UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

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

SGSI basado en ISO/IEC_27001:2022 para la protección de activos de información de una entidad pública del Sector Defensa, Lima 2024

TESIS PARA OBTENER EL GRADO ACADÉMICO DE:

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

AUTORA:

Coronado Farroñan, Gladys Leonor (orcid.org/0009-0007-4191-473X)

ASESORES:

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

Mg. Puente Zamora, Jonathan Alexis (orcid.org/0009-0007-1034-1617)

LÍNEA DE INVESTIGACIÓN:

Auditoria de Sistemas y Seguridad de la Información

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:

Desarrollo económico, empleo y emprendimiento

LIMA – PERÚ

2024

UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

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

Declaratoria de Autenticidad del Asesor

Yo, ACUÑA BENITES MARLON FRANK, docente de la ESCUELA DE POSGRADO MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA NORTE, asesor de Tesis titulada: "SGSI basado en ISO/IEC_27001:2022 para la protección de activos de información de una entidad pública del Sector Defensa, Lima 2024", cuyo autor es CORONADO FARROÑAN GLADYS LEONOR, constato que la investigación tiene un índice de similitud de 17.00%, 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, 07 de Agosto del 2024

Apellidos y Nombres del Asesor:	**Firma**
ACUÑA BENITES MARLON FRANK **DNI:** 42097456 **ORCID:** 0000-0001-5207-9353	Firmado electrónicamente por: MACUNABE el 09-08-2024 09:05:35

Código documento Trilce: TRI - 0852691

INVESTIGA UCV

UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

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

Declaratoria de Originalidad del Autor

Yo, CORONADO FARROÑAN GLADYS LEONOR 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: "SGSI basado en ISO/IEC_27001:2022 para la protección de activos de información de una entidad pública del Sector Defensa, Lima 2024", 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
GLADYS LEONOR CORONADO FARROÑAN **DNI:** 16806402 **ORCID:** 0009-0007-4191-473X	Firmado electrónicamente por: GCORONADOF el 07-08-2024 22:35:03

Código documento Trilce: TRI - 0852690

INVESTIGA UCV

DEDICATORIA

"Lo que se llama suerte, es en realidad una bendición de Dios, lo que se considera casualidad es sólo Su propósito, y lo que entendemos como esfuerzo es simplemente su Gracia."

A mi amado Dios, fuente infinita de sabiduría, amor y guía, gracias por tus bendiciones, y a mi Madre María Santísima por iluminar siempre mi camino y llenar mi vida de esperanza.

A mi querido padre José Eladio C.S (QEPD y DDG), cuya memoria sigue siendo un faro de fortaleza y amor en mi existencia; aunque ya no estás físicamente, tu legado, espíritu de superación, esfuerzo y amor por vernos realizados como personas y profesionales, vive en cada rincón de mi ser.

A mis queridas hermanas Marleny y Alicia C.F (QEPD y DDG), cuyos ejemplos de valentía, perseverancia y amor siguen inspirándome. Sus memorias son testimonio de una lucha constante ante los desafíos de la vida, su dedicación y entrega a la familia, son el impacto más bonito y profundo que dejaron en mí.

Y a mi madre Esperanza Farroñán, cuyo amor incondicional y apoyo constante son una demostración del sentido de familia y de resiliencia. Gracias por ser mi roca y mi refugio, por tu ternura, afecto, entrega y abnegación.

Con amor eterno y gratitud

Gladys Leonor Coronado Farroñán

AGRADECIMIENTOS

Quiero expresar mi más sincero agradecimiento a quienes, con su apoyo, soporte, dedicación y constante aliento, han sido esenciales para lograr la culminación de esta tesis:

A mi líder y amigo el MAY.FAP Gary Lizardo Pérez Barrantes, Jefe de la Oficina de informática de la ACFFAA, por su invaluable apoyo, aportes y sus valiosas recomendaciones durante todo el proceso, los cuales fueron un soporte para mí, siempre dispuesto a ayudarme con su experiencia y conocimiento.

A la Dra. Helga Ruth Majo Marrufo, Jefa de la Escuela de Posgrado de la UCV, por su constante ánimo e inestimables consejos que me motivaron para seguir adelante.

Al Dr. David Flores Zafra, profesor, colega y amigo, por su apoyo esencial y entusiasmo lo cual ha sido una constante fuente de motivación. Sin su asistencia y contribuciones en los momentos decisivos, no habría logrado alcanzar esta meta.

A mis asesores, el Dr. Marlon Acuña Benites y al Mg. Jhonatan Alexis Puente Zamora, por su guía, comprensión y apoyo durante todo el proceso, lo cual ha sido preponderante para el éxito de la presente investigación.

A mis hermanos Jesús, Javier, y especialmente a Williams, por su motivación constante y su presencia en cada momento. Su hermandad han sido un pilar en esta travesía.

A mis preciados sobrinos, Emanuel y Daniel, que han sido una motivación para mí, por su ánimo y apoyo inquebrantable. Su compañía y aliento han hecho este camino mucho más llevadero.

A mis amistades, colegas de las diferentes instituciones en donde compartí experiencia y conocimiento, a mis profesores de la UCV y otras universidades del Perú y del mundo, que estuvieron a mi lado y que siempre creyeron en mí a pesar de todo. Su amistad y confianza han sido una luz en los momentos más oscuros.

A todos ustedes y a los que omití mencionar pero que no se olvidaron de la suscrita, gracias, Sin su ayuda y respaldo, esta tesis no hubiera sido posible.

Con gratitud y estima,

Gladys Leonor Coronado Farroñán

Índice de Contenidos

CARÁTULA i
DECLARATORIA DE AUTENTICIDAD DEL ASESOR ii
DECLARATORIA DE ORIGINALIDAD DEL AUTOR iii
DEDICATORIA iv
AGRADECIMIENTO v
Índice de Contenidos vi
Índice de tablas vii
Índice de figuras viii
RESUMEN ix
ABSTRACT x
I. INTRODUCCIÓN 1
II. METODOLOGÍA 13
III. RESULTADOS 23
IV. DISCUSIÓN 42
V. CONCLUSIONES 49
VI. RECOMENDACIONES 51
VII. REFERENCIAS 53
VIII. ANEXOS 64
8.1. Anexo 1: Tabla de Operacionalización de Variables o Tabla de Categorización .....
8.2. Anexo 2: Instrumento de Recolección de Datos - Fichas De Observación .....
8.3. Anexo 3: Evaluación por Juicio de Experto .....
8.4. Anexo 4: Consentimiento o asentimiento informado UCV .....
8.5. Anexo 5: Reporte de Similitud en Software Turnitin .....
8.6. Anexo 6: Autorización de la institución para la ejecución de la investigación .....
8.7. Anexo 7: Otras evidencias .....

Índice de tablas

Tabla 1. Datos referidos a la Dimensión Confidencialidad 24
Tabla 2. Datos referidos a la Dimensión Integridad 25
Tabla 3. Datos referidos a la Dimensión Disponibilidad 26
Tabla 4. Resultado Descriptivo Dimensión Confidencialidad 27
Tabla 5. Análisis Descriptivo: Frecuencias. Pre-test y Post-test– Dimensión Confidencialidad 27
Tabla 6. Resultado Descriptivo Dimensión Integridad 28
Tabla 7. Análisis Descriptivo: Frecuencias. Pretest y Postest– Dimensión Integridad 29
Tabla 8. Resultado Descriptivo Dimensión Disponibilidad 30
Tabla 9. Análisis Descriptivo: Frecuencias. Pretest y Postest– Dimensión Disponibilidad 30
Tabla 10. Procesamiento de Datos respecto al Pre test (2023) y Post Test (2024) 31
Tabla 11. Consolidación de los 3 indicadores 33
Tabla 12. Porcentaje de incidentes incremental que afectan a la confidencialidad 34
Tabla 13. Prueba de normalidad en HE 1c. 35
Tabla 14. Prueba T-Student – indicador Porcentaje de incidentes que afectan la confidencialidad 36
Tabla 15. Prueba T-Student –Incidentes en confidencialidad 36
Tabla 16. Porcentaje de incidentes incremental que afectan a la Integridad 37
Tabla 17. Prueba de normalidad en HE 1i. 38
Tabla 18. Prueba T-Student – indicador Porcentaje de incidentes que afectan la Integridad 38
Tabla 19. Prueba T-Student –Incidentes en Integridad 39
Tabla 20. Porcentaje de incidentes incremental que afectan a la Disponibilidad 39
Tabla 21. Prueba de normalidad en HE 1d. 40
Tabla 22. Prueba T-Student – indicador Porcentaje de incidentes que afectan la Disponibilidad 41
Tabla 23. Prueba T-Student –Incidentes en Disponibilidad 41

Índice de figuras

Figura 1. Activos de Información 13
Figura 2. Pilares de la Seguridad de la Información 18
Figura 3. Procesamiento de los datos antes y después de la aplicación de controles 32
Figura 4. Consistencia del porcentaje de incidentes que afectan a la confidencialidad 35
Figura 5. Consistencia del porcentaje de incidentes que afectan a la integridad 37
Figura 6. Consistencia del porcentaje de incidentes que afectan a la Disponibilidad 40

RESUMEN

La investigación determinó que el SGSI basado en la ISO/IEC 27001:2022 protege los activos de información en una entidad pública del Sector Defensa en Lima, 2024. Alineado con el ODS 9, mejora la seguridad y resiliencia tecnológica promoviendo desarrollo sostenible y capacidad de innovación, y con el ODS 8, contribuye a un entorno económico seguro y sostenible, promoviendo un desarrollo económico inclusivo. Se utilizó un diseño experimental con subdiseño pre-experimental, con enfoque cuantitativo y aplicado, empleando métodos: deductivo, hipotético y analítico. Se analizó una población de 30 controles clave de la norma, determinados previo diagnóstico en el proceso core, para proteger a la confidencialidad, integridad y disponibilidad de la información y sus activos, abarcando la Seguridad de Redes, Control de Accesos y Continuidad, alcanzando un nivel de confianza del 95%. Se aplicó la técnica de observación y sus guías como instrumentos. La aplicación de controles del SGSI, basados en el "Anexo A" de la norma ISO/IEC 27001:2022 y complementados por la ISO/IEC 27002:2022, utilizando T-Student en la estadística inferencial, demostró una reducción significativa en incidentes: 87.66% en confidencialidad, 77.81% en integridad y 86.70% en disponibilidad. Estos resultados confirman que el SGSI basado en ISO/IEC 27001:2022 protege efectivamente los activos de información.

Palabras clave : *SGSI,* ISO/IEC_27001:2022, Seguridad, Información, Activos de información.

ABSTRACT

The research determined that the ISMS based on ISO/IEC 27001:2022 protects information assets in a public entity of the Defence Sector in Lima, 2024. Aligned with SDG 9, it enhances technological security and resilience, promoting sustainable development and innovation capacity, and with SDG 8, it contributes to a secure and sustainable economic environment, promoting inclusive economic development. An experimental design with a pre-experimental sub-design was used, with a quantitative and applied approach, employing deductive, hypothetical and analytical methods. A population of 30 key controls of the standard were analysed, determined prior diagnosis in the core process, to protect the confidentiality, integrity and availability of information and its assets, covering Network Security, Access Control and Continuity, reaching a confidence level of 95%. The observation technique and its guides were applied as instruments. The application of ISMS controls, based on "Annex A" of ISO/IEC 27001:2022 and complemented by ISO/IEC 27002:2022, using T-Student in the inferential statistics, showed a significant reduction in incidents: 87.66% in confidentiality, 77.81% in integrity and 86.70% in availability. These results confirm that the ISMS based on ISO/IEC 27001:2022 effectively protects information assets.

Keywords: ISMS, ISO/IEC_27001:2022, Security, Information, information assets.

I. INTRODUCCIÓN

En la actualidad, estamos inmersos en una transformación digital sin igual, impulsada por el rápido crecimiento de tecnologías: blockchain, IoT, IA, Cloud Computing, entre otras. Estas innovaciones permiten a las organizaciones revolucionar sus modelos de negocio y ganar una ventaja competitiva (Ladu et al., 2024). No obstante, este progreso tecnológico también presenta nuevos desafíos de seguridad que deben ser abordados a fin de lograr una madurez digital completa.

Las entidades dependen de la información valiosa, como datos personales, de salud, financiera y de seguridad nacional; si esta información se ve comprometida, podría generar consecuencias negativas. Por ende, es esencial proteger esta información a fin de asegurar su funcionamiento, evitando daños y un impacto negativo fuerte. Las instituciones deben tomar medidas para minimizar los riesgos asociados y salvaguardar la información confidencial.

Asimismo, la creciente sofisticación y alcance global que caracteriza a muchos sucesos negativos referidos a la salvaguarda y confianza digital refuerza con mayor relevancia, el tener en cuenta este tema primordial, tanto a gobiernos como para actores internacionales, tal es así que, en el 2023, los incidentes de ciberseguridad y ciberdelitos a nivel mundial experimentaron un aumento, y varios países enfrentan desafíos en la salvaguarda de sus activos sobre todo, en la lucha ante los crímenes cibernéticos.

Al respecto, en el año 2023, INCIBE gestionó 83,517 incidentes de ciberseguridad, lo que representó un aumento del 24% respecto al año anterior; más de 58,000 afectaron a ciudadanos y más de 22,000 a empresas, incluyendo pymes y autónomos. Los sectores más impactados fueron el suministro de agua (4,58%), las TIC’s (18,33%), los softwares financieros y tributarios (25,42%), la energía (22,08%) y el transporte (25%). Asimismo, se detectaron 183,077 sistemas con vulnerabilidades, comparables con una cerradura rota que permite la entrada de intrusos y provoca problemas, Estos ataques inutilizaron más de 9,000 dispositivos, incluyendo equipos y teléfonos móviles, y se informaron más de 28,000 casos de fraude.

También, América Latina en el primer semestre, enfrentó más de 63,000 millones de ciberataques, con México y Colombia como los países más golpeados.

Según Rojas (2024), la región experimentó una vulnerabilidad crítica, se resalta el fortalecer las medidas o controles de ciberseguridad, entre sus ataques más frecuentes figuran el phishing (suplantación de identidad a través de correo electrónico) el cual fue el delito más común, con 300,497 denuncias y pérdidas superiores a 10,300 millones de dólares, Otros incidentes destacados incluyen fraudes online, virus informáticos y secuestros digitales.

Según Carvajal et al. (2019), las entidades públicas no están implementando los controles necesarios para salvaguardar su información confidencial. Esto significa que la información confidencial de la población sea personal, financiera y de salud, se encuentra en riesgo de ser filtrada o robada. Es urgente se implementen medidas para fortalecer la protección de su información confidencial en las entidades públicas

De igual forma Kirilova (2024) indica que, para garantizar los niveles de protección, tanto la investigación científica como las aplicaciones prácticas de diversas plataformas, tecnologías y herramientas, han experimentado un importante desarrollo, y considera principalmente en sus resultados, aumentar la privacidad cibernética de la institución, el monitoreo de su perímetro externo, así como gestionar los peligros a los cuales están expuestos los activos, dejando entrever que existen falencias en la salvaguarda de los mismos.

Según Patrick et al. (2018), expresan que es necesario un plan completo para la administración de la protección en este ámbito, el cual revolucione el enfoque de la entidad para administrar los riesgos cibernéticos, resguardar su infraestructura, dispositivos y datos e ineluctablemente perfeccionar el gobierno de las TICs y así obtener una mejor rendición de cuentas ante los ciudadanos.

A nivel nacional, se ha encontrado similar problemática, tal es así que, Delgado (2023) menciona que, en el 2023, Perú enfrentó una creciente ciberdelincuencia, con atacantes utilizando inteligencia artificial para automatizar los mismos. La clonación de voz y la especialización delictiva también representaron desafíos significativos para la seguridad digital. Las denuncias por estafas digitales y robos a través de aplicaciones se incrementaron en un 150%. Además, se reportaron más de 5 casos de cibercrimen por hora, una cifra que no refleja completamente el alcance real de esta nueva amenaza. Además, los delitos informáticos se han incrementado en el Perú ya que, durante el año 2023, la DIVINDAT de la PNP registró 2,485 casos, con

predominio de estafas en línea y suplantación de identidad. Entre las modalidades más denunciadas ante la DIVINDAT se encuentran el phishing, carding y las aplicaciones falsas (Editora Perú, 2024). Además, los fraudes informáticos y la suplantación de identidad son los actos delictivos cibernéticos más predominantes.

Es así como la salvaguarda de la información confidencial y la infraestructura crítica debe convertirse en una prioridad absoluta. De acuerdo con Fortinet, Perú registró 5000 millones de intentos de ciberataques en 2023 (“El Perú sufrió 5.000.000 de intentos de ciberataques en 2023, según Fortinet”, 2024), lo que destaca la urgente necesidad de fortalecer los controles de seguridad digital en el país. Por lo tanto, es esencial implementar medidas de ciberseguridad robustas para enfrentar la creciente amenaza de los ciberataques.

Guevara-Vega et al. (2023), en su artículo, afirman que, a medida que avanzaba el tiempo y la tecnología, la salvaguarda de los entes de información se vio afectada por múltiples ataques que se creían en cierta forma no preponderantes. Sin embargo, actualmente es necesario controlar recursos informáticos, ya que estarán expuestos a las amenazas y vulnerabilidades que conlleva el avance de la tecnología.

En la región, también se encuentra que existe una falta de protección en los activos de información en las entidades públicas, tal es el caso de la entidad del Sector Defensa, en donde se realiza la investigación, la cual tiene más de doce (12) años de existencia y que presenta inconvenientes respecto a la falta de sus medidas de seguridad en la infraestructura física, controles referidos a la seguridad lógica, así como la información de carácter sensible que se relaciona con su proceso de compras públicas en el mercado nacional y extranjero, y que se soporta en el SIGCO, el cual es utilizado por los funcionarios y las entidades vinculadas con el desarrollo y la seguridad estratégica del país, por ende, la entidad en mención, no se exime de ello, para poder cumplir en salvaguardar a su información y los activos relacionados, por ende, requiere de un SGSI.

En este contexto, se destaca la relevancia de la protección de la información, especialmente la ciberseguridad; en el Perú. los ciberdelincuentes ahora tienen en la mira objetivos específicos, con una mayor posibilidad de éxito. Es fundamental que las instituciones y los ciudadanos estén alerta y tomen medidas para protegerse contra estas amenazas en constante evolución.

En concordancia con lo expuesto por los autores anteriormente citados, y tomando en consideración la importancia de salvaguardar los recursos de información sensibles, se hace evidente la imperiosa necesidad de implementar controles robustos de seguridad digital en el Perú y en el mundo. Las alarmantes cifras de ciberataques y delitos informáticos, junto con la creciente sofisticación de las amenazas, ponen en controversia a la Seguridad de la Información tanto a nivel internacional, nacional como regional.

Así, se plantea la siguiente interrogante: ¿El SGSI basado en ISO/IEC_27001:2022 mejora la protección de los activos de información de una entidad pública del Sector Defensa en Lima, 2024?, en cuanto a los problemas específicos se tiene: primero ¿El SGSI basado en ISO/IEC_27001:2022 mejora la protección de la confidencialidad de los activos de información de una entidad pública del Sector Defensa en Lima, 2024? luego, ¿El SGSI basado en ISO/IEC_27001:2022 mejora la protección de la integridad de los activos de información de una entidad pública del Sector Defensa en Lima, 2024? y finalmente ¿El SGSI basado en ISO/IEC_27001:2022 mejora la protección de la disponibilidad de los activos de información de una entidad pública del Sector Defensa en Lima, 2024?

En réplica a esta pregunta, se plantea la siguiente afirmación: “El SGSI basado en ISO/IEC_27001:2022, protege a los activos de información de una entidad pública del Sector Defensa, Lima, 2024” considerando las siguientes hipótesis específicas: a) El SGSI basado en ISO/IEC_27001:2022, protege la confidencialidad de los activos de información de una entidad pública del Sector Defensa, Lima, 2024. b) El SGSI basado en ISO/IEC_27001:2022, protege la integridad de los activos de información, de una entidad pública del Sector Defensa, Lima, 2024. c) El SGSI basado en ISO/IEC_27001:2022 protege la disponibilidad de los activos de información, de una entidad pública del Sector Defensa, Lima, 2024.

De acuerdo con Hernández y Mendoza (2018), la justificación de una investigación, fundamentada en elementos teóricos, prácticos y metodológicos, es crucial para demostrar la relevancia del estudio y su potencial impacto en el conocimiento o la práctica. En esta instancia, abordar una brecha en la protección de los activos de información es necesario para aumentar la salvaguarda de estos recursos invaluables, lo que justifica la investigación desde el punto de vista

metodológico. Para ello, se sugiere que los controles seleccionados del Anexo A se implementen de conformidad con la norma ISO/IEC 27001:2022.

Lo cual no solo sirve como base para nuevas investigaciones, sino que también fortalece el proceso metodológico en general (Villela, 2019). Se argumentó de manera teórica para abordar la falta de claridad en los conceptos vinculados a la salvaguarda de la información, al tiempo que se respaldó desde una perspectiva de investigación para asistir a otros expertos en su comprensión más profunda del tema (Fernández, 2020). Se tiene una justificación práctica porque un SGSI, es esencial para garantizar que los datos, la información y los activos que los soportan estén protegidos en una organización. La falta de visibilidad de los datos, la presencia de demasiados usuarios privilegiados, el incumplimiento de las regulaciones gubernamentales, la mayor probabilidad de ataques debido a usuarios inactivos y contraseñas que no caducan son algunos problemas comunes en la gestión de la seguridad (Grupo de Medios Digitales de TI, 2020).

Es así como, el propósito general, por tanto, fue: Determinar si el SGSI, basado en ISO/IEC_27001:2022, mejora la protección de los activos de información de una entidad pública del Sector Defensa, Lima, 2024. Además, se mencionaron los objetivos específicos: Primero, Determinar si el SGSI, basado en ISO/IEC_27001:2022, mejora la protección de la confidencialidad de los activos de información de una entidad pública del Sector Defensa, Lima, 2024, después, Determinar si SGSI basado en ISO/IEC 27001:2022 mejora la protección de la integridad de los activos de información en una entidad pública del Sector Defensa en Lima, 2024 y finalmente Determinar si el SGSI basado en ISO/IEC 27001:2022 mejora la protección de la disponibilidad de los activos de información en una entidad pública del sector de la Defensa en Lima.

Por ello, para demostrar la eficacia del SGSI se emprendió a realizar una investigación aplicada pre - experimental como guía para alcanzar los objetivos planteados. Para las mediciones, se utilizó un pre-test y un post-test. Los datos se obtuvieron utilizando herramientas de levantamiento de información confiables y probadas teniendo la suscrita el comportamiento de auditora, y las muestras utilizadas fueron significativas para el análisis realizado.

Por lo tanto, El SGSI fomenta una cultura de seguridad de la información en toda la organización, involucrando activamente a los empleados. Implementa prácticas óptimas para la gestión de la seguridad de la información empresarial, lo que refuerza la confianza en la protección de datos y recursos asociados. (¿Qué es la seguridad de la información?). La seguridad de datos: Definición y descripción general | IBM, nd).

Los siguientes estudios previos respaldan esta investigación, a nivel internacional, el artículo sobre la Seguridad de la Información en el intercambio dentro de las cadenas de suministro analiza cómo las filtraciones de información impactan negativamente en el intercambio de datos en estas cadenas, afectando la productividad, las ganancias y la competitividad. La revisión sistemática, realizada según el método PRISMA y basada en datos recopilados entre 2018 y 2022, concluye que la seguridad de la información es fundamental para proteger la privacidad. Esta protección no solo se logra mediante soluciones técnicas como blockchain, sino también a través de un control de acceso más eficaz (Intercambio de información en la cadena de suministro. Ciencia e Ingeniería, s. f.).

Frank (2023), en su tesis, profundiza en la evaluación del impacto de la norma ISO/IEC_27001:2022 en la gestión de la seguridad dentro del departamento de TI de una empresa industrial en Lima durante el año 2023, empleando una metodología cuantitativa, causal-correlacional y básica, el estudio involucró a 31 empleados del departamento de TI. Se empleó un muestreo censal no probabilístico, seleccionando a toda la población como muestra. Se utilizó una encuesta que abordaba temas relacionados con ISO/IEC 27001 y la gestión de sistemas de información. Los resultados revelaron una influencia estadísticamente significativa de ISO/IEC 27001 en el SGSI en el ámbito de TI de una empresa industrial, evidenciado por un valor p menor a 0.05. Se concluyó que la variable ISO/IEC 27001 ejercía una influencia significativa del 22% sobre el SGSI

El estudio de Luis (2023) revela un panorama en expansión de la educación en línea en Ecuador. Aunque esta modalidad educativa ha visto un aumento en su popularidad, también ha suscitado inquietudes sobre la seguridad de los activos digitales. En respuesta a estas preocupaciones, se ha desarrollado una Política de SGSI (PGSI) para abordar los desafíos relacionados con la educación virtual.

Según Fernandes et al. (2024) afirma que las entidades se ven obligadas a cumplir con una variedad de políticas, reglas y estándares en el contexto regulatorio. Para evitar sanciones severas, pérdida de reputación y perjuicio financiero, implementan controles de cumplimiento. Sin embargo, esta duplicación de esfuerzos conlleva a costos innecesarios. Por ello, los investigadores están trabajando en mapear e integrar estos estándares para evitar la duplicación, agilizar el cumplimiento e identificar las mejores prácticas. Este estudio se centra en los campos de Riesgo, Seguridad y Continuidad del Negocio, buscando mejorar su comprensión al explorar los beneficios y desafíos de estos procesos, así como identificar métodos o artefactos reutilizables para el futuro.

Como lo señala Paun (2018), la salvaguarda de la información es un componente esencial para la estabilidad y la confianza de los sistemas digitales y la economía global en un mundo cada vez más interconectado. Además de salvaguardar la confidencialidad y los derechos de los usuarios, la implementación efectiva de prácticas de seguridad de la información protege a las organizaciones de pérdidas financieras y daños reputacionales.

El artículo de Riesgo (2005) aborda el tema perenne y fundamental de la seguridad, explorando su preponderante relación con la información y la comunicación. El autor enfatiza la relevancia de la gestión adecuada de la información en la cobertura de asuntos relacionados con la seguridad ciudadana, subrayando la responsabilidad inherente a tal tarea debido a la sensibilidad y trascendencia de estos temas.

Santos-Olmo et al. (2024) destacan la necesidad de que las empresas establezcan controles de seguridad para detectar y reducir los riesgos a los que están expuestas. No obstante, señalan que estos controles por sí solos no son suficientes. Para lograr una protección completa, es necesario implementar esquemas de gestión (SGSI) que garanticen la seguridad a largo plazo.

En el ámbito nacional, Roberto (2023) presenta una propuesta innovadora a nivel nacional para la Clínica San Pedro Chimbote. Esta iniciativa busca fortalecer la protección de la información y la administración del riesgo informático en la institución. Durante la investigación, se explicaron los conceptos del SGSI y su aplicación para mejorar la administración del riesgo informático en la clínica, haciendo hincapié en la

importancia de basarse en la ISO/IEC 27001:2022. Se utilizó un diseño de investigación aplicada con mediciones previas y posteriores de la variable dependiente. Los resultados indicaron que el SGSI mejoró notablemente la gestión del riesgo en la clínica, lo que sugiere su viabilidad para otras instituciones similares.

Teniendo en cuenta lo expuesto, la seguridad de la información surge debido al aumento de incidentes de seguridad que afectan directamente la información misma del proceso central de la institución. El impacto de una amenaza que pueda aprovechar ciertas vulnerabilidades podría resultar en pérdidas financieras, disminución de la productividad o daños a la institución, en particular a su reputación (IT Digital Media Group, 2020).

La seguridad de la información abarca diversas medidas físicas, técnicas y administrativas destinadas a salvaguardar los tres aspectos esenciales de la información: disponibilidad, integridad y confidencialidad, tal como lo describen Whitman y Mattord (2018).

La gestión de las tecnologías de la información (TIC) está estrechamente relacionada con la seguridad de la información. Su principal objetivo es garantizar que los dispositivos tecnológicos que manejan la información en todas sus fases, desde la recopilación hasta la presentación, estén protegidos contra riesgos aceptables. Los métodos para salvaguardar los pilares de la información y los recursos que la respaldan están definidos en la norma ISO/IEC 27001 (ISO/IEC 27000, 2017).

Los pilares de la información y sus activos relacionados son: la confidencialidad, la integridad y la disponibilidad de la información y sus activos deben protegerse contra los ataques cibernéticos, el robo de identidad, el fraude y otros peligros relacionados. Esto incluye evidencia secreta, documentos y datos de usuarios. Información gubernamental o militar, así como datos de investigación y desarrollo. Estos aspectos deben ser priorizados para asegurar la continuidad de los procesos esenciales en cualquier entidad. (García, 2023).

Una estrategia holística es esencial para garantizar la seguridad organizacional. Esta, abarca la gestión de riesgos, el análisis de impacto y la adherencia a estándares de seguridad reconocidos como ISO/IEC 27001 y NIST SP 800-53. Este enfoque global proporciona una defensa robusta para los activos de

información críticos, protegiéndolos contra diversas amenazas, tanto internas como externas.

Igualmente, un elemento clave del SGSI es la identificación y salvaguarda de activos críticos de información. Esto incluye la protección óptima de datos sensibles de clientes, información financiera, secretos comerciales, propiedad intelectual de I+D, y datos gubernamentales y militares, entre otros. Asegurar eficazmente estos activos es vital para mantener el CID, siendo un aspecto fundamental de la seguridad informática organizacional.

Foster (2021) advierte sobre la fragilidad de la protección de la privacidad en un mundo sin normativas internacionales robustas que prioricen los derechos de los usuarios por encima de los intereses de las corporaciones e incluso los gobiernos. Sin embargo, destaca la tendencia positiva de un creciente número de países que están promulgando leyes que reconocen el derecho a la privacidad como un principio fundamental.

De lo antecedido, es importante hablar sobre el antecedente de la Variable Independiente: SGSI basada en ISO/IEC 27001:2022, la cual resalta en su importancia:

En la norma ISO/IEC 27002:2022 ofrece una amplia gama de recomendaciones de mejores prácticas para la gestión de seguridad, complementando los controles del Anexo A de ISO/IEC 27001:2022. Estos controles son aplicables a diversas organizaciones y están destinados a quienes desarrollan o mantienen el SGSI. El estándar agrupa noventa y tres (93) controles en cuatro categorías principales. En esencia, mientras ISO/IEC 27001:2022 establece los controles del Anexo A, ISO/IEC 27002:2022 proporciona orientación detallada sobre la implementación de cada uno de estos controles.

El Círculo de Mejora Continua, también llamado Ciclo de Deming o método PHVA (Planificar, Hacer, Verificar y Actuar), fue creado por Shewhart y difundido por Deming en Japón durante los años 50. Este enfoque se centra en perfeccionar constantemente los procesos y productos organizacionales. El ciclo abarca la planificación, implementación y control en los sistemas de gestión. Su enfoque sistemático permite un análisis y toma de decisiones objetivos, apoyándose en herramientas gráficas y estadísticas. Este método es valorado por su capacidad para

promover una mejora continua y estructurada en las organizaciones. (Mercado & Valenzuela, 2022).

La norma ISO/IEC 27001 ha cambiado el modelo PDCA, y la versión de 2013 ha introducido un cambio significativo al no hacerlo necesario para la mejora continua. Su uso dentro del estándar se entiende, aunque no se menciona explícitamente. Entender los principios fundamentales de este proceso es esencial.

Planificar, según Gómez y Fernández (2018), la planificación, la definición de objetivos y las políticas del Sistema de Gestión de Seguridad de la Información (SGSI) de la organización marcan el inicio de un proceso crucial. Esta etapa inicial establece el camino que seguirá la organización en cuanto a la seguridad de la información y establece las bases para las acciones posteriores.

Esta etapa inicial consiste en determinar los objetivos que se pretenden alcanzar en seguridad de la información, identificar los problemas o áreas de mejora, establecer un plan de acción detallado determinando para la implementación los recursos necesarios.

Hacer, en esta etapa, inicia el SGSI, asegurando que las políticas y los controles estén en línea con el análisis de riesgos previamente realizado, así como con las responsabilidades y capacitaciones del personal. Es el momento en el que se ejecutan las actividades planificadas. (Gómez & Fernández, 2018).

Verificar, aquí se monitorea y revisa el desempeño del SGSI, es decir, para concretar los objetivos establecidos se asegura que los procesos sean efectivos. En resumen, esta etapa implica la supervisión de las tareas para evaluar su rendimiento.

Actuar, permite realizar mejoras manteniendo el SGSI, En esta etapa se llevan a cabo evaluaciones para identificar posibles deficiencias en la etapa anterior. Es el momento de identificar errores y aplicar mejoras (Gómez & Fernández, 2018).

De acuerdo con ControlTech (2020), la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) no solo protege la información confidencial de una organización, sino que también la convierte en un activo estratégico que impulsa su competitividad, en conclusión un SGSI va más allá de la protección de datos, convirtiéndose en una herramienta para el éxito empresarial, su adecuada gestión de riesgos, la reducción de costos y la demostración de un

compromiso con la seguridad son pilares clave de la competitividad. Apostar por un SGSI es una inversión a futuro para las entidades.

Respecto a la definición de Incidencia se tiene que es cualquier evento o situación que pueda comprometer la confidencialidad, integridad o disponibilidad de la información dentro de una organización (NIST, 2018). Estos incidentes pueden variar en gravedad y pueden incluir una amplia gama de problemas, como ataques cibernéticos que son intentos de intrusión por parte de hackers, malware, ransomware, phishing, etc., así como filtraciones de datos, pérdida o exposición de la data o información sin autorización. También, errores humanos, o acciones no intencionadas que comprometen la seguridad, tales como el envío de datos sensibles a destinatarios incorrectos. Además de fallas en sistemas, problemas técnicos o malfuncionamientos que afectan la protección de la información. Finalmente se puede dar el acceso no permitido, cuando personas no autorizadas obtengan acceso a sistemas o datos restringidos.

Gestionar una incidencia en seguridad de la información implica identificar el problema, contenerlo, erradicar la causa raíz, y luego llevar a cabo un proceso de recuperación para restaurar la normalidad. Además, es crucial realizar una revisión post-incidencia para aprender de la situación y mejorar los mecanismos de seguridad para prevenir futuros incidentes.

Es esencial tener una actitud proactiva en cuanto a la seguridad de la información, destacando la protección de los recursos de información delicada. Para lograr este propósito, se necesita la implementación de un SGSI; un SGSI sólido permitirá a las organizaciones identificar, clasificar y proteger adecuadamente sus activos de información, estableciendo controles de seguridad individualizados para cada uno de ellos. La implementación de medidas de protección física y lógica adecuadas, así como la capacitación continua del personal en materia de seguridad digital, son elementos esenciales para reforzar la postura de seguridad de cualquier organización.

Existen teorías que apoyan la protección de la información y sus activos: la Teoría de Juegos, que se utiliza en la ciberseguridad, es ampliamente reconocida por su eficacia en la detección y prevención de amenazas. Su análisis identifica una variedad de métodos de ataque, incluyendo oscilación, inflación y deflación. Además

de brindar una comprensión y sensibilización fundamental sobre lecciones aprendidas y principios algorítmicos fundamentales, esta teoría aborda estrategias defensivas, como la detección de valores atípicos y la selección de umbral adaptativo. Según Hernández (2018), los usuarios pueden reconocer fácilmente a los intrusos y abordar situaciones adversas de manera sistemática mediante el uso de la teoría de juegos.

Teoría de la Gestión de la Privacidad, según Mariarteta (2019), esta teoría se centra en salvaguardar la información personal y confidencial de las personas, lo que implica examinar tanto las consideraciones éticas como legales relacionadas con la recopilación, almacenamiento, procesamiento y compartición de datos personales. Describe cómo las personas gestionan la dicotomía entre revelar y ocultar información privada. Está fundamentada en suposiciones acerca de cómo las personas piensan y se comunican, así como en suposiciones sobre la naturaleza humana. Estas incluyen la idea de que los individuos establecen y siguen reglas, y que sus decisiones se basan en consideraciones tanto hacia los demás como hacia sí mismos.

Teoría de la Seguridad, intentando explicar las relaciones y causas que la afectan, proporciona un contexto para comprender los conceptos de seguridad, . Define la perspectiva, la representación y cómo será interpretada en diferentes niveles. La seguridad, como objeto de estudio teórico, es investigada para organizar y consolidar el conocimiento sobre ella. Esto implica identificar y clasificar eventos históricos que han influido en la construcción de hipótesis a lo largo del tiempo, relacionando conceptos tradicionales y nuevos sobre amenazas, conflictos, violencia, relaciones internacionales para el estudio de la seguridad (Yépez, 2018)

En síntesis, sobre la base de las teorías mencionadas, es imperativo adoptar un enfoque holístico para abordar los retos actuales de la seguridad de la información. Este enfoque debe combinar controles técnicos avanzados, políticas de gestión eficaces y una cultura organizativa que fomente la vigilancia continua y la mejora sistemática. La única manera de mejorar la protección de los activos de información y crear un entorno más seguro y resistente frente a las nuevas amenazas es integrar estos componentes.

II. METODOLOGÍA

La investigación titulada “SGSI basado en ISO/IEC 27001:2022 (en adelante la norma) para la protección de activos de información (en adelante recursos) en una entidad pública del Sector Defensa, Lima, 2024” se fundamenta en un enfoque metodológico que integra la formulación de hipótesis, el razonamiento deductivo y el análisis.

Antes se debe recordar que los activos de información son los pilares que sustentan la información valiosa para una organización (Nor27cyg, s. f.). Esto incluye archivos, correos electrónicos, sistemas, redes, dispositivos y bases de datos (Redvoiss, 2024). La protección de estos activos es crucial para prevenir el acceso sin autorización o el uso indebido de la información. La confidencialidad, la discreción y la salvaguarda de la persona dependen de la efectiva protección de los activos de información.

Es así como, cualquier segmento de datos o información que tenga valor para una entidad se denomina activo de información. Estos incluyen dispositivos, datos, documentos, sistemas, redes y software. Para garantizar la CID de la información, además de prevenir ciberataques se debe proteger a estos recursos. Los mismos, comparten características como valor, confidencialidad, integridad, disponibilidad, sensibilidad, interdependencia y evolución constante (García, 2023)

Figura 1

Activos de Información

Nota. Fuente: Seguridad de la Información UV
https://www.uv.mx/infosegura/general/infografia_activosinformacion/#gallery

El método hipotético deductivo se distingue por ser una teoría que no se reconoce como verdadera hasta que sea refutada; este método incluye la formulación de hipótesis, basada en la data recopilada, y el uso de la deducción para llegar a conclusiones antes de la experimentación, según Puebla (2010). Se utilizará el método hipotético debido a que se evaluará la hipótesis asociada con la variable dependiente (Andrade & Trujillo, 2023).

Carvajal (2013) indica que el método deductivo se utiliza para tratar problemas generales a partir de cuestiones específicas, con el objetivo de identificar mejoras en la CID de la información. Este enfoque se fundamenta en la premisa de que, si la premisa es correcta, la conclusión derivada también lo será, de acuerdo con el razonamiento argumentado (Rodríguez & Rodríguez, 2020c).

Respecto al método analítico, Gómez (2012) menciona que se emplea para interpretar datos tabulados y representarlos gráficamente, con el propósito de evaluar la validez de las hipótesis planteadas. Este método descompone el todo en sus partes constituyentes para analizar su naturaleza, lo que puede conducir al desarrollo de nuevas teorías.

Tipo, enfoque y Diseño de Investigación: La presente investigación se clasifica como aplicada, ya que se fundamenta en una base teórica que respalda la aplicación de la teoría en resultados prácticos. Según Lozada (2014), este tipo de investigación tiene como objetivo adquirir conocimiento y resolver problemas específicos y prácticos. Por lo tanto, esta investigación se clasifica como investigación aplicada ya que busca soluciones prácticas para mejorar la salvaguarda en el Sector Defensa.

Con relación al enfoque, este es del tipo cuantitativo, porque se manipuló la variable “protección de los activos de información” que es el símil de “Seguridad de la información” estimulada por la otra variable “SGSI basado en ISO/IEC 27001:2022”, para demostrar sí se protege a los activos de información. La investigación cuantitativa requiere ciertas características específicas, como mantener la imparcialidad, evaluar hipótesis, utilizar herramientas estadísticas inferenciales, controlar variables y seguir un enfoque deductivo en el método de investigación (Flores & Gardi, 2020).

Respecto al diseño de investigación, en un análisis experimental, el investigador manipula deliberadamente la variable independiente, junto con una o más variables dependientes, dentro de un entorno controlado (Hernández et al., 2018). Para esta investigación se empleó un diseño experimental de sub diseño preexperimental, enfocado en la variable dependiente "protección (seguridad) de activos de información". El objetivo del estudio es evidenciar que la implementación de controles específicos, fundamentados en la norma, en el proceso misional de una entidad del sector defensa, asegura la protección de los activos de información. Esto se demostrará mediante la reducción de incidencias relacionadas con esos controles, observando que la tasa de incidencias es significativamente menor en el post test en comparación con los resultados del pre test.

Variables/categorías: La presente investigación, busca proteger a los activos de información que tiene la institución en su proceso core o misional, denominado “Compras” a través de los controles que se detalla en el estándar “ISO/IEC_27001:2022”, normado en el Perú como NTP.

La variable independiente en este caso es el "SGSI basado en ISO/IEC 27001:2022", mientras que la variable dependiente es la "protección de activos de información", también referida como "seguridad de la información". Visto lo antecedido, se detallan estos conceptos:

Variable Independiente: SGSI basado en ISO/IEC_27001:2022; el SGSI, según lo establece la norma, actúa como un marco integral que incluye políticas, procedimientos, controles y procesos destinados a salvaguardar la información confidencial de una organización. Su objetivo primordial es garantizar el CID de la información, aspectos fundamentales para la seguridad de cualquier entidad. El principal indicador consistió en monitorizar la aparición de incidentes de seguridad de la información en la entidad, con el fin de aplicar controles del SGSI basados en la norma.

Para brindar una protección completa de la información, el SGSI está compuesto por múltiples componentes interconectados. Las políticas de seguridad de la información, la administración de riesgos, los controles de seguridad, la administración de incidentes, la auditoría y la mejora continua son parte de estos componentes. El SGSI basado en la norma se establece como un sistema esencial

para las empresas que tienen como objetivo proteger su información confidencial y garantizar la continuidad de sus operaciones en un ambiente cada vez más complejo y susceptible a ciberataques (ISO/IEC 27001:2022, s. f.).

Chopra y Chaudhary (2020) describen el SGSI como un conjunto de políticas, prácticas, tecnologías y procedimientos que se utilizan en una organización para proteger su información. El objetivo principal del SGSI es proteger la información en sus tres componentes principales: 1) Disponibilidad, que significa que la información esté disponible para aquellos que la necesiten en el momento adecuado. 2) Integridad: permite asegurarse de que la información sea precisa, completa y confiable, libre de cambios no autorizados; y 3) Confidencialidad: implica proteger la información para que solo las personas autorizadas puedan acceder a ella.

En este contexto, el SGSI no solo se ajusta a estándares y regulaciones, sino que también se adapta para evaluar su impacto en la seguridad de la información mediante estudios e investigaciones. La flexibilidad del SGSI facilita el análisis de su efecto en variables como la efectividad de las medidas de seguridad, la percepción de los empleados y la frecuencia de incidentes. El objetivo principal es perfeccionar el SGSI para reforzar la seguridad de forma integral.

La Seguridad de la Información, no se restringe únicamente a los sistemas electrónicos, como correos electrónicos, videos corporativos y bases de datos, sino que también incluye aspectos físicos, como documentos manuscritos e impresiones. El propósito principal del SGSI es asegurar la protección de los activos tecnológicos de una organización en la era digital.

Variable Dependiente: Protección de activos (Seguridad de la Información), Desde una perspectiva conceptual, la protección de los activos de información, en esencia, se refiere a la Seguridad de la Información y a los activos relacionados. Por lo tanto, se define como un conjunto de medidas destinadas a preservar el CID de la información en sus diversos formatos y estados. Su propósito principal es mitigar riesgos como el acceso no autorizado, el robo o la alteración de la información, mediante la implementación de controles de seguridad, gestión de riesgos, capacitación del personal y cumplimiento de normativas. En esencia, busca asegurar que la información esté protegida contra amenazas internas y externas, garantizando la operación segura y confiable.

La seguridad de la información se refiere a las acciones y procedimientos específicos adoptados para garantizar que la información dentro de una organización esté protegida, de acuerdo con su definición operativa. Esto incluye la preparación para la respuesta a incidentes de seguridad y la recuperación; la realización de auditorías y pruebas de seguridad; la identificación y clasificación de la información sensible; el uso de controles de acceso adecuados; y la formación del personal en prácticas de seguridad (Publicación Especial 811 | NIST, 2020). El objetivo fundamental de la seguridad de la información es reducir las amenazas y peligros que podrían comprometer la seguridad de la información, tanto internos como externos.

La norma NTP ISO/IEC 27001:2022, establece que la seguridad de la información busca prevenir amenazas y garantizar la continuidad de los servicios. Observa la presencia de información y sus activos en diversas formas, tanto de forma física como en forma digital sea insitu u online. En cualquier medio de transmisión, es esencial proteger y resguardar la información de manera adecuada para mantener la triada CID. Esto se logra mediante un SGSI, que es primordial para la entidad de forma efectiva.

Asimismo, la información es el activo crucial de la entidad. Por lo tanto, debe protegerse cuidadosamente utilizando las mejores prácticas y herramientas al alcance. Esto implica que la información esté siempre disponible, íntegra y solo accesible para personas autorizadas. Así, la organización puede manejar tanto las amenazas internas como las externas, garantizando la continuidad de sus operaciones, manteniendo su competitividad en el mercado, reforzando la confianza de los clientes, asegurando la rentabilidad y cumpliendo con las obligaciones legales necesarias para alcanzar sus objetivos

Para desarrollar los pilares de la información se tiene:

Dimensión 1: Confidencialidad, según Gómez (2019), la pertenencia es el factor que evita la divulgación de información a terceras personas, así como sistemas sin permiso para acceder a dicha información. Solo las personas autorizadas tienen acceso exclusivo a la información.

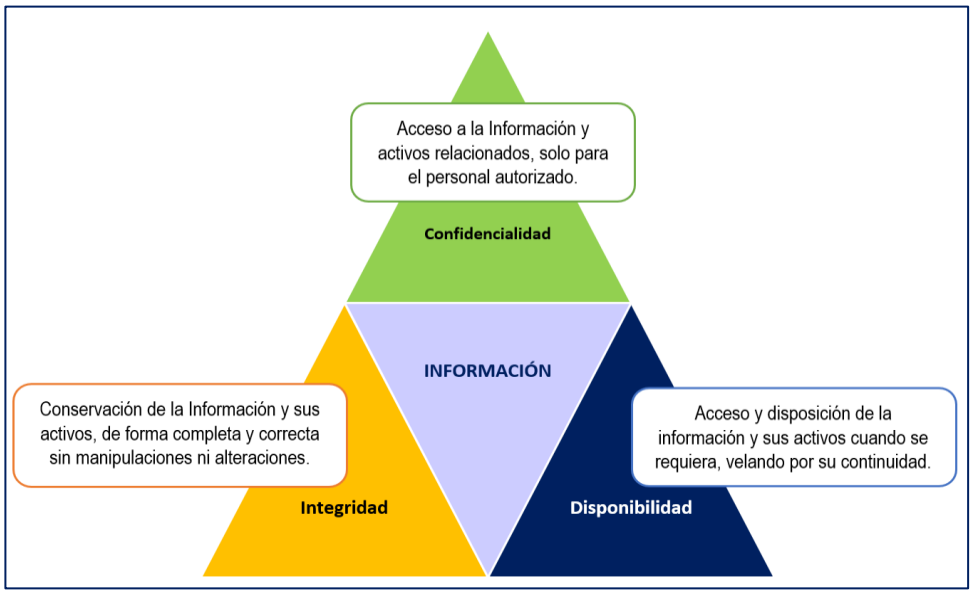
Dimensión 2: Integridad, según Gómez (2019), implica mantener la información sin cambiar, garantizando su exactitud en todo momento. Esta propiedad garantiza que la información no pueda ser alterada por personas no autorizadas o

sistemas. Por lo tanto, la integridad apoya la confiabilidad y la exactitud de la información cuando es necesaria.

Dimensión 3: Disponibilidad, la Disponibilidad es una dimensión importante en la seguridad de la información. Según Gómez (2019), esta cualidad garantiza que la información esté siempre disponible para las personas, sistemas o procesos autorizados. El acceso a la data se realiza de manera segura y oportuna.

Figura 2.

Pilares de la Seguridad de la Información (CID)



Nota. Fuente: Elaboración propia.

Diferencias entre la seguridad de la información con la ciberseguridad y la seguridad informática.

Respecto a la diferencia en estas tres definiciones se tiene: Seguridad de la Información: Se centra en preservar la tríada CID (Confidencialidad, Integridad y Disponibilidad) de la información. Su objetivo es proteger la información contra cualquier riesgo, ya sea que se encuentre en medios físicos o digitales (Alexander, 2015). Seguridad Informática: Su finalidad es mantener el funcionamiento adecuado de los activos de información, las redes de datos y los sistemas en un entorno digital. Se enfoca en proteger la información que circula a través de medios digitales, excluyendo los medios físicos (Fernández, 2015). Ciberseguridad: Sirve para proteger sistemas, redes y software de ataques digitales en línea (como transacciones

bancarias y consultas web en tiempo real, entre otros), que suelen dirigirse a la manipulación, acceso o destrucción de datos confidenciales, así como al chantaje de usuarios o la interrupción de operaciones. El aumento del número de dispositivos conectados, el superávit de usuarios y la creciente creatividad de los atacantes hoy en día justifican la adopción de medidas de seguridad digital.

Población: Carrillo (2015) expresa que la población se puede definir como un conjunto de personas, objetos u cosas que tienen características únicas, que los hacen aptos para ser investigados. Esto significa que la población no se limita solo a las personas, sino que también incluye cualquier entidad que muestre características que la conviertan en objeto de estudio. Creswell (2014), proporciona una guía exhaustiva de diseño de investigación, incluyendo la definición de poblaciones y cómo éstas se relacionan con variables independientes y dependientes, asimismo Kerlinger y Lee (2000), ofrecen una base sólida sobre cómo seleccionar y definir poblaciones en estudios de investigación, incluyendo cómo la población se define independientemente de las variables dependientes, en consecuencia, teniendo el sustento en estas referencias en la presente investigación, dado que a un activo de información se le puede aplicar uno o más controles relacionados con las dimensiones referidas al CID y ya que los controles forman parte de la dimensión de la norma y lo que se requiere es conocer si dichos controles protegen o no a los activos de información teniendo como indicador a las incidencias de los mismos, se seleccionó como población los controles del SGSI basados en la norma ISO/IEC 27001:2022, que están listados en el Anexo A. De los noventa y tres (93) controles especificados, estos se agrupan en cuatro categorías principales: Controles organizacionales (37), Controles de personas (8), Controles físicos (14) y Controles tecnológicos (34), todos los cuales están orientados a la salvaguarda de los recursos de información, sin embargo, se seleccionaron y aplicaron en la entidad los controles tecnológicos. Estos últimos, que se eligieron por coherencia y juicio, que suman un total de treinta (30), fueron elegidos en función de su pertinencia, clasificados por cada dimensión de la variable dependiente y según la identificación de los recursos que se tiene de forma preponderante, del proceso core seleccionado por la entidad.

Cabe resaltar también que, en el proceso de implementación del SGSI, se subraya la importancia de las guías de observación como herramienta clave para asegurar el éxito. Estas guías se utilizaron tanto antes como después de la

implementación, abarcando los controles seleccionados para la entidad designados para la protección de activos.

De otro lado, en el examen de normalidad se aplicó el estudio de Shapiro & Wilk (1965), ya que evalúa si una muestra sigue una distribución normal, siendo especialmente efectiva para muestras pequeñas a moderadas (menores que 50), ya que detecta desviaciones de la normalidad mejor que otras pruebas, ya que al seleccionar como alcance el proceso de compras, se determinaron a los activos de información más sensibles para poder salvaguardarlos, identificados los mismos, se procedió a denotar el nivel de riesgo, para poder implementar los controles, finalmente esto se midió en un post test de nuevo a fin de apreciar y demostrar que el SGSI protege a los activos de información de la entidad.

Muestra: Tal como indica Toledo (2016), al elegir la muestra, es necesario identificar ciertas características que la población debe poseer para ser objeto de estudio. Esto significa que la muestra debe cumplir con los criterios establecidos para su selección en la investigación. Dado que la población está compuesta por treinta y cuatro (34) controles, se estableció un nivel de confianza del 95% con un margen de error del 5% esto significa que cuanto menor sea el margen de error el resultado será más preciso en relación con el nivel de confianza especificado. Como resultado del cálculo del tamaño muestral, se determinó un promedio de treinta (30) controles que deben ser establecidos y que refieren a la temática de Seguridad de Redes, Control de accesos y las operaciones de los sistemas, todo ello relacionado a Tecnologías de la Información, se excluyeron a cuatro (4) controles por no tener relación respecto a los activos de información que se identificaron en la entidad.

Muestreo: Otzen y Manterola (2017) sostienen que el principio esencial del muestreo es analizar la distribución de una variable tanto en la muestra estudiada como en la población total. Por lo tanto, es fundamental establecer criterios claros para agrupar la población y la muestra que se utilizará en la investigación. Dado que hay alrededor de 30 controles de seguridad disponibles en este contexto, el uso del muestreo se descarta al ser significativo, el concepto de "descartar" el muestreo en el contexto de “significación estadística” describe que los resultados obtenidos son suficientes para tomar decisiones, y por lo tanto, no es necesario recolectar más datos (Salkind, 2010).

Técnicas e instrumentos de recolección de Datos: Técnicas, Según Hernández (2014), la recolección de datos es fundamental y se puede realizar mediante diversas técnicas, como observación, encuestas, entrevistas, análisis documental y contenido. Estas técnicas deben estar alineadas con la problemática planteada y las hipótesis de estudio. Se utilizó la observación en el estudio como técnica principal de la variable dependiente: protección de la información mediante la implementación del “SGSI basado en la ISO/IEC 27001:2022” que es la variable independiente, comparándose las incidencias generadas en el antes y el después de la aplicación de controles.

Instrumentos: Se emplearon guías de observación, dado que el diseño experimental es del sub-diseño pre-experimental. Los datos recopilados, de naturaleza cuantitativa, fueron evaluados comparando la situación antes y después de implementar los controles tecnológicos. de la norma, si bien este tipo de instrumento no requiere juicios de expertos para la validación, a fin de aumentar la confiabilidad, se tuvo la evaluación de tres (3) expertos (Ver anexo n.°3) los cuales verificaron la validación. Estas herramientas de observación permiten al investigador concentrarse en un hecho o fenómeno para recopilar datos o información. En conclusión, para el estudio en cuestión, se utilizaron fichas o formularios de observación como instrumento de recolección de datos (Campos & Lule, 2012) teniendo el comportamiento de auditor para la toma de datos.

Métodos para análisis de datos; para llevar a cabo el procesamiento en un diseño experimental de enfoque cuantitativo, se desarrolló un instrumento basado en la "Protección de activos”, que fue manipulado por la variable independiente "SGSI basado en ISO/IEC 27001:2022". La validación de expertos no fue necesaria, ya que estos instrumentos consisten en fichas de observación, aunque se buscó el juicio de tres (3) expertos para mejorar la confiabilidad. Se aplicó la técnica de observación para registrar las incidencias que afectan la seguridad pre y post de implementar los controles tecnológicos de la norma en la institución. Los datos obtenidos se detallaron en el Excel y se analizaron con el SPSS, utilizando la prueba de doble masas para garantizar la consistencia y la aceptación de los datos.

Asimismo, se realizó un análisis descriptivo para calcular la suma, el promedio, la varianza y la media de los datos recolectados antes y después de aplicar los

controles establecidos por la norma ISO/IEC 27001:2022 para los activos de información identificados. Tras finalizar el análisis estadístico inferencial, se llevó a cabo una prueba de consistencia para evaluar la fiabilidad de los datos, seguida de una prueba de normalidad para la población. Finalmente, se realizó una prueba de contraste para validar las hipótesis, presentando las sugerencias y los resultados obtenidos.

Se utilizaron fichas de observación para recopilar los resultados del análisis de los datos. Para evaluar la confiabilidad tanto antes como después de la prueba, se aplicó una prueba de doble masa. A continuación, se utilizó la prueba de Shapiro-Wilk para determinar si los datos se ajustan a una distribución paramétrica. Finalmente, para evaluar los resultados, se utilizó una prueba de comparación adecuada a la normalidad de los datos. En resumen, se emplearon la prueba T-Student para los datos que resultaron ser paramétricos.

Aspectos éticos: La autora de la presente investigación llevó a cabo de manera individual la recolección, procesamiento y análisis de datos. Las referencias bibliográficas fueron citadas siguiendo las normas APA en su séptima edición. El trabajo fue evaluado por el software Turnitin para verificar su originalidad, como lo establece la Resolución del Vicerrectorado de Investigación N°081-2024-VI-UCV. Se cumplieron con las pautas establecidas en la resolución rectoral número 0470-2022/UCV. Según lo describió la investigadora, las fichas de observación se utilizaron para recopilar datos tanto antes como después de la implementación del SGSI. Conforme a la Ley n.º 29733: Ley de Protección de Datos Personales y su reglamento, aprobado mediante el Decreto Supremo N.º 003-2013-JUS, en vigor desde el 22 de marzo de 2013, se brindó información detallada sobre la investigación y se aseguró la protección y confidencialidad de los participantes.

III. RESULTADOS

Se tiene en cuenta que el anexo A de la norma ISO/IEC 27001:2022 contiene 93 controles en total, que se clasifican en cuatro categorías principales: 34 Controles Tecnológicos, 37 Controles Organizativos, 8 Controles Humanos, 14 Controles Físicos y 8 Controles de Personas. Para los efectos siguientes, se requiere este conocimiento. Estos controles están agrupados según el área temática que debe cubrir la norma.

En la institución del sector defensa, se decidió implementar los controles tecnológicos tras un diagnóstico previo, abarcando áreas como el Control de accesos, Seguridad de redes, y la Gestión de las operaciones de sistemas relacionados con Tecnologías de Información. En consecuencia, se optó por establecer el SGSI con un enfoque principal en proteger a los recursos en relación a las TICs. La data se recopiló mediante fichas de observación, adoptando la suscrita el rol de un auditor para identificar imparcialmente las incidencias relacionadas con los controles tecnológicos seleccionados durante el año. De acuerdo con las dimensiones abordadas en esta investigación en relación con la variable dependiente, se eligieron treinta (30) de los controles revisados para aplicar a la entidad. Estos controles se distribuyeron en diez (10) categorías: confidencialidad, integridad y disponibilidad. La información recolectada también fue procesada utilizando el programa estadístico IBM SPSS Statistics Versión 29.0.2.0, el cual arrojó los resultados que se mostrarán en esta sección.

Asimismo, para procesar los cálculos de la PIA(C/I/D): Porcentaje de incidentes que impactan negativamente en la CID, se tuvo la siguiente fórmula:

Fórmula: PIA(C/I/D) = (NIC/NITC)*100

Cuya leyenda es la siguiente:

NI(C/I/D): Número de incidentes asociados con la protección del CID de los recursos, según sea pertinente.

NIT(C/I/D): Incidentes totales relativos, según proceda, a la preservación de la disponibilidad, integridad o reserva de los activos de información.

De otro lado, el número de incidencias que afectaron a la protección de activos de información referidos al antes del Test (pre) y después del test (pos), según los controles mencionados fueron:

- Respecto a **Confidencialidad**, que refiere a implementar controles para proteger a la información y sus activos contra accesos no autorizados, aquí se presenta los resultados del levantamiento de información, en el antes y en el después:

Tabla 1

Datos referidos a la Dimensión Confidencialidad

				PRE – TEST (2023)			POST TEST (2024)		
N°	**ACT. DE INFORMACIÓN IDENTIFICADO (S)**	**CÓD. DE CONTROL SEGÚN ISO/IEC 27001:2022 "ANEXO A"**	**CONTROLES ANEXO A" DE LA NTP ISO/IEC 27001:2022**	**NIC**	**NITC**	**PIAC**	**NIC**	**NITC**	**PIAC**
1	PC/LAPTOP	A.8.1	*Dispositivos Pcs de usuario*	100	2229	4.486316734	25	275	9.090909091
2	SERVIDORES	A.8.2	*Derechos de acceso privilegiado*	150	2229	6.729475101	12	275	4.363636364
3	SERVIDORES	A.8.5	*Authentication Security*	126	2229	5.652759085	19	275	6.909090909
4	SERVIDORES	A.8.7	*Protection contra malware*	230	2229	10.31852849	20	275	7.272727273
5	PC/LAPTOP	A.8.10	*Elimination de information*	265	2229	11.88873934	43	275	15.63636364
6	PC/LAPTOP	A.8.19	*Instalación de software en sistemas operativos*	215	2229	9.645580978	31	275	11.27272727
7	SGD Y CORREO ELECTRONICO INSTITUCIONAL	A.8.24	*Uso de cryptographic*	341	2229	15.29834006	48	275	17.45454545
8	SIGCO	A.8.26	*Requisitos de seguridad de las aplicaciones*	325	2229	14.58052939	26	275	9.454545455
9	SIGCO	A.8.27	*Principios de arquitectura y ingeniería de sistemas seguros*	152	2229	6.819201436	25	275	9.090909091
10	SIGCO	A.8.28	*Codification security*	325	2229	14.58052939	26	275	9.454545455
TOTAL ITEMS EVALUADOS				**2229**			**275**		

Nota. Fuente: Elaboración propia.

- **Integridad:** que refiere a implementar controles para proteger a la información y sus activos de modificaciones no autorizadas, aquí se presenta los resultados, en el antes y en el después:

Tabla 2

Datos referidos a la Dimensión Integridad

				PRE – TEST (2023)			POST TEST (2024)		
N°	**ACT. DE INFORMACIÓN IDENTIFICADO (S)**	**CÓD. DE CONTROL SEGÚN ISO/IEC 27001:2022 "ANEXO A"**	**CONTROLES REFERIDO AL "ANEXO A" DE LA NTP ISO/IEC 27001:2022**	**NIC**	**NITC**	**PIAC**	**NIC**	**NITC**	**PIAC**
11	PORTAL GOB.PE	A.8.3	*Restricción de acceso a la información*	250	1965	12.72265	52	436	11.9266055
12	SIGCO	A.8.4	*Acceso al Código fuente*	225	1965	11.45038	52	436	11.9266055
13	SERVIDORES	A.8.9	*Gestion de la configuration*	163	1965	8.295165	41	436	9.40366972
14	BASE DE DATOS	A.8.11	*Enmascaramiento de datos*	125	1965	6.361323	55	436	12.6146789
15	SIGCO	A.8.12	*Prevención de pérdida de datos*	350	1965	17.8117	50	436	11.4678899
16	SGD	A.8.18	*Uso de programas de utilidad con privilegios*	95	1965	4.834606	35	436	8.02752294
17	SIGCO	A.8.25	*Ciclo de vida seguro de desarrollo*	164	1965	8.346056	22	436	5.04587156
18	RPME	A.8.30	*Desarrollo subcontratado*	283	1965	14.40204	34	436	7.79816514
19	SIGCO	A.8.32	*Gestión del cambio*	180	1965	9.160305	48	436	11.0091743
20	SIGCO	A.8.34	*Protección de los sistemas de información durante las pruebas de auditoría*	130	1965	6.615776	47	436	10.7798165
TOTAL ITEMS EVALUADOS				**1965**			**436**		

Nota. Fuente: Elaboración propia.

- **Disponibilidad:** que refiere a implementar controles para proteger a la información y sus activos asegurando que los mismos estén disponibles cuando se necesiten, aquí se presenta lo que se obtuvo en la toma de datos, en el antes y en el después:

Tabla 3

Datos referidos a la Dimensión Disponibilidad

				PRE - TEST			POST TEST		
N°	**ACT. DE INFORMACIÓN IDENTIFICADO (S)**	**CÓD. DE CONTROL SEGÚN ISO/IEC 27001:2022 "ANEXO A"**	**CONTROLES "ANEXO A" DE LA NTP ISO/IEC 27001:2022**	**NIC**	**NITC**	**PIAC**	**NIC**	**NITC**	**PIAC**
21	SERVICIO DE INTERNET	A.8.6	*Gestión de capacidad*	275	2158	12.7432808	48	287	16.724739
22	PCs/ LAPTOPs	A.8.8	*Technical vulnerability management*	332	2158	15.3846154	30	287	10.452962
23	STORAGES	A.8.13	*Copia de seguridad de la información*	214	2158	9.91658943	12	287	4.1811847
24	SITIO ALTERNO	A.8.14	*Redundancia de las instalaciones de procesamiento de información*	148	2158	6.85820204	50	287	17.421603
25	SOFTWARE DE MONITOREO	A.8.16	*Monitoreo de actividades*	251	2158	11.6311399	21	287	7.3170732
26	SOFTWARE ANTIVIRUS	A.8.20	*Seguridad de redes*	116	2158	5.37534754	24	287	8.3623693
27	SWITCHES	A.8.21	*Security of network services*	145	2158	6.71918443	26	287	9.0592334
28	RED DE DATOS	A.8.22	*Segregación de redes*	208	2158	9.63855422	14	287	4.8780488
29	FIREWALL	A.8.23	*Filtrado web*	305	2158	14.1334569	26	287	9.0592334
30	SERVIDORES	A.8.31	*Separación de entornos de desarrollo, pruebas y producción*	164	2158	7.59962929	36	287	12.543554
TOTAL ITEMS EVALUADOS				**2158**			**287**		

Nota. Fuente: Elaboración propia.

3.1. ANÁLISIS DESCRIPTIVO

La data de las incidencias que refieren a las 3 dimensiones de la variable dependiente se procesó, esto correspondiente a los cuadros anteriores, estos datos se obtuvieron del SPSS, obteniéndose lo siguiente:

3.1.1. Dimensión 1: Confidencialidad

Tabla 4

Resultado Descriptivo Dimensión Confidencialidad

	Casos					
	Vál		Perd		T	
	N	%	N	%	N	%
CONFI.PRE	10	100,0%	0	0,0%	10	100,0%
CONFI.POS	10	100,0%	0	0,0%	10	100,0%

Nota. Fuente: Elaboración propia.

En la “Tabla 4”, se muestra los resultados sobre confidencialidad referida a la información y sus activos, se observa 10 números validos al 100% con ningún número perdido obteniendo el 100% de porcentaje total.

Tabla 5

Análisis Descriptivo: Frecuencias. Pre-test y Post-test– Dimensión Confidencialidad

			Estadístico	Desv. Error
CONFI.PRE	Mdia.		222.90	28,189
	95% IC para la mdia.	Lím.inf.	159.13	
		Lím. Sup.	286.67	
	Mdia rec al 5%		223.17	
	Mdana		222.50	
	Vza		7946,322	
	Desv. Est.		89,142	
	Mín		100	
	Máx		341	
	Rang.		241	
	Rang. intercuartil		181	

			Estadístico	Desv. Error
	Asimetría		0.067	0.687
	Curtosis		-1.627	1.334
CONFI.POS	Mdia.		27.50	3.429
	95% IC para la mdia.	Lím.inf.	19.74	
		Lím. Sup.	35.26	
	Mdia rec al 5%		27.22	
	Mdana.		25.50	
	Vza		117,611	
	Desv. Est.		10,845	
	Mín		12	
	Máx		48	
	Rang.		36	
	Rang. intercuartil		14	
	Asimetría		0.826	0.687
	Curtosis		*0.405*	*1.334*

Nota. Fuente: Elaboración propia.

3.1.2. Dimensión 2: Integridad

Tabla 6

Resultado Descriptivo Dimensión Integridad

	Casos					
	Vál		Perd		T	
	N	%	N	N	%	N
INTE.PRE	10	100,0%	0	0,0%	10	100,0%
INTE.POS	10	100,0%	0	0,0%	10	100,0%

Nota. Fuente: Elaboración propia.

En la “Tabla 6”, se muestra los resultados respecto a la dimensión Integridad referido a la información y sus activos, se observa 10 datos válidos al 100% con ningún número perdido obteniendo el 100% de porcentaje total.

Tabla 7

Análisis Descriptivo: Frecuencias. Pretest y Postest– Dimensión Integridad

			Estadístico	Desv. Error
INTE.PRE	Mdia.		196.50	25.168
	95% IC para la mdia.	Lím.inf.	139.57	
		Lím. Sup.	253.43	
	Mdia rec al 5%		193.61	
	Mdana		172.00	
	Vza		6334,056	
	Desv. Est.		79,587	
	Mín		95	
	Máx		350	
	Rang.		255	
	Rang. intercuartil		130	
	Asimetría		0,732	0,687
	Curtosis		0,127	1,334
INTE.POS	Mdia.		43,60	3,304
	95% IC para la mdia.	Lím.inf.	36,13	
		Lím. Sup.	51,07	
	Mdia rec al 5%		44,17	
	Mdana.		47,50	
	Vza		109,156	
	Desv. Est.		10,448	
	Mín		22	
	Máx		55	
	Rang.		33	
	Rang. intercuartil		17	
	Asimetría		-1,043	0,687
	Curtosis		0,437	1,334

Nota. Fuente: Elaboración propia.

3.1.3. Dimensión Disponibilidad

Tabla 8

Resultado Descriptivo Dimensión Disponibilidad

	Casos					
	Vál		Perd		T	
	N	%	N	N	%	N
DISPO.PRE	10	100,0%	0	0,0%	10	100,0%
DISPO.POS	10	100,0%	0	0,0%	10	100,0%

Nota. Fuente: Elaboración propia.

En la “Tabla 8” se presentan los resultados sobre la disponibilidad de la información y sus activos, donde se observa que 10 datos son completamente válidos, sin ningún dato faltante, logrando así un porcentaje total del 100%.

Tabla 9

Análisis Descriptivo: Frecuencias. Pretest y Postest– Dimensión Disponibilidad

			Estadístico	Desv. Error
DISPO.PRE	Mdia.		215,80	23,219
	95% IC para la mdia.	Lím.inf.	163,28	
		Lím. Sup.	268,32	
	Mdia rec al 5%		214,89	
	Mdana.		211,00	
	Vza		5391,067	
	Desv. Est.		73,424	
	Mín		116	
	Máx		332	
	Rang.		216	
	Rang. intercuartil		135	
	Asimetría		0,256	,687
	Curtosis		-1,245	1,334
DISPO.POS	Mdia.		28,70	4,044
	95% IC para la mdia.	Lím.inf.	19,55	

		Estadístico	Desv. Error
	Lím. Sup.	37,85	
	Mdia rec al 5%	28,44	
	Mdana.	26,00	
	Vza	163.567	
	Desv. Est.	12.789	
	Mín	12	
	Máx	50	
	Rang.	38	
	Rang. intercuartil	20	
	Asimetría	0,585	0,687
	Curtosis	-0,456	1,334

Nota. Fuente: Elaboración propia.

Se presenta el siguiente cuadro resumen con la media en porcentaje, de lo anteriormente expuesto, a fin de compendiar las tres dimensiones referido al tipo de testo considerando las principales medidas que se detallan a continuación:

Tabla 10

Procesamiento de Datos respecto al Pre test (2023) y Post Test (2024)

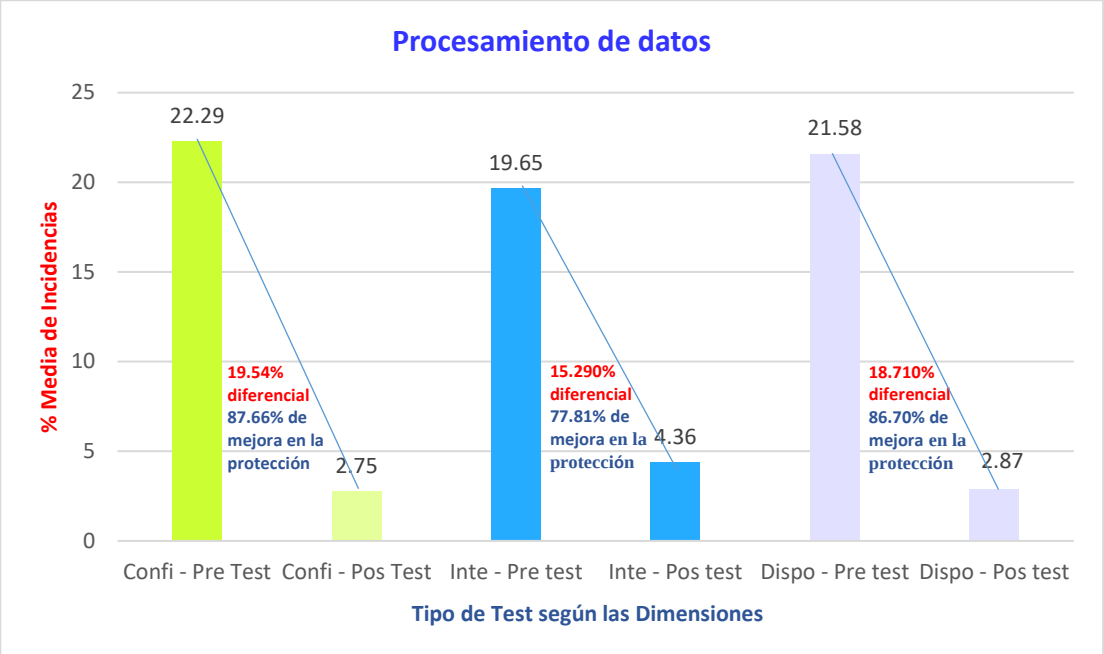
Dimensión/ Tipo de Test	N	Rango (Max - Min)	Mini mo	Máxi mo	Suma	Mdia %	Desv. Est	Diferen cial de mdias %	% de Mejora
Confi - Pre Test	10	241	100	341	2229	22.29	89.142	19.54	87.66
Confi - Pos Test	10	36	12	48	275	2.75	10.845		
Inte - Pre test	10	255	95	350	1965	19.65	79.59	15.29	77.81
Inte - Pos test	10	33	22	55	436	4.36	10.45		
Dispo - Pre test	10	216	116	332	2158	21.58	73.42	18.71	86.70
Dispo - Pos test	10	38	12	50	287	2.87	12.79		

Nota. Fuente: Elaboración propia.

Del cuadro anterior se obtiene el siguiente gráfico:

Figura 3

Procesamiento de los datos antes y después de la aplicación de controles



Nota. Fuente: Elaboración propia.

La “Tabla 10” y la “Figura 3” muestran una diferencia del 19,54% en el porcentaje de incidentes que afectan a la confidencialidad entre la media estadística de la preprueba y la posprueba. La proporción de incidentes en el pre-test fue del 22,29%; en el post-test, descendió al 2,5%.

Además, el porcentaje de incidentes que comprometen la integridad difiere en un 15,29% entre las medias estadísticas del pretest y el postest. El porcentaje de incidentes en el pre-test fue del 19,65%; en el post-test, del 4,36%. El porcentaje de incidentes que afectan a la disponibilidad también varía, con una media del 21,58% en la preprueba y un 2,87% en la posprueba.

Como resultado del análisis de la investigación, la protección de la confidencialidad ha mejorado en un 87,66%, la protección de la integridad ha mejorado en un 77,81% y la disponibilidad se ha salvaguardado en un 86,70%. Se realizaron pruebas de normalidad y contraste para evaluar la hipótesis H1 en relación con la aplicación de los controles contenidos en la implantación del SGSI para garantizar lo anterior.

3.2. ANÁLISIS DE NORMALIDAD E INFERENCIAL

La comprobación de hipótesis es un proceso estadístico para determinar si una hipótesis o afirmación sobre una población es válida examinando si una muestra de datos contiene pruebas suficientes para apoyar esta conclusión. Requiere evaluar dos hipótesis rivales: la hipótesis alternativa (H1) y la hipótesis nula (H0). Basándose en los datos y en un nivel de significación predefinido, la prueba ayuda a determinar si se rechaza o no la hipótesis nula, por ende la hipótesis general se sustenta en el comportamiento de las sub hipótesis, en ese sentido, se buscó analizar la misma, en sus dimensiones.

Asimismo, la consistencia de los datos es la clasificación de estos, que presentan un patrón de uniformidad y regularidad en su selección, según Peña (2017). En síntesis, la similitud de los datos se organizó de acuerdo a los eventos que impactaron en la protección de los activos de información en este caso. Tanto para el pre-test como para el post-test, se consideró un periodo de observación de seis meses.

Los indicadores se resumen en el cuadro siguiente: Los porcentajes anteriores y posteriores a la prueba para la proporción de incidencias que comprometen la confidencialidad variaron entre el 4,49% y el 15,30% en el pre y entre el 4,36% y el 17,45% en el pos, respectivamente. Los porcentajes de incidencias que afectan a la integridad variaron entre el 4,83% y el 17,81% en el pretest y entre el 5,05% y el 12,61% en el postest y en el pretest reveló porcentajes que oscilaban entre el 5,38% y el 15,38% en el pre mientras que el postest reveló valores que oscilaban entre el 4,18% y el 17,42%, para las incidencias que afectan a la disponibilidad.

Tabla 11.

Consolidación de los 3 indicadores

Confi - Pre	Confi – Post	Inte - Pre	Inte – Post	Dispo – Pre	Dispo – Post
4.49	9.09	12.72	11.93	12.74	16.72
6.73	4.36	11.45	11.93	15.38	10.45
5.65	6.9	8.3	9.4	9.92	4.18
10.32	7.27	6.36	12.61	6.86	17.42
11.89	15.64	17.81	11.47	11.63	7.32

Confi - Pre	Confi – Post	Inte - Pre	Inte – Post	Dispo – Pre	Dispo – Post
9.65	11.27	4.83	8.03	5.38	8.36
15.30	17.45	8.34	5.05	6.72	9.06
14.59	9.45	14.4	7.8	9.64	4.88
6.82	9.09	9.16	11	14.13	9.06
14.58	9.45	6.62	10.78	7.6	12.54

Nota. Fuente: Elaboración propia.

Hipótesis específica 1c (HE1c): El SGSI basado en ISO/IEC_27001:2022, protege la confidencialidad de los activos de información de una entidad pública del Sector Defensa, Lima, 2024.

Se presenta la data que se ha utilizado para determinar su consistencia, obteniendo lo siguiente:

a. Consistencia

Tabla 12.

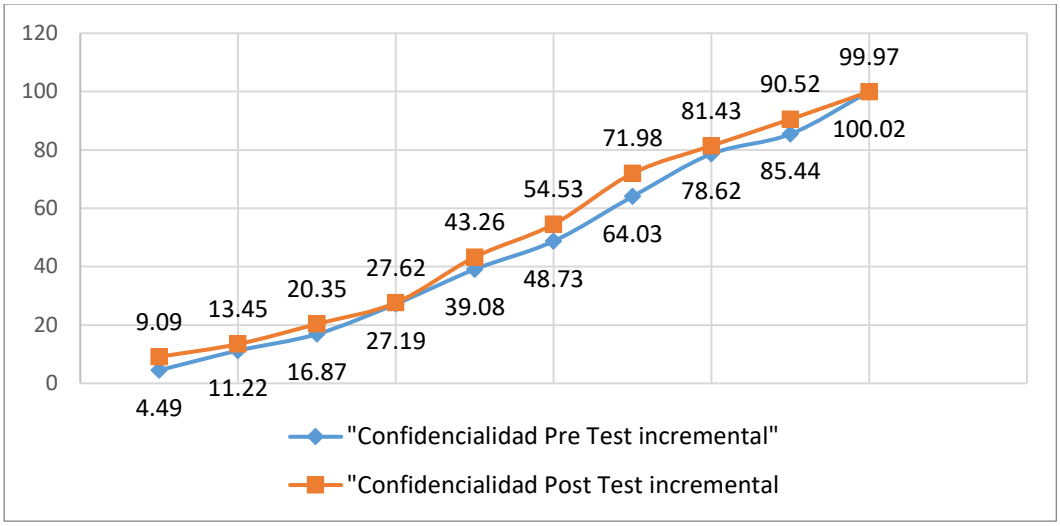
Porcentaje de incidentes incremental que afectan a la confidencialidad

Incremental Confi - Pre	Incremental Confi - Post
4.49	9.09
11.22	13.45
16.87	20.35
27.19	27.62
39.08	43.26
48.73	54.53
64.03	71.98
78.62	81.43
85.44	90.52
100.02	99.97

Nota. Fuente: Elaboración propia.

Figura 4

Consistencia del porcentaje de incidentes que afectan a la confidencialidad



Nota. Fuente: Elaboración propia.

Basándose en la información de la “Tabla 12”, el gráfico de la “Figura 4” de los valores consolidados de la fracción de ocurrencias relacionadas con la confidencialidad muestra una tendencia creciente, lo que sugiere que los datos son fiables. En resumen, la prueba de doble masa confirma que los datos combinados son coherentes, lo que garantiza que las pruebas de normalidad y contraste HE1c se desarrollarán sin problemas.

b. Normalidad

Tabla 13.

Prueba de normalidad en HE1c

	Shapiro-Wilk		
	Estadístico	**gl**	**Sig.**
CONFI.PRE	0,914	10	0,312
CONFI.POS	0,912	10	0,295

Nota. Fuente: Elaboración propia.

El porcentaje de incidentes que afectan a la confidencialidad, tanto en el pretest como en el post-test, que incluye datos paramétricos, se muestra en la “Tabla 13”. Según el análisis estadístico de la prueba de Shp-Wilk, el valor de significación (Sig.) es superior a 0,05.

c. Contraste

H0c: El SGSI basado en ISO/IEC_27001:2022 no protege la confidencialidad de los activos de información.

Tabla 14.

Prueba T-Student – indicador Porcentaje de incidentes que afectan la confidencialidad

Estadísticas para muestras pareadas					
		Media (%)	N	Desv. Est.	Desv. Error promedio
Par 1	CONFI.PRE	22.29	10	89,142	28,189
	CONFI.POS	2.750	10	10,845	3,429

Nota. Fuente: Elaboración propia.

Tabla 15.

Prueba T-Student –Incidentes en confidencialidad

Prueba de muestras emparejadas									
		Diferencias emparejadas							
		Media	Desv. Est.	Desv. Error promedio	95% de intervalo de confianza de la diferencia		t	gl	Sig. (bilateral)
					Inferior	Superior			
Par 1	CONFI.PRE - CONFI.POS	195.400	83.218	26.316	135.870	254.930	7.42	9	0.000

Nota. Fuente: Elaboración propia.

El total promedio de los dos porcentajes de eventos de confidencialidad en las “Tablas 14” y “15” es significativo; indica un promedio de 22,29% en el pre-test y 2,75% en el post-test. La muestra también se emparejó para la prueba T-Student y los resultados mostraron que el "Sig." El valor en el porcentaje de incidencias que afectan a la confidencialidad es inferior a 0,05. Como resultado, se rechaza la hipótesis nula (H0c) y se acepta que los controles SGSI elegidos, basados en la norma ISO/IEC 27001:2022, protegen la confidencialidad de los activos de información de una entidad pública del Sector Defensa, Lima, 2024.

<u>Hipótesis específica 1i (HE1i)</u>: El SGSI basado en ISO/IEC_27001:2022, protege la integridad de los activos de información de una entidad pública del Sector Defensa, Lima, 2024.

Se presenta la data que se ha utilizado para determinar su consistencia, obteniendo lo siguiente:

a. Consistencia

Tabla 16.

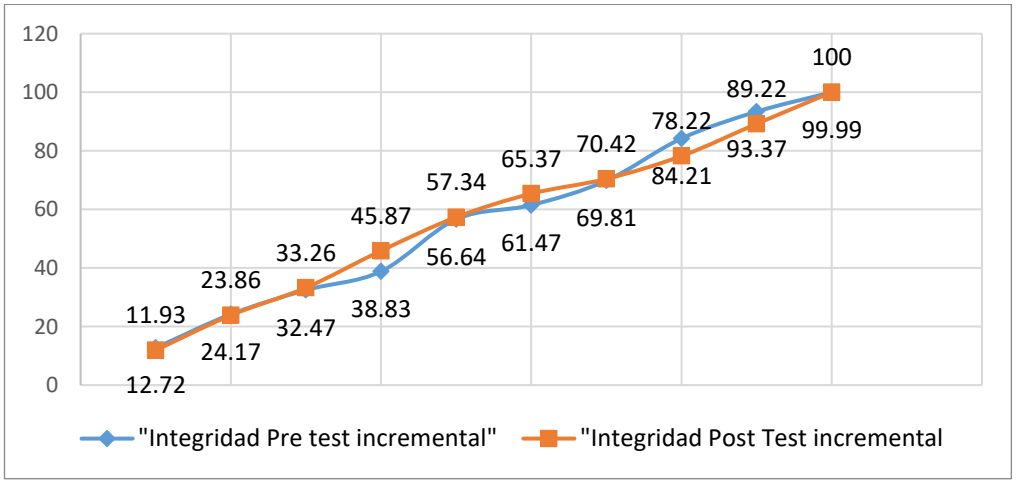
Porcentaje de incidentes incremental que afectan a la Integridad

Incremental Inte - Pre	Incremental Inte - Post
12.72	11.93
24.17	23.86
32.47	33.26
38.83	45.87
56.64	57.34
61.47	65.37
69.81	70.42
84.21	78.22
93.37	89.22
99.99	100

Nota. Fuente: Elaboración propia.

Figura 5

Consistencia del porcentaje de incidentes que afectan a la integridad



Nota. Fuente: Elaboración propia.

En la “Figura 5”, utilizando los datos de la “Tabla 16”, se observa que los valores consolidados de la tasa de incidentes relacionados con la integridad presentan una línea ascendente, lo que indica que los datos son coherentes. En resumen, la prueba de doble masas nos afirma que los datos acumulados son confiables, es decir, no habrá ningún problema al realizar la prueba de normalidad y de contraste en la HE1i.

b. Normalidad

Tabla 17

Prueba de normalidad en HE1i.

	Shapiro-Wilk		
	Estadístico	**gl**	**Sig.**
INTE.PRE	0.946	10	0.624
INTE.POS	0.894	10	0.190

Nota. Fuente: Elaboración propia.

La “Tabla 17” muestra que los datos paramétricos están incluidos en el índice de incidentes que afectan a la integridad tanto en el pretest como en el postest; según el análisis estadístico para la prueba de Shapiro-Wilk, el valor de significación (Sig.) es superior a 0,05.

c. Contraste

H0i: El SGSI basado en ISO/IEC_27001:2022 no protege la integridad de los activos de información.

Tabla 18

Prueba T-Student – indicador Porcentaje de incidentes que afectan la Integridad

Estadísticas para muestras pareadas					
		Media (%)	**N**	**Desv. Est.**	**Desv. Error promedio**
Par 1	**INTE.PRE**	19.65	10	79,587	25,168
	INTE.POS	4.360	10	10,448	3,304

Nota. Fuente: Elaboración propia.

Tabla 19.

Prueba T-Student –Incidentes en Integridad

Prueba de muestras emparejadas									
		Diferencias emparejadas							
		Media	Desv. Est.	Desv. Error promedio	95% de intervalo de confianza de la diferencia		t	gl	Sig. (bilateral)
					Inferior	Superior			
Par 1	INTE.PRE - INTE.POS	152.90	78.323	24.768	96.871	208.929	6.173	9	0.000

Nota. Fuente: Elaboración propia.

En la “Tabla 18” y “19”, se verifica que el promedio de los 2 porcentajes es notable respecto a integridad, al mostrar 19.65% de promedio en el pre-test y del 4.36% en post-test. Asimismo, se emparejo la muestra en la prueba de T-Student, donde se apreció que el valor "Sig." es menor que 0.05 en la tasa de incidentes que afecta la integridad, por lo que, se acepta que los controles seleccionados del SGSI basado en la ISO/IEC 27001:2022, protegen la integridad de los activos de información de una entidad pública del Sector Defensa, Lima, 2024, rechazando la hipótesis nula (H0i).

Hipótesis específica 1d (HE1d): El SGSI basado en ISO/IEC_27001:2022, protege la disponibilidad de los activos de información de una entidad pública del Sector Defensa, Lima, 2024.

Se presenta la data que se ha utilizado para determinar su consistencia, obteniendo lo siguiente:

a. Consistencia

Tabla 20

Porcentaje de incidentes incremental que afectan a la Disponibilidad

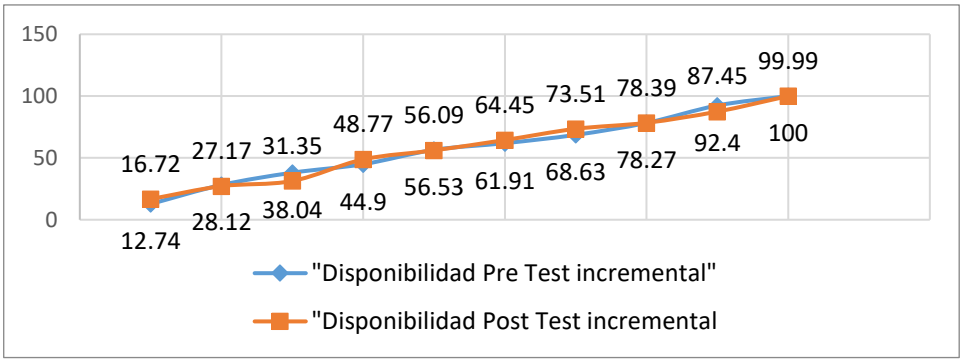
incremental Dispo - Pre	incremental Dispo - Post
12.74	16.72
28.12	27.17
38.04	31.35
44.9	48.77
56.53	56.09
61.91	64.45

incremental Dispo - Pre	incremental Dispo - Post
68.63	73.51
78.27	78.39
92.4	87.45
100	99.99

Nota. Fuente: Elaboración propia.

Figura 6

Consistencia del porcentaje de incidentes que afectan a la Disponibilidad



Nota. Fuente: Elaboración propia.

En la “Figura 6”, tomando los datos de la “Tabla 20”, se evidencia que los valores consolidados de la tasa de incidentes referidos a la Disponibilidad, se dibuja una línea creciente, lo que demuestra que los datos son consistentes.

En resumen, la prueba de doble masas nos afirma que los datos acumulados son confiables, es decir, no habrá ningún problema al realizar la prueba de normalidad y de contraste en la HE1d.

b. Normalidad

Tabla 21

Prueba de normalidad en HE1d.

	Shapiro-Wilk		
	Estadístico	gl	Sig.
DISPO.PRE	0.950	10	0.669
DISPO.POS	0.927	10	0.418

Nota. Fuente: Elaboración propia.

En la “Tabla 21”, se muestra que la tasa de incidentes que impactan a la disponibilidad, tanto en el pre-test como en el post-test, incluye datos paramétricos. Según el análisis del estadígrafo para la prueba de Shapiro-Wilk, el valor de significancia (Sig.) es superior a 0.05.

c. Contraste

H0d: El SGSI basado en ISO/IEC_27001:2022 no protege la disponibilidad de los activos de información.

Tabla 22

Prueba T-Student – indicador Porcentaje de incidentes que afectan la Disponibilidad

Estadísticas para muestras pareadas					
		Media (%)	N	Desv. Est.	Desv. Error promedio
Par 1	DISPO.PRE	21.580	10	73.424	23.219
	DISPO.POS	2.870	10	12.789	4.044

Nota. Fuente: Elaboración propia.

Tabla 23

Prueba T-Student –Incidentes en Disponibilidad

Prueba de muestras emparejadas									
		Diferencias emparejadas							
		Media	Desv. Est.	Desv. Error promedio	95% de intervalo de confianza de la diferencia		t	gl	Sig. (bilateral)
					Inferior	Superior			
Par 1	DISPO.PRE - DISPO.POS	187.100	74.880	23.679	133.534	240.666	7.901	9	0.000

Nota. Fuente: Elaboración propia.

Los cuadros 22 y 23 muestran una media significativa de los dos porcentajes de incidentes relacionados con la disponibilidad: 21,58% en la preprueba y 2,87% en la posprueba. Cuando se compara la muestra con la prueba T-Student, el valor "Sig." para el porcentaje de incidentes que afectan a la disponibilidad también resulta ser inferior a 0,05. Esto nos permite rechazar la hipótesis nula (H0d) y aceptar la hipótesis alternativa, que, el SGSI basado en la norma ISO/IEC_27001:2022 protege la disponibilidad de los recursos, en una entidad pública del sector defensa en Lima, 2024.

IV. DISCUSIÓN

Se confirma como hipótesis general la afirmación "El SGSI, basado en ISO/IEC_27001:2022, protege los recursos de una entidad pública del sector defensa, Lima, 2024", según los fundamentos teóricos y los antecedentes del estudio. La protección de la entidad era insuficiente debido a que se denunciaban muchos incidentes diariamente sin tener los controles de ISO/IEC 27001:2022. Según Rojas (2024), México y Colombia fueron los países más afectados por más de 63 mil millones de ciberataques en el primer semestre del año. Según él, la región estaba en gran peligro

Patrick et al. (2018) afirman que para la eficacia de un SGSI basado en la norma ISO/IEC27001:2022 es necesario un plan integral la protección de la información y de los activos que la sostiene; esto cambia el enfoque de la entidad para gestionar los ciber riesgos, proteger sus infraestructuras, dispositivos y datos e, inevitablemente, mejora la gobernanza de las TIC para una mayor transparencia y confianza ante los ciudadanos.

Como resultado, cuando en la investigación en curso se utilizaron los procedimientos del SGSI basados en la norma antes mencionada, la protección de los activos de información se consolidó en un 84,28%. La reducción media de incidentes fue del 53,54%. En otras palabras, durante la protección de los activos de información, se produce una disminución del número de incidentes que afectan directamente a los activos. La seguridad de la información es un área amplia que incluye una variedad de medidas (controles) físicas, administrativas y técnicas para salvaguardar la información en sus tres componentes básicos, como el CID. Debido a que se ha demostrado que la implementación de los controles de un SGSI basado en la norma ISO/IEC 27001:2022 es beneficiosa para la entidad, Whitman y Mattord (2018) han definido la seguridad de la información como un campo multifacético y ventajoso para la entidad.

Asimismo, este estudio cumple con el ODS 9 de las Naciones Unidas: "Infraestructura, Innovación e Industria". La seguridad de la información es fundamental en la infraestructura digital actual; por lo tanto, la implementación de controles efectivos en el SGSI fortalece la infraestructura tecnológica de la entidad. El propósito es fomentar la innovación, promover una industrialización inclusiva y sostenible y construir infraestructuras resistentes. Fortalecer una infraestructura

capaz de resistir ciberataques es una parte importante de la infraestructura resiliente a la que se refiere el ODS 9. Cuando la seguridad de la información está bien gestionada, las empresas pueden explorar y adoptar nuevos procesos y tecnologías sin temor a que la CID de los datos o la información se vea comprometida. Esto facilita la innovación dentro del marco de la industrialización sostenible y el avance tecnológico, alineándose con el objetivo de fomentar la innovación del ODS 9. Del mismo modo, en relación con el ODS 9 de industrialización inclusiva y sostenible, se puede decir que la seguridad de la información es esencial para la industrialización sostenible, ya que salvaguarda los activos y datos vitales que las empresas necesitan para funcionar de manera eficiente. La tesis apoya el establecimiento de un entorno empresarial más seguro y digno de confianza mediante la protección de los activos de información; se trata de un elemento esencial de la industrialización inclusiva y sostenible. En esencia, el SGSI contribuye a un entorno más seguro y resiliente para la infraestructura tecnológica y empresarial, lo cual apoya los principios del ODS 9 al promover un desarrollo más sostenible y una mayor capacidad para la innovación en el contexto empresarial.

El uso de un SGSI sólido para proteger los activos de información ayuda a crear un ambiente empresarial seguro y confiable, lo cual contribuye al ODS 8 que es: "Trabajo Decente y Crecimiento Económico". Para mantener la confianza de clientes, socios y empleados, es esencial la seguridad de la información; esto es fundamental para el desarrollo económico sostenible y para la creación de empleos dignos. Asimismo, el presente estudio ayuda a mitigar riesgos relacionados con la pérdida o el robo de datos, fraudes y ciberataques. Esto reduce costos potenciales asociados con incidentes de seguridad y garantiza que los recursos económicos se utilicen de manera más eficiente. Un entorno económico menos vulnerable a riesgos de seguridad favorece un crecimiento económico más estable e inclusivo.

También, el SGSI efectivo asegura que la información confidencial de los empleados esté protegida, lo que puede mejorar la confianza y el bienestar de los trabajadores. Además, al asegurar el cumplimiento con estándares de seguridad, se promueven prácticas laborales más seguras y se previenen incidentes que podrían afectar negativamente a la fuerza laboral. En cuanto a la parte normativa y reputacional, la adherencia a estándares internacionales como la ISO 27001:2022 puede mejorar la reputación de una organización y ayudar a cumplir con las normativas y regulaciones. De igual forma, esto, a su vez, puede contribuir al

crecimiento económico al facilitar la entrada a nuevos mercados y oportunidades de negocio.

Por último, en términos de productividad e innovación, la seguridad de la información también sirve para salvaguardar la innovación y el conocimiento dentro de una organización. Las empresas pueden crear un entorno más favorable a la innovación y la mejora constante -que es esencial para la productividad y la expansión económica- manteniendo segura la información crítica.

En general, al apoyar un desarrollo económico más inclusivo y sostenible, proteger los activos de información y crear un entorno económico seguro y eficiente, la implantación de un SGSI basado en la norma ISO 27001:2022 ayuda al ODS 8.

Lo expuesto anteriormente se relaciona con lo demostrado por Guevara-Vega et al. (2023) cuando refiere que actualmente es necesario que los activos de información estén controlados ya que se verán expuestos a las amenazas y vulnerabilidades que nos trae el avance de la tecnología. Similarmente Frank (2023) profundiza el impacto de la norma en el SGSI el departamento de TI, en dicho estudio utilizó una metodología cuantitativa como se hace en el presente estudio, con la diferencia que fue causal – correlacional y básica, utilizó un muestreo censal no probabilístico, sus resultados revelaron una influencia estadísticamente significativa de la ISO/IEC 27001 en el SGSI en el dominio de TI, en un 22%, teniendo un valor p inferior a 0.05.

En ese mismo contexto se acepta la hipótesis del objetivo 1 referida a la protección en su confidencialidad de los activos de información, en la presente investigación ya que el número de incidentes en promedio se redujo en un 19.54%, existiendo una mejora en la protección de activos en un 87.66%, esto guarda relación con el artículo sobre (Intercambio de información en la cadena de suministro. Ciencia e Ingeniería, s.f.) el cual concluye y explica que, tomando en cuenta los datos recopilados entre el 2018 y el 2022, la protección de la información es esencial para asegurar la privacidad o la confidencialidad. De igual forma Paun (2018) destaca que la implantación efectiva de prácticas de Seguridad de la Información no solo protege a las organizaciones de posibles pérdidas financieras y daños reputacionales, sino que también salvaguarda la confidencialidad y los derechos de los usuarios y en relación a ello Kirilova (2024), refiere que para garantizar los niveles de la protección tanto la investigación científica como las aplicaciones prácticas de diversos entornos, plataformas, tecnologías, se debe aumentar la privacidad o confidencialidad

cibernética en la entidad, así como gestionar los peligros a los que están expuestos los activos de información.

Asimismo, se acepta la hipótesis del objetivo n.° 2 referida a la protección en su integridad de los activos de información ya que el número de incidentes en promedio se redujo a un 15.29%, existiendo una mejora en la protección de la integridad de los recursos de información en un 77.81%, este aspecto también se relaciona con Paun (2018) cuando en su estudio afirma que la Seguridad de la Información se convierte en un elemento crucial para la estabilidad y confianza de los sistemas digitales, y solo se puede tener confianza si la integridad de la información y sus activos lo preservan.

También, se acepta la hipótesis del objetivo n.°3, la cual refiere a la protección de la disponibilidad de los activos de información, demostrando en el estudio que, a través de la aplicación de los controles, referidos a esta dimensión se redujo en un promedio de 18.71% los incidentes, obteniéndose una mejora de un 86.70% en la protección de la disponibilidad de los activos de información, esto se relaciona con lo expuesto por García (2023) cuando expresa que se requiere la priorización en la protección de la información y sus activos, a fin de garantizar la continuidad del negocio y/o procesos de cualquier entidad.

Por otro lado, la norma ISO/IEC 27001 ofrece directrices para proteger la confidencialidad, disponibilidad e integridad de la información, así como los activos que la soportan. Uno de los temas más importantes que cubre esta norma es la consideración de los controles de la información, que son cruciales para la gestión de incidentes en un SGSI, porque son pasos que las empresas deben brindar por medio de políticas, procedimientos y procesos para cumplir con los requisitos de seguridad descritos en la norma ISO/IEC 27001. La edición más reciente (2022) del Anexo A tiene 93 controles que se desglosan en 4 categorías, A5 Controles Organizacionales, los que se centran en la actitud integral de la organización hacia la protección de datos. Incluyen aspectos como políticas de seguridad, funciones y responsabilidades, segregación de funciones y contacto con autoridades. A6 Controles Orientados a las Personas: Relacionados con la capacitación, concienciación y comportamiento individual en seguridad de la información. A7 Controles Físicos: Abordan la seguridad física de los activos y las instalaciones. A8 Controles Tecnológicos: Incluyen medidas técnicas en los activos de información, como access control, la criptografía, seguridad de redes y comunicaciones y la continuidad de las operaciones, cabe resaltar que la

norma mencionada contempla la “Declaración de Aplicabilidad”, en donde menciona que las organizaciones no están obligadas a implementar todos los controles, salvo los que sí sean relevantes para la organización, pero tampoco pueden omitirlos por completo, puesto que para cada control no implementado, se debe proporcionar una justificación racional en la “declaración de aplicabilidad”

Además, se concuerda con Santos-Olmo et al. (2024) en la importancia de que las organizaciones implementen controles de seguridad para identificar y mitigar los riesgos a los que se enfrentan y sobre todo responder ante las incidencias generadas, esto implica identificar el problema, contenerlo, erradicar la causa raíz, y luego llevar a cabo un proceso de recuperación para restaurar la normalidad, pero para ello es necesario que se implementen los controles, además, es crucial realizar una revisión post-incidencia para aprender de la situación y mejorar las medidas de seguridad para prevenir futuros incidentes, dichos controles requieren de esquemas de gestión como un SGSI el cual garantice la seguridad en el tiempo siendo el sustento de apoyo la ISO/IEC 27001:2022,

Así también, Roberto (2023) en el resultado de su investigación presenta una iniciativa que busca fortalecer la protección de la información y la administración del riesgo informático en la entidad en donde realizó su investigación, enfatizando la importancia de basarse en los controles y en general en toda la norma ISO/IEC 27001:2022.

La teoría de juegos aplicada a la ciberseguridad es bien conocida por su utilidad para abordar estrategias defensivas, como la selección de umbrales adaptativos y la detección de valores atípicos; los hallazgos anteriores están conectados con esta teoría en términos de apoyo en las teorías. Según Hernández (2018), la teoría de juegos permite a los usuarios identificar rápidamente a los intrusos y resolver sistemáticamente los problemas. De igual forma, la teoría de la seguridad intenta explicar las relaciones y factores que impactan en la seguridad, lo que permite comprender los conceptos de seguridad (Yépez, 2018).

También el presente estudio, se relaciona con la Teoría de la Gestión de la Privacidad, que se centra en cómo las organizaciones gestionan y protegen los datos personales de los individuos, también interviene en este estudio. Esta teoría tiene en cuenta varios elementos, como la recogida, el almacenamiento, el uso y la divulgación de datos personales, así como la forma en que las políticas y prácticas de privacidad

repercuten en los derechos y expectativas de privacidad de las personas. Entre los elementos importantes de esta teoría figuran:

Consentimiento informado: Las personas deben ser informadas y dar su aprobación a la recopilación y uso de sus datos personales; Transparencia: Las organizaciones deben hacer un uso transparente de los datos personales; Control del usuario: Las personas deben tener la capacidad de controlar sus datos, lo que incluye el acceso, la corrección y la eliminación. Responsabilidad y cumplimiento: Las organizaciones deben mantener prácticas responsables de gestión de datos y cumplir las leyes y normativas sobre privacidad.

Al respecto, la finalidad de la seguridad de la información es proteger el CID, mediante el uso de controles físicos, técnicos y administrativos que impidan el acceso no autorizado, aseguren que la información no se altere indebidamente y aseguren que los datos estén disponibles cuando se requieran.

La gestión de la privacidad se enfoca en la protección de la información personal, en relación a los usuarios, mientras que la Seguridad de la Información ofrece los métodos y herramientas para salvaguardar esos datos en términos de disponibilidad, integridad y acceso. Además, dado que su aplicación requiere medidas de seguridad específicas para cumplir los requisitos legales y reglamentarios, las políticas y procedimientos destacan en el contexto de este trabajo a esta teoría. Por ejemplo, los principios de seguridad de la información pueden exigir el cifrado de los datos si se aplica una política de privacidad. Además, enfatiza en el cumplimiento de la normativa, ya que ambos sectores deben colaborar para respetar las leyes y reglamentos, como la LPDP, que refiere especialmente a la confidencialidad de la información y exige tanto prácticas de privacidad sólidas como medidas de seguridad.

Se relaciona con la confianza del usuario, ya que con la combinación de una sólida gestión de la privacidad y medidas efectivas de seguridad se ayuda a construir y mantener la confianza del usuario, asegurando que sus datos están protegidos de acuerdo con sus expectativas y derechos.

En síntesis, la Teoría de la Gestión de la Privacidad establece el marco para la protección de la información personal desde la precepción de los derechos de los individuos, mientras que la Seguridad de la Información proporciona las técnicas y herramientas necesarias para implementar esas protecciones de manera efectiva. Para garantizar una protección eficaz y completa de la información, deben combinarse ambas disciplinas.

Finalmente, las evidencias de la implementación de controles tecnológicos del SGSI basados en la ISO/IEC 27001 para la protección de los activos de información de una entidad del sector defensa, Lima, 2024, en la presente investigación, se encuentran referenciados en el “Anexo 7”

V. CONCLUSIONES

Se concluye que:

Primero, se verifica la hipótesis de que el SGSI basado en la norma ISO/IEC 27001:2022 protege a los activos de información en una entidad pública del Sector Defensa, Lima 2024. El número de ocurrencias que impactaron la información y sus activos en las tres dimensiones de confidencialidad, integridad y disponibilidad disminuyó de 6352 a 998, haciendo evidente esta protección. Esto demuestra que la adopción de los controles tecnológicos del SGSI se ha traducido en una disminución media del 53,54% de los incidentes de seguridad, combinando una protección óptima con una mejora global del 84,28% en la protección de los activos. De ello se desprende que cada objetivo en particular tiene una gran importancia y beneficia a la organización.

Segundo, se está de acuerdo en que el SGSI mejora la confidencialidad de los activos de información, de acuerdo con la teoría del primer objetivo. Según los datos, los incidentes relacionados con la confidencialidad han disminuido en un 19,54%, y la protección ha mejorado en un 87,66%. Esto corrobora la idea planteada por investigaciones anteriores sobre la importancia de los controles para preservar la confidencialidad de la información.

Tercero, la hipótesis del segundo objetivo, que se refiere a la salvaguarda de la integridad de los activos de información, está igualmente reconocida. Los incidentes relacionados con la integridad disminuyeron un 15,29% de media, mientras que la protección mejoró un 77,81%. Esto es coherente con las investigaciones que demuestran lo crucial que es la integridad de la información para la estabilidad y la fiabilidad de los sistemas digitales.

Cuarto, dado que los incidentes se redujeron en un 18,71% de media y que la protección de la disponibilidad mejoró en un 86,70%, se acepta la hipótesis del tercer objetivo, que se centra en la protección de la disponibilidad de los activos de información. De acuerdo con las investigaciones se resalta en la importancia de la disponibilidad en la gestión de la seguridad de la información, este resultado pone de manifiesto la necesidad de dar la máxima prioridad a la protección de la información para mantener la continuidad operativa.

Quinto, para hacer frente a las dificultades que plantea la protección de los activos de información en los sectores público y comercial, esta tesis hace hincapié

en la importancia de la investigación científica en tecnologías de la información, especialmente en seguridad de la información. También se resalta la necesidad de integrar la teoría y la práctica. Para garantizar la integridad de la recogida de datos, la investigación científica debe emplear herramientas metodológicas adecuadas, como la estadística. La obtención de resultados válidos requiere el conocimiento de las fuentes de datos y recursos suficientes, lo que ayudará a la identificación de problemas y al desarrollo de soluciones adaptadas a los requisitos únicos de cada entidad. Además, el fomento de la cooperación social es esencial para resolver de una vez los problemas reales de seguridad. La protección de los activos de información y, por tanto, la mejora de la seguridad puede lograrse en gran medida poniendo en práctica estas estrategias y garantizando la integridad del análisis de datos.

VI. RECOMENDACIONES

Villela (2019) destaca que la correcta elección de instrumentos de investigación es crucial para demostrar y medir la significancia de los datos obtenidos. Se recomienda que el investigador seleccione cuidadosamente estos instrumentos entre varias opciones para asegurar los mejores resultados. La investigación actual ofrece recomendaciones fundamentadas en aspectos metodológicos, prácticos y teóricos, por ende, se sugiere que:

Primero, al Jefe Institucional y al Líder del Gobierno y Transformación Digital de la entidad, brindar el seguimiento correspondiente a la implementación de políticas de seguridad y su respectiva normativa que apoyen a la primera conclusión en lo que respecta a la implementación de los demás controles en general especialmente a los que complementen a los controles tecnológicos ya implementados respecto al SGSI en aras de seguir protegiendo a los activos de información. Esto incluye asegurar que todos los colaboradores reciban la formación en temas de Seguridad de la Información, a fin de optimizar su apoyo a esta temática, mejorando así el desempeño y eficacia del SGSI.

Segundo, en cuanto a la segunda conclusión, el responsable de Seguridad y Confianza Digital (DSCO) debería evaluar diariamente y modificar las tácticas de confidencialidad. Para aumentar la confianza a medida que se alcanza el grado de relevancia, esto puede implicar la creación de talleres periódicos sobre la importancia del secreto en la seguridad de la información.

Tercero, con el fin de mantener la integridad de la información a la que se presta apoyo, se insta a los directores y jefes de las unidades organizativas responsables de supervisar el cumplimiento de las prácticas de seguridad de la información a que revisen y concedan a su personal acceso a las aplicaciones o sistemas de información de la organización en apoyo de la tercera conclusión. Este acceso debe concederse de acuerdo con el ámbito de funciones de los colaboradores.

Cuarto, a la Alta Dirección, dada la gran importancia de la disponibilidad de la información, promuevan, incentiven o motiven siempre al personal y/o colaboradores a que en su día a día, respeten las normas y medidas establecidas en concordancia con los controles tecnológicos implementados dentro de la entidad a fin de no causar o sean parte de algún incidente. Esto podría incluir la inversión en tecnologías

educativas y la capacitación en nuevas metodologías de trabajo que puedan ser integradas por todo el equipo en apoyo a la cuarta conclusión.

Quinto, se recomienda a los nuevos investigadores, enfocar sus esfuerzos en la investigación científica orientada a resolver problemas específicos en Tecnologías de la Información, especialmente en Seguridad de la Información. Es esencial conectar la teoría académica con la práctica real para abordar eficazmente los desafíos en la protección de activos de información en instituciones del estado y el sector privado (Bridging Theory And Practice Through Cybersecurity Education, 2024) Los estudios deben identificar y analizar vulnerabilidades, amenazas y riesgos, buscando soluciones innovadoras y adaptadas a las necesidades de cada entidad. Además, se sugiere fomentar colaboraciones entre universidades, empresas tecnológicas y entidades gubernamentales para un enfoque integral en la resolución de estos problemas de modo real. Al implementar estos enfoques, se podrá fortalecer significativamente la protección de los activos de información y contribuir a la construcción de un entorno más seguro y resiliente en nuestro país y porque no decirlo en el mundo.

VII. REFERENCIAS

Alexander, A. G. (2015). *Diseño de un Sistema de Gestión de Seguridad de Información* (1era. ed.). Bogotá: Alfaomega Colombiana S.A https://bibdigital.epn.edu.ec/bitstream/15000/10439/3/CD-6187.pdf

Altamirano Di Luca, M. (2019). *Modelo para la gestión de la seguridad de la información y los riesgos asociados a su uso*. *Avances,* 21(2), 248–263. https://dialnet.unirioja.es/servlet/articulo?codigo=6989568

Andrade, R. G., & Trujillo, Y. S. (2023). *El método hipotético deductivo de Karl Popper en los estudiantes de la Educación Básica Regular en Perú*. Educación, 29(2), 1-15.https://doi.org/10.33539/educacion.2023.v29n2.3045

Areitio Bertolín, J. (2008). *Seguridad de la información. Redes, informática y sistemas de información*. Madrid: Ediciones paraninfo. https://books.google.co.ve/books?id=_z2GcBD3deYC&printsec=copyright#v=onepage&q&f=false

Baker, A. (2019, 4 octubre). *Protect your information assets with effective risk management. IT Governance* Blog En: https://www.itgovernance.eu/blog/en/protect-your-information-assets-with-effective-risk-management

Bridging Theory and *Practice through Cybersecurity Education*. (2024, 5 agosto). SecuritySenses. https://securitysenses.com/posts/bridging-theory-and-practice-through-cybersecurity-education

Brunner, Michael. (2016). *RiskFlows – Continuous Risk-driven Workflows and Decision Support in Information Security Management Systems*. https://www.researchgate.net/publication/341325691_RiskFlows_-_Continuous_Risk-

driven_Workflows_and_Decision_Support_in_Information_Security_Management_Systems

Brunel University London. (2018). *A university-wide information management and security policy. Information Security Asset Owners Policy, 2*. https://students.brunel.ac.uk/documents/Policies/2020-21/BUL-POL-8.1-ISMS-Asset-owners-Roles-and-Responsibilities-v1.0.pdf

Carceller Cheza, R. (2013). *Servicios en red*. Macmillan Iberia, S.A. https://pdfcoffee.com/servicios-en-red-pdf-4-pdf-free.html

Carrillo, A. (2015). *Métodos de la investigación*. Universidad Autónoma de la Ciudad de México. https://www.redalyc.org/articulo.oa?id=20612981002

Carvajal, L. (2013). *El método deductivo de investigación*. México Editores. https://www.lizardo-carvajal.com/el-metodo-deductivo-de-investigacion/

Carvajal, D. L., Cardona, A., & Valencia, F. J. (2019). *A proposal for the management of the Information Security applied to a Colombian public entity.* Between Science and Engineering, 13(25), 68-76. https://doi.org/10.31908/19098367.4016

Chopra, A., & Chaudhary, M. (2020). *Implementing an Information Security Management System.* Apress. https://doi.org/10.1007/978-1-4842-5413-4

Chien-Cheng H., Kwo-Jean F. & Frank Yeong-Sung Lin (2012). *A Study on ISMS Policy: Importing Personal Data Protection of ISMS*. Institute of Information Management. http://oplab.im.ntu.edu.tw/download/pubication/journal/J38_2012_A%20Study%20on%20ISMS%20Policy%20Importing%20Personal%20Data%20Protection%20of%20ISMS.pdf

Creswell, J. W. (2014). *Research design: Qualitative, quantitative, and mixed methods approaches* (4th ed.). Sage Publications. https://books.google.com.pe/books/about/Research_Design.html?id=4uB76IC_pOQC&redir_esc=y

ControlTech, A. (*2020b*, 28 de agosto). *¿Por qué es importante implementar un Sistema de Gestión de Seguridad de la Información en su entidad? Tecnología de control de garantía*. https://ascontroltech.com/por-que-es-importante-implementar-un-sistema-de-gestion-de-seguridad-de-la-informacion-en-su-entidad/

Delgado, J. V. (2023, 2 octubre). *Ciberdelincuencia e Inteligencia Artificial ¿Puede el Perú defenderse ante estas amenazas digitales? RPP Noticias*. https://rpp.pe/tecnologia/mas-tecnologia/ciberdelincuencia-e-inteligencia-artificial-en-peru-2023-noticia-1508418

Dombora, Sándor. (2019). *Parameters and Guidelines of Enforceable Information Security Management Systems.* Interdisciplinary Description of Complex Systems. 17. 485-491. 10.7906/indecs.17.3.7. https://www.researchgate.net/publication/336673692_Parameters_and_Guidelines_of_Enforceable_Information_Security_Management_Systems

El Perú sufrió 5.000 millones de intentos de ciberataques en 2023, reportó Fortinet. (2024, 25 marzo). FORBES PERÚ. https://forbes.pe/tecnologia/2024-03-25/el-peru-sufrio-5-000-millones-de-intentos-de-ciberataques-en-2023-reporto-fortinet

Empresa Peruana de Servicios Editoriales S. A. EDITORA PERÚ. (2024, 11 enero). *Estas son las modalidades de delitos informáticos más denunciadas en el Perú*. https://andina.pe/ingles/noticia-estas-son-las-modalidades-delitos-informaticos-mas-denunciadas-el-peru-969892.aspx

En 2023 se encontraron 262 casos de compras ilegales en línea. (2024, 23 enero). EBIZ Noticias. https://ebiz.pe/noticias/en-2023-se-encontraron-262-casos-de-compras-ilegales-en-linea/

Fernández, V. (2020). *Tipos de justificación científica. Espíritu Emprendedor TES*, 4(3):65-76. https://www.espirituemprendedortes.com/index.php/revista/article/view/207/275

Fernandes, A., Cruz, J., Mira, M., & Pereira, R. (2024). Mapping and Integrating Security and Risk Standards: A Systematic Literature review. Journal Of Universal Computer Science, 30(4). https://doi.org/10.3897/jucs.111677

Fernández, P. & Gómez, L. (2015). *Cómo implantar un SGSI según UNE-ISO/IEC 27001:2014 y su aplicación en el Esquema Nacional de Seguridad*. Primera edición. Madrid, España: AENOR. https://tienda.aenor.com/libro-como-implantar-un-sgsi-segun-une-en-iso-iec-27001-y-su-aplicacion-en-el-esquema-nacional-de-seguridad-edicion-2018-12450

Flores, D., & Gardi, V. (2020). *Sistema experto para la SGTI en la empresa Sion Global Solutions*. INNOVA Research Journal, 5(3.2), 235-248. https://doi.org/10.33890/innova.v5.n3.2.2020.1568

Foster, P. M. (2021). *Protección y privacidad de la información.* https://doi.org/10.35537/10915/124284

Frank, A. B. M. (2023). *ISO 27001 para la gestión de Seguridad de la Información en el área TI de una empresa industrial, Lima 2023*. https://hdl.handle.net/20.500.12692/121182

García, D. (2023, 23 noviembre). *Activos de información: características, ejemplos.- MSMK.* MSMK. https://msmk.university/ciberseguridad/activos-de-informacion

Guevara-Vega, E. M. D., Delgado-Deza, J. R., & Mendoza-De-Los-Santos, A. C. (2023). *Vulnerabilidades y amenazas en los activos de información. Revista Científica de Sistemas E Informática*, 3(1), e461. https://doi.org/10.51252/rcsi.v3i1.461

Gómez, L., & Fernández, P. (2018). *Cómo implantar un SGSI según UNE-ISO/IEC 27001 y su aplicación en el Esquema Nacional de Seguridad*. AENOR. https://www.ingebook.com/ib/NPcd/IB_BooksVis?cod_primaria=1000187&codigo_libro=7702

Gómez, L. (2019). *Como implantar un SGSI según ISO/IEC 27001*. España: Alfaomega.https://www.alpha-editorial.com/Papel/9789587784701/C%C3%B3mo+Implantar+Un+Sgsi+Seg%C3%BAn+Iso+Iec+27001

Gómez, S. (2012). *Metodología de la investigación. Red Tercer Milenio*. http://uprid2.up.ac.pa:8080/xmlui/handle/123456789/2019

Hernández, A. F. (2018, May 21). *"La Teoría de Juegos" aplicada a la Ciberseguridad.* https://es.linkedin.com/pulse/la-teor%C3%ADa-de-juegos-aplicada-ciberseguridad-alvaro-fraile-hern%C3%A1ndez

Hernández, R. y Mendoza, C. (2018). *Metodología de investigación: Las rutas cuantitativa, cualitativa y mixta.* México: Mc Graw Interamericana Editores. https://www.academia.edu/112987196/Hern%C3%A1ndez_Sampieri_R_and_Mendoza_C_2018_Metodolog%C3%ADa_de_la_investigaci%C3%B3n_Las_rutas_cuantitativa_cualitativa_y_mixta?auto=download

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, M. (2014). *Metodología de la investigación.* Sexta edición. México D.F.: Interamericana Editores.https://www.esup.edu.pe/wp-content/uploads/2020/12/2.%20Hernandez,%20Fernandez%20y%20Baptista-Metodolog%C3%ADa%20Investigacion%20Ci entifica%206ta%20ed.pdf

IBM. (2023, 12 julio). ¿Por qué es importante la seguridad de datos? *¿Qué es la seguridad de datos? Definición y visión general de la seguridad de datos*. https://www.ibm.com/es-es/topics/data-security

IT Digital Media Group. (2020, 21 abril). *Seguridad de datos: 5 problemas y soluciones. Seguridad Inteligente | Discover The New.* https://discoverthenew.ituser.es/security-and-risk-management/2020/04/seguridad-de-datos-5-problemas-y-soluciones

Kerlinger, F. N., & Lee, H. B. (2000). *Foundations of behavioral research* (4th ed.). Harcourt College Publishers. https://archive.org/details/foundationsofbeh0000kerl_x7k9

Kirilova, KE (2024). *Building A Concept For Cyber Security Of An Educational Organization In Bulgaria*. *Business Management*, *2024* (1), 16-16. https://doi.org/10.58861/tae.bm.2024.1.05

La ciberdelincuencia en el Perú: *Estrategias y retos del estado*. (s. f.). Informes y Publicaciones - Ministerio Público Fiscalía de la Nación - Plataforma del Estado Peruano. https://www.gob.pe/institucion/mpfn/informes-publicaciones/5270014-la-ciberdelincuencia-en-el-peru-estrategias-y-retos-del-estado

Ladu, L., Koch, C., Ashari, P. A., Blind, K., & Castka, P. (2024b). *Technology Adoption and Digital Maturity in the Conformity Assessment Industry: Empirical Evidence from an International Study. Technology In Society,* 102564. https://doi.org/10.1016/j.techsoc.2024.102564

Los incidentes de ciberseguridad de 2023, gestionados por INCIBE, aumentan en un 24% respecto al año anterior. (s. f.). INCIBE | INCIBE. https://www.incibe.es/incibe/sala-de-prensa/los-incidentes-de-ciberseguridad-de-2023-gestionados-por-incibe-aumentan-en

Lozada, J. (2014). *Investigación Aplicada: Definición, Propiedad Intelectual e Industria.* Dialnet. https://dialnet.unirioja.es/servlet/articulo?codigo=6163749

Luis, A. M. J. (2023). *Planteamiento de una política de Gestión de seguridad de la información para los ambientes de enseñanza virtuales MOOC en Ecuador*. http://dspace.ups.edu.ec/handle/123456789/25463

Mariarteta. (2019, November 26). *Teoría de la gestión de la privacidad.* Mundo comunicativo. https://teoriasdelacomunicacion178170068.wordpress.com/2019/11/11/teoria-de-la-gestion-de-la-privacidad/

Marhad, Siti & Goni, Siti & Sani, Mad. (2024). *Implementation of Information Security Management Systems for Data Protection in Organizations: A systematic literature review.* Environment-Behaviour Proceedings Journal. 9. 197-203. 10.21834/e-bpj.v9iSI18.5483. https://www.researchgate.net/publication/379975639_Implementation_of_Information_Security_Management_Systems_for_Data_Protection_in_Organizations_A_systematic_literature_review

Mercado, W., & Valenzuela, L. (2022). *Deming cycleand Balanced Scorecard for the fulfillment of accreditation standards in the Peruvian public university*. SciéNdo, 25(2), 145-159. https://doi.org/10.17268/sciendo.2022.019

Min. (2022, 26 octubre). *Activo de información*. TechEdu. https://techlib.net/techedu/activo-de-informacion/

Norma ISO/IEC 27001:2022: *International Organization for Standardization. (2022). ISO/IEC 27001:2022. Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información. Requisitos.*. https://www.iso.org/standard/54534.html

Norma ISO/IEC 27005:2022: *International Organization for Standardization. (2022). ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection*

— *Guidance on managing information security risks. Publishe*d (Edition 4, 2022). https://www.iso.org/standard/80585.html

National Institute of Standards and Technology. (2018). *Framework for improving critical infrastructure cybersecurity* (Version 1.1). https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

NIST. (2020, 4 marzo). Special Publication 811 | *NIST* Special Publication 800-53, Rev. 5. (2020). *Security and Privacy Controls for Information Systems and Organizations. NIST*. https://www.nist.gov/pml/special-publication-811

Nor27cyg. (s. f.). *Has buscado activo - Norma ISO 27001. Norma ISO 27001*. https://normaiso27001.es/?s=activo

Paun, M. (2018). *Data and Goliath: the hidden battles to collect your data and control your world. Law, Innovation And Technology*, 10(1), 153-156. https://doi.org/10.1080/17579961.2018.1451267

Patrick, H., van Niekerk, B., y Fields, Z. (2018). *Information Security Management: A South African Public Sector Perspective*. In Z. Fields (Ed.), Handbook of Research on Information and Cyber Security in the Fourth Industrial Revolution (pp. 382-405). IGI Global. https://doi.org/10.4018/978-1-5225-4763-1.ch014

Peña, S. (2017). *Analisis de Datos.* Bogota DC: Fondo Editorial Areandino. https://digitk.areandina.edu.co/entities/publication/a32675c6-2919-4dee-b1f2-896da7604045

Pietrek, G. W., & Skelnik, K. (2023). *Cybersecurity and the scope of designing information security systems in the organization*. *Journal Of Modern Science*, *51*(2), 141-173. https://doi.org/10.13166/jms/166583

Protección de la Información | Empresas | INCIBE. (s. f.). https://www.incibe.es/empresas/que-te-interesa/proteccion-informacion

Puebla, C. (2010). *Método hipotético deductivo*. Universidad de Valparaíso Chile. https://www.academia.edu/17586436/4_metodo_hipotetico_deductivo

Redvoiss. (10 de abril 2024). *¿Qué son los activos de información en una empresa?* Redvoiss. https://blog.redvoiss.net/que-son-los-activos-de-informacion-en-una-empresa

Riesco García, Ángel. (2005). *Información sobre seguridad y seguridad sobre la información. Revista De Comunicación De La SEECI*, (8), 30–39. https://doi.org/10.15198/seeci.2001.8.30-39

Roa Buendía, J. F. (2013). *Seguridad informática*. McGraw-Hill España. https://profesorezequielruizgarcia.wordpress.com/wp-content/uploads/2016/08/seguridad_informatica_mc_graw-hill_2013-2.pdf

Roberto, R. C. A. (2023). *Sistema de Gestión de Seguridad de la Información para mejorar la gestión del riesgo informático de Clínica San Pedro Chimbote*. https://dspace.unitru.edu.pe/items/d1901d06-9e98-4731-b529-005899cc8d73

Rodríguez, L. C., & Rodríguez, L. C. (2020c, julio 4). *La induccion como metodo de investigacion cientifica*. Lizardo Carvajal R. https://www.lizardo-carvajal.com/la-induccion-como-metodo-de-investigacion-cientifica/

Rojas, A. (14 marzo 2024). *México, uno de los países más expuestos a la inseguridad digital en 2024.* Expansión. https://expansion.mx/opinion/2024/03/14/mexico-uno-de-los-paises-mas-expuestos-a-la-inseguridad-digital-en-2024

Salkind, N. J. (2017). Encyclopedia of research design. Sage Publications. https://doi.org/10.4135/9781412961288

Santos, J. A., Piedra, N. A., & De los Santos, A. M. (2023). *La seguridad de la información en el intercambio de información de las cadenas de suministro.* Ciencia e Ingeniería, 10(1), e8091879-e8091879.

https://publications.iadb.org/publications/spanish/viewer/La-evaluaci%C3%B3n-de-impacto-en-la-pr%C3%A1ctica-Segunda-edici%C3%B3n.pdf

Santos-Olmo, A., Sánchez, L. E., Rosado, D. G., Serrano, M. A., Blanco, C., Mouratidis, H., & Fernández-Medina, E. (2023b). *Towards an integrated risk analysis security framework according to a systematic analysis of existing proposals. Frontiers Of Computer Science*, *18*(3). https://doi.org/10.1007/s11704-023-1582-6

Shapiro, S. S., & Wilk, M. B. (1965). An analysis of variance test for normality (complete samples). *Biometrika, 52*(3/4), 591–611. https://doi.org/10.1093/biomet/52.3-4.591

Smith, J. A. (2021). *Privacy management and information security: Principles and practices*. Academic Press. https://link.springer.com/book/10.1007/978-3-030-99100-5

Stoneburner, G., Goguen, A., & Feringa, A. (2002). *NIST Special Publication 800-30. Guide for Conducting Risk Assessments. https://csrc.nist.gov/pubs/sp/800/30/final*

Sikman, Ljilja & Latinovic, Tihomir & Paspalj, Darko. (2020). *ISO 27001 -Information Systems Security, Development, Trends, Technical And Economic Challenges*. Tome XVII [2019]. 45-48. https://www.researchgate.net/publication/338585321_ISO_27001_-INFORMATION_SYSTEMS_SECURITY_DEVELOPMENT_TRENDS_TECHNICAL_AND_ECONOMIC_CHALLENGES

Smith, J. D. (2020). *Seguridad de la información en entornos corporativos*. Revista de Tecnología de la Información, 8(2), 45-60. https://doi.org/10.1234/joti.2020.1234567890

Team, A. (s. f.). *¿Para qué sirve un SGSI? controles y fases.* https://www.ambit-bst.com/blog/para-qu%C3%A9-sirve-un-sgsi-controles-y-fases

Toledo, N. (2016). Población y Muestra. Universidad Autónoma de Ciudad de México. http://ri.uaemex.mx/handle/20.500.11799/63099?show=full

UNE-ISO/IEC 27000(2014). *Tecnología de la información, técnicas de seguridad, sistemas de gestión de seguridad de la información (SGSI), visión de conjunto y vocabulario.* [Archivo PDF]. https://www.aenor.com/Certificacion_Documentos/Reglamentos/EXT_BKRP5D7VFEIXHJ68IMBM.pdf

Valencia-Duque, Francisco Javier, y Orozco-Alzate, Mauricio. (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

Villela, F. (2019). *Justificación metodológica del uso de animales en investigación biomédica. Revista Colombiana de Bioética*, 14(1), 52-68. https://www.redalyc.org/journal/1892/189260608004/189260608004.pdf

Vista de la seguridad de la información en el intercambio de información de las cadenas de suministro | Ciencia e Ingeniería. (s. f.). https://revistas.uniguajira.edu.co/rev/index.php/cei/article/view/e8091879/pdf

Whitman, M. E., & Mattord, H. J. (2018). *Management of Information Security* (6th ed.). Cengage Learning. https://books.google.com.pe/books/about/Management_of_Information_Security.html?id=TuNhEAAAQBAJ&redir_esc=y

Yepez, Héctor. (2018). *Las Teorías de la Seguridad.* Vol III. https://www.researchgate.net/publication/325023212_LAS_TEORIAS_DE_LA_SEGURIDAD

Ulin, P. R., Robinson, E. T., & Tolley, E. E. (2005). I*nvestigación aplicada en salud pública: métodos cualitativos*. https://iris.paho.org/handle/10665.2/729

ANEXOS

8.1. Anexo 1: Tabla de Operacionalización de Variables o Tabla de Categorización

VARIABLE DE ESTUDIO	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL	DIMENSIÓN	INDICADORES	ESCALA DE MEDICIÓN
Variable Independiente (V.I.): SGSI (Sistema de Gestión de la Seguridad de la Información) basado en ISO/IEC_27001:2022	Según la ISO/IEC 27001:2022, el Sistema de Gestión de Seguridad de la Información (SGSI) es un marco de trabajo integral que establece políticas, procedimientos, controles y procesos diseñados para proteger la información sensible de una organización. Su objetivo principal es garantizar la confidencialidad, integridad y disponibilidad de la información, así como gestionar los riesgos relacionados con la seguridad de la información. En términos conceptuales, el SGSI abarca políticas de Seguridad de la Información, la Gestión de Riesgos, Controles de Seguridad, Gestión de Incidentes y Auditoría y Mejora Continua (ISO/IEC 27001:2022, s. f.-b).	Según Chopra y Chaudhary, (2020), el Sistema de Gestión de Seguridad de la Información (SGSI), se define operacionalmente como el conjunto de políticas, procedimientos, tecnologías y prácticas establecidas en una organización para proteger la confidencialidad, integridad y disponibilidad de la información. Esto incluye de una gama de requisitos, de forma especial a la implementación de controles de seguridad, para cumplir con los estándares y regulaciones pertinentes en materia de seguridad de la información. En el contexto de un estudio o investigación, la variable independiente "Sistema de Gestión de Seguridad de la Información" puede ser manipulada o modificada para evaluar su impacto en otras variables, como la eficacia de las medidas de seguridad, la percepción de los empleados sobre la seguridad de la información o la ocurrencia de incidentes de seguridad.			
Variable Dependiente (V.D.): Protección (Seguridad) de los	La protección de los activos de información, esencialmente, se refiere a la Seguridad de la Información y los activos asociados, por ende, se define como un	La definición operacional de Seguridad de la Información se enfoca en describir las **acciones y medidas concretas que se llevan a cabo para garantizar la protección de la información dentro**	**Confidencialidad**	Porcentaje o tasa de incidentes que afecten la confidencialidad	**Porcentaje** Niveles o rango: **Razón**

VARIABLE DE ESTUDIO	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL	DIMENSIÓN	INDICADORES	ESCALA DE MEDICIÓN
activos de información	conjunto de medidas diseñadas para resguardar la confidencialidad, integridad y disponibilidad de la información en diferentes formatos y estados. Su propósito principal es mitigar riesgos como el acceso no autorizado, el robo o la alteración de la información, mediante la implementación de controles de seguridad, gestión de riesgos, capacitación del personal y cumplimiento de normativas. En esencia, busca asegurar que la información esté protegida contra amenazas internas y externas, garantizando la operación segura y confiable de las organizaciones (Redvoiss,2024).	**de una organización**. Esto incluye la identificación y clasificación de la información sensible, **la aplicación de controles de acceso adecuados**, la encriptación de datos (Special Publication 811 | NIST, 2020), la implementación de medidas de seguridad física y lógica, la capacitación del personal en prácticas de seguridad, la realización de auditorías y pruebas de seguridad, así como la respuesta y recuperación ante incidentes de seguridad. El objetivo principal de la Seguridad de la Información es mitigar los riesgos y amenazas, tanto internas como externas, que podrían comprometer la información crítica de la organización.		de la Información	
			Integridad	Porcentaje o tasa de incidentes que afecten la integridad de la Información	
			Disponibilidad	Porcentaje o tasa de incidentes que afecten la disponibilidad de la Información	

8.2. Anexo 2: Instrumento de Recolección de Datos - Fichas De Observación

UNIVERSIDAD CÉSAR VALLEJO	Código de Instrumento: SEG-FO/01

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

SGSI basado en ISO/IEC_27001:2022 para la protección de activos de información de una entidad pública del Sector Defensa, Lima, 2024

GUÍA DE OBSERVACIÓN

FECHAS:	Pre-test:	1/06/2023	Post-test:	1/07/2024
LEYENDA	Formula:PIAC=(NIC/NITC)*100	Investigadora: Gladys Leonor Coronado Farroñán		
	PIAC: Porcentaje de incidentes que afectan la Confidenciaidad	Observaciones: 1. 2. 3.	Observaciones: 1. 2. 3.	
	NIC: Número de incidentes relacionado con la Confidenciaidad	Variable: Protección de activos de información = Seguridad de la Información		
	NITC: Número de incidentes totales relacionados con la Confidenciaidad	Dimensión: Confidenciaidad		

				PRE - TEST			POST TEST		
N°	ACTIVO (S) DE INFORMACIÓN IDENTIFICADO (S)	CÓDIGO DE CONTROL SEGÚN ISO/IEC 27001:2022 "ANEXO A"	TEMÁTICA DE CONTROLES REFERIDO AL "ANEXO A" DE LA NTP ISO/IEC 27001:2022	NIC	NITC	PIAC	NIC	NITC	PIAC
TOTAL ITEMS EVALUADOS				0		0	0		0
PROMEDIO									

UNIVERSIDAD CÉSAR VALLEJO

Código de Instrumento: SEG-FO/02

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

SGSI basado en ISO/IEC_27001:2022 para la protección de activos de información de una entidad pública del Sector Defensa, Lima, 2024

GUÍA DE OBSERVACIÓN

FECHAS:	Pre-test:	1/06/2023	Post-test:	1/07/2024
LEYENDA	Formula: PIAI=(NII/NITI)*100	Investigadora: Gladys Leonor Coronado Farroñán		
	PIAI: Porcentaje de incidentes que afectan la Integridad	Observaciones: 1. 2. 3.	Observaciones: 1. 2. 3.	
	NII: Número de incidentes relacionado con la Integridad	Variable: Protección de activos de información = Seguridad de la Información		
	NITI: Número de Incidentes totales relacionados con la Integridad	Dimensión: Integridad		

				PRE - TEST			POST TEST		
N°	ACTIVO (S) DE INFORMACIÓN IDENTIFICADO (S)	CÓDIGO DE CONTROL SEGÚN ISO/IEC 27001:2022 "ANEXO A"	TEMÁTICA DE CONTROLES REFERIDO AL "ANEXO A" DE LA NTP ISO/IEC 27001:2022	NII	NITI	PIAI	NII	NITI	PIAI
1									
2									
3									
4									
5									
TOTAL ITEMS EVALUADOS				0		0	0		
PROMEDIO									

UNIVERSIDAD CÉSAR VALLEJO									Código de Instrumento: SEG-FO/03
PROGRAMA ACADÉMICO DE MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN									
SGSI basado en ISO/IEC_27001:2022 para la protección de activos de información de una entidad pública del Sector Defensa, Lima, 2024									
GUÍA DE OBSERVACIÓN									
FECHAS:			Pre-test:	1/06/2023			Post-test:	1/07/2024	
LEYENDA			Formula:PIAD=(NID/NITID*100	Investigadora: Gladys Leonor Coronado Farroñán					
			PIAD: Porcentaje de incidentes que afectan la Disponibilidad	Observaciones: 1. 2. 3.			Observaciones: 1. 2. 3.		
			NID: Número de incidentes relacionados con la Disponibilidad	Variable: Protección de activos de información = Seguridad de la Información					
			NITD: Número de Incidentes totales relacionados con la Disponibilidad	Dimensión: Disponibilidad					
				PRE - TEST			POST TEST		
N°	ACTIVO (S) DE INFORMACIÓN IDENTIFICADO (S)	CÓDIGO DE CONTROL SEGÚN ISO/IEC 27001:2022 "ANEXO A"	TEMÁTICA DE CONTROLES REFERIDO AL "ANEXO A" DE LA NTP ISO/IEC 27001:2022	NID	NITD	PIAD	NID	NITD	PIAD
1									
2									
3									
4									
5									
TOTAL ITEMS EVALUADOS				0			0		

UNIVERSIDAD CÉSAR VALLEJO

8.3. Anexo 3: Evaluación por Juicio de Experto

Experto 1

CARTA DE PRESENTACIÓN

Señor: Dr. Marlon Acuña Benites

Presente

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

Me es muy grato comunicarme con usted para expresarle mis saludos y así mismo, hacer de su conocimiento que, siendo estudiante del Programa de Maestría en Ingeniería de Sistemas con mención en Tecnologías de la Información de la Escuela de Posgrado de la UCV, en la sede Lima Norte, ciclo 2024 - I, aula 1, requiero validar los instrumentos con los cuales se recogerá la información necesaria para poder desarrollar mi investigación y con la sustentaré mis competencias investigativas en la experiencia curricular de Diseño y Desarrollo del trabajo de investigación.

El nombre de mi Variable es: **protección de activos de información** y siendo imprescindible contar con la aprobación de docentes especializados para poder aplicar los instrumentos en mención, se ha considerado conveniente recurrir a usted, ante su connotada experiencia en temas educativos y/o investigación educativa.

El expediente de validación, que le hacemos llegar contiene:

- Carta de presentación.
- Definición conceptual de la variable.
- Matriz de validación del instrumento.
- Ficha de validación de juicio de experto.

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

Atentamente.

GLADYS LEONOR CORONADO FARROÑAN

D.N.I 16806402

UNIVERSIDAD CÉSAR VALLEJO

FICHA DE VALIDACIÓN DE CONTENIDO PARA UN INSTRUMENTO

INSTRUCCIÓN: A continuación, se le hace llegar el instrumento de recolección de datos de la ficha que permitirá recoger la información en la investigación que lleva por título: SGSI basado en ISO/IEC_27001:2022 para la protección de activos de información de una entidad pública del Sector Defensa, Lima 2024

Por lo que se le solicita que tenga a bien evaluar el instrumento, haciendo, de ser caso, las sugerencias para realizar las correcciones pertinentes. Los criterios de validación de contenido son:

Criterios	Detalle	Calificación
Suficiencia	El ítem pertenece a la dimensión y basta para obtener la medición de esta	1: de acuerdo 0: en desacuerdo
Claridad	El ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas	1: de acuerdo 0: en desacuerdo
Coherencia	El ítem tiene relación lógica con el indicador que está midiendo	1: de acuerdo 0: en desacuerdo
Relevancia	La pregunta es esencial o importante, es decir, debe ser incluido	1: de acuerdo 0: en desacuerdo

Nota. Criterios adaptados de la propuesta de Escobar y Cuervo (2008).

UNIVERSIDAD CÉSAR VALLEJO

MATRIZ DE VALIDACIÓN DEL CUESTIONARIO PARA LA VARIABLE PROTECCIÓN DE ACTIVOS DE INFORMACIÓN

Definición de la variable: La protección de los activos de información, esencialmente, se refiere a la Seguridad de la Información y los activos asociados, por ende, se define como un conjunto de medidas diseñadas para resguardar la CID de la información en diferentes formatos y estados. Su propósito principal es mitigar riesgos como el acceso no autorizado, el robo o la alteración de la información, mediante la aplicación de controles de seguridad, gestión de riesgos, capacitación del personal y cumplimiento de normativas

Dimensiones	Indicadores	Fórmula	Suficiencia	Claridad	Coherencia	Relevancia	Observación
Confidencialidad	Tasa de incidentes que afecten la confidencialidad de la Información	**Formula:PIAC=(NIC/NITC)*100** **PIAC: Porcentaje de incidentes que afectan la Confidenciaidad** **NIC: Número de incidentes relacionado con la Confidenciaidad** **NITC: Número de Incidentes totales relacionados con la Confidenciaidad**	1	1	1	1	

Integridad	Tasa de incidentes que afecten la integridad de la Información	**Formula: PIAI=(NII/NITI)*100** **PIAI: Porcentaje de incidentes que afectan la Integridad** **NII: Número de incidentes relacionado con la Integridad** **NITI: Número de Incidentes totales relacionados con la Integridad**	1	1	1	1	
Disponibilidad	Tasa de incidentes que afecten la disponibilidad de la Información	**Formula:PIAD=(NID/NITD*100** **PIAD: Porcentaje de incidentes que afectan la Disponibilidad** **NID: Número de incidentes relacionados con la Disponibilidad** **NITD: Número de Incidentes totales relacionados con la Disponibilidad**	1	1	1	1	

UNIVERSIDAD CÉSAR VALLEJO

FICHA DE VALIDACIÓN DE JUICIO DE EXPERTO

Nombre del instrumento	Ficha de observación
Objetivo del instrumento	El objetivo del instrumento es medir la variable protección de activos de información a través de las siguientes dimensiones: Confidencialidad, Integridad y Disponibilidad y así determinar la validez de contenido del mismo.
Nombres y apellidos del experto	Marlon Frank Acuña Benites
Documento de identidad	42097456
Años de experiencia en el área	8
Máximo Grado Académico	Doctor
Nacionalidad	Peruano
Institución	UCV
Cargo	Docente Asesor
Número telefónico	934290418
Firma	 Dr. Marlon Acuña Benites DNI: 42097456 Ing. de Sistemas / Investigador
Fecha	**30 de mayo** del **2024**

Experto 2

CARTA DE PRESENTACIÓN

Señor: Dr. David Flores Zafra

Presente

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

Me es muy grato comunicarme con usted para expresarle mis saludos y así mismo, hacer de su conocimiento que, siendo estudiante del Programa de Maestría en Ingeniería de Sistemas con mención en Tecnologías de la Información de la Escuela de Posgrado de la UCV, en la sede Lima Norte, ciclo 2024 - I, aula 1, requiero validar los instrumentos con los cuales se recogerá la información necesaria para poder desarrollar mi investigación y con la sustentaré mis competencias investigativas en la experiencia curricular de Diseño y Desarrollo del trabajo de investigación.

El nombre de mi Variable es: **protección de activos de información** y siendo imprescindible contar con la aprobación de docentes especializados para poder aplicar los instrumentos en mención, se ha considerado conveniente recurrir a usted, ante su connotada experiencia en temas educativos y/o investigación educativa.

El expediente de validación, que le hacemos llegar contiene:

- Carta de presentación.
- Definición conceptual de la variable.
- Matriz de validación del instrumento.
- Ficha de validación de juicio de experto.

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

Atentamente.

GLADYS LEONOR CORONADO FARROÑAN

D.N.I 16806402

UNIVERSIDAD CÉSAR VALLEJO

FICHA DE VALIDACIÓN DE CONTENIDO PARA UN INSTRUMENTO

INSTRUCCIÓN: A continuación, se le hace llegar el instrumento de recolección de datos de la ficha que permitirá recoger la información en la investigación que lleva por título: SGSI basado en ISO/IEC_27001:2022 para la protección de activos de información de una entidad pública del Sector Defensa, Lima 2024

Por lo que se le solicita que tenga a bien evaluar el instrumento, haciendo, de ser caso, las sugerencias para realizar las correcciones pertinentes. Los criterios de validación de contenido son:

Criterios	Detalle	Calificación
Suficiencia	El ítem pertenece a la dimensión y basta para obtener la medición de esta	1: de acuerdo 0: en desacuerdo
Claridad	El ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas	1: de acuerdo 0: en desacuerdo
Coherencia	El ítem tiene relación lógica con el indicador que está midiendo	1: de acuerdo 0: en desacuerdo
Relevancia	La pregunta es esencial o importante, es decir, debe ser incluido	1: de acuerdo 0: en desacuerdo

Nota. Criterios adaptados de la propuesta de Escobar y Cuervo (2008).

UNIVERSIDAD CÉSAR VALLEJO

MATRIZ DE VALIDACIÓN DEL CUESTIONARIO PARA LA VARIABLE PROTECCIÓN DE ACTIVOS DE INFORMACIÓN

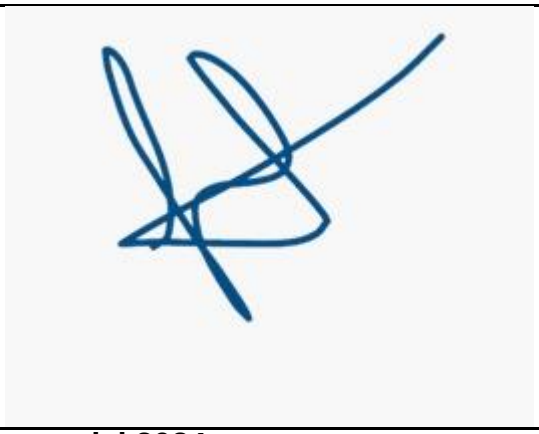
Definición de la variable: La protección de los activos de información, esencialmente, se refiere a la Seguridad de la Información y los activos asociados, por ende, se define como un conjunto de medidas diseñadas para resguardar la CID de la información en diferentes formatos y estados. Su propósito principal es mitigar riesgos como el acceso no autorizado, el robo o la alteración de la información, mediante la aplicación de controles de seguridad, gestión de riesgos, capacitación del personal y cumplimiento de normativas

Dimensiones	Indicadores	Fórmula	Suficiencia	Claridad	Coherencia	Relevancia	Observación
Confidencialidad	Tasa de incidentes que afecten la confidencialidad de la Información	**Formula:PIAC=(NIC/NITC)*100** **PIAC: Porcentaje de incidentes que afectan la Confidenciaidad** **NIC: Número de incidentes relacionado con la Confidenciaidad** **NITC: Número de Incidentes totales relacionados con la Confidenciaidad**	1	1	1	1	

Integridad	Tasa de incidentes que afecten la integridad de la Información	**Formula: PIAI=(NII/NITI)*100** **PIAI: Porcentaje de incidentes que afectan la Integridad** **NII: Número de incidentes relacionado con la Integridad** **NITI: Número de Incidentes totales relacionados con la Integridad**	1	1	1	1	
Disponibilidad	Tasa de incidentes que afecten la disponibilidad de la Información	**Formula:PIAD=(NID/NITID*100** **PIAD: Porcentaje de incidentes que afectan la Disponibilidad** **NID: Número de incidentes relacionados con la Disponibilidad** **NITD: Número de Incidentes totales relacionados con la Disponibilidad**	1	1	1	1	

UNIVERSIDAD CÉSAR VALLEJO

FICHA DE VALIDACIÓN DE JUICIO DE EXPERTO

Nombre del instrumento	Ficha de observación
Objetivo del instrumento	El objetivo del instrumento es medir la variable protección de activos de información a través de las siguientes dimensiones: Confidencialidad, Integridad y Disponibilidad y así determinar la validez de contenido del mismo.
Nombres y apellidos del experto	David Flores Zafra
Documento de identidad	41541647
Años de experiencia en el área	11
Máximo Grado Académico	Maestro en Ingeniería de Sistemas con mención en Gestión de Tecnologías de la Información
Nacionalidad	Peruana
Institución	IBM
Cargo	Gerente de Proyectos
Número telefónico	956940566
Firma	
Fecha	**30 de mayo del 2024**

Experto 3

CARTA DE PRESENTACIÓN

Señor: Mg. Fredy Antonio Castillo Paz

Presente

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

Me es muy grato comunicarme con usted para expresarle mis saludos y así mismo, hacer de su conocimiento que, siendo estudiante del Programa de Maestría en Ingeniería de Sistemas con mención en Tecnologías de la Información de la Escuela de Posgrado de la UCV, en la sede Lima Norte, ciclo 2024 - I, aula 1, requiero validar los instrumentos con los cuales se recogerá la información necesaria para poder desarrollar mi investigación y con la sustentaré mis competencias investigativas en la experiencia curricular de Diseño y Desarrollo del trabajo de investigación.

El nombre de mi Variable es: **protección de activos de información** y siendo imprescindible contar con la aprobación de docentes especializados para poder aplicar los instrumentos en mención, se ha considerado conveniente recurrir a usted, ante su connotada experiencia en temas educativos y/o investigación educativa.

El expediente de validación, que le hacemos llegar contiene:

- Carta de presentación.
- Definición conceptual de la variable.
- Matriz de validación del instrumento.
- Ficha de validación de juicio de experto.

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

Atentamente.

GLADYS LEONOR CORONADO FARROÑAN

D.N.I 16806402

UNIVERSIDAD CÉSAR VALLEJO

FICHA DE VALIDACIÓN DE CONTENIDO PARA UN INSTRUMENTO

INSTRUCCIÓN: A continuación, se le hace llegar el instrumento de recolección de datos de la ficha que permitirá recoger la información en la investigación que lleva por título: SGSI basado en ISO/IEC_27001:2022 para la protección de activos de información de una entidad pública del Sector Defensa, Lima 2024

Por lo que se le solicita que tenga a bien evaluar el instrumento, haciendo, de ser caso, las sugerencias para realizar las correcciones pertinentes. Los criterios de validación de contenido son:

Criterios	Detalle	Calificación
Suficiencia	El ítem pertenece a la dimensión y basta para obtener la medición de esta	1: de acuerdo 0: en desacuerdo
Claridad	El ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas	1: de acuerdo 0: en desacuerdo
Coherencia	El ítem tiene relación lógica con el indicador que está midiendo	1: de acuerdo 0: en desacuerdo
Relevancia	La pregunta es esencial o importante, es decir, debe ser incluido	1: de acuerdo 0: en desacuerdo

Nota. Criterios adaptados de la propuesta de Escobar y Cuervo (2008).

UNIVERSIDAD CÉSAR VALLEJO

MATRIZ DE VALIDACIÓN DEL CUESTIONARIO PARA LA VARIABLE PROTECCIÓN DE ACTIVOS DE INFORMACIÓN

Definición de la variable: La protección de los activos de información, esencialmente, se refiere a la Seguridad de la Información y los activos asociados, por ende, se define como un conjunto de medidas diseñadas para resguardar la CID de la información en diferentes formatos y estados. Su propósito principal es mitigar riesgos como el acceso no autorizado, el robo o la alteración de la información, mediante la aplicación de controles de seguridad, gestión de riesgos, capacitación del personal y cumplimiento de normativas.

Dimensiones	Indicadores	Fórmula	Suficiencia	Claridad	Coherencia	Relevancia	Observación
Confidencialidad	Tasa de incidentes que afecten la confidencialidad de la Información	**Formula:PIAC=(NIC/NITC)*100** **PIAC: Porcentaje de incidentes que afectan la Confidenciaidad** **NIC: Número de incidentes relacionado con la Confidenciaidad** **NITC: Número de Incidentes totales relacionados con la Confidenciaidad**	1	1	1	1	

Integridad	Tasa de incidentes que afecten la integridad de la Información	**Formula: PIAI=(NII/NITI)*100** **PIAI: Porcentaje de incidentes que afectan la Integridad** **NII: Número de incidentes relacionado con la Integridad** **NITI: Número de Incidentes totales relacionados con la Integridad**	1	1	1	1	
Disponibilidad	Tasa de incidentes que afecten la disponibilidad de la Información	**Formula:PIAD=(NID/NITID*100** **PIAD: Porcentaje de incidentes que afectan la Disponibilidad** **NID: Número de incidentes relacionados con la Disponibilidad** **NITD: Número de Incidentes totales relacionados con la Disponibilidad**	1	1	1	1	

UNIVERSIDAD CÉSAR VALLEJO

FICHA DE VALIDACIÓN DE JUICIO DE EXPERTO

Nombre del instrumento	Ficha de observación
Objetivo del instrumento	El objetivo del instrumento es medir la variable protección de activos de información a través de las siguientes dimensiones: Confidencialidad, Integridad y Disponibilidad y así determinar la validez de contenido del mismo.
Nombres y apellidos del experto	Fredy Antonio Castillo Paz
Documento de identidad	07262059
Años de experiencia en el área	20
Máximo Grado Académico	Maestro en Ingeniería de Sistemas con mención en Tecnologías de Información
Nacionalidad	Peruana
Institución	Municipalidad Distrital de Barranco
Cargo	Subgerente de Sistemas y Tecnologías de la Información
Número telefónico	956940566
Firma	
Fecha	**30 de mayo del 2024**

8.4. Anexo 4: Consentimiento o asentimiento informado UCV

UNIVERSIDAD CÉSAR VALLEJO

AUTORIZACIÓN DE LA ORGANIZACIÓN PARA PUBLICAR SU IDENTIDAD EN LOS RESULTADOS DE LAS INVESTIGACIONES

Datos Generales

Consentimiento:

De conformidad con lo establecido en el artículo 7°, literal "f" del Código de Ética en Investigación de la Universidad César Vallejo (*), autorizo [X], no autorizo [ ] publicar la identidad de la organización, en la cual se lleva a cabo la investigación:

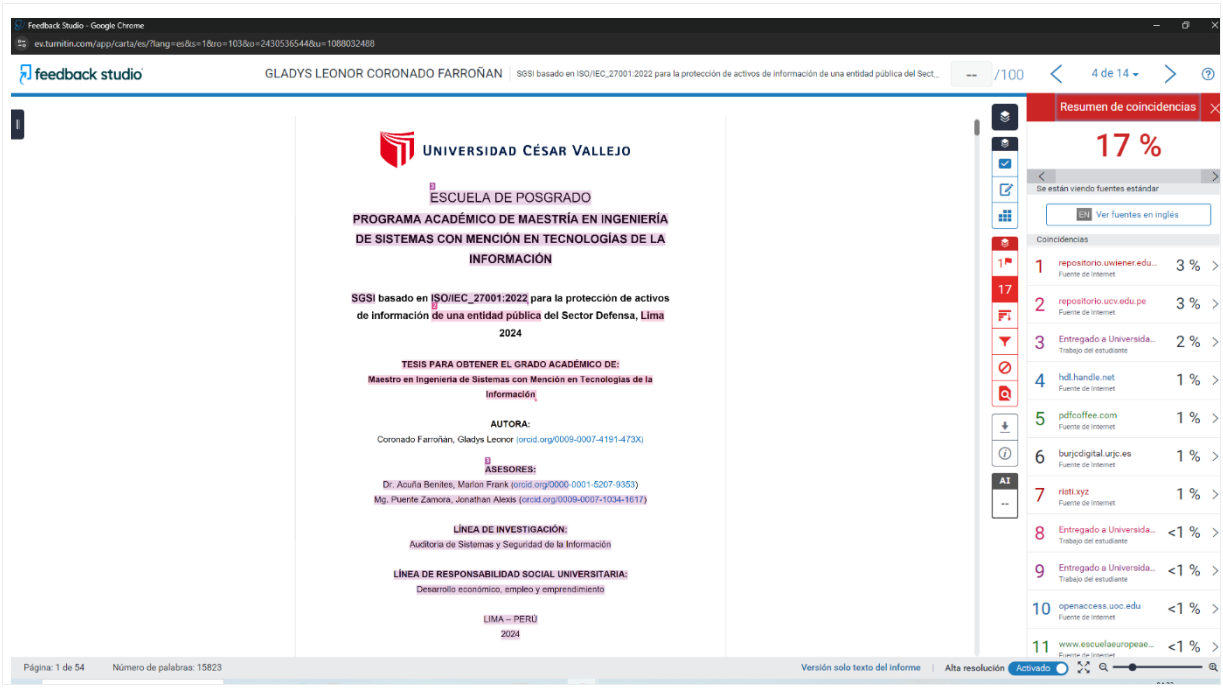
Nombre del Trabajo de Investigación:	
SGSI para la protección de los activos de información de una entidad pública del Sector Defensa, Lima, 2024	
Nombre del Programa Académico: Maestría en Ingeniería de Sistemas con mención en Tecnologías de la Información	
Autora: Nombres y Apellidos Gladys Leonor Coronado Farroñán	**DNI:** 16806402

En caso de autorizarse, soy consciente que la investigación será alojada en el Repositorio Institucional de la UCV, la misma que será de acceso abierto para los usuarios y podrá ser referenciada en futuras investigaciones, dejando en claro que los derechos de propiedad intelectual corresponden exclusivamente a la autora del estudio.

Lima, 23 de mayo de 2024

(*) Código de Ética en Investigación de la Universidad César Vallejo-Artículo 7º, literal " f " **Para difundir o publicar los resultados de un trabajo de investigación es necesario mantener bajo anonimato el nombre de la institución donde se llevó a cabo el estudio, salvo el caso en que haya un acuerdo formal con el gerente o director de la organización, para que se difunda la identidad de la institución. Por ello, tanto en los proyectos de investigación como en los informes o tesis, no se deberá incluir la denominación de la organización, pero sí será necesario describir sus características.**

8.5. Anexo 5: Reporte de Similitud en Software Turnitin



8.6. Anexo 6: Autorización de la institución para la ejecución de la investigación

"Decenio de la Igualdad de Oportunidades para mujeres y hombres"
"Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho"

Lima, 23 de mayo de 2024

CARTA N° 001-2024

Ing. Gladys Leonor Coronado Farroñán
Av. Brasil 911 – Jesús María - Lima

ASUNTO: Solicitud de autorización para realizar Investigación Académica

De mi mayor consideración:

Tengo el agrado de dirigirme a usted, en atención a su solicitud de autorización para realizar la investigación académica, denominada: *"SGSI para la protección de los activos de información de una entidad pública del Sector Defensa, Lima, 2024"* del Programa Académico de Maestría en Ingeniería de Sistemas, con Mención en Tecnologías de la Información de la Universidad Cesar Vallejo, con sede en Lima Norte.

Al respecto le comunicamos que se le estará brindando las facilidades para acceder a la información requerida, recabando la misma, contemplando el compromiso de que dicha información, será tratada con la responsabilidad y cuidado que amerita, siempre que no esté protegida por la Ley N° 29733: Ley de Protección de Datos personales y su reglamento y/o no esté catalogada como información confidencial o reservada en la entidad.

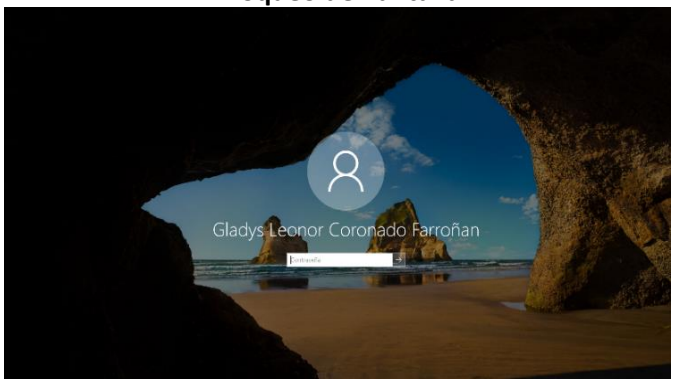
Se adjunta el anexo *"Autorización de la organización para publicar su identidad en los resultados de las investigaciones"* con la respectiva aceptación correspondiente.

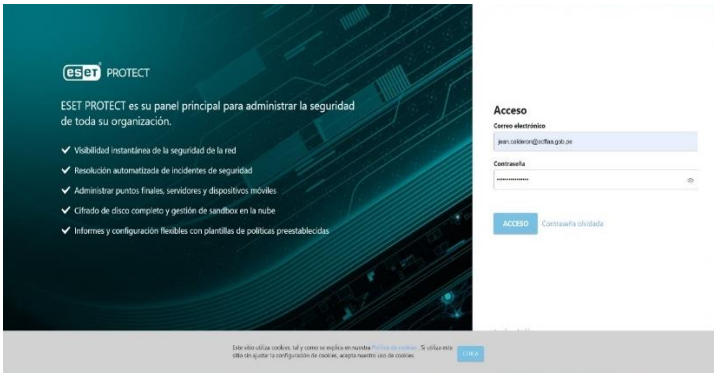
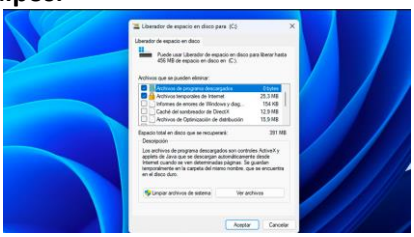
Sin otro particular, hago propicia la ocasión para expresarle mi consideración y estima personal.

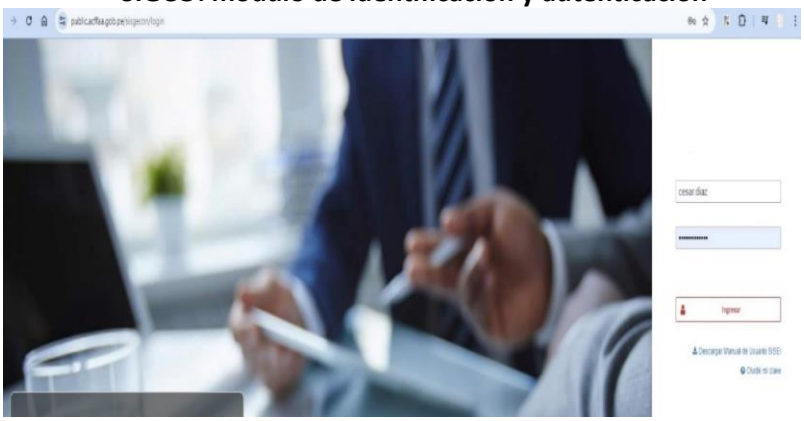
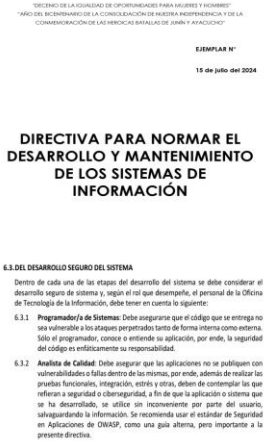
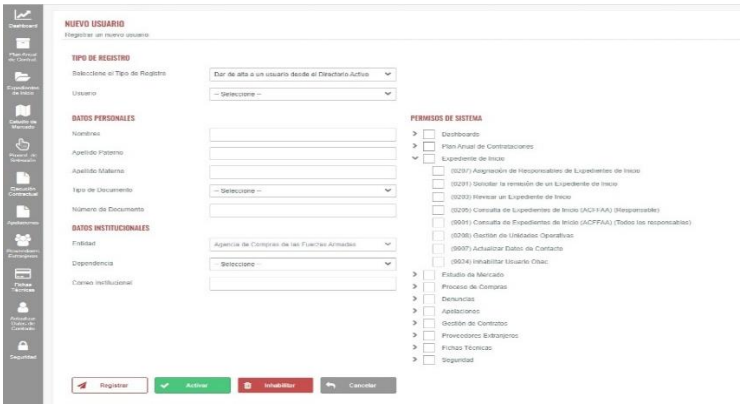
Atentamente,

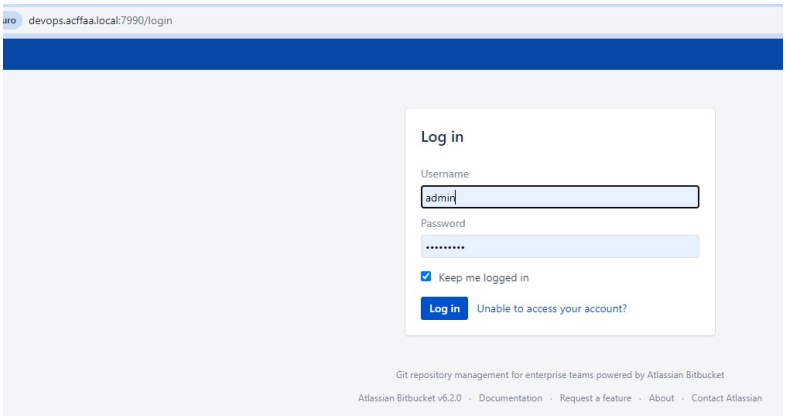
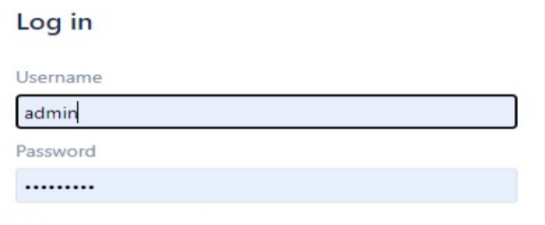
8.7. Anexo 7: Otras evidencias

CONTROLES TECNOLÓGICOS DEL SGSI, EXTRAÍDOS DE LA "ISO/IEC 27001:2022 - ANEXO A" IMPLEMENTADOS EN LA ENTIDAD DEL SECTOR DEFENSA, LIMA 2024

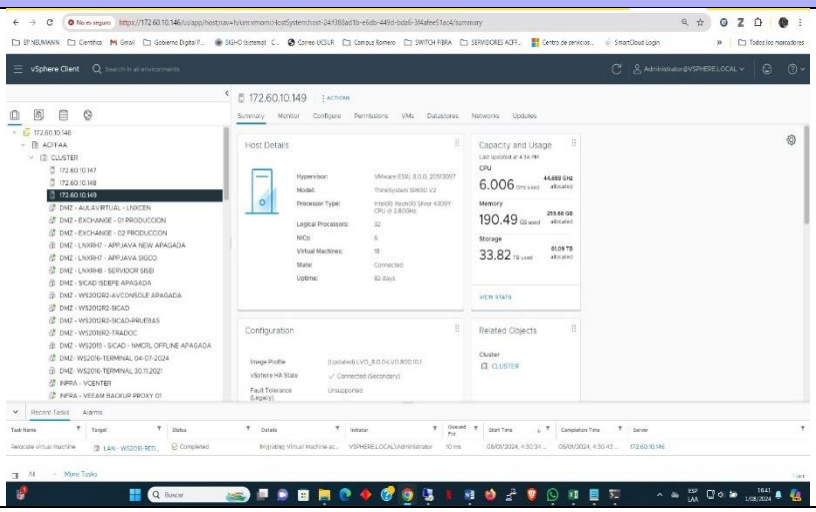
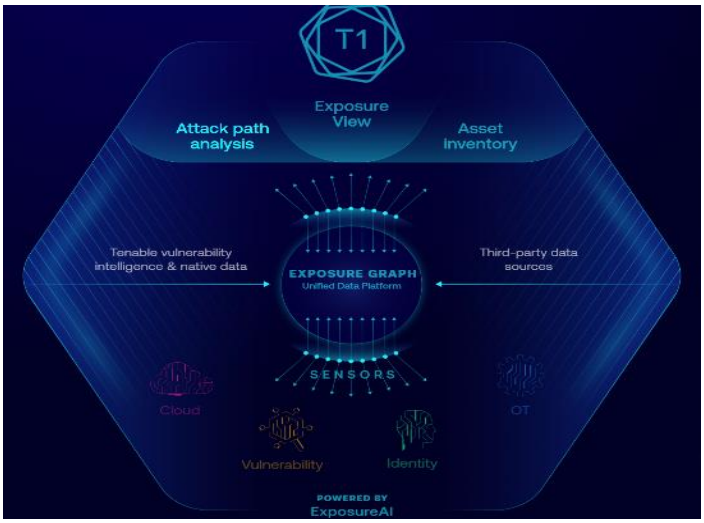
N°	*CONTROL SELECCIONADO SEGÚN ANÁLISIS REALIZADO*	EVIDENCIA DE IMPLEMENTACIÓN (SI ES QUE SE REQUIERE)
1	***Dispositivos de punto final de usuario.***	**Bloqueo de Pantalla** 
2	***Derechos de acceso privilegiado.***	**Identificación e Autenticación del Servidor Principal** 
3	***Autenticación segura.***	**Token utilizado para las Firmas Digitales, documentos con valor legal en el entorno Digital**  

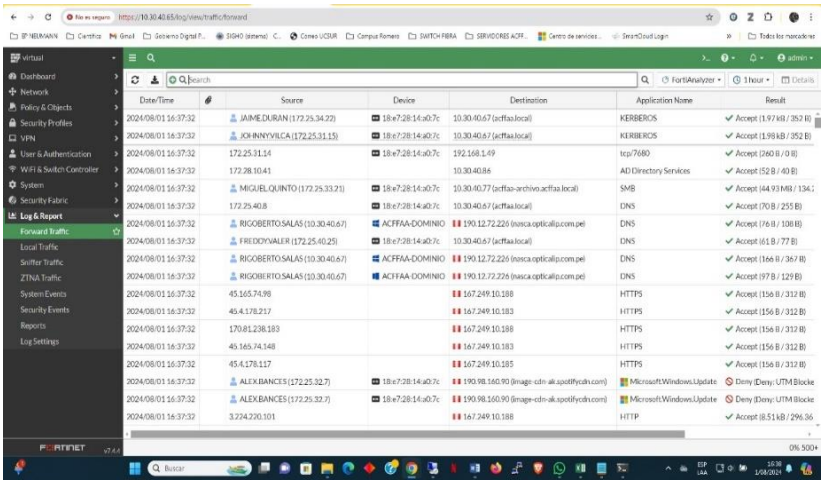
N°	CONTROL SELECCIONADO SEGÚN ANÁLISIS REALIZADO	EVIDENCIA DE IMPLEMENTACIÓN (SI ES QUE SE REQUIERE)
4	*Protección contra malware.*	**Software antivirus administrado desde el servidor** 
5	*Eliminación de información.*	**Software que elimina información como parte del hardening en los equipos.**  
6	*Instalación de software en sistemas operativos*	**Se realiza, pero no se detalla por confidencialidad.**
7	*Uso de criptografía*	**Entorno del SGD y Documento Digital Firmado**  N° Acta de Reunión 004 — Código del Acta AR - CGTD-004-2024 Jefe de la Oficina de Informática (OI)/ Secretario Técnico del CGTD. — Si — Firmado digitalmente por PEREZ BARRANTES Gary Lizardo FAU 20556939781 hard. Motivo: Soy el autor del documento. Fecha: 17.07.2024 13:35:43 -05:00

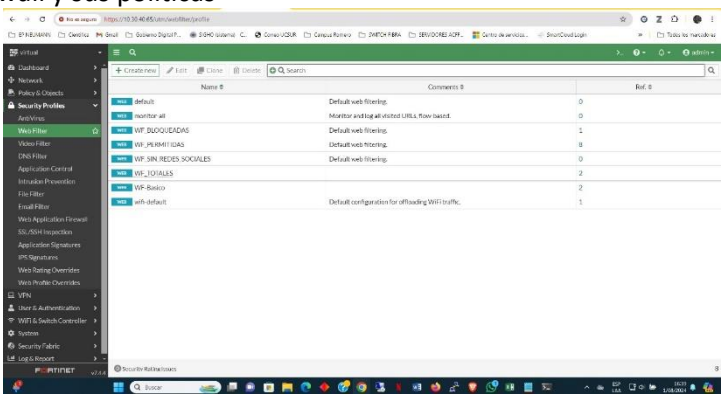
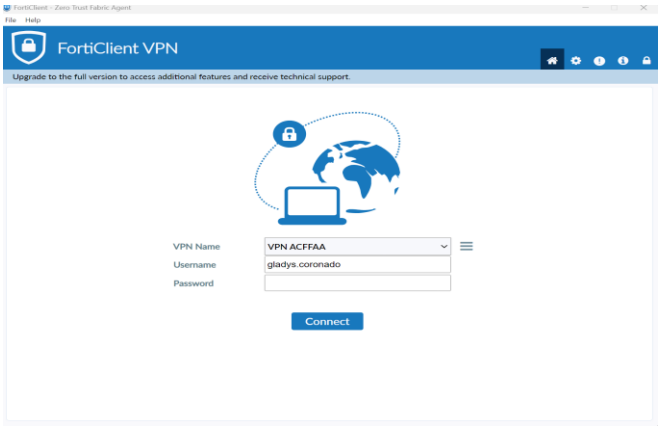
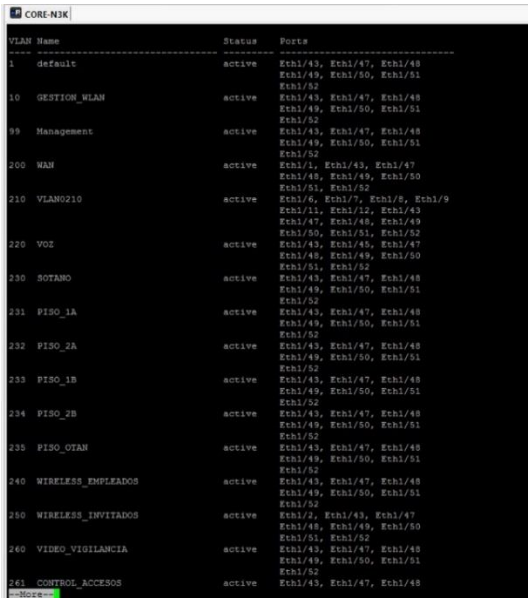
N°	CONTROL SELECCIONADO SEGÚN ANÁLISIS REALIZADO	EVIDENCIA DE IMPLEMENTACIÓN (SI ES QUE SE REQUIERE)
8	*Requisitos de seguridad de las aplicaciones.*	**SIGCO: módulo de identificación y autenticación** 
9	*Principios de arquitectura y ingeniería de sistemas seguros*	**Directiva para Normar el Desarrollo y Mantenimiento de los Sistemas de Información en la entidad.**  "DECENIO DE LA IGUALDAD DE OPORTUNIDADES PARA MUJERES Y HOMBRES" "AÑO DEL BICENTENARIO DE LA CONSOLIDACIÓN DE NUESTRA INDEPENDENCIA Y DE LA CONMEMORACIÓN DE LAS HEROICAS BATALLAS DE JUNÍN Y AYACUCHO" EJEMPLAR N° 15 de julio del 2024 DIRECTIVA PARA NORMAR EL DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN 6.3. DEL DESARROLLO SEGURO DEL SISTEMA Dentro de cada una de las etapas del desarrollo del sistema se debe considerar el desarrollo seguro de sistema y, según el rol que desempeñe, el personal de la Oficina de Tecnología de la Información, debe tener en cuenta lo siguiente: 6.3.1 **Programador/a de Sistemas**: Debe asegurarse que el código que se entrega no sea vulnerable a los ataques perpetrados tanto de forma interna como externa. Sólo el programador, conoce o entiende su aplicación, por ende, la seguridad del código es enfáticamente su responsabilidad. 6.3.2 **Analista de Calidad**: Debe asegurar que las aplicaciones no se publiquen con vulnerabilidades o fallas dentro de las mismas, por ende, además de realizar las pruebas funcionales, integración, estrés y otras, deben de contemplar las que refieran a seguridad o ciberseguridad, a fin de que la aplicación o sistema que se ha desarrollado, se utilice sin inconveniente por parte del usuario, salvaguardando la información. Se recomienda usar el estándar de Seguridad en Aplicaciones de OWASP, como una guía alterna, pero importante a la presente directiva.
10	*Codificación segura*	**Se implementa, pero no se detalla por confidencialidad.**
11	*Restricción de acceso a la información*	**Módulo de Registro de Usuario, Identificación y Autenticación**  NUEVO USUARIO Registrar un nuevo usuario TIPO DE REGISTRO Seleccione el Tipo de Registro Dar de alta a un usuario desde el Directorio Activo Usuario -- Seleccione -- DATOS PERSONALES Nombres Apellido Paterno Apellido Materno Tipo de Documento -- Seleccione -- Número de Documento DATOS INSTITUCIONALES Entidad Agencia de Compras de las Fuerzas Armadas Dependencia -- Seleccione -- Correo Institucional PERMISOS DE SISTEMA Dashboard Plan Anual de Contrataciones Expediente de Inicio Estudio de Mercado Proceso de Compras Denuncias Apelaciones Gestión de Contratos Proveedores Extranjeros Fichas Técnicas Seguridad Registrar Activar Inhabilitar Cancelar

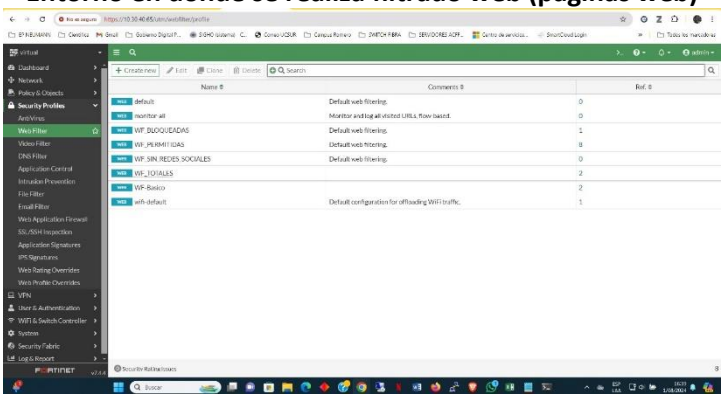
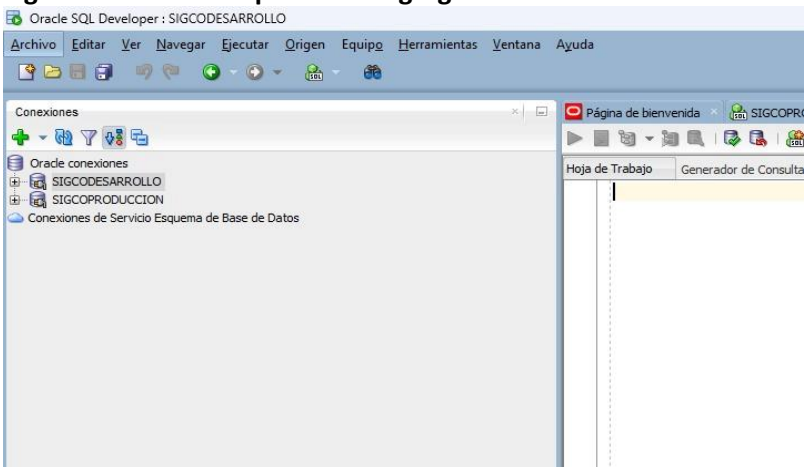
N°	CONTROL SELECCIONADO SEGÚN ANÁLISIS REALIZADO	EVIDENCIA DE IMPLEMENTACIÓN (SI ES QUE SE REQUIERE)
12	*Acceso al código fuente*	**Acceso al entorno de Desarrollo de Sistemas de Información** 
13	*Gestión de la configuración*	**Se utiliza Bitbucket Cloud es una herramienta de colaboración y alojamiento de código.** 
14	*Enmascaramiento de datos*	**Se realiza dentro de código a través de sentencias, el resultado es:** 

N°	CONTROL SELECCIONADO SEGÚN ANÁLISIS REALIZADO	EVIDENCIA DE IMPLEMENTACIÓN (SI ES QUE SE REQUIERE)
15	*Prevención de pérdida de datos*	**A través de este gestor de código fuente alojado en los servidores, el código fuente no puede perderse, sino actualizarse.**
16	*Uso de programas de utilidad con privilegios*	**Se utilizan cada cierto tiempo como por ejemplo los parches de los Sistemas Operativos que son previamente probados.**
17	*Ciclo de vida seguro de desarrollo*	**Se ha contemplado este control dentro de la Directiva de Desarrollo de Sistemas de Información.** 2.2. FASES DE LA METODOLOGÍA Las fases del desarrollo del sistema de información a utilizar son en base a la Norma Técnica Peruana ISO/IEC 12207:2016, y adecuadas a las necesidades de la ACFFAA, cada fase consta de etapas en las cuales se detalla el desarrollo de la metodología. Las fases y etapas son las siguientes: a. **Fase de Inicio** Identificar el alcance inicial del proyecto y de la arquitectura del sistema es crucial para establecer una base sólida desde el inicio. Obtener el presupuesto inicial y, sobre todo, asegurar la aceptación de los involucrados son pasos fundamentales para el éxito del proyecto. La Oficina de Informática, en coordinación con el(las) área(s) solicitante(s), y de acuerdo a su competencia, identifica, analiza y
18	*Desarrollo subcontratado*	**Si se desea contratar a externos, también tienen su perfil en el gestor de colaboración.**
19	*Gestión del cambio*	**Dentro del Desarrollo de Sistemas de Información y de Software se ha implementado este control.**
20	*Protección de los sistemas de información durante las pruebas de auditoría*	**Se contempla que, para cada ejercicio de auditoría, los auditores tengan un acceso en modo consulta, así no alteran data o información sensible en el entorno de producción.**
21	*Gestión de capacidad*	**Por ejemplo, en las redes de datos, para el tema de ancho de banda del servicio de internet se tiene alertas que hacen que se liberen sitios para brindar un mayor consumo al servicio que se requiera, así como prevenir la adquisición de storages para el almacenamiento. En la Figura se aprecia el seguimiento de estos activos de información:**

N°	CONTROL SELECCIONADO SEGÚN ANÁLISIS REALIZADO	EVIDENCIA DE IMPLEMENTACIÓN (SI ES QUE SE REQUIERE)
		
22	*Gestión de vulnerabilidades técnicas.*	**Software para la detección de vulnerabilidades en las aplicaciones** 
23	*Copia de seguridad de la información*	**Storages en donde se respalda la información** 

N°	CONTROL SELECCIONADO SEGÚN ANÁLISIS REALIZADO	EVIDENCIA DE IMPLEMENTACIÓN (SI ES QUE SE REQUIERE)
24	***Redundancia de las instalaciones de procesamiento de información***	**Rack de comunicaciones alterno de la entidad.** 
25	***Monitoreo de actividades***	**Se observa mediante este monitoreo los recursos de la red** 

N°	CONTROL SELECCIONADO SEGÚN ANÁLISIS REALIZADO	EVIDENCIA DE IMPLEMENTACIÓN (SI ES QUE SE REQUIERE)
26	Seguridad de redes	Firewall y sus políticas 
27	Seguridad de los servicios de red	**Pantallazos de como acceder a la VPN en escritorio remoto** 
28	Segregación de redes	**Segmentación de redes en la entidad:** 

N°	CONTROL SELECCIONADO SEGÚN ANÁLISIS REALIZADO	EVIDENCIA DE IMPLEMENTACIÓN (SI ES QUE SE REQUIERE)
29	*Filtrado web*	**Entorno en donde se realiza filtrado web (páginas web)** 
30	*Separación de entornos de desarrollo, pruebas y producción*	**Figura en donde se aprecia la disgregación de estos entornos:** 
I	**Política General de Seguridad de la Información que Sostiene la Implementación del SGSI**