne, D., & Kauffman, L. (2018). IT asset management: financial services. https://doi.org/10.6028/NIST.SP.1800-5

Tonysé, M. (2021) Automatización de un sistema de gestión deseguridad de la información basado en la NormaISO/IEC 27001. ISSN 2218-3620 http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2218-36202021000500495

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

Varela, A. M., Méxas, M. P., & Drumond, G. M. (2018). The scenario of software asset management (SAM) in large and midsize companies. Independent Journal of Management & Production, 9(2), 301-320. doi:10.14807/ijmp.v9i2.730

Vega G., Deza D & De los Santos M. (2023) Vulnerabilidades y amenazas en los activos de información: una revisión sistemática Universidad de trujillo DOI:10.51252/rcsi.v3i1.461

WANG, Y. et al. (2015). The interaction effect of IT assets an IT management on firm performance: A system perspective. International Journal of Information Management, v. 35, n. 5, p. 580-593. DOI: 10.1016/j.ijinfomgt.2015.06.006

Zapata C. (2020), Inteligencia artificial para la toma de decisiones ISSN: 2389-8186 doi: https://doi.org/10.16967/23898186.663

ANEXOS

Anexo 1. Matriz de consistencia

<table>
<tr><td colspan="7"><u>Título:</u> Norma internacional ISO/IEC 27001:2022 para la Gestión de Activos de TI en la SUNARP Zona Registral No XI</td></tr>
<tr><td colspan="7"><u>Autores:</u> Ronald Enrique Reyes Ramirez</td></tr>
<tr><th>Problema General</th><th>Objetivo General</th><th>Hipótesis General</th><th>Variables</th><th>Dimensiones</th><th>Indicadores</th><th>Método de investigación</th></tr>
<tr><td>PG: ¿Cómo influye la norma internacional ISO/IEC 27001:2022 en la Gestión de Activos de TI en una institución pública, Ica 2023?</td><td>OG: Determinar la influencia de la norma internacional ISO/IEC 27001:2022 en la Gestión de Activos de TI en una institución pública, Ica 2023.</td><td>HG: La norma internacional ISO/IEC 27001:2022 influye significativamente en la Gestión de Activos de TI en una institución pública, Ica 2023</td><td>Independiente: SGSI según ISO/IEC 27001:2022</td><td colspan="2"></td><td rowspan="17">Tipo de investigación: Aplicada.

Diseño de investigación: Experimental - Pre Experimental.

Enfoque de investigación: Cuantitativo.

Método de investigación: Hipotético-deductivo.

Técnicas e instrumentos de recolección de datos: Encuesta, cuestionario

Población: 11 trabajadores

Muestra: 11 trabajadores

Muestreo: Aleatorio Simple</td></tr>
<tr><th>Problema Específico</th><th>Objetivo Específico</th><th>Hipótesis Específico</th><td rowspan="16">Dependiente: Gestión de Activos de TI</td><td rowspan="5">D1: Activos de Hardware</td><td>I1: Inventario de activos de Hardware</td></tr>
<tr><td>PE1: ¿De qué manera la norma internacional ISO/IEC 27001:2022 influye en la gestión de activos de hardware en una institución pública, Ica 2023?</td><td>OE1: Determinar la influencia de la norma internacional ISO/IEC 27001:2022 en los activos de hardware de la Gestión de Activos de TI en una institución pública, Ica 2023</td><td>HE1: Norma internacional ISO/IEC 27001:2022 influye en los activos de hardware de la Gestión de Activos de TI en una institución pública, Ica 2023</td><td>I2: Clasificación de Activos de Hardware</td></tr>
<tr><td></td><td></td><td></td><td>I3: Vulnerabilidades de Activos de Hardware</td></tr>
<tr><td></td><td></td><td></td><td>I4: Recuperación ante desastres y continuidad del negocio</td></tr>
<tr><td></td><td></td><td></td><td>I5: Cumplimiento de políticas de activos de hardware</td></tr>
<tr><td rowspan="5">PE2: ¿De qué manera la norma internacional ISO/IEC 27001:2022 influye en la gestión de activos de software en una institución pública, Ica 2023?</td><td rowspan="5">OE2: Determinar la influencia de la norma internacional ISO/IEC 27001:2022 en los activos de software de la Gestión de Activos de TI en una institución pública, Ica 2023</td><td rowspan="5">HE2: Norma internacional ISO/IEC 27001:2022 influye en los activos de software de la Gestión de Activos de TI en una institución pública, Ica 2023</td><td rowspan="5">D2: Activos de Software</td><td>I6: Inventario de activos de Software</td></tr>
<tr><td>I7: Clasificación de Activos de Software</td></tr>
<tr><td>I8: Parches y actualizaciones de software</td></tr>
<tr><td>I9: Control de acceso al software</td></tr>
<tr><td>I10:Cumplimiento de políticas de Seguridad de software</td></tr>
<tr><td rowspan="5">PE3: ¿De qué manera la norma internacional ISO/IEC 27001:2022 influye en la gestión de activos de información en una institución pública, Ica 2023?</td><td rowspan="5">OE3: Determinar la influencia de la norma internacional ISO/IEC 27001:2022 en los activos de información de la Gestión de Activos de TI en una institución pública, Ica 2023</td><td rowspan="5">HE3: Norma internacional ISO/IEC 27001:2022 influye en los activos de información de la Gestión de Activos de TI en una institución pública, Ica 2023.</td><td rowspan="5">D3: Activo de Información</td><td>I11: Inventario de activos de información</td></tr>
<tr><td>I12: Clasificación de Activos de información</td></tr>
<tr><td>I13: Propietarios de activos de información</td></tr>
<tr><td>I14: Control de acceso a activos de información</td></tr>
<tr><td>I15:Cumplimiento de políticas de Activos de Información</td></tr>
</table>

Anexo 2. Matriz de Operacionalización y variables

Variable	Definición Conceptual	Definición Operacional	Dimensión	Indicador	Ítems	Instrumentos	Escala de Medición
Norma internacional ISO/IEC 27001:2022	Según ISO/CEI 27001:2022 Tercera edición, proporciona a las empresas de cualquier tamaño y de todos los sectores de actividad una guía para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información aplicando los tres principios Confidencialidad, Integridad de la información y disponibilidad de los datos.	Se variable SGSI operacionalizó en 3 dimensiones, definidas como confidencialidad, integridad y disponibilidad de la información					
Gestión de Activos de TI	Axelos Limited (2019) es cualquier componente de valor financiero que pueda contribuir a la entrega de un producto o servicio de TI. incluye todo el software, hardware, redes, servicios en la nube y dispositivos cliente; también puede incluir activos que no son de TI como edificios o información	Se variable Gestión de Activos de TI operacionalizó en 3 dimensiones, definidas como Activos de Hardware, Activos de Software y Activos de Información.	D1: Activos de Hardware	I1: Inventario de activos de Hardware	1 - 2	Cuestionario	Ordinal
				I2: Clasificación de Activos de Hardware	3 - 4		
				I3: Vulnerabilidades de Activos de Hardware	5 - 6		
				I4: Recuperación ante desastres y continuidad del negocio	7 - 8		
				I5: Cumplimiento de políticas de activos de hardware	9 - 10		
			D2: Activos de Software	I6: Inventario de activos de Software	11 - 12		
				I7: Clasificación de Activos de Software	13 - 14		
				I8: Parches y actualizaciones de software	15 - 16		
				I9: Control de acceso al software	17 - 18		
				I10:Cumplimiento de políticas de Seguridad de software	19 - 20		
			D3: Activo de Información	I11: Inventario de activos de información	21 - 22		
				I12: Clasificación de Activos de información	23 - 24		
				I13: Propietarios de activos de información	25 - 26		
				I14: Control de acceso a activos de información	27 - 28		
				I15:Cumplimiento de políticas de Activos de Información	29 - 30		

Anexo 3. Operacionalización de variable

Tabla 8

Operacionalización de la variable Gestión de Activos de TI

Dimensiones	Indicadores	Ítems	Escalas	Nivel y rango
Activos de Hardware	▪ I1: Inventario de activos de Hardware ▪ I2: Clasificación de Activos de Hardware ▪ I3: Vulnerabilidades y parches de seguridad ▪ I4: Recuperación ante desastres y continuidad del negocio ▪ I5: Cumplimiento de políticas de activos de hardware	1, 2, 3, 4,5, 6, 7, 8, 9, 10	Escala ordinal. Opciones de respuesta: No se ha practicado ni documentado (1) Se ha practicado, pero no documentado o se ha documentado pero no practicado (2) Se ha practicado y documentado (3) Se ha practicado, documentado y revisado en el último año (4) Se ha practicado, documentado, revisado y armonizado según la estrategia empresarial o de TI (5)	Escasa [15 – 34] Regular [35 – 54] Adecuada [55 – 75]
Activos de Software	▪ I6: Inventario de activos de Software ▪ I7: Clasificación de Activos de Software ▪ I8: Parches y actualizaciones de software ▪ I9: Control de acceso al software ▪ I10:Cumplimiento de políticas de Seguridad de software	11, 12, 13, 14, 15, 16, 17, 18, 19, 20		
Activo de Información	▪ I11: Inventario de activos de información ▪ I12: Clasificación de Activos de información ▪ I13: Propietarios de activos de información ▪ I14: Control de acceso a activos de información ▪ I15:Cumplimiento de políticas de Seguridad de software	21, 22, 23, 24, 25, 26, 27, 28, 29, 30		

Anexo 4. Instrumentos de recolección de datos

Encuesta de Gestión de Activos de TI

Se ha diseñado el presente cuestionario con el objeto de tener un buen procedimiento de medición sobre la seguridad de la información, por lo que Necesitamos de su colaboración. Marcar con una (X) de acuerdo a la valoración que usted lo asigna considerando la siguiente leyenda:

1) No se ha practicado ni documentado
2) Se ha practicado pero no documentado o se ha documentado pero no practicado
3) Se ha practicado y documentado
4) Se ha practicado, documentado y revisado en el último año
5) Se ha practicado, documentado, revisado y armonizado según la estrategia empresarial o de TI

		ESCALA				
	DIMENSIONES	1	2	3	4	5
	Dimensión 1. Activos de Hardware					
1	¿Tiene la organización un inventario actualizado y clasificado de activos de hardware?					
2	¿Tiene la organización control del ciclo de vida de los activos de hardware?					
3	¿Tiene la organización clasificado activos de hardware según su importancia y sensibilidad?					
4	¿Tiene la organización identificados los responsables de los activos de información?					
5	¿Tienes un proceso de alertas físicas de activos del Data Center?					
6	¿Tiene un procedimiento para el control de accesos al Data Center?					
7	¿Tiene la organización procedimiento de recuperación ante desastres y continuidad de negocio?					
8	¿Tiene un procedimiento de registro de indisponibilidad de servicios de Red?					
9	¿Tiene un procedimiento para detectar y/o prevenir accesos no autorizados en activos de TI?					
10	¿Tiene un lineamiento para la gestión de interrupción programada de los servicios informáticos?					
	Dimensión 2. Activos de Software					
11	¿Tiene la organización un inventario actualizado y clasificado de activos de software?					
12	¿Tiene un proceso de alertas de servicios críticos de TI?					
13	¿Tiene la organización clasificado los activos de software según su importancia y nivel de riesgo para la organización?					
14	¿Tiene la organización evaluaciones automáticas de vulnerabilidades en el software?					
15	¿Tienes un proceso de detección y respuesta de vulnerabilidades cibernéticas?					
16	¿Tienes un proceso de log de eventos de ataques cibernéticos?					
17	¿Tiene la organización controles de autenticación para garantizar que solo los usuarios autorizados tengan acceso a los activos de software?					
18	¿Tiene un proceso de protección lógica de activos de TI?					
19	¿Tiene un proceso para identificar cambios no autorizados en sistemas de Información?					
20	¿Tienes un procedimiento de Inicio y detención de Base Datos Oracle?					
	Dimensión 3. Activos de Información					
21	¿Tiene la organización un inventario de activos de información críticos de la organización?					
22	¿Tiene un procedimiento de Backup y restore de activos críticos de TI?					
23	¿Tiene la organización clasificada los activos de información según su importancia y sensibilidad?					
24	¿Tiene un proceso para prevenir la fuga de información?					
25	¿Tienes un proceso de control de contratos de servicios de TI?					
26	¿Tiene una directiva para el acceso a las plataformas de TICs?					
27	¿Tiene un procedimiento de revisiones periódicas de los controles de acceso de sistema de información?					
28	¿Tiene un proceso de concientización sobre seguridad de la información y ciberseguridad?					
29	¿Tiene la organización planes de respaldo y recuperación de datos para los activos de información?					
30	¿Tiene un proceso de prevención de errores de Backup de información?					

Anexo 5. Consentimiento

PERÚ | Ministerio de Justicia y Derechos Humanos | Superintendencia Nacional de los Registros Públicos

"Decenio de la Igualdad de oportunidades para mujeres y hombres"
"Año de la unidad, la paz y el desarrollo"

sunarp

Firmado digitalmente por: CARRASCO BENDEZU Carlos Alberto FAU 20163582156 hard
Motivo: Soy Autor del Documento
Fecha: 2023/12/11 09:53:18-0500

ICA, 11 de diciembre de 2023

CARTA No 00283-2023-SUNARP/ZRXI/UA

Sr.
RONALD ENRIQUE REYES RAMIREZ
ICA.-

Asunto Respuesta a Solicitud de fecha 06/12/2023

Referencia Solicitud de fecha 06-12-2023

Es grato dirigirnos a usted con la finalidad de manifestarle que de acuerdo a lo señado en su solicitud, este despacho le otorga el PERMISO, a fin de que pueda obtener información para su trabajo de investigación denominada ***NORMAL INTERNACIONAL ISO/IEC 27001:2022 PARA LA GESTIÓN DE ACTIVOS DE TI EN UNA INSTITUCIÓN PÚBLICA, ICA 2023.***

Sin otro particular, quedo de usted.

Atentamente.

Firmado digitalmente
CARLOS CARRASCO BENDEZU
Jefe (e) Unidad de Administración
ZONA REGISTRAL N° XI SEDE ICA – SUNARP

BICENTENARIO DEL PERÚ 2021 - 2024

Esta es una copia autentica imprimible de un documento electronico archivado por la SUNARP, aplicando lo dispuesto por el Art. 25 del Decreto Supremo No 070-2013-PCM y la Tercera Disposicion Complementaria Final del Decreto Supremo No 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a traves de la siguiente direccion web: https://verificador.sunarp.gob.pe
CVD: 0638836032

Superintendencia Nacional de los Registros Públicos
Sede Central: Av. Primavera N° 1878
Santiago de Surco – Lima
Teléfono: 208-3100 / https://www.gob.pe/sunarp
Canales anticorrupción:
(01) 345 0063 anticorrupcion@sunarp.gob.pe
Buzón anticorrupción: https://anticorrupcion.sunarp.gob.pe/Anticorrupcion

Con Punche Perú

Anexo 6. Matriz Evaluación por juicio de expertos

Primer experto

UCV
UNIVERSIDAD CÉSAR VALLEJO

Evaluación por juicio de expertos

Respetado juez: Usted ha sido seleccionado para evaluar el instrumento "Cuestionario de madurez". La evaluación del instrumento es de gran relevancia para lograr que sea válido y que los resultados obtenidos a partir de éste sean utilizados eficientemente; aportando al quehacer psicológico. Agradecemos su valiosa colaboración.

1. Datos generales del juez

Nombre del juez:	Dr. Cruces José Hernández Guerra
Grado profesional:	Maestría ( ) Doctorado (X)
Área de formación académica:	Clínica ( ) Social ( ) Educativa (X) Organizacional ( )
Áreas de experiencia profesional:	Ingeniería de Sistemas – Docente Investigador en Ingeniería y Comunicación
Institución donde labora:	Universidad Nacional San Luis Gonzaga - Ica
Tiempo de experiencia profesional en el área:	2 a 4 años ( ) Más de 5 años (X)
Experiencia en Investigación Psicométrica: (si corresponde)	-

2. Propósito de la evaluación:

Validar el contenido del instrumento, por juicio de expertos.

3. Datos

Nombre de la Prueba:	Cuestionario de madurez
Autor (a):	Reyes Ramirez Ronald Enrique
Procedencia:	Perú
Administración:	Autocumplimentado
Tiempo de aplicación:	20 minutos
Ámbito de aplicación:	Trabajadores de la Unidad de Tecnología de la Informacion de una institución pública de Ica
Significación:	Nivel de significancia: 0.05

UCV
UNIVERSIDAD CÉSAR VALLEJO

4. Soporte teórico

Variable	Dimensiones	Definición
Gestion de Activos de TI	Activos de Hardware	Axelos Limited (2019) es cualquier componente de valor financiero que pueda contribuir a la entrega de un producto o servicio de TI. incluye todo el software, hardware, redes, servicios en la nube y dispositivos cliente; también puede incluir activos que no son de TI como edificios o información
	Activos de Software	
	Activo de Información	

5. Presentación de instrucciones para el juez:

A continuación, a usted presento el cuestionario de madurez de la Gestion de Activos de TI. De acuerdo con los siguientes indicadores califique cada uno de los ítems según corresponda:

Categoría	Calificación	Indicador
CLARIDAD El ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas.	1. No cumple con el criterio	El ítem no es claro.
	2. Bajo Nivel	El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de estas.
	3. Moderado nivel	Se requiere una modificación muy específica de algunos de los términos del ítem.
	4. Alto nivel	El ítem es claro, tiene semántica y sintaxis adecuada.
COHERENCIA El ítem tiene relación lógica con la dimensión o indicador que está midiendo.	1. Totalmente en desacuerdo (no cumple con el criterio)	El ítem no tiene relación lógica con la dimensión.
	2. Desacuerdo (bajo nivel de acuerdo)	El ítem tiene una relación tangencial /lejana con la dimensión.
	3. Acuerdo (moderado nivel)	El ítem tiene una relación moderada con la dimensión que se está midiendo.
	4. Totalmente de acuerdo (alto nivel)	El ítem se encuentra está relacionado con la dimensión que está midiendo.
RELEVANCIA El ítem es esencial o importante, es decir debe ser incluido.	1. No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión.
	2. Bajo Nivel	El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide éste.
	3. Moderado nivel	El ítem es relativamente importante.
	4. Alto nivel	El ítem es muy relevante y debe ser incluido.

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

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

UCV
UNIVERSIDAD CÉSAR VALLEJO

CERTIFICADO DE VALIDEZ POR JUICIO DE EXPERTOS QUE MIDE LA VARIABLE GESTION DE ACTIVOS DE TI

Cada indicador o ítem debe ser calificado de acuerdo al numeral 5 del presente documento.

Dimensiones del instrumento: Gestion de Activos de TI

- **Primera dimensión: Activos de Hardware**
- Objetivos de la Dimensión: El objetivo de esta dimensión es determinar la madurez de los activos de Hardware con respecto a la norma internacional ISO/IEC 27001:2022 y enfocado a la estrategia institucional, percibido por los trabajadores de la unidad de tecnología de la informacion de una institución pública.

Indicadores	Ítem	Claridad				Coherencia				Relevancia				Observaciones/ Recomendaciones
		1	2	3	4	1	2	3	4	1	2	3	4	
Inventario de activos de Hardware	¿Tiene la organización un inventario actualizado y clasificado de activos de hardware?				✓				✓				✓	
	¿Tiene la organización control del ciclo de vida de los activos de hardware?													
Clasificación de Activos de Hardware	¿Tiene la organización clasificado activos de hardware según su importancia y sensibilidad?				✓				✓				✓	
	¿Tiene la organización identificados los responsables de los activos de información?													
Vulnerabilidades y parches de seguridad	¿Tienes un proceso de alertas físicas de activos del Data Center?				✓				✓				✓	
	¿Tiene un procedimiento para el control de accesos al Data Center?													
Recuperación ante desastres y continuidad del negocio	¿Tiene la organización procedimiento de recuperación ante desastres y continuidad de negocio?				✓				✓				✓	
	¿Tiene un procedimiento de registro de indisponibilidad de servicios de Red?													
Cumplimiento de políticas de activos de hardware	¿Tiene un procedimiento para detectar y/o prevenir accesos no autorizados en activos de TI?				✓				✓				✓	
	¿Tiene un lineamiento para la gestion de interrupción programada de los servicios informáticos?													

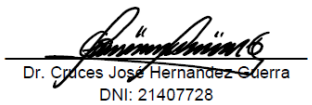
UCV
UNIVERSIDAD CÉSAR VALLEJO

- **Segunda dimensión: Activos de Software**
- Objetivos de la Dimensión: El objetivo de esta dimensión es determinar la madurez de los activos de Software con respecto a la norma internacional ISO/IEC 27001:2022 y enfocado a la estrategia institucional, percibido por los trabajadores de la unidad de tecnología de la informacion de una institución pública.

Indicadores	Ítem	Claridad				Coherencia				Relevancia				Observaciones/ Recomendaciones
		1	2	3	4	1	2	3	4	1	2	3	4	
Inventario de activos de Software	¿Tiene la organización un inventario actualizado y clasificado de activos de software?				✓				✓				✓	
	¿Tiene un proceso de alertas de servicios críticos de TI?													
Clasificación de Activos de Software	¿Tiene la organización clasificado los activos de software según su importancia y nivel de riesgo para la organización?				✓				✓				✓	
	¿Tiene la organización evaluaciones automáticas de vulnerabilidades en el software?													
Parches y actualizaciones de software	¿Tienes un proceso de detección y respuesta de vulnerabilidades cibernéticas?				✓				✓				✓	
	¿Tienes un proceso de log de eventos de ataques cibernéticos?													
Control de acceso al software	¿Tiene la organización controles de autenticación para garantizar que solo los usuarios autorizados tengan acceso a los activos de software?				✓				✓				✓	
	¿Tiene un proceso de protección lógica de activos de TI?													
Cumplimiento de políticas de Seguridad de software	¿Tiene un proceso para identificar cambios no autorizados en sistemas de Informacion?				✓				✓				✓	
	¿Tienes un procedimiento de Inicio y detención de Base Datos Oracle?													

- **Tercera dimensión: Activo de Información**
- Objetivos de la Dimensión: El objetivo de esta dimensión es determinar la madurez de los activos de Informacion con respecto a la norma internacional ISO/IEC 27001:2022 y enfocado a la estrategia institucional, percibido por los trabajadores de la unidad de tecnología de la informacion de una institución pública.

Indicadores	Ítem	Claridad				Coherencia				Relevancia				Observaciones/ Recomendaciones
		1	2	3	4	1	2	3	4	1	2	3	4	
Inventario de activos de informacion	¿Tiene la organización un inventario de activos de información críticos de la organización?				✓				✓				✓	
	¿Tiene un procedimiento de Backup y restore de activos críticos de TI?													
Clasificación de Activos de informacion	¿Tiene la organización clasificada los activos de información según su importancia y sensibilidad?				✓				✓				✓	
	¿Tiene un proceso para prevenir la fuga de informacion?													
Propietarios de activos de información	¿Tienes un proceso de control de contratos de servicios de TI?				✓				✓				✓	
	¿Tiene una directiva para el acceso a las plataformas de TICs?													
Control de acceso a activos de información	¿Tiene un procedimiento de revisiones periódicas de los controles de acceso de sistema de informacion?				✓				✓				✓	
	¿Tiene un proceso de concientización sobre seguridad de la informacion y ciberseguridad?													
Cumplimiento de políticas de Activos de Información	¿Tiene la organización planes de respaldo y recuperación de datos para los activos de información?				✓				✓				✓	
	¿Tiene un proceso de prevención de errores de Backup de informacion?													



Dr. Cruces Jose Hernandez Guerra
DNI: 21407728

Segundo experto

UCV
UNIVERSIDAD CÉSAR VALLEJO

Evaluación por juicio de expertos

Respetado juez: Usted ha sido seleccionado para evaluar el instrumento "Cuestionario de madurez". La evaluación del instrumento es de gran relevancia para lograr que sea válido y que los resultados obtenidos a partir de éste sean utilizados eficientemente; aportando al quehacer psicológico. Agradecemos su valiosa colaboración.

1. Datos generales del juez

Nombre del juez:	Rojas de la cruz, A. Raúl
Grado profesional:	Maestría (X) Doctorado ( )
Área de formación académica:	Clínica ( ) Social ( ) Educativa ( ) Organizacional (X)
Áreas de experiencia profesional:	Unidad de tecnología de la Información
Institución donde labora:	Superintendencia Nacional de los Registral Públicos
Tiempo de experiencia profesional en el área:	2 a 4 años ( ) Más de 5 años (X)
Experiencia en Investigación Psicométrica: (si corresponde)	-

2. Propósito de la evaluación:

Validar el contenido del instrumento, por juicio de expertos.

3. Datos

Nombre de la Prueba:	Cuestionario de madurez
Autor (a):	Reyes Ramirez Ronald Enrique
Procedencia:	Perú
Administración:	Autocumplimentado
Tiempo de aplicación:	20 minutos
Ámbito de aplicación:	Trabajadores de la Unidad de Tecnología de la Informacion de una institución pública de Ica
Significación:	Nivel de significancia: 0.05

UCV
UNIVERSIDAD CÉSAR VALLEJO

4. Soporte teórico

Variable	Dimensiones	Definición
Gestion de Activos de TI	Activos de Hardware	Axelos Limited (2019) es cualquier componente de valor financiero que pueda contribuir a la entrega de un producto o servicio de TI. incluye todo el software, hardware, redes, servicios en la nube y dispositivos cliente; también puede incluir activos que no son de TI como edificios o información
	Activos de Software	
	Activo de Información	

5. Presentación de instrucciones para el juez:

A continuación, a usted presento el cuestionario de cuestionario de madurez de la Gestion de Activos de TI. De acuerdo con los siguientes indicadores califique cada uno de los ítems según corresponda:

Categoría	Calificación	Indicador
CLARIDAD El ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas.	1. No cumple con el criterio	El ítem no es claro.
	2. Bajo Nivel	El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de estas.
	3. Moderado nivel	Se requiere una modificación muy específica de algunos de los términos del ítem.
	4. Alto nivel	El ítem es claro, tiene semántica y sintaxis adecuada.
COHERENCIA El ítem tiene relación lógica con la dimensión o indicador que está midiendo.	1. Totalmente en desacuerdo (no cumple con el criterio)	El ítem no tiene relación lógica con la dimensión.
	2. Desacuerdo (bajo nivel de acuerdo)	El ítem tiene una relación tangencial /lejana con la dimensión.
	3. Acuerdo (moderado nivel)	El ítem tiene una relación moderada con la dimensión que se está midiendo.
	4. Totalmente de acuerdo (alto nivel)	El ítem se encuentra está relacionado con la dimensión que está midiendo.
RELEVANCIA El ítem es esencial o importante, es decir debe ser incluido.	1. No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión.
	2. Bajo Nivel	El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide éste.
	3. Moderado nivel	El ítem es relativamente importante.
	4. Alto nivel	El ítem es muy relevante y debe ser incluido.

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

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

UCV
UNIVERSIDAD CÉSAR VALLEJO

CERTIFICADO DE VALIDEZ POR JUICIO DE EXPERTOS QUE MIDE LA VARIABLE GESTION DE ACTIVOS DE TI

Cada Indicador o Ítem debe ser calificado de acuerdo al numeral 5 del presente documento.

Dimensiones del instrumento: Gestion de Activos de TI

- **Primera dimensión: Activos de Hardware**
- Objetivos de la Dimensión: El objetivo de esta dimensión es determinar la madurez de los activos de Hardware con respecto a la norma internacional ISO/IEC 27001:2022 y enfocado a la estrategia institucional, percibido por los trabajadores de la unidad de tecnología de la informacion de una institución pública.

Indicadores	Ítem	Claridad				Coherencia				Relevancia				Observaciones/ Recomendaciones
		1	2	3	4	1	2	3	4	1	2	3	4	
Inventario de activos de Hardware	¿Tiene la organización un inventario actualizado y clasificado de activos de hardware?				✓				✓				✓	
	¿Tiene la organización control del ciclo de vida de los activos de hardware?													
Clasificación de Activos de Hardware	¿Tiene la organización clasificado activos de hardware según su importancia y sensibilidad?				✓				✓				✓	
	¿Tiene la organización identificados los responsables de los activos de información?													
Vulnerabilidades y parches de seguridad	¿Tienes un proceso de alertas físicas de activos del Data Center?				✓				✓				✓	
	¿Tiene un procedimiento para el control de accesos al Data Center?													
Recuperación ante desastres y continuidad del negocio	¿Tiene la organización procedimiento de recuperación ante desastres y continuidad de negocio?				✓				✓				✓	
	¿Tiene un procedimiento de registro de indisponibilidad de servicios de Red?													
Cumplimiento de políticas de activos de hardware	¿Tiene un procedimiento para detectar y/o prevenir accesos no autorizados en activos de TI?				✓				✓				✓	
	¿Tiene un lineamiento para la gestion de interrupción programada de los servicios informáticos?													

UCV
UNIVERSIDAD CÉSAR VALLEJO

- **Segunda dimensión: Activos de Software**
- Objetivos de la Dimensión: El objetivo de esta dimensión es determinar la madurez de los activos de Software con respecto a la norma internacional ISO/IEC 27001:2022 y enfocado a la estrategia institucional, percibido por los trabajadores de la unidad de tecnología de la informacion de una institución pública.

Indicadores	Ítem	Claridad				Coherencia				Relevancia				Observaciones/ Recomendaciones
		1	2	3	4	1	2	3	4	1	2	3	4	
Inventario de activos de Software	¿Tiene la organización un inventario actualizado y clasificado de activos de software?				✓				✓				✓	
	¿Tiene un proceso de alertas de servicios críticos de TI?													
Clasificación de Activos de Software	¿Tiene la organización clasificado los activos de software según su importancia y nivel de riesgo para la organización?				✓				✓				✓	
	¿Tiene la organización evaluaciones automáticas de vulnerabilidades en el software?													
Parches y actualizaciones de software	¿Tienes un proceso de detección y respuesta de vulnerabilidades cibernéticas?				✓				✓				✓	
	¿Tienes un proceso de log de eventos de ataques cibernéticos?													
Control de acceso al software	¿Tiene la organización controles de autenticación para garantizar que solo los usuarios autorizados tengan acceso a los activos de software?				✓				✓				✓	
	¿Tiene un proceso de protección lógica de activos de TI?													
Cumplimiento de políticas de Seguridad de software	¿Tiene un proceso para identificar cambios no autorizados en sistemas de Informacion?				✓				✓				✓	
	¿Tienes un procedimiento de Inicio y detención de Base Datos Oracle?													

UCV
UNIVERSIDAD CÉSAR VALLEJO

- **Tercera dimensión: Activo de Información**
- Objetivos de la Dimensión: El objetivo de esta dimensión es determinar la madurez de los activos de Informacion con respecto a la norma internacional ISO/IEC 27001:2022 y enfocado a la estrategia institucional, percibido por los trabajadores de la unidad de tecnología de la informacion de una institución pública.

Indicadores	Ítem	Claridad				Coherencia				Relevancia				Observaciones/ Recomendaciones
		1	2	3	4	1	2	3	4	1	2	3	4	
Inventario de activos de informacion	¿Tiene la organización un inventario de activos de información críticos de la organización?				✓				✓				✓	
	¿Tiene un procedimiento de Backup y restore de activos críticos de TI?													
Clasificación de Activos de informacion	¿Tiene la organización clasificada los activos de información según su importancia y sensibilidad?				✓				✓				✓	
	¿Tiene un proceso para prevenir la fuga de informacion?													
Propietarios de activos de información	¿Tienes un proceso de control de contratos de servicios de TI?				✓				✓				✓	
	¿Tiene una directiva para el acceso a las plataformas de TICs?													
Control de acceso a activos de información	¿Tiene un procedimiento de revisiones periódicas de los controles de acceso de sistema de informacion?				✓				✓				✓	
	¿Tiene un proceso de concientización sobre seguridad de la informacion y ciberseguridad?													
Cumplimiento de políticas de Activos de Información	¿Tiene la organización planes de respaldo y recuperación de datos para los activos de información?				✓				✓				✓	
	¿Tiene un proceso de prevención de errores de Backup de informacion?													

A Raul Rojas de la Cruz
DNI: 10113760

Tercer experto

UCV
UNIVERSIDAD CÉSAR VALLEJO

Evaluación por juicio de expertos

Respetado juez: Usted ha sido seleccionado para evaluar el instrumento "Cuestionario de madurez". La evaluación del instrumento es de gran relevancia para lograr que sea válido y que los resultados obtenidos a partir de éste sean utilizados eficientemente; aportando al quehacer psicológico. Agradecemos su valiosa colaboración.

1. Datos generales del juez

Nombre del juez:	Quispe Tincopa, Lino Martin
Grado profesional:	Maestría ( ) Doctorado (X)
Área de formación académica:	Clínica ( ) Social ( ) Educativa (X) Organizacional (X)
Áreas de experiencia profesional:	Catedrático
Institución donde labora:	Universidad Nacional San Luis Gonzaga de Ica
Tiempo de experiencia profesional en el área:	2 a 4 años ( ) Más de 5 años (X)
Experiencia en Investigación Psicométrica: (si corresponde)	-

2. Propósito de la evaluación:

Validar el contenido del instrumento, por juicio de expertos.

3. Datos

Nombre de la Prueba:	Cuestionario de madurez
Autor (a):	Reyes Ramirez Ronald Enrique
Procedencia:	Perú
Administración:	Autocumplimentado
Tiempo de aplicación:	20 minutos
Ámbito de aplicación:	Trabajadores de la Unidad de Tecnología de la Informacion de una institución pública de Ica
Significación:	Nivel de significancia: 0.05

UCV
UNIVERSIDAD CÉSAR VALLEJO

4. Soporte teórico

Variable	Dimensiones	Definición
Gestion de Activos de TI	Activos de Hardware	Axelos Limited (2019) es cualquier componente de valor financiero que pueda contribuir a la entrega de un producto o servicio de TI. incluye todo el software, hardware, redes, servicios en la nube y dispositivos cliente; también puede incluir activos que no son de TI como edificios o información
	Activos de Software	
	Activo de Información	

5. Presentación de instrucciones para el juez:

A continuación, a usted presento el cuestionario de cuestionario de madurez de la Gestion de Activos de TI. De acuerdo con los siguientes indicadores califique cada uno de los ítems según corresponda:

Categoría	Calificación	Indicador
CLARIDAD El ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas.	1. No cumple con el criterio	El ítem no es claro.
	2. Bajo Nivel	El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de estas.
	3. Moderado nivel	Se requiere una modificación muy específica de algunos de los términos del ítem.
	4. Alto nivel	El ítem es claro, tiene semántica y sintaxis adecuada.
COHERENCIA El ítem tiene relación lógica con la dimensión o indicador que está midiendo.	1. Totalmente en desacuerdo (no cumple con el criterio)	El ítem no tiene relación lógica con la dimensión.
	2. Desacuerdo (bajo nivel de acuerdo)	El ítem tiene una relación tangencial /lejana con la dimensión.
	3. Acuerdo (moderado nivel)	El ítem tiene una relación moderada con la dimensión que se está midiendo.
	4. Totalmente de acuerdo (alto nivel)	El ítem se encuentra está relacionado con la dimensión que está midiendo.
RELEVANCIA El ítem es esencial o importante, es decir debe ser incluido.	1. No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión.
	2. Bajo Nivel	El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide éste.
	3. Moderado nivel	El ítem es relativamente importante.
	4. Alto nivel	El ítem es muy relevante y debe ser incluido.

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

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

UCV
UNIVERSIDAD CÉSAR VALLEJO

CERTIFICADO DE VALIDEZ POR JUICIO DE EXPERTOS QUE MIDE LA VARIABLE GESTION DE ACTIVOS DE TI

Cada indicador o ítem debe ser calificado de acuerdo al numeral 5 del presente documento.

Dimensiones del instrumento: Gestion de Activos de TI

- **Primera dimensión: Activos de Hardware**
- Objetivos de la Dimensión: El objetivo de esta dimensión es determinar la madurez de los activos de Hardware con respecto a la norma internacional ISO/IEC 27001:2022 y enfocado a la estrategia institucional, percibido por los trabajadores de la unidad de tecnología de la informacion de una institución pública.

Indicadores	Ítem	Claridad				Coherencia				Relevancia				Observaciones/ Recomendaciones
		1	2	3	4	1	2	3	4	1	2	3	4	
Inventario de activos de Hardware	¿Tiene la organización un inventario actualizado y clasificado de activos de hardware?				✓				✓				✓	
	¿Tiene la organización control del ciclo de vida de los activos de hardware?													
Clasificación de Activos de Hardware	¿Tiene la organización clasificado activos de hardware según su importancia y sensibilidad?				✓				✓				✓	
	¿Tiene la organización identificados los responsables de los activos de información?													
Vulnerabilidades y parches de seguridad	¿Tienes un proceso de alertas físicas de activos del Data Center?				✓				✓				✓	
	¿Tiene un procedimiento para el control de accesos al Data Center?													
Recuperación ante desastres y continuidad del negocio	¿Tiene la organización procedimiento de recuperación ante desastres y continuidad de negocio?				✓				✓				✓	
	¿Tiene un procedimiento de registro de indisponibilidad de servicios de Red?													
Cumplimiento de políticas de activos de hardware	¿Tiene un procedimiento para detectar y/o prevenir accesos no autorizados en activos de TI?				✓				✓				✓	
	¿Tiene un lineamiento para la gestion de interrupción programada de los servicios informáticos?													

UCV
UNIVERSIDAD CÉSAR VALLEJO

- **Segunda dimensión: Activos de Software**
- Objetivos de la Dimensión: El objetivo de esta dimensión es determinar la madurez de los activos de Software con respecto a la norma internacional ISO/IEC 27001:2022 y enfocado a la estrategia institucional, percibido por los trabajadores de la unidad de tecnología de la informacion de una institución pública.

Indicadores	Ítem	Claridad				Coherencia				Relevancia				Observaciones/ Recomendaciones
		1	2	3	4	1	2	3	4	1	2	3	4	
Inventario de activos de Software	¿Tiene la organización un inventario actualizado y clasificado de activos de software?				✓				✓				✓	
	¿Tiene un proceso de alertas de servicios críticos de TI?													
Clasificación de Activos de Software	¿Tiene la organización clasificado los activos de software según su importancia y nivel de riesgo para la organización?				✓				✓				✓	
	¿Tiene la organización evaluaciones automáticas de vulnerabilidades en el software?													
Parches y actualizaciones de software	¿Tienes un proceso de detección y respuesta de vulnerabilidades cibernéticas?				✓				✓				✓	
	¿Tienes un proceso de log de eventos de ataques cibernéticos?													
Control de acceso al software	¿Tiene la organización controles de autenticación para garantizar que solo los usuarios autorizados tengan acceso a los activos de software?				✓				✓				✓	
	¿Tiene un proceso de protección lógica de activos de TI?													
Cumplimiento de políticas de Seguridad de software	¿Tiene un proceso para identificar cambios no autorizados en sistemas de Informacion?				✓				✓				✓	
	¿Tienes un procedimiento de Inicio y detención de Base Datos Oracle?													

UCV
UNIVERSIDAD CÉSAR VALLEJO

- **Tercera dimensión: Activo de Información**
- Objetivos de la Dimensión: El objetivo de esta dimensión es determinar la madurez de los activos de Informacion con respecto a la norma internacional ISO/IEC 27001:2022 y enfocado a la estrategia institucional, percibido por los trabajadores de la unidad de tecnología de la informacion de una institución pública.

Indicadores	Ítem	Claridad				Coherencia				Relevancia				Observaciones/ Recomendaciones
		1	2	3	4	1	2	3	4	1	2	3	4	
Inventario de activos de informacion	¿Tiene la organización un inventario de activos de información críticos de la organización?				✓				✓				✓	
	¿Tiene un procedimiento de Backup y restore de activos críticos de TI?													
Clasificación de Activos de informacion	¿Tiene la organización clasificada los activos de información según su importancia y sensibilidad?				✓				✓				✓	
	¿Tiene un proceso para prevenir la fuga de informacion?													
Propietarios de activos de información	¿Tienes un proceso de control de contratos de servicios de TI?				✓				✓				✓	
	¿Tiene una directiva para el acceso a las plataformas de TICs?													
Control de acceso a activos de información	¿Tiene un procedimiento de revisiones periódicas de los controles de acceso de sistema de informacion?				✓				✓				✓	
	¿Tiene un proceso de concientización sobre seguridad de la informacion y ciberseguridad?													
Cumplimiento de políticas de Activos de Información	¿Tiene la organización planes de respaldo y recuperación de datos para los activos de información?				✓				✓				✓	
	¿Tiene un proceso de prevención de errores de Backup de informacion?													

Lino M. Quispe Tinpoca
DNI: 21564811

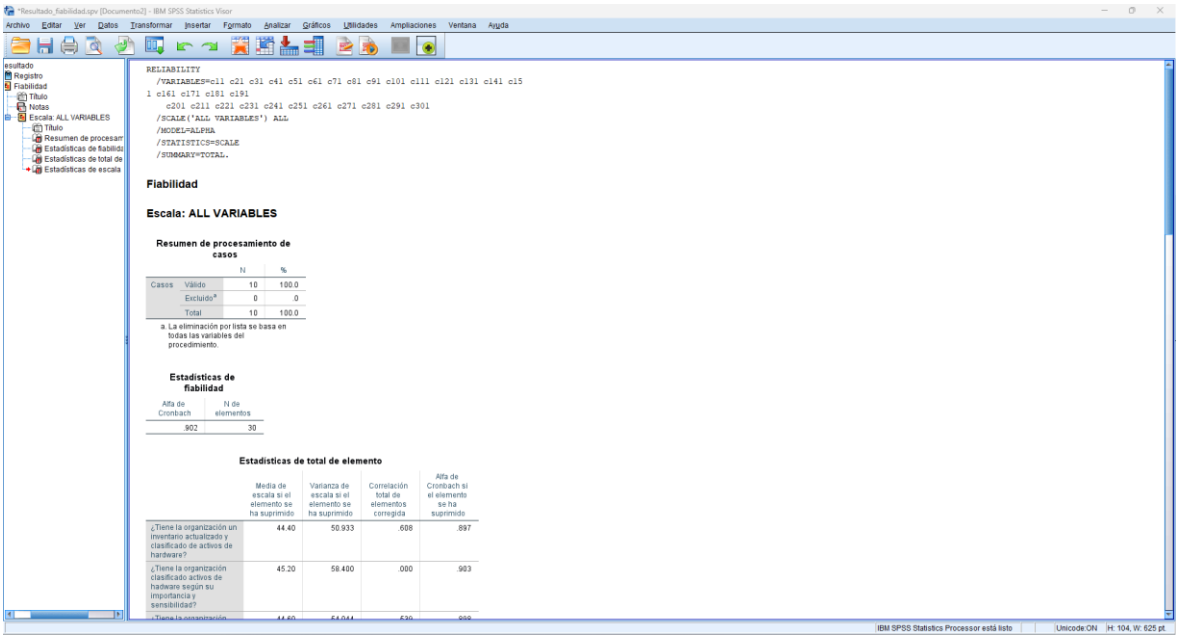
Anexo 7. Confiabilidad

Tabla 9

Análisis de fiabilidad

Instrumento	Alfa de Cronbach	N° de elementos
Cuestionario de Gestión de activos	0.902	30

Confiabilidad del cuestionario de Gestión de activos



```
RELIABILITY
  /VARIABLES=c11 c21 c31 c41 c51 c61 c71 c81 c91 c101 c111 c121 c131 c141 c15
1 c161 c171 c181 c191
    c201 c211 c221 c231 c241 c251 c261 c271 c281 c291 c301
  /SCALE('ALL VARIABLES') ALL
  /MODEL=ALPHA
  /STATISTICS=SCALE
  /SUMMARY=TOTAL.
```

Fiabilidad

Escala: ALL VARIABLES

Resumen de procesamiento de casos

		N	%
Casos	Válido	10	100.0
	Excluido[a]	0	.0
	Total	10	100.0

a. La eliminación por lista se basa en todas las variables del procedimiento.

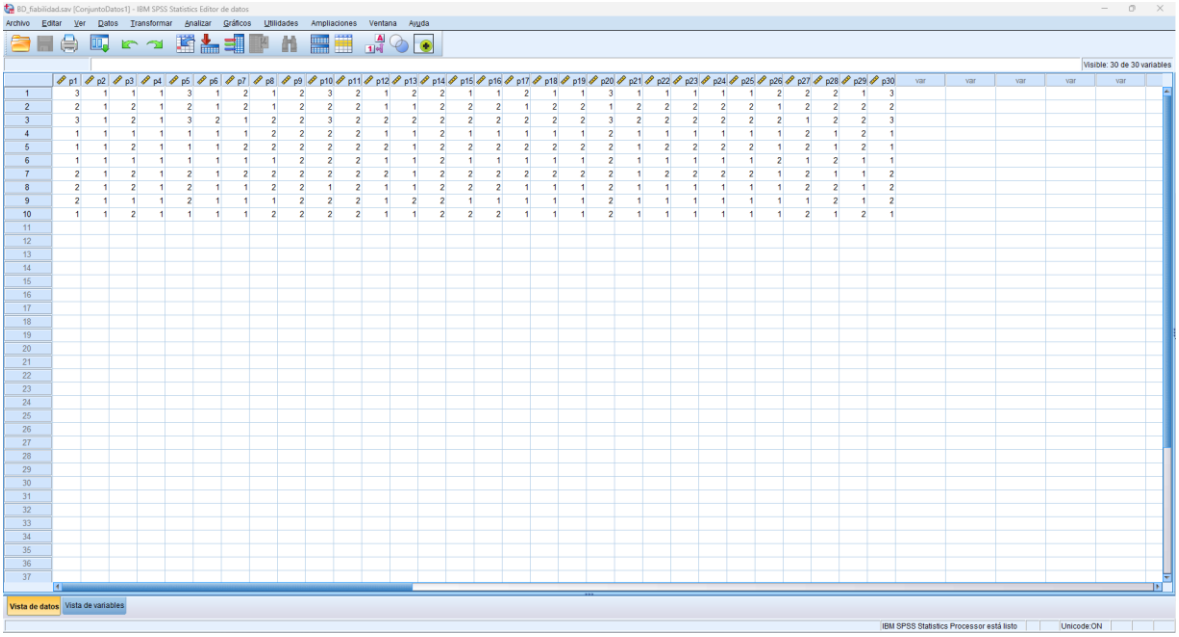
Estadísticas de fiabilidad

Alfa de Cronbach	N de elementos
.902	30

Estadísticas de total de elemento

	Media de escala si el elemento se ha suprimido	Varianza de escala si el elemento se ha suprimido	Correlación total de elementos corregida	Alfa de Cronbach si el elemento se ha suprimido
¿Tiene la organización un inventario actualizado y clasificado de activos de hardware?	44.40	50.933	.608	.897
¿Tiene la organización clasificado activos de hardware segun su importancia y sensibilidad?	45.20	58.400	.000	.903

Base de datos de la prueba piloto



	p1	p2	p3	p4	p5	p6	p7	p8	p9	p10	p11	p12	p13	p14	p15	p16	p17	p18	p19	p20	p21	p22	p23	p24	p25	p26	p27	p28	p29	p30
1	3	1	1	1	3	1	2	1	2	3	2	1	2	2	1	1	2	1	1	3	1	1	1	1	1	2	2	2	1	3
2	2	1	2	1	2	1	2	1	2	2	2	1	1	2	2	2	1	2	2	1	2	2	2	2	2	1	2	2	2	2
3	3	1	2	1	3	2	1	2	2	3	2	2	2	2	2	2	2	2	2	3	2	2	2	2	2	2	1	2	2	3
4	1	1	1	1	1	1	1	2	2	2	2	1	1	2	1	1	1	1	1	2	1	1	1	1	1	1	2	1	2	1
5	1	1	2	1	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	2	1	2	2	2	2	1	2	1	2	1
6	1	1	1	1	1	1	1	1	2	2	2	1	1	2	1	1	1	1	1	2	1	1	1	1	1	2	1	2	1	1
7	2	1	2	1	2	1	2	2	2	2	2	2	1	2	2	2	2	2	2	2	1	2	2	2	2	1	2	1	1	2
8	2	1	2	1	2	1	1	2	2	1	2	1	1	2	2	2	1	1	1	2	1	1	1	1	1	1	2	2	1	2
9	2	1	1	1	2	1	1	1	2	2	2	1	2	2	1	1	1	1	1	2	1	1	1	1	1	1	2	1	2	2
10	1	1	2	1	1	1	1	2	2	2	2	1	1	2	2	2	1	1	1	2	1	1	1	1	1	1	2	1	2	1

Anexo 8. Base de datos

Base de datos del pretest

Gestión de activos de TI

	Activos de hardware									Activos de software										Activos de información									
	c1	c2	c3	c4	c5	c6	c7	c8	c9	c10	c11	c12	c13	c14	c15	c16	c17	c18	c19	c20	c21	c22	c23	c24	c25	c26	c27	c28	c29	c30
1	2	1	1	1	2	1	1	1	2	2	2	1	1	2	2	2	1	2	1	2	1	1	2	2	1	2	1	2	1	1
2	2	1	2	1	1	1	2	2	2	2	2	2	1	2	1	1	2	2	2	2	1	2	2	2	2	1	2	1	1	2
3	2	1	2	1	2	1	1	2	2	1	2	1	1	2	2	2	1	1	2	2	1	2	1	2	1	1	2	2	1	2
4	2	1	1	1	1	1	1	1	2	2	2	1	2	2	1	2	1	1	1	2	1	2	2	3	1	1	1	2	1	2
5	1	1	2	1	1	1	2	2	2	2	2	2	1	2	2	2	2	2	1	2	1	2	1	2	2	1	2	1	2	1
6	1	1	2	1	2	1	2	2	2	2	2	1	1	1	2	2	2	2	2	1	1	1	2	3	1	2	1	1	2	1
7	2	2	2	1	1	1	2	1	2	3	2	1	2	2	1	2	2	2	1	3	1	1	1	3	1	2	2	2	1	3
8	2	1	1	1	2	1	2	1	2	2	2	1	1	2	1	2	1	2	1	1	2	1	2	3	2	1	2	2	2	2
9	2	1	2	1	2	2	1	2	2	3	2	2	2	2	2	1	2	1	1	3	2	1	2	2	2	2	1	2	2	3
10	2	1	2	1	2	1	1	2	2	2	2	1	1	2	2	1	1	2	2	2	1	1	2	2	1	1	2	1	2	1
11	2	1	1	1	1	1	1	1	2	2	2	1	2	2	2	1	2	2	2	2	2	1	1	2	1	2	2	1	1	1

Base de datos del postest

Gestión de activos de TI

Activos de hardware										Activos de software										Activos de información									
c1	c2	c3	c4	c5	c6	c7	c8	c9	c10	c11	c12	c13	c14	c15	c16	c17	c18	c19	c20	c21	c22	c23	c24	c25	c26	c27	c28	c29	c30
5	5	3	4	4	4	4	4	5	5	3	3	5	5	5	4	3	4	3	4	3	5	3	5	4	5	3	4	5	4
3	4	5	5	4	4	4	5	4	5	5	3	3	4	4	3	4	4	4	5	3	5	3	5	3	4	3	4	5	5
3	3	4	5	3	4	4	5	4	5	4	3	5	3	4	4	4	3	5	4	4	4	5	4	5	4	3	4	5	5
5	3	3	4	4	3	5	4	4	4	3	4	3	3	5	4	4	5	3	4	4	3	5	5	5	5	5	4	3	3
3	4	3	3	3	5	4	5	5	5	5	3	4	5	4	3	3	5	4	5	3	3	3	5	4	4	5	5	4	3
5	3	5	4	5	4	5	4	4	4	5	3	3	5	4	3	4	3	4	4	3	3	5	5	3	4	4	4	5	3
5	3	5	3	3	3	4	4	5	4	3	5	4	4	3	5	4	3	5	5	4	4	3	5	5	4	3	4	5	3
5	5	4	5	4	4	4	5	4	5	3	3	4	5	4	4	4	3	4	5	4	5	3	4	4	5	5	4	3	5
4	5	3	3	5	3	4	4	5	5	5	5	3	5	3	4	3	5	5	4	4	3	3	5	4	4	5	4	4	4
4	4	5	3	4	5	4	5	4	4	3	3	4	3	4	4	4	4	4	5	4	5	3	5	3	4	3	4	5	5
3	5	5	3	5	3	5	4	4	4	5	4	3	5	5	4	3	5	5	5	4	4	3	5	5	4	4	4	5	3

Anexo 9. Evidencias de implementación y de metodología utilizada.

ANEXO 01 - INVENTARIO Y CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN

N°	ACTIVO	DESCRIPCIÓN	CATEGORÍA	SBN	UBICACIÓN FÍSICA	UBICACIÓN ELECTRÓNICA (LÓGICA)	CLASIFICACIÓN			FRECUENCIA DE USO					PROPIETARIO	CUSTODIO	REQUISITOS LEGALES, REGULATORIOS Y CONTRACTUALES	VALOR DEL			VALOR DEL ACTIVO	NIVEL DE TASACIÓN
							PÚBLICA	USO INTERNO	USO RESTRINGIDO	DIARIO	SEMANAL	QUINCENAL	MENSUAL	EVENTUAL				CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD		
ACTIVOS DE INFORMACIÓN																						
27	UPS CENTIEL 1	UPS REDUNDANTE DE CENTRO DE DATOS	F5		Centro de Datos			X	X	X					UTI	UTI		2	5	5	4,00	Alto
28	UPS CENTIEL 2	UPS REDUNDANTE DE CENTRO DE DATOS	F5		Centro de Datos			X	X	X					UTI	UTI		2	5	5	4,00	Alto
29	FIREWALL FG601E	FIREWALL FORTINET FG601E	F2	8195	Centro de Datos			X	X	X					UTI	UTI		1	1	5	2,33	Medio
30	FIREWALL FG601E	FIREWALL FORTINET FG601E	F2	8196	Centro de Datos			X	X	X					UTI	UTI		1	1	5	2,33	Medio
31	SERVIDOR DELL POWER EDGE R640	SERVIDOR SIGA	F1	7694	Centro de Datos			X	X	X					UTI	UTI		2	5	5	4,00	Alto
32	SERVIDOR DELL POWER EDGE R640	SERVIDOR DE BACKUP VERITAS	F1	7693	Centro de Datos			X	X	X					UTI	UTI		2	5	5	4,00	Alto
33	IBM MONITOR PLANO	IBM MONITOR PLANO	F5	4486	Centro de Datos			X	X	X					UTI	UTI		1	1	1	1,00	Bajo
34	IBM SWITCH PARA RED	IBM SWITCH KVM	F5	4499	Centro de Datos			X	X	X					UTI	UTI		1	1	1	1,00	Bajo
35	LIBRERÍA DE BACKUP	LIBRERÍA DE BACKUP TS 3100	F1	6820	Centro de Datos			X	X	X					UTI	UTI		2	5	5	4,00	Alto
36	SERVIDOR PROLIANT DL360 P GEN 8	Servidor de Directorio Activo	F1	6572	Centro de Datos			X	X	X					UTI	UTI		2	5	5	4,00	Alto
37	STORAGE EXPANSIÓN V7000	STORAGE V7000 EXPANSION	F3	4785	Centro de Datos			X	X	X					UTI	UTI		2	3	4	3,00	Medio
38	STORAGE CONTROLADORA PRINCIPAL V7000	STORAGE V7000	F3	4485	Centro de Datos			X	X	X					UTI	UTI		2	3	4	3,00	Medio
39	SERVIDOR CHASIS BLADE	Servidor de Virtualización de contingencia	F1	4481	Centro de Datos			X	X	X					UTI	UTI		2	3	4	3,00	Medio
40	SW RED BLADE 1	Servidor de Virtualización de contingencia	F2		Centro de Datos			X	X	X					UTI	UTI		2	3	4	3,00	Medio
41	SW RED BLADE 2	Servidor de Virtualización de contingencia	F2		Centro de Datos			X	X	X					UTI	UTI		2	3	4	3,00	Medio
42	SAN FO BLADE 1	Servidor de Virtualización de contingencia	F2		Centro de Datos			X	X	X					UTI	UTI		2	3	4	3,00	Medio
43	SAN FO BLADE 2	Servidor de Virtualización de contingencia	F2		Centro de Datos			X	X	X					UTI	UTI		2	3	4	3,00	Medio
44	SERVIDOR BLADE 1	Servidor de Virtualización de contingencia	F1	4482	Centro de Datos			X	X	X					UTI	UTI		2	3	4	3,00	Medio
45	SERVIDOR BLADE 2	Servidor de Virtualización de contingencia	F1	4483	Centro de Datos			X	X	X					UTI	UTI		2	3	4	3,00	Medio
46	SERVIDOR BLADE 3	Servidor de Virtualización de contingencia	F1	4484	Centro de Datos			X	X	X					UTI	UTI		2	3	4	3,00	Medio
47	SERVIDOR BLADE 4	Servidor de Virtualización de contingencia	F1	4487	Centro de Datos			X	X	X					UTI	UTI		2	3	4	3,00	Medio
48	SERVIDOR BLADE 5	Servidor de Virtualización de contingencia	F1	4782	Centro de Datos			X	X	X					UTI	UTI		2	3	4	3,00	Medio
49	SERVIDOR BLADE 6	Servidor de Virtualización de contingencia	F1	4783	Centro de Datos			X	X	X					UTI	UTI		2	3	4	3,00	Medio
50	SERVIDOR BLADE 7	Servidor de Virtualización de contingencia	F1	4784	Centro de Datos			X	X	X					UTI	UTI		2	3	4	3,00	Medio
51	SERVIDOR ALLOT	ALLOT SSG200-200M	F1	-	Centro de Datos			X	X	X					UTI	UTI		1	2	2	1,67	Bajo
52	SWITCH CORE HPE 5510-24G	SWITCH CORE HPE 5510-24G	F2	6748	Centro de Datos			X	X	X					UTI	UTI		2	5	5	4,00	Alto
53	SWITCH CORE HPE 5510-48G	SWITCH CORE HPE 5510-48G	F2	6749	Centro de Datos			X	X	X					UTI	UTI		2	5	5	4,00	Alto
54	SWITCH PISO	SWITCH PISO 2 - 5510-48G-4SFP	F2	7746	Centro de Datos			X	X	X					UTI	UTI		1	2	3	2,00	Medio
55	SWITCH PISO	SWITCH PISO 2 - HPE 5130 - JH324A	F2	6753	Centro de Datos			X	X	X					UTI	UTI		1	2	3	2,00	Medio
56	Switch	SWITCH C9200L 48 4X10G	F2	7830	Centro de Datos			X	X	X					UTI	UTI		1	2	3	2,00	Medio
57	NVR DAHUA	DAHUA	F5	7319	Centro de Datos			X	X	X					UTI	UTI		1	1	1	1,00	Bajo
58	NVR HIKVISION	HIKVISION DS-7608NI	F5	7742	Centro de Datos			X	X	X					UTI	UTI		1	1	1	1,00	Bajo
59	CMC III	SENSORES DE IOT RITAL	F5	-	Centro de Datos			X	X	X					UTI	UTI		1	1	1	1,00	Bajo
60	CENTRAL TELEFÓNICA	CENTRAL TELEFÓNICA HUAWEI	F2	7434	Centro de Datos			X	X	X					UTI	UTI		1	1	1	1,00	Bajo
61	FIREWALL	FIREWALL FORTINET FG-100E	F2	8184	Centro de Datos			X	X	X					UTI	UTI		1	1	1	1,00	Bajo
62	Switch cisco	SWITCH CISCO C2960-X SERIES	F2	-	Centro de Datos	172.20.117.10		X	X	X					TERCEROS	UTI		1	1	1	1,00	Bajo

ANEXO 02 - ANÁLISIS DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

N°	TIPO DE ACTIVO	ACTIVO	AMENAZA		MECANISMO DE PROTECCIÓN EXISTENTE						VULNERABILIDAD		RIESGO	
			Descripción de la Amenaza	Nivel prob. de Amenaza	Preventivo (antes)	Nivel de Capacidad	Detectivo (durante)	Nivel de Capacidad	Correctivo (después)	Nivel de Capacidad	Descripción	Nivel de Vulnerabilidad	Probabilidad de Ocurrencia	Nivel de Probabilidad de Ocurrencia
SERVICIOS														
1	SERVICIOS DE TI	SERVICIO DE TRANSMISIÓN DE DATOS SERVICIO DE INTERNET	Naturales o ambientales (Terremoto, tsunami, inundación, tormenta eléctrica, etc.)	1	Ninguno	1	Ninguno	1	Capacidad de respuesta según contrato con proveedor de servicios	1	No se cuenta con un site alterno de contingencia desde el cual se pueda recibir el servicio del proveedor	5,00	3,00	Medio
			Accidentales (Inundaciones, Incendios, etc.)	1	Gestión del servicio a cargo del contratista	4	Gestión del servicio a cargo del contratista	4	Capacidad de respuesta según contrato con proveedor de servicios	4	No se cuenta con un site alterno de contingencia desde el cual se pueda recibir el servicio del proveedor.	2,00	1,50	Bajo
			Accidentales (Error humano, Impericia)	1	Gestión del servicio a cargo del contratista	4	Gestión del servicio a cargo del contratista	4	Gestión del servicio a cargo del contratista	4	Gestión del servicio a cargo del contratista	2,00	1,50	Bajo
			Tecnológicos (error de software, hardware, vulnerabilidades)	1	Gestión del servicio a cargo del contratista	4	Gestión del servicio a cargo del contratista	4	Gestión del servicio a cargo del contratista	4	Gestión del servicio a cargo del contratista	2,00	1,50	Bajo
2	SERVICIOS DE TI	BASE DE DATOS ORACLE	Naturales o ambientales (Terremoto, tsunami, inundación, tormenta eléctrica, etc.)	1	Ninguno	1	Ninguno	1	Ninguno	1	No se cuenta con un site alterno para la activación de servicios de contingencia	5,00	3,00	Medio
			Accidentales (Inundaciones, Incendios, etc.)	1	Sistema contra incendios Sensores de aniegos Sensores de temperatura Sistemas redundantes	3	Detectores de Humo y aniegos Monitoreo de centro de datos	3	Capacidad de respuesta a nivel del personal de UTI, según recursos disponibles	3	No se cuenta con un informe que evidencie la operatividad actual de los mecanismos preventivos de seguridad del centro de datos.	3,00	2,00	Medio
			Accidentales (Error humano, Impericia)	2	Instructivos de operación de Bases de Datos Cluster de Base de Datos Contratos de mantenimiento preventivo y soporte técnico. Backup de la información	3	Supervisión de personal de UTI	1	Informe de ocurrencia de incidente y acciones de respuesta inmediata de acuerdo a procedimientos establecidos.	2	Dependencia de proveedores externos para el soporte Falta de conocimiento avanzados en la Gestión del servicio de base de datos para el personal de UTI	4,00	3,00	Medio
			Tecnológicos (error de software, hardware, vulnerabilidades)	3	Contratos de mantenimiento preventivo y soporte técnico. Backup de la información	2	Contratos de mantenimiento preventivo y soporte técnico. Apoyo del personal de OTI	2	Contratos de mantenimiento preventivo y soporte técnico	1	Dependencia de proveedores externos para el soporte. Garantía de fabricante del hardware del storage vencida	4,33	3,67	Alto
		SERVICIO DE DIRECTORIO ACTIVO	Naturales o ambientales (Terremoto, tsunami, inundación, tormenta eléctrica, etc.)	1	Ninguno	1	Ninguno	2	Redundancia de controladores de Directorio Activo a nivel Nacional	3	No se cuenta con un site alterno para la activación de servicios de contingencia	4,00	2,50	Medio
			Accidentales (Inundaciones, Incendios, etc.)	1	Sistema contra incendios Sensores de aniegos Sensores de temperatura Sistemas de energía redundantes	3	Detectores de Humo y aniegos Monitoreo de centro de datos	4	Redundancia de controladores de Directorio Activo a nivel Nacional	4	No se cuenta con un informe que evidencie la operatividad actual de los mecanismos preventivos de seguridad del centro de datos.	2,33	1,67	Bajo
			Accidentales (Error humano, Impericia)	1	La administración del servicio esta a cargo de la Sede Central	3	Monitoreo por el personal de UTI	3	La administración del servicio esta a cargo de la Sede Central	4	Dependencia de proveedores externos para el soporte. Soporte técnico únicamente a nivel de hardware. En caso de impericia el impacto es a nivel nacional	2,67	1,83	Medio
			Tecnológicos (error de software, hardware, vulnerabilidades)	1	Contratos de mantenimiento preventivo y soporte técnico. Redundancia en controladores de directorio Activo a nivel nacional.	3	Contratos de mantenimiento preventivo y soporte técnico	3	Redundancia de controladores de Directorio Activo a nivel Nacional. Apoyo del personal de OTI	4	Garantía de fabricante del hardware vencida En caso de impericia el impacto es a nivel nacional	2,67	1,83	Medio
HARDWARE														
3	HARDWARE	SWITCH DELL S4148T SWITCH DELL S4148T SERVIDOR IBM SYSTEM X3650 M4 SERVIDOR IBM SYSTEM X3650 M4 SERVIDOR IBM SYSTEM X3650 M4 SERVIDOR DELL POWER EDGE R640 SERVIDOR DELL POWER EDGE R640 UPS CENTIEL 1 UPS CENTIEL 1 SWITCH CORE HPE 5510-24G SWITCH CORE HPE 5510-48G STORAGE EMC UNITY 300	Naturales o ambientales (Terremoto, tsunami, inundación, tormenta eléctrica, etc.)	1	Ninguno	1	Ninguno	1	Ninguno	1	No se cuenta con un site alterno para la activación de servicios de contingencia	5,00	3,00	Medio
			Accidentales (Inundaciones, Incendios, etc.)	1	Sistema contra incendios Sensores de aniegos Sensores de temperatura Sistemas de energía redundantes	3	Detectores de Humo y aniegos Monitoreo de centro de datos	4	Capacidad de respuesta a nivel del personal de UTI, según recursos disponibles	1	No se cuenta con un site alterno para la activación de servicios de contingencia	3,33	2,17	Medio
			Accidentales (Error humano, impericia)	1	Contratos de mantenimiento preventivo y soporte técnico. Redundancia en componentes críticos	3	Supervisión por el personal de UTI	3	Se dispone de componentes redundantes. Capacidad de respuesta por proveedor de servicios y del personal de UTI, según recursos disponibles	4	Dependencia de servicios especializado de terceros. Necesidad de Garantía extendida de fabricante.	2,67	1,83	Medio
			Tecnológicos (error de software, hardware, vulnerabilidades)	3	Contratos de mantenimiento preventivo y soporte técnico. Redundancia en componentes críticos	2	Respuesta según contratos de mantenimiento preventivo y soporte técnico.	2	Se dispone de componentes redundantes. Capacidad de respuesta por proveedor de servicios y del personal de UTI, según recursos disponibles.	2	Dependencia de servicios especializado de terceros. Necesidad de Garantía extendida de fabricante. Recursos existentes limitados para soportar los requerimientos de procesamiento y memoria en caso de daño en hardware.	4,00	3,50	Alto
4	HARDWARE	SERVIDOR DELL POWER EDGE R640 SERVIDOR DELL POWER EDGE R640 LIBRERÍA DE BACKUP TS 3100 SERVIDOR PROLIANT DL360 P GEN 8	Naturales o ambientales (Terremoto, tsunami, inundación, tormenta eléctrica, etc.)	1	Ninguno	1	Ninguno	1	Ninguno	1	No se cuenta con un site alterno para la activación de servicios de contingencia	5,00	3,00	Medio
			Accidentales (Inundaciones, Incendios, etc.)	1	Sistema contra incendios Sensores de aniegos Sensores de temperatura Sistemas de energía redundantes	3	Detectores de Humo y aniegos Monitoreo de centro de datos	4	Capacidad de respuesta a nivel del personal de UTI, según recursos disponibles	1	No se cuenta con un site alterno para la activación de servicios de contingencia	3,33	2,17	Medio
			Accidentales (Error humano, impericia)	1	Contratos de mantenimiento preventivo y soporte técnico.	3	Supervisión por el personal de UTI	3	Se dispone de componentes redundantes. Capacidad de respuesta por proveedor de servicios y del personal de UTI, según recursos disponibles	4	Dependencia de servicios especializado de terceros. Necesidad de Garantía extendida de fabricante.	2,67	1,83	Medio

ANEXO 03 - EVALUACIÓN DE RIESGOS

N°	ACTIVO	Descripción del Activo	AMENAZA	Impacto				Probabilidad de Ocurrencia	Valor del Activo	Nivel de Exposición	Nivel de Riesgo
				Impacto Legal	Impacto Económico	Impacto Operacional	Nivel de Impacto				
SERVICIOS											
1	SERVICIOS DE TI	BASE DE DATOS ORACLE	Naturales o ambientales (Terremoto, tsunami, inundación, tormenta eléctrica, etc.)	1	5	5	3,67	3,00	4,67	3,78	Crítico
			Accidentales (Inundaciones, Incendios, etc.)	1	4	4	3,00	2,00	4,67	3,22	Moderado
			Accidentales (Error humano, impericia)	1	2	2	1,67	3,00	4,67	3,11	Moderado
			Tecnológicos (error de software, hardware, vulnerabilidades)	1	3	4	2,67	3,67	4,67	3,67	Crítico
HARDWARE											
2	HARDWARE	SWITCH DELL S4148T SWITCH DELL S4148T SERVIDOR IBM SYSTEM X3650 M4 SERVIDOR IBM SYSTEM X3650 M4 SERVIDOR IBM SYSTEM X3650 M4 SERVIDOR DELL POWER EDGE R640 SERVIDOR DELL POWER EDGE R640 UPS CENTIEL 1 UPS CENTIEL 1 SWITCH CORE HPE 5510-24G SWITCH CORE HPE 5510-48G STORAGE EMC UNITY 300	Naturales o ambientales (Terremoto, tsunami, inundación, tormenta eléctrica, etc.)	1	5	5	3,67	3,00	4,00	3,56	Crítico
			Accidentales (Inundaciones, Incendios, etc.)	1	4	4	3,00	2,17	4,00	3,06	Moderado
			Accidentales (Error humano, impericia)	1	2	2	1,67	1,83	4,00	2,50	Moderado
			Tecnológicos (error de software, hardware, vulnerabilidades)	1	3	4	2,67	3,50	4,00	3,39	Crítico
3		SERVIDOR DELL POWER EDGE R640 SERVIDOR DELL POWER EDGE R640 LIBRERÍA DE BACKUP TS 3100 SERVIDOR PROLIANT DL360 P GEN 8	Naturales o ambientales (Terremoto, tsunami, inundación, tormenta eléctrica, etc.)	1	5	5	3,67	3,00	4,00	3,56	Crítico
			Accidentales (Inundaciones, Incendios, etc.)	1	4	4	3,00	2,17	4,00	3,06	Moderado
			Accidentales (Error humano, impericia)	1	2	2	1,67	1,83	4,00	2,50	Moderado
			Tecnológicos (error de software, hardware, vulnerabilidades)	1	2	2	1,67	3,50	4,00	3,06	Moderado