UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

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

SGSI en la gestión de riesgos en el área de infraestructura y operaciones en una entidad pública, Callao 2023

TESIS PARA OBTENER EL GRADO ACADÉMICO DE:
Maestro en Ingeniería de Sistemas con Mención en Tecnologías de la Información

AUTOR:

Huamanteca Damian, Henry Frank (orcid.org/0000-0002-0519-7952)

ASESORES:

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

Mg. García Calderón, Luis Eduardo (orcid.org/0000-0002-6299-3453)

LÍNEA DE INVESTIGACIÓN:

Auditoría de Sistemas y Seguridad de la Información

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:

Desarrollo económico, empleo y emprendimiento

LIMA — PERÚ

2023

Dedicatoria

A mi querida madre Graciela Damian Camahuali, por ser un ejemplo de vida, un ejemplo de esfuerzo, coraje y valentía, que me impulsa a seguir creciendo tanto personal como profesionalmente, que me enseña a no rendirme antes las adversidades. A mi hijo Angel Huamanteca Peche, por ser mi inspiración, motor y motivo de ser un mejor padre y un mejor hombre de bien.

Agradecimiento
Agradezco a mi familia y amigos que me apoyaron y me alentaron para el desarrollo y culminación de esta tesis.

Al Dr. Marlon Benites Acuña, por brindarme su asesoría permanente en la realización de esta tesis.

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 Completa titulada: "SGSI en la Gestión de Riesgos en el área de Infraestructura y Operaciones en una entidad pública, Callao 2023", cuyo autor es HUAMANTECA DAMIAN HENRY FRANK, constato que la investigación tiene un índice de similitud de 14.00%, 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 Completa cumple con todas las normas para el uso de citas y referencias establecidas por la Universidad César Vallejo.

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

LIMA, 31 de Julio del 2023

Apellidos y Nombres del Asesor:	**Firma**
ACUÑA BENITES MARLON FRANK **DNI:** 42097456 **ORCID:** 0000-0001-5207-9353	Firmado electrónicamente por: MACUNABE el 31-07-2023 23:58:08

Código documento Trilce: TRI - 0632396

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, HUAMANTECA DAMIAN HENRY FRANK estudiante de la ESCUELA DE POSGRADO del programa de 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 en la Gestión de Riesgos en el área de Infraestructura y Operaciones en una entidad pública, Callao 2023", es de mi autoría, por lo tanto, declaro que la Tesis:

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

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

Nombres y Apellidos	Firma
HUAMANTECA DAMIAN HENRY FRANK **DNI:** 43230482 **ORCID:** 0000-0002-0519-7952	Firmado electrónicamente por: HHUAMANTECAD el 01-08-2023 00:39:20

Código documento Trilce: INV - 1240406

INVESTIGA UCV

Índice de contenidos

Dedicatoria ii

Agradecimiento iii

Declaratoria de autenticidad del asesor iv

Declaratoria de originalidad del autor v

Índice de contenidos vi

Índice de tablas vii

Índice de gráficos y figuras viii

Resumen ix

Abstract x

I. INTRODUCCIÓN 1

II. MARCO TEÓRICO 5

III. METODOLOGÍA 22

Tipo y Diseño de Investigación 22

Variables y operacionalización 23

Población y muestra 24

Técnicas e instrumentos de recolección de datos 25

Procedimientos 27

Método de análisis de datos 28

Aspectos éticos 28

IV. RESULTADOS 29

V. DISCUSIÓN 41

VI. CONCLUSIONES 47

VII. RECOMENDACIONES 48

REFERENCIAS 49

ANEXOS

Índice de tablas

Pg.

Tabla 1 Validez del instrumento Ficha de observación de análisis, nivel y número de controles aplicados 26
Tabla 2 Niveles de confiabilidad 26
Tabla 3 Estadística de fiabilidad 27
Tabla 4 Resultados descriptivos del Nivel de probabilidad 29
Tabla 5 Resultados descriptivos del Nivel de riesgo 31
Tabla 6 Resultados descriptivos del Número de controles aplicados 32
Tabla 7 Prueba de normalidad – Nivel de Probabilidad 34
Tabla 8 Prueba de normalidad – Nivel de Riesgo 35
Tabla 9 Prueba de normalidad – Número de controles 35
Tabla 10 Prueba de hipótesis de Nivel de Probabilidad 37
Tabla 11 Prueba de hipótesis de Nivel de Riesgo 39
Tabla 12 Prueba de hipótesis de Número de controles aplicados 40

Índice de gráficos y figuras

Pg.

Figura 1 Fases – ISO 27001 16

Figura 2 Proceso de gestión del riesgo en la seguridad de la información – ISO 27005 18

Figura 3 Diseño Pre-Experimental 22

Figura 4 Nivel de Probabilidad antes y después de aplicar un SGSI 30

Figura 5 Nivel de Probabilidad antes y después de aplicar un SGSI 31

Figura 6 Número de controles aplicados antes y después de un SGSI 33

Resumen

El presente estudio tiene como objetivo general, determinar la influencia de un SGSI en la gestión de riesgos en el área de infraestructura y operaciones en una entidad pública, callao 2023.

Debido a ello, para la implementación del SGSI nos apoyamos en la metodología NTP ISO/IEC 27001:2014, el tipo de investigación es aplicada, el diseño es pre-experimental y de enfoque cuantitativo.

Los resultados demostraron que un SGSI reduce el nivel de probabilidad en la gestión de riesgos de 2.54 puntos a 1.47 puntos, lo que equivale una reducción del 21.4%. Igualmente, se demostró que un SGSI influye de manera positiva reduciendo en el nivel de riesgo en la gestión de riesgos de 10.30 puntos a 5.98 puntos, lo que equivale a una reducción de 17.28%. De la misma manera se demostró que un SGSI influye de manera positiva incrementando el número de controles aplicados en la gestión de riesgos de 79.82% (91 controles), subió a 99.12% (113 controles), mostrando un claro incremento de 12 controles, lo que equivale a un 17.28%.

Debido a los resultados, se concluye que un SGSI mejora la gestión de riesgos en el área de infraestructura y operaciones en una entidad pública, Callao 2023.

Palabras clave: SGSI, ISO 27001, gestion de riesgos, información, sistema de gestión de seguridad de la información.

Abstract

The general objective of this study is to determine the influence of an ISMS on risk management in the area of infrastructure and operations in a public entity, Callao 2023.

Due to this, for the implementation of the ISMS we rely on the methodology NTP ISO/IEC 27001:2014, the type of research is applied, the design is pre-experimental and quantitative approach.

The results showed that an ISMS reduces the level of probability in risk management from 2.54 points to 1.47 points, which is equivalent to a reduction of 21.4%. Likewise, it was shown that an ISMS has a positive influence in reducing the level of risk in risk management from 10.30 points to 5.98 points, which is equivalent to a reduction of 17.28%. In the same way, it was demonstrated that an ISMS has a positive influence by increasing the number of controls applied in risk management from 79.82% (91 controls) to 99.12% (113 controls), showing a clear increase of 12 controls, which is equivalent to 17.28%.

Due to the results, it is concluded that an ISMS improves risk management in the area of infrastructure and operations in a public entity, Callao 2023.

Keywords: ISMS, ISO 27001, Risk Management, Information, Information Security Management System.

I.INTRODUCCIÓN

En el escenario internacional, exactamente en la Unión Europea (UE), según Uriel Bekerman (2020), en el 2018 reconocieron que los países que conforman la UE se enfrentaban a una amenaza sin precedentes de ciberataques estatales y por motivos políticos, ciberdelincuencia y ciberterrorismo, que el ciberespacio ha sido ampliamente reconocido por las fuerzas armadas como un quinto escenario de guerra, lo que permite el desarrollo de capacidades de ciberdefensa. A su vez en Bolivia, Sarmiento (2020) quien estudió las ventajas de utilizar metodologías para implantar SGSI. Así, tiene como propósito destacar la relevancia de aplicar métodos para implementar SGSI en todos los procesos empresariales para garantizar en la información, el aspecto confidencial, íntegro y disponible. En la realización de la encuesta se explicó a cada empresa la importancia de las normas internas, en particular aquella que están relacionadas a la seguridad de la información. El 84% de instituciones estaría interesada en implementar estas normas, mientras que el 16% restante indicó que estaría interesada pero que no contaba con el presupuesto para hacerlo, pero que comenzaría a implementar normas internas en su institución.

A su vez, en Colombia para Guerra et al. (2021), las bibliotecas gestionan información de carácter confidencial con respecto a sus usuarios, que son los principales activos de la entidad, y un inventario de todos los bienes que componen la biblioteca. Toda esta información requiere un cierto grado de seguridad y debe ser protegida eficazmente desde el momento en que es descubierta. Por lo cual se aplicó un SGSI basado en una estrategia para identificar y analizar riesgos a los procesos en la biblioteca universitaria, la cual no tiene automatizados los procesos relacionados con la seguridad y la normalización y no dispone un SGSI. Las técnicas de gestión de la calidad y normalización no están reguladas por métricas y normas, lo que da lugar a robos, pérdidas e indisponibilidad de la información, de ahí la necesidad de un SGSI basado en la norma ISO 27001. Como resultado el riesgo real en caso de amenazas es de 74,82 %, pero se reduciría al 25,18 % debido a la existencia de salvaguardas.

Por otro lado, en el escenario nacional, en la ciudad de Trujillo para Cerezo (2022) la empresa Guru-IT, parte del Grupo Gurusoft, que gestiona un gran volumen de información, la cual debe estar protegida, cosa que no es fácil y los problemas aumentan con el tiempo y el crecimiento de la empresa. Ni siquiera contar con el personal cualificado y la adquisición de mejores equipos era garantía de salvaguardar la seguridad de la información, porque no se dispone de un SGSI que proporcione los lineamientos, por lo cual no se podía identificar y estudiar los riesgos asociados a la información y a los procesos de la empresa. Por lo tanto, una vez que se dispone de un SGSI, es necesario identificar los activos de información cuyo impacto es crucial en la organización y realizar una gestión de riesgos para reducir la probabilidad de que las amenazas perjudiquen a la empresa. Como resultado, la proporción de elementos vulnerables de la infraestructura informática disminuyó en un 13,55% y la proporción de elementos vulnerables de la infraestructura informática disminuyó en un 9,75% en comparación con la situación anterior a la prueba, lo que contribuyó a mantener la seguridad de los dispositivos y a reducir el riesgo de ataques.

Igualmente, para Moscaiza (2018) en Lima, Ahorro y Crédito ABC, cooperativa supervisada por la SBS y que, por tanto, debe aportar valor añadido a sus procesos de negocio, mejoró su gestión de riesgos en un 22,22% respecto a la línea de base, gracias a la introducción de un SGSI, y alcanzó un resultado final del 15% de cumplimiento de los requisitos de los capítulos de la normativa, y del 25% en el ámbito de los controles del Anexo A. Se han logrado beneficios para el mercado como resultado del aumento en la eficiencia y por otro lado, una reducción en los costes, lo que ha supuesto una diferenciación en el mercado.

Una entidad pública no es ajena a ello, por lo que implementó un SGSI, en la cual, dentro del alcance se encuentra los procesos core “Gestión de Licencias” y “Recepción y despacho de Naves”, asimismo se encuentra el proceso de soporte “Sistemas de Información”, adicional a ello, en el 2018 obtuvo la certificación en la NTP-ISO/IEC 27001:2014 por la casa certificadora NQA. Sin embargo, el proceso

de “Infraestructura y Operaciones” no se encuentra dentro del alcance del SGSI de la entidad pública.

Por lo descrito líneas arriba, se plantea el siguiente problema general ¿Cómo influye un SGSI en la Gestión de Riesgos en el área de Infraestructura y Operaciones en una entidad pública, 2023? De igual manera se plantean los siguientes problemas específicos: ¿Cómo influye un SGSI en el nivel de probabilidad en la Gestión de Riesgos en el área de Infraestructura y Operaciones en una entidad pública, 2023? ¿Cómo influye un SGSI en el nivel de riesgo en la Gestión de Riesgos en el área de Infraestructura y Operaciones en una entidad pública, 2023? ¿Cómo influye un SGSI en los controles empleados en la Gestión de Riesgos en el área de Infraestructura y Operaciones en una entidad pública, 2023?

La **justificación teórica** para la presente investigación radica en aplicar la norma ISO 27001, para mejorar la Gestión de Riesgos en el área de Infraestructura y Operaciones en una entidad pública. El cual obtendrá resultados que serán contrastados con otras investigaciones y permitirá conocer la realidad y el impacto de un SGSI en la Gestión de Riesgos en el área de Infraestructura y Operaciones en una entidad pública. La **justificación práctica** en la presente indagación se considera desde la postura de la Seguridad de la Información, la necesidad de proteger la información y los activos, debido a que el área de Infraestructura y Operaciones de la entidad pública no se encuentra dentro del alcance del SGSI, por lo cual no se cuenta con los controles necesarios para mitigar las amenazas interna y externas. La **justificación metodológica** de la indagación se basa en la aplicabilidad de un SGSI en la Gestión de Riesgos en el área de Infraestructura y Operaciones en una entidad pública bajo la norma ISO 27001 y la demostración de su validez y confiabilidad a través del método científico el cual nos permitirá evaluar el nivel de la Gestión de Riesgos usando ficha de observación y el procesamiento de data a través del Software IBM SPSS Statics 25. El alcance de la presente

indagación abarca la aplicación del SGSI para mejorar la Gestión de Riesgos en el área de Infraestructura y Operaciones en una entidad pública, 2023.

En este sentido, el objetivo principal de la investigación es: Determinar la influencia de un SGSI en la Gestión de Riesgos en el área de Infraestructura y Operaciones en una entidad pública, 2023. Asimismo, los objetivos específicos son: Determinar de qué manera influye el SGSI en el nivel de probabilidad en la Gestión de Riesgos en el área de Infraestructura y Operaciones en una entidad pública, 2023. Determinar de qué manera influye el SGSI en el nivel de riesgo en la Gestión de Riesgos en el área de Infraestructura y Operaciones en una entidad pública, 2023. Determinar de qué manera influye el SGSI en los controles aplicados en la Gestión de Riesgos en el área de Infraestructura y Operaciones en una entidad pública, 2023.

Surgiendo la hipótesis general: La aplicabilidad de un SGSI mejora la Gestión de Riesgos en el área de Infraestructura y Operaciones en una entidad pública, 2023. Asimismo, surgen las hipótesis específicas: La aplicabilidad de un SGSI influye positivamente reduciendo el nivel de probabilidad en la Gestión de Riesgos en el área de Infraestructura y Operaciones en una entidad pública, 2023. La aplicabilidad de un SGSI influye positivamente reduciendo el nivel del riesgo en la Gestión de Riesgos en el área de Infraestructura y Operaciones en una entidad pública, 2023. La aplicación del SGSI influye de manera positiva incrementando el número de controles en la Gestión de Riesgos en el área de Infraestructura y Operaciones en una entidad pública, 2023.

II.MARCO TEÓRICO

Para Jara (2018) una entidad pública (Municipalidad de Carabayllo) que no contaba con un SGSI en los procedimientos del negocio, cuyo nivel de seguridad de la información es bajo, por ello el objetivo principal fue poner en marcha un SGSI. En la población y muestra, se consideraron 31 activos y 114 controles. Por lo cual, se utilizó una investigación de aplicada, pre-experimental. Para la interpretación de los resultados, se utiliza un enfoque cuantitativo. Como resultado, el promedio del nivel del riesgo se redujo en 4.06 puntos, por otro lado, aumentaron el N° controles aplicados en un 91.2%. Por lo que concluyó, que un SGSI mejora la gestión de riesgos en una entidad pública.

Igualmente, para Huerta (2019) la empresa Coopsol, sufrió un ciberataque de tipo Ransomware, ocasionando una pérdida del 90% de la información. Evidencio que la aplicabilidad de un SGSI mejora la gestión de riesgos. Para la muestra se consideraron 24 activos críticos y 114 controles del anexo A, los cuales fueron registrados en fichas de observación. Debido a ello, utilizó una investigación aplicada, pre-experimental. Los resultados fueron validados mediante un enfoque cuantitativo. Gracias a ello se demostró que el nivel del riesgo se redujo en 3.62 puntos y que los controles aplicados aumentaron en número, elevando el nivel de seguridad en un 81.6%. Por lo que concluyó, que la aplicabilidad de un SGSI mejora la gestión de riesgos en una entidad pública.

Por otro lado, para Atencio (2019) la dirección general de informática de una universidad pública cuenta con un plan de seguridad, la cual no está basada en un SGSI, por lo tanto, la organización es vulnerable y susceptible a ataques informáticos. El objetivo de esta indagación es diseñar un SGSI en base a la ISO27001. Por tanto, se basa en un estudio aplicado y pre-experimental descriptivo. Se consideró como población y muestra al director y adicionalmente a 8 trabajadores administrativos. Se identifica que, en un gran número de incidentes se encuentran relacionados al sistema operativo y la manipulación de información, asimismo, las transacciones no son realizadas de manera correcta, lo que genera errores e interrupciones. Estos incidentes se deben a la carencia de personal

calificado, lo cual afecta a la información y su seguridad. Tras la implementación y aplicación del SGSI se concluye que el cumplimiento de la norma aumentó de manera significativa del 35% al 41%.

Del mismo modo, para Aquino (2020) en la Universidad Nacional Micaela Bastidas, la Dirección de TI no cuenta con alguna norma o directiva que indique cómo se debe proteger la información. En su investigación se plantea aplicar un SGSI en base ISO 27001. Utilizó una investigación aplicada, pre-experimental. Los resultados revelaron que los riesgos de seguridad respecto a los controles tenían un nivel de 86.15%, el cual se redujo a un 11.15%; mostrando claramente una reducción del 75%. Por otro lado, se incrementó el número de controles de seguridad, ya que antes solo eran 18 lo cual representa un 15,78%, estos incrementaron a 65 controles lo que representa un 57,01%; lo cual refleja un crecimiento de 41,23%.

Así mismo para Guardia (2020) en una entidad que carece de un SGSI, es potencialmente vulnerable y susceptible a los riesgos y amenazas informáticas. Es por ello que realizó una investigación aplicada correlacional de enfoque cuantitativo, cuyo objetivo es desarrollar un SGSI y que los riesgos informáticos sean minimizados. Se tomó como población y muestra del área de secretaría académica a 20 trabajadores. Como resultado se observa que el porcentaje de colaboradores con conocimiento de tratamiento de riesgos, asciende al 99%, por lo que los riesgos frente a un ataque se minimizaron.

Agregando a lo anterior, para Izquierdo (2021) en su investigación realizó la uniformización de los estándares respecto a la gestión de la seguridad de la información con la finalidad de preparar un marco que se ajuste a los procedimientos del negocio relacionados a cada farmacia de los hospitales en la región Amazonas. El cual consistió en 4 fases, relacionados a 14 procesos, estos a su vez se relacionan a 6 subprocesos, por último, se aplicaron 15 plantillas y para el monitoreo se consideró una herramienta. Por último, se consideraron para la muestra 41 empleados. Gracias al estudio se encontró en los controles una mejora

de un 31% de eficiencia. En ese mismo sentido, el control de acceso muestra una mejora del 70%.

En esa misma línea, para Narro (2021) en la universidad pública de Cajamarca, si bien cuenta con política y procedimientos, no son suficientes para asegurar la seguridad en sus activos, ya que, si se materializa alguna amenaza, sufriría una pérdida del 70% en su información crítica. Se apoyó en una indagación cuantitativa, de tipo “no experimental” y correlacional. Los resultados demuestran que la gestión de riesgos, existe un 20% de nivel de cumplimiento, asimismo, en la prueba estadística de Pearson, arrojó un grado de significancia equivalente 76%, sobrepasando el límite (5%), por lo cual, la hipótesis que planteo, fue rechazada y demostrando que, con el SGSI y el respectivo cumplimiento de este, mayor será el nivel de seguridad en la gestión de riesgos.

De igual forma, para Cuenca (2023) la empresa privada de Outsourcing que brinda servicios de manera remota no cuenta con un SGSI, lo cual genera un alto e inherente riesgo. Por tanto, se basa en un estudio cuantitativo y experimental preliminar. La muestra estaba formada por 20 empleados de TI. Tras la introducción del SGSI, se intensificó el seguimiento y se constató que los empleados encuestados tienen actualmente un buen grado de conocimientos: el 35% y el 40% de los encuestados tienen un nivel medio de conocimientos. Esto refleja una mejora significativa en la organización.

Incluso para Achmadi et al., (2018) el centro de datos debe estar protegido física y lógicamente para proteger el sistema informático de ataques a la seguridad. Cualquier violación, como el robo de información, la denegación de servicio y el acceso no autorizado, puede tener consecuencias negativas para la empresa, como la pérdida de ingresos, reputación y confianza de los clientes. Implantar un SGSI puede ayudar a definir, gestionar y aplacar las amenazas. La norma generalmente aceptada para un SGSI es la ISO 27001, pero, por lo que sabemos, no existe ninguna norma SGSI específica desarrollada para los centros de datos. Las normas existentes, como la ISO 27001, están diseñadas para la seguridad general de la información y pueden utilizarse en distintos entornos. En este estudio

se aplicó un marco SGSI desarrollado específicamente para que los centros de datos y se gestionan la disponibilidad, confidencialidad e integridad de la seguridad de la información. Se trata de aplicar una perspectiva humana, de procesos y tecnológico a la seguridad de la información en el database. Se ha desarrollado sobre la base de la norma ISO 27001, Anexo A. Este estudio ayudó a demostrar que mediante la aplicabilidad de este marco SGSI, la dirección redujo las amenazas a la seguridad en el centro de datos en un 17.8%.

Por otro lado, Martinez (2020) afirma que existen beneficios en utilizar metodologías para implementar un SGSI de manera que se pueda mitigar los riesgos y preservar los 3 pilares que garantizan la seguridad de la información. Utilizó una investigación exploratoria, descriptiva, de manera que se pueda explicar los beneficios de cada metodología. Como muestra se considera a 25 empresas entre públicas y privadas. Luego de explicar los beneficios a las organizaciones, los resultados indican que el 84% de las empresas están dispuestas a aplicar una metodología, el 16% restante no cuenta con el presupuesto. Asimismo, se muestra que la metodología más votada en las empresas privadas es la familia de la ISO 27000 con un 24%.

En ese sentido, Sánchez (2021) afirma que una cooperativa de ahorro no cuenta con SGSI implementado, se encuentra muy expuesta su seguridad de la información, a todos tipos de ciberataques, provocando pérdidas a la organización. Se basó en un estudio experimental descriptivo, de enfoque cuantitativo. Se consideran a 21 personas para la muestra. Los resultados revelan que el 90% considera que la seguridad de la información es vital y que no se cuenta con estrategias para proteger la información, en cuanto a las vulnerabilidades se encuentra que el 14% es vulnerable, 48% medianamente vulnerable y 38% muy vulnerable. Se concluye que implementar un SGSI en la cooperativa, mejora y reduce el nivel en la exposición al riesgo respecto a la información y su seguridad.

Igualmente, para Fonseca et al (2021) la organización Geoconsult CS, un SGSI es una herramienta importante para administrar y controlar la seguridad de la información, ya que concede preservar y garantizar los pilares de seguridad

respecto a los activos y reducir el nivel del riesgo, ya sea mitigando, transfiriendo o controlándolos. Es por ello, que se decidió aplicar un modelo de SGSI a un caso real. Como resultado satisfactorio, obtuvieron que gracias a la aplicabilidad del estándar NTC-ISO/IEC 27001, se identificaron activos, las vulnerabilidades y los riesgos aplicados. Así mismo se observa la necesidad de añadir un plan de continuidad para actualizar el SGSI. Los resultados demuestran que se llega a un 21% de cumplimientos de las condiciones mínimas, 49% de cumplimiento en los controles referidos al Anexo A, finalmente con respecto a las vulnerabilidades se encuentra un 76% son de parámetros conforme, 20% no críticas y 4% críticas. Como conclusión se afirma que el aplicar un modelo de SGSI es crucial dentro de una organización ya que permite obtener un valor diferencial en las operaciones de los servicios, mejorando los procesos.

En ese misma línea, Mirtsch, Kinne y Blind (2021) en su estudio, exploran la adopción una norma, la ISO/IEC 27001 (SGSI) en Alemania y los factores que impulsan a las organizaciones a certificarse, utilizaron el database de Mannheim Enterprise Panel (MUP) como muestra, encuentran que, tras una década de la publicación de la norma, el crecimiento de aceptación no es el esperado, aun así, de la mayoría de las empresas alemanas que buscan certificarse, la mitad pertenece al sector de servicios de TI. Uno de los factores más críticos para la implementación del SGSI en las empresas grandes, es la certificación. Se mostró que, de las 2664 empresas identificadas, solo 792 cuentan con la certificación, lo que representa aproximadamente el 60% de los certificados válidos. Finalmente concluyen que, la implementación de la norma SGSI es un buen punto de partida para aumentar el nivel general de seguridad y que las empresas se ven beneficiadas al implementar el SGSI sin necesidad de certificarse.

De la misma manera, Mirtsch (2021) afirma que su estudio pretende ampliar los conocimientos sobre la implantación de un SGSI acorde a la normativa internacional ISO/IEC 27001, ampliamente utilizada. Presenta los motivos, las repercusiones experimentadas y los obstáculos relacionados con la implantación deI estándar internacional ISO/IEC 27001 utilizando data de una encuesta realizada a 125 empresas alemanas con certificación ISO/IEC 27001. Se analizó

la adopción del estándar internacional ISO 27001 a través del prisma de las innovaciones organizativas preventivas. Los resultados revelan un 31,6% en el impacto preventivo, el 46% en el impacto del cumplimiento legal, el 47,1% en el impacto del mercado y el 45,9% en la percepción global de los beneficios. Se concluye que existe una necesidad legítima de considerar el enfoque de prevención como una característica distintiva de la norma ISO 27001 en comparación con otras normas.

Además, Alsahafi et al., (2022) afirma que en su investigación se analiza el cumplimiento del marco NCA-ECC por parte de las organizaciones saudíes en relación con la implantación de un SGSI. Se constató que el cumplimiento del SGSI sólo garantiza parcialmente el cumplimiento del NCA-ECC. Se seleccionaron como muestra tres universidades públicas sauditas certificadas con un SGSI y se evaluó su cumplimiento del NCA-ECC en cuanto a la aplicación de los controles esenciales de un SGSI (29 controles en total). Los resultados revelan que la aplicación de un SGSI no es suficiente para el cumplimiento del NCA-ECC, ya que varios controles esenciales sólo se aplican parcialmente o no se aplican en absoluto. Se observa que, de los 29 controles esenciales, sólo 12 se aplican (41%), 13 se aplican parcialmente (45%), 3 no se aplican y, por último, (4%) no se aplican en las universidades. Puede concluirse que las organizaciones con certificación ISO/IEC 27001 sólo cumplen los requisitos de NCA-ECC en el 64% de los casos (ya que el 41% de los controles están totalmente implantados y el 45% lo están parcialmente, lo que supone un 23%, es decir, una media del 64%). Este marco puede ayudar no sólo a las universidades, sino también a todas las organizaciones de Arabia Saudí, a migrar rápidamente y en menos tiempo de ISO/IEC 27001 a NCA-ECC-ECC.

Del mismo modo, Razikin y Soewito (2022) en su trabajo proponen un modelo para el diseño de sistemas de seguridad informática basado en el análisis de riesgos y el marco de ciberseguridad ISO/IEC 27001. El objetivo del modelo propuesto es encontrar el mejor sistema de seguridad para mitigar las amenazas a la seguridad. El modelo construido es capaz de vincular el valor de prioridad de reducción de amenazas basado en la puntuación relativa de amenazas con la puntuación relativa que obedece a la norma ISO 27001. El valor de prioridad de

reducción de amenazas es clave para priorizar las recomendaciones para construir un SGSI fundamentado en el marco ISO/IEC 27001. Además, el impacto de una correcta aplicación de las buenas prácticas para el sistema de seguridad informática se comprueba realizando ataques de seguridad directamente sobre el sistema en construcción. Por último, se realiza una evaluación estadística del sistema construido sobre la base de las recomendaciones del sistema de seguridad informática. Los resultados arrojan una puntuación media de conformidad con la norma ISO/IEC 27001 aumentó del 36,27% al 82,37%. Además, la puntuación media de criticidad de la amenaza basada en 12 tipos de amenazas disminuyó de 8,75 a 4,00. Los resultados de la evaluación de la relación entre la aplicación de las recomendaciones del sistema de seguridad y la mitigación de los ciberataques muestran un aumento de la eficacia de la mitigación de los ciberataques de una puntuación media del 18,32% al 40,74%.

De igual forma, Lopes et al., (2019) afirman que proteger la data personal ha sido uno de los temas más debatidos últimamente y motivo de gran preocupación entre las organizaciones. Se considera un cambio importante en estos 20 años, propuesto por la UE. Su objeto de estudio es en qué medida la implantación de las normas ISO 27001 puede representar un factor que facilite a las organizaciones el cumplimiento del RGPD. Se considera apropiado seguir un método de investigación cuantitativo. Por lo tanto, se analiza el contenido de los 15 sitios web, se presentan de modo resumido algunos aspectos que merecen ser destacados a la hora de evaluar si la puesta en marcha de la norma ISO 27001 podría ser un factor facilitador para que las organizaciones cumplan con el RGPD. Tras analizar los sitios web en relación a la siguiente afirmación: si la implantación de la ISO 27001 identifica la data personal como un activo de seguridad de la información, encontramos que en 9 (60%) sitios hay información que está de acuerdo con esta afirmación y en los otros 6 (40%), no hay mención alguna al respecto. Se observa, 11 sitios (73%) están de acuerdo en que la norma ISO 27001 es un excelente marco para el cumplimiento del RGPD de la UE, 3 (20%) no mencionan este aspecto, y sólo 1 (7%) de los sitios web analizados se muestra en desacuerdo. A partir de estos resultados, concluye que existe consenso en que, aunque la norma ISO 27001 no incluye ciertos controles importantes, su aplicación

se considera un factor que facilita a las organizaciones el cumplimiento del nuevo reglamento de datos personales.

Asimismo, Chinyemba y Phiri (2018) manifiestan que las organizaciones públicas de Zambia son vulnerables a los ataques internos debido a una serie de causas entre los que se incluyen la complejidad tecnológica, la escasez de personal, los beneficios financieros, la ausencia de políticas, procedimientos y directivas de seguridad y la falta de adopción y aplicación de marcos y normas de seguridad internacionales como ISO 27000 y COBIT. Las amenazas internas pueden clasificarse en tres dimensiones: sabotaje informático, fraude financiero y robo de propiedad intelectual. Este estudio revela los resultados de tres organizaciones públicas de Zambia. Estas se encuentran entre las pocas que parecen reconocer las ciberamenazas y han adoptado parcialmente algunas partes de las prácticas básicas de seguridad y normas internacionales de seguridad de la información como COBIT 5.0 y el estándar ISO 27001.

El estudio tiene como objeto evaluar las brechas de seguridad utilizando el estándar internacional ISO 27001:2013 del SGSI. El enfoque del estudio utilizado fue cuantitativo y cualitativo con cuestionarios de encuesta y entrevistas como herramientas de evaluación para el acopio de datos empíricos. El estudio muestra que el sector público de Zambia tiene retos relacionados con la mitigación de los ataques internos que requieren esfuerzos considerados en el desarrollo de medidas para la mitigación de estos desafíos con el fin de garantizar la preparación nacional de seguridad cibernética y la mejora de la privacidad de los datos. Según el estudio, la mayoría de las organizaciones evaluadas carecen de políticas disuasorias de la seguridad interna, como el control de acceso, los acuerdos de confidencialidad (NDA), la selección previa a la contratación y el uso inaceptable. Además, los resultados indican que, en gran número, las organizaciones públicas no han hecho ningún esfuerzo para prepararse para la ciberseguridad, mientras que sólo alrededor del 33% ha adoptado algunas prácticas básicas de seguridad. Además, utilizando la Teoría de Redes de Actores (ANT) y la Teoría del Comportamiento Planificado (TPB), el estudio propuso un modelo de mitigación de

información privilegiada expeditivo con énfasis en la conciencia del usuario y el control de acceso, considerando que es difícil modelar el comportamiento humano.

Referentes a las bases teóricas, tenemos como **variable independiente** el SGSI, la NTP ISO/IEC 17799 (2007) establece que la información es el recurso cuyo valor es sumamente valioso e imprescindible para una organización como otros activos empresariales críticos y que debe protegerse en consecuencia. Con la creciente conectividad, se encuentra sometida a un peligroso número de amenazas y vulnerabilidades. La información adopta muchos modos, sea cual sea su forma, se intercambie o almacene como se almacene, debe salvaguardarse de forma adecuada. La seguridad de la información garantiza la continuidad de la actividad, minimiza los daños en la empresa y maximiza el rendimiento de la inversión y aquellas oportunidades ligadas al negocio. Mediante la aplicación de un conjunto de controles se puede conseguir un SGSI, en base a políticas, procedimientos, directivas, ejercicios, estructuras organizativas y capacidades a nivel de software y hardware. Estos deben ser aplicados, supervisados, auditados y mejorados según lo amerite, de manera que se alcance los objetivos específicos correspondiente a la seguridad y del negocio de la empresa. Es por ello, que la International Electrotechnical Commission (CEI) y la International Organization for Standardization (ISO) han creado comités técnicos con el fin de desarrollar y respaldar el conjunto de herramientas internacionales del SGSI. La ISO 27001 es un marco de nivel internacional ISO/IEC JTC 1 SC27 WG1 para el SGSI (ISO/IEC 27001: 2013; Boehmer, 2008).

Asimismo, se afirma que la finalidad principal de la seguridad de la información es salvaguardar los activos valiosos de la empresa (Peltier, 2013); que la información y la seguridad de la información adicionalmente se define como un subgrupo del gobierno eficaz de las TI (Calder, 2009). En los últimos años, las normas y marcos pertinentes, así como la bibliografía, han proporcionado una explicación práctica de la creciente dependencia de casi todas las organizaciones del tratamiento seguro de la información pertinente (Álvaro, 2009). Como consecuencia, se ha desarrollado y validado en la literatura una lista de normas y medidas de buenas acciones direccionadas y desarrolladas para el correcto y

oportuno SGSI, en este sentido se afirma, que la serie ISO 27000 es la norma principal para el desarrollo y funcionamiento del SGSI. (Boehmer, 2008)

En este sentido, Merino y Cañizares (2012) explican que la seguridad de la información es esencial y debe ser considerada en todo proceso de negocio, ya sea manual o automatizado, porque todo proceso involucra personas, tecnología y las vinculaciones con los asociados del negocio, clientes y/o terceros, por lo que la información de una empresa es un componente esencial de todo proceso. Además, Joyanes (2015) afirma que la seguridad de la información implica la puesta en práctica de un grupo de acciones para mantener los pilares de seguridad en los activos de un sistema informático, incluyendo hardware, software, data que se procesa, almacena y transmite. En este sentido, Dutton (2016) afirma que los activos de información son una pieza o conjunto de data en poder de una organización que se identifica y gestiona como un todo para que pueda ser efectivamente comprendida, compartida, protegida y recuperada para crear el máximo valor. Es algo que no puede sustituirse sin coste, tiempo, competencias y recursos.

La norma ISO 27001 abarca estipulaciones, directrices para la organización, implantación, funcionamiento y mejora de un SGSI. Los requisitos están ampliamente diseñados para satisfacer las necesidades de todas las organizaciones, pero varían en función del tamaño de la organización, sus objetivos, modelo de negocio, ubicación, etc. Aunque la norma ISO 27001 no contiene requisitos para tecnologías específicas (Brenner, 2007), sí incluye requisitos para los procesos básicos de un SGSI y, por lo tanto, esta norma es la base para definir los procesos básicos de un SGSI en este estudio.

Esta evolución se ve respaldada por el hecho de que el debate sobre la relación coste-beneficio ha influido en las prácticas de los últimos años con respecto a la información y su seguridad (Whitman y Mattord, 2013). La pertinencia y el beneficio son factores claves para maximizar el éxito de un SGSI. La información y su importancia se encuentra justificada en el costo de protegerla (Peltier, 2013). La conciencia de la finalidad es esencial para ordenar los

procedimientos de un SGSI en la empresa con respecto a su misión organizacional (Fakhri, Fahimah e Ibrahim, 2015). La alineación con la organización y el beneficio son factores importantes para el éxito de un SGSI, y los artículos de estudio deben abarcar ambos aspectos de forma que permitan identificar los procedimientos del SGSI indispensable y adecuados como parte integrante de cualquier SGSI.

Para Nancylia et al., (2014) está claro que, para toda organización, la información es el activo más valioso y debe estar bien protegido, por tal, debe ser accesible y estar protegida de accesos no autorizados. Si la información es utilizada por individuos sin autorización, puede usarse con los fines de perjudicar a la organización. Es por ello, que la seguridad de la información debe aplicarse de forma correcta para mitigar y reducir en lo más mínimo las pérdidas en la organización. Se deben salvaguardar los pilares de seguridad (confidentiality, integrity and availability) que garanticen la seguridad.

La data y la información que son importantes para las empresas, se convierten en activos críticos. Ya que las organizaciones se vuelven más susceptibles a diversas vulnerabilidades y amenazas contra la seguridad de la información, por lo cual es primordial y muy necesario abordar continuamente las cuestiones de seguridad. Una correcta gestión de riesgos brinda una perspectiva valiosa para cuantificar la seguridad mediante la valoración, mitigación y evaluación de riesgos (Borek, Parlikad, Webb y Woodall, 2013).

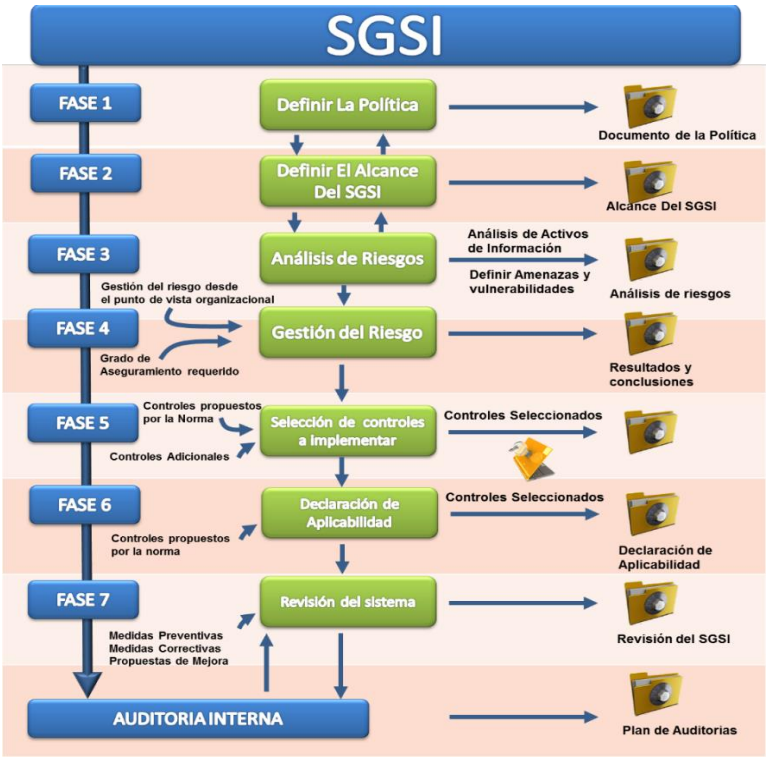
Para escudar los activos críticos de información en toda entidad, un proceso fundamental, es gestionar los riesgos de forma adecuada, de manera que se salvaguarde la información y su seguridad. Normalmente involucra establecer y evaluar los activos, el análisis de las amenazas de los riesgos y el planeamiento y ejecución de medidas preventivas (Breier y Schindler, 2014). Un factor de éxito en el procedimiento, es la acción de evaluar de forma precisa y eficaz los riesgos de la información y su seguridad, y es muy necesario y de suma importancia para comprender y entender las circunstancias o condiciones de seguridad de la información y los riesgos ligados a los activos empresariales.

Como un enfoque teórico específico para el SGSI se encuadra la metodología ISO/IEC 27001:2014, ya que requiere un esfuerzo centrado en garantizar el SGSI. Por lo mencionado, es indispensable desarrollar un estándar que plantee sistemáticamente esta responsabilidad y la fundamenta en objetivos precisos de seguridad y en una correcta y eficiente evaluación de los riesgos vinculados a la información en una institución.

Finalmente, la ISO/IEC 27001 (2013) afirma que la implantación de un SGSI es un conjunto de acciones estratégicas para una empresa y que debe ajustarse a sus objetivos, requerimientos de seguridad, procesos organizativos, tamaño y complejidad. ISO/IEC 27001:2013 es el marco internacional para los SGSI que pueden utilizar las empresas. Esta norma puede utilizarse para realizar auditorías y monitorear la eficacia de un SGSI (Nancylia et al., 2014). En la figura 1 podemos observar las fases del marco.

Figura 1

Fases – ISO 27001



Nota. Adaptado de ISO 27001 [imagen], por Normas ISO (https://www.normas-iso.com/iso-27001/)

La **variable dependiente** es la gestión de riesgos, el estándar internacional ISO 31000 (2009), menciona que todas las acciones de una entidad están relacionadas con el riesgo. Las organizaciones gestionan los riesgos identificándolos, analizándolos y evaluando si es necesario modificarlos para que cumplan sus criterios. Todas las entidades gestionan los riesgos en cierta medida.

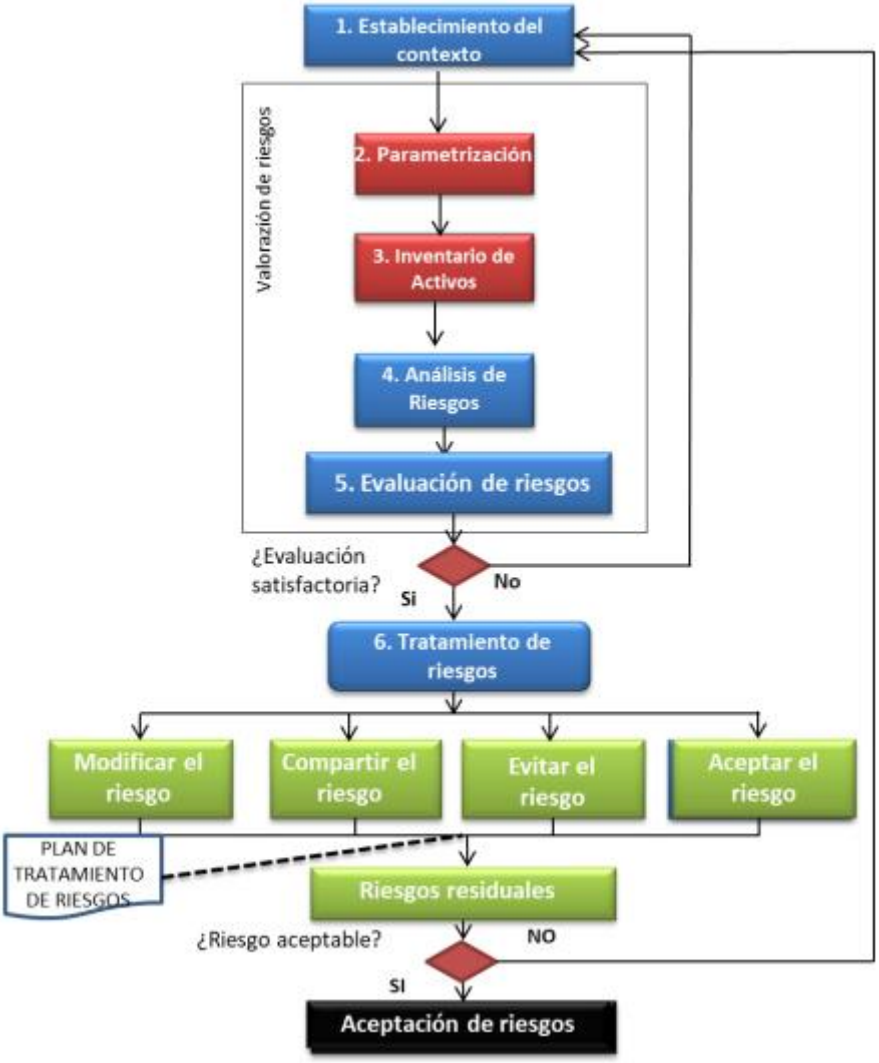
Asimismo, el estándar nacional NTP ISO/IEC 27005 (2018), afirma que la gestión de riesgos tiene como su fortaleza ser iterativo en el contexto de evaluar y/o tratar los riesgos. Utilizando una perspectiva iterativa en el estudio de riesgos, aumenta en cada repetición, la profundidad y el detalle de la estimación. Asimismo, ofrece un buen equilibrio al reducir el tiempo y esfuerzo necesario para establecer los controles y la garantía de que los riesgos elevados se evalúan. correctamente. En la figura 2 podemos visualizar las fases del estándar.

Según el SP 800-30 (NIST), debe interpretarse del siguiente modo: la metodología utilizada por la autoridad local se basa en la concepción de métodos de gestión de riesgos informáticos mundialmente reconocidos, como la ISO 31000, Mageri, Montecarlo e ISO 27005, en las que la gestión de riesgos se reconoce como pieza crítica de las buenas prácticas de gestión. Se trata de un proceso iterativo de múltiples fases que, cuando se aplica de forma coherente, permite una mejora continua.Es un procedimiento lógico y metódico de contextualizar, definir, evaluar, valorar, gestionar, supervisar y comunicar los riesgos inherentes, de manera que permite a las empresas aminorar las pérdidas e incrementar las oportunidades. La gestión de riesgos se enfoca en la explotación de oportunidades, así como en la prevención o reducción de pérdidas.

Agregando a lo anterior, Pritchard (2015) describe con más detalle el concepto de proceso de gestión de riesgos y afirma que la acción ante la amenaza un riesgo es clave del proceso de gestión de riesgos, que define qué acciones se llevarán a cabo para la evaluación y cuantificación del riesgo. El autor enfatiza en la criticidad de responder al riesgo antes de que este haya sido evaluado y definido. En este estudio se optó por aplicar la metodología de acuerdo con la norma NTP ISO/IEC 27005.

Figura 2

Proceso de gestión del riesgo en la seguridad de la información – ISO 27005



Fuente: ISO 27005:2011

La evaluación de riesgos se apoya en la normativa nacional NTP-ISO/IEC 27005:2018, resulta en exponer la definición del valor de cada activo crítico de información, identificar las amenazas válidas, de las vulnerabilidades potenciales, la definición de los controles preventivos existentes y su impacto en los riesgos identificados, establecer las consecuencias potenciales y, por último, la priorización de los riesgos resultantes y su clasificación de acuerdo con los criterios de evaluación de riesgos en el contexto definido

Seguidamente, estándar nacional NTP ISO/IEC 27005 (2018), define que establecer el contexto es sumamente necesario y crucial para una correcta y eficaz administración de riesgos de seguridad de la información, esto significa definir los enfoques básicos y necesarios, la delimitación y el alcance, y constituir una adecuada organización para garantizar el éxito en la aplicación del SGSI.

En este sentido, la identificación de los riesgos tiene como finalidad identificar, definir y gestionar aquellos riesgos que ayudan o dificultan a las organizaciones a la consecución de resultados (ISO 31000, 2018). También es importante que toda la información oportuna, relevante y, lo que es más importante, actualizada esté disponible para gestionar los riesgos. Es la determinación de identificar lo que podría suceder para causar una pérdida crítica y establecer cómo, cuándo y el por qué podría ocurrir (NTP-ISO/IEC 27005, 2018).

De todos estos enfoques, las dimensiones de las variables de este estudio se enmarcan en términos de análisis de riesgo, evaluación de riesgo y tratamiento de riesgo. ISOTools (2019) caracteriza el riesgo como la probabilidad de sufrir perjuicios o carencias. Puede ser un riesgo relacionado con el ser humano o un riesgo no relacionado con el ser humano. Por otro lado, es más probable que la amenaza sea un componente del riesgo causado por una acción que puede tener un resultado inesperado o indeseable. Las consecuencias de una amenaza pueden causar una serie de perjuicios: pérdida de ventas o de clientes, pérdida de diferenciación en el mercado, costes de respuesta a incidentes y de reparación, costes de multas o sanciones, etc.

Adicionalmente a lo mencionado, el **análisis de riesgos** se utiliza para el riesgo, su naturaleza y sus características, incluido el nivel potencial de riesgo. También es esencial realizar la valoración en detalle, de todas las incertidumbres, los orígenes del riesgo, las consecuencias, las probabilidades, los eventos e incidentes, los escenarios, los controles y su desempeño (ISO 31000, 2018). El análisis de riesgos se realiza en diversos niveles de detalle tomando en cuenta la

gravedad de los activos críticos, la magnitud de las debilidades y de los incidentes en los que la empresa se vio comprometida (NTP ISO/IEC 27005, 2018).

Por último, el estándar nacional NTP ISO/IEC 27005 (2018), define la **evaluación de riesgos**, como el uso de los conocimientos procedentes del análisis de riesgos para tomar decisiones futuras. En este contexto, Araujo (2017) afirma que el estudio de riesgos permite a una organización considerar los riesgos potencialmente perjudiciales para el logro de sus objetivos y, por lo tanto, para las metas de la organización. En la práctica, se lleva a cabo especificando cómo se realizará el estudio de las cuestiones relacionadas únicamente con los riesgos, cuyo objetivo es presentar toda la información relacionada con los riesgos para que se puedan evaluar sus consecuencias, duración, recurrencia e impacto. La evaluación de riesgos es el motivo en el que se basan todas las decisiones. Requiere que el producto del análisis de riesgos se compare con los requisitos de riesgo definidos para establecer cuándo se requieren nuevas medidas (ISO 31000, 2018).

En este sentido, Halvorson (2008) afirma que evento o incidente, es un riesgo si amenaza a los propósitos de una organización; estos riesgos tienen el potencial de ocurrir y son calculados multiplicando el impacto por la probabilidad. Por otro lado, según Peltier (2014), el procedimiento de la gestión de riesgos implica definir el riesgo, tasar la posibilidad de ocurrencia y tomar acciones que mitiguen los riesgos potenciales.

El **tratamiento de riesgos** es uno de los pasos en el procedimiento de de gestionar los riesgos, implica la aplicabilidad de un programa de reacción a los riesgos, el seguimiento y la activación de eventos, la aplicación de planes de preventivos y/o reactivos, y el seguimiento de los riesgos emergentes (Olaf y Pebbling, 2010).

La evaluación de riesgos se apoya en el estándar nacional NTP-ISO/IEC 27005:2018, resulta en exponer la definición del valor de cada activo crítico de información, identificar las amenazas válidas, de las vulnerabilidades potenciales,

la definición de los controles preventivos existentes y su impacto en los riesgos identificados, establecer las consecuencias potenciales y, por último, la priorización de los riesgos resultantes y su clasificación de acuerdo con los criterios de evaluación de riesgos en el contexto definido

El proceso de seguridad de la información tiene procedimientos y controles que estructuran la operatividad real del SGSI y son los documentos indispensables que garantizan la planificación, el desarrollo y el control. El contexto de la evaluación de riesgos nos describe la estrategia de trabajo que debe aplicarse, los criterios de riesgos y niveles aceptables. El plan de gestión de riesgos describe las actividades, medios, responsabilidades y prioridades de la gestión de riesgos. Finalmente, la declaración de aplicabilidad enumera los controles identificados en el SGSI y su estado de intervención, así como la justificación por la que se han incluido o excluido.

III.METODOLOGÍA

Tipo y Diseño de Investigación

Tipo de estudio

La finalidad de este estudio de tipo aplicada, es que el proceso de gestión de riesgos mejore mediante la introducción de un SGSI y reducir los riesgos identificados utilizando la técnica PDCA, que puede definirse como investigación aplicada en el sentido de que puede mostrar resultados concretos en poco tiempo (Valderrama, 2013).

Diseño

En este estudio es pre-experimental como lo describen Hernández et al., (2014), es decir, un diseño en el cual se aplica un tratamiento pre-experimental a la población antes del tratamiento experimental, luego se aplica el tratamiento y finalmente se aplica un diseño post-experimental, donde la medida inicial es la medición del nivel de la variable dependiente en la población antes del estímulo, y se monitorea a la población cuando se aplica este diseño. A efectos de este estudio, se ilustra esquemáticamente en la próxima figura.

Figura 3

Diseño Pre-Experimental

Fuente: Hernández-Sampieri & Mendoza (2020, p. 163)

G: Grupo experimental, utilizado para evaluar la gestión de riesgos y medir análisis del riesgo, la evaluación del riesgo y el tratamiento del riesgo. X: Grupo de tratamiento, que representa la utilización del SGSI en la gestión de los riesgos infraestructurales y operativos en las organizaciones públicas, a partir de dos evaluaciones (pre prueba y post prueba). M1: Pre-test, que mide el grupo experimental antes de la utilización del SGSI en la gestión de los riesgos. M2: Post-test, que mide el grupo experimental después de la utilización del SGSI en la gestión de los riesgos. La medición de los dos grupos se realiza por medio de cuestionarios, observaciones, tests, etc.

Enfoque

Este estudio sigue el enfoque cuantitativo de Hernández et al., (2014), quien explica que la recolección de datos como base de mediciones numéricas para la comprobación conductual y teórica admite la comprobación de hipótesis y el análisis estadístico.

Variables y operacionalización

Variable Independiente: SGSI

Definición conceptual:

El estándar nacional NTP-IO/IEC 27001 (2014) constituye que un SGSI mantiene el aspecto confidencial, íntegro y disponible de la información por medio del establecimiento de procedimientos de gestión de riesgos y proporciona garantía de que los riesgos se gestionan adecuadamente.

Definición operacional:

La R.M. Nº 004-2016-PCM autoriza la implementación obligatoria de la NTP ISO/IEC 27001:2014 sobre el SGSI en las instituciones públicas que son parte del sistema nacional de información. El SGSI implica el establecimiento de un plan

para diseñar, implementar y mantener un conjunto de políticas, directivas, manuales, instructivos, actividades e indicadores para la gestión eficaz de la información que garantice el aspecto íntegro, confidencial y disponible con respecto a la información. Al emplear el método de gestión de riesgos fundamentado en la ISO 27005 en el área infraestructura y operaciones de una organización pública proporciona una seguridad a los 3 pilares, mediante la implementación de diversas actividades.

Variable Dependiente: Gestion de Riesgos

Definición conceptual:

Para Peltier (2014), el procedimiento de la gestión de riesgos implica definir el riesgo, tasar la posibilidad de ocurrencia y tomar medidas para mitigar los riesgos potenciales.

Definición operacional:

La gestión de riesgos se encuadra en 3 dimensiones: análisis del riesgo, evaluación del riesgo y tratamiento del riesgo. Se puntualiza el riesgo como la probabilidad de sufrir daños o pérdidas (ISOTools, 2019). El control de riesgos es uno de los pasos en el procedimiento de gestión de riesgos, trae consigo la desarrollar y poner en práctica un plan de reacción a los riesgos, el seguimiento y la activación de eventos, la aplicación de planes de preventivos y/o reactivos, y el seguimiento de los riesgos emergentes (Olaf y Pebbling, 2010).

Población y muestra

De acuerdo con la NTP ISO 27005, la identificación de los activos debe llevarse a cabo de manera detallada y adecuada que proporcione información relevante para una correcta evaluación de riesgos basada en un proceso documentado de recopilación de información en consulta con el personal profesional y técnico en el desarrollo de los sistemas operativos, controles y funciones de seguridad de la

información. En este contexto, según Valderrama (2013), una población es una colección de objetos o cosas que pueden ser de tamaño finito o infinito, comparten características o propiedades comunes y pueden ser observadas.

En este estudio se consideró una población conformada por 74 activos y 114 controles. Según Hernández, citado en Castro (2003), una muestra es equivalente a una población si ésta contiene menos de 50 sujetos; por lo tanto, si la población no supera estas unidades, no hay necesidad de muestrear; la muestra en este estudio será toda la población.

Técnicas e instrumentos de recolección de datos

El método utilizado en este estudio para calcular las variables de la investigación es la observación mediante tablas de observación, que permite recoger datos de cada indicador para establecer el verdadero estado del problema de la gestión del riesgo (Hernández et al., 2010).

Validación y confiabilidad de los instrumentos

Validación de los instrumentos

En general Hernández et al., (2014) sostiene que la legitimación de un artefacto de medición alude al grado en que el artefacto de medición calcula de manera certera la variable que se supone debe medir. La legitimación por expertos consiste en preguntar a los expertos respecto a la pertinencia, oportunidad, claridad y adecuación de los diferentes elementos de un determinado instrumento de medición.

Tabla 1

Validez del instrumento Ficha de observación de análisis, nivel y número de controles aplicados

Experto	El instrumento de medición presenta				Condición final
	Pertinencia	Relevancia	Claridad	Suficiencia	
LEZAMA GONZALES, PEDRO	si	si	si	si	Aplicable
ACUÑA BENITES, FRANK	si	si	si	si	Aplicable
MUÑOZ LA RIVA, WALDIR	si	si	si	si	Aplicable

El cuadro señala que los expertos consideran que el cuestionario de análisis de riesgo, nivel de riesgo y número de controles aplicados contiene ítems con pertinencia, relevancia, claridad y suficiencia que proporcionan una verificación lícita de la variable dependiente respecto a la gestión de riesgos.

Confiabilidad de los instrumentos

Según Correa (2019), el procedimiento de confiabilidad se refiere a un método utilizado por los investigadores para definir la relación básica entre el objeto y el objeto de la investigación mediante la aplicabilidad de reglas y métodos, esta técnica permite definir si los instrumentos utilizados para recolectar información son confiables o no. Debido a ello, es necesario realizar mediciones con base en un coeficiente.

Tabla 2

Niveles de confiabilidad

Valor	Confiabilidad
0.80 – 1.00	Elevado
0.60 – 0.80	Aceptable
0.40 – 0.60	Regular
0.20 – 0.40	Bajo
0.00 – 0.20	Muy Bajo

Fuente: Ruiz (2002, p.70)

Según Galindo (2020), este es un procedimiento mediante el cual, después de obtener mediciones de una misma muestra con un mismo instrumento en dos períodos, si la correlación entre ellas se encuentra en un nivel aceptable, se dice que el instrumento es confiable.

El instrumento se sometió a una prueba piloto con el software SPSS v. 25 y, a continuación, se analizó mediante alfa de Cronbach.

Tabla 3

Estadística de fiabilidad

	Estadísticas de fiabilidad	
Dimensión	Alfa de Cronbach	N de elementos
Nivel de Riesgo	0,903	74
Nivel de Probabilidad	0,84	74
Numero de Controles	0,794	114

Se mostró una alta fiabilidad con un alfa de Cronbach para el ítem "Nivel de riesgo" de 0,903, ítem "Nivel de probabilidad" de 0,84 y el ítem "Número de controles" de 0,794.

Procedimientos

El procedimiento es el siguiente: Al principio de la recogida de datos, se debe llegar a un acuerdo con el responsable de TI y los técnicos pertinentes. Se explicará el propósito que se pretende alcanzar con la aplicación de un cuestionario y las dimensiones que se evaluarán para cada variable identificada, así como su importancia para la recogida, el análisis y la explicación de los datos. Tras obtener el acuerdo de los informáticos, se diseñará la encuesta y se definirán las herramientas de recogida de datos. A continuación, se formularán los objetivos de la encuesta, empezando por la identificación y evaluación de los antecedentes que contribuirán al diseño de la encuesta. A continuación, se utilizarán fichas de observación para medir y analizar con más detalle las carencias identificadas en materia de TI. Del mismo modo, se analizarán los datos recogidos para elaborar

tablas interpretadas que permitan la valuación de las hipótesis enunciadas en la tesis de investigación.

Método de análisis de datos

El proceso de recogida de la data se llevará a cabo mediante el uso de formularios de observación para recoger datos tanto para el análisis de riesgo, nivel de riesgo como el N° de controles aplicados. Los datos recogidos se utilizarán para crear una matriz de data, recalcular los valores según una escala definida y continuar el análisis para presentar conclusiones y recomendaciones para el informe final. Se utilizarán estadísticas descriptivas e inferenciales para el análisis y presentar los datos recogidos durante el estudio. Estos resultados se presentarán utilizando estadísticas que ayudarán a explicar y comprender el estudio. Se utilizará el procedimiento estadístico inferencial de Wilcoxon para comparar las hipótesis.

Aspectos éticos

Vidal (2018) explica que la ética científica se refiere a una reflexión sobre los valores utilizados para evitar errores en diferentes momentos de la investigación científica, y que la ética científica determina cuándo nos encontramos con errores en la investigación científica. Esta investigación es un trabajo personal del autor. Se utilizó como guía de referencias y citas la 7ª edición de la American Psychological Association (APA). Además, este estudio fue evaluado por el programa Turnitin, que genera un informe de originalidad de acuerdo con la resolución de la Agencia Nacional de Investigación española número 281-2022-VI-UCV. Para la recogida de datos se utilizaron fichas de observación. El alcance de la investigación utilizada fue una auditoría de sistemas y una investigación de seguridad de la información conforme a la RCU N° 0340-2021-UCV.

IV.RESULTADOS

En este estudio, desarrollamos un SGSI se aplicó a la gestión de riesgos en el área de infraestructura y operaciones en una entidad pública para identificar, clasificar y evaluar riesgos y amenazas, y a continuación elaboramos un conjunto de acciones para tratar los riesgos y calcular los indicadores propuestos.

Por último, los resultados se analizaron mediante estadísticas descriptivas e inferenciales presentadas en tablas y gráficos para la interpretación de cada indicador.

Estadística descriptiva

Se comparan los resultados en los dos momentos de la evaluación, es decir, antes y después de la introducción del SGSI

Indicador 1: Nivel de probabilidad

Tabla 4

Resultados descriptivos del Nivel de probabilidad

Estadísticos descriptivos					
	N	Media	Desv. Desviación	Mínimo	Máximo
Nivel Probabilidad (Pre-Test)	74	2,5405	,49315	2,00	3,00
Nivel Probabilidad (Post-Test)	74	1,4703	,49171	1,00	2,00

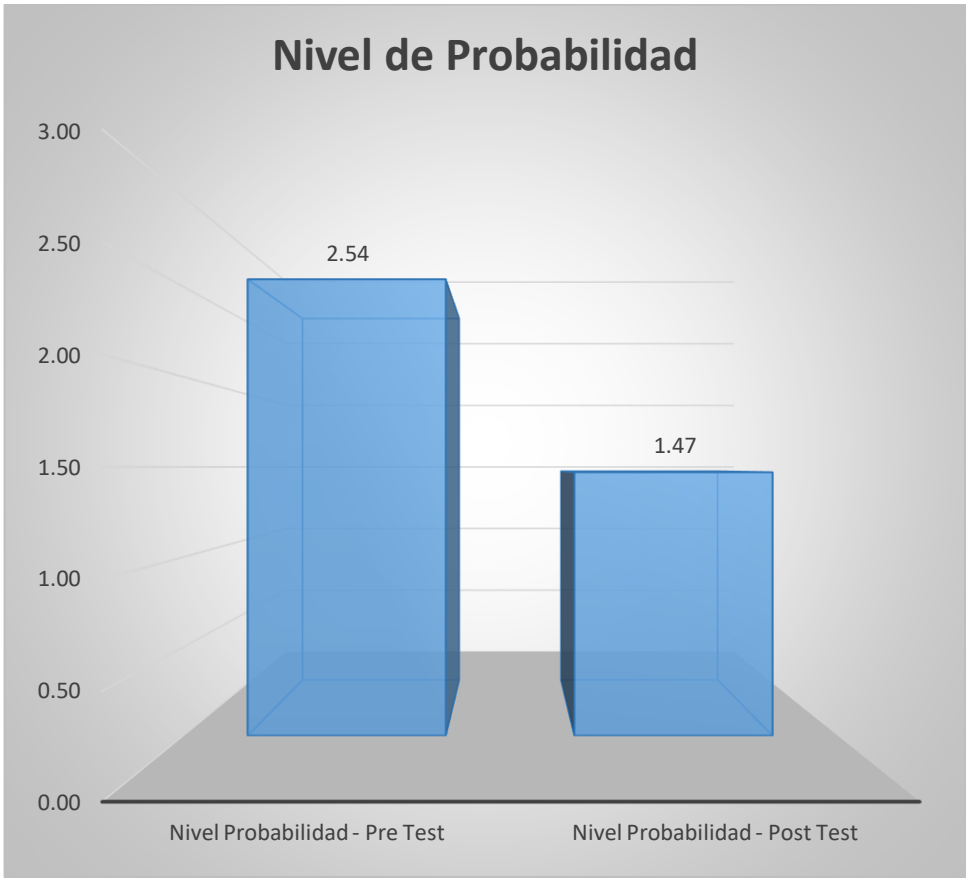
Fuente: Elaboración propia

Como muestra el cuadro 4, los resultados de la verificación previa al SGSI en el nivel de probabilidad es de 2,54 puntos en la media, con una desviación estándar de +/- 0,493 puntos, un máximo de 3 puntos y un mínimo de 2 puntos. En cambio,

los resultados posteriores a la verificación muestran una media en el nivel de probabilidad de 1,47 puntos, con una desviación estándar de +/- 0,491 puntos, un máximo de 2 puntos y un mínimo de 1 punto.

Figura 4

Nivel de Probabilidad antes y después de aplicar un SGSI



Estos resultados reflejan que existe una clara diferencia en el nivel de probabilidad antes y después de la introducción del SGSI.

Indicador 2: Nivel de riesgo

Tabla 5

Resultados descriptivos del Nivel de riesgo

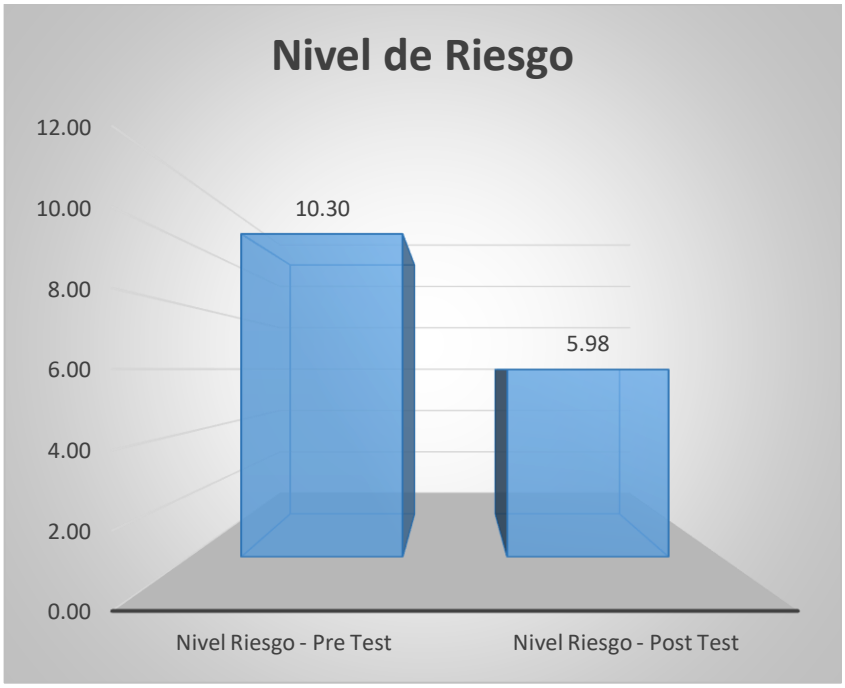
Estadísticos descriptivos					
	N	Media	Desv. Desviación	Mínimo	Máximo
Nivel Riesgo (Pre-Test)	74	10,2973	2,13085	8,00	15,00
Nivel Riesgo (Post-Test)	74	5,9847	1,90727	4,00	8,67

Fuente: Elaboración propia

Como muestra el cuadro 5, los resultados de la verificación previa al SGSI en el nivel de riesgo es de 10,30 puntos en la media, con una desviación estándar de +/- 2,13 puntos, un máximo de 15 puntos y un mínimo de 8 puntos. En cambio, los resultados posteriores a la verificación muestran una media en el nivel de riesgo de 5,98 puntos, con una desviación estándar de +/- 1,91 puntos, un máximo de 8,67 puntos y un mínimo de 4 puntos.

Figura 5

Nivel de Probabilidad antes y después de aplicar un SGSI



Estos resultados reflejan que existe una clara diferencia en el nivel de riesgo antes y después de la introducción del SGSI.

Indicador 3: Número de controles aplicados

Tabla 6

Resultados descriptivos del Número de controles aplicados

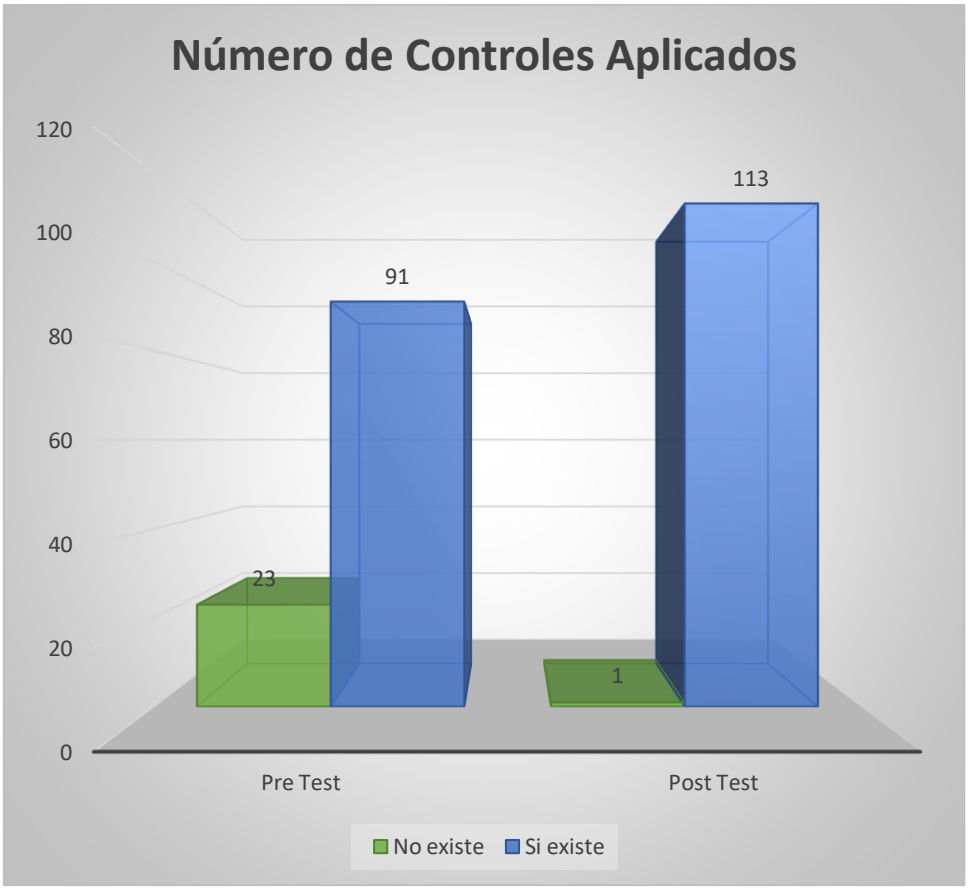
Tabla cruzada de Control * Momento Experimental					
			Momento Experimental		Total
			Pre Test	Post Test	
Aplicación de Control	No existe	Frecuencia	23	1	24
		%	20,18	0,88	10,53
	Si existe	Frecuencia	91	113	204
		%	79,82	99,12	89,47
Total		Frecuencia	114	114	228
		%	100	100	100

Fuente: Elaboración propia

Como muestra el cuadro 6, los resultados de la verificación previa al SGSI en el número de controles aplicados, existe un 79,82% mientras que no existen un 20,18%. En cambio, los resultados posteriores a la verificación muestran en el número de controles aplicados, existen alcanza un 99,12% y no existen un 0,82%.

Figura 6

Número de controles aplicados antes y después de un SGSI



Estos resultados reflejan que existe una clara diferencia en el número de controles aplicados antes y después de la introducción del SGSI.

Estadística Inferencial

Prueba de normalidad

Hipótesis de normalidad

H0: Los datos siguen una distribución normal

H1: Los datos no siguen una distribución normal

Nivel de significancia

Grado de confianza equivalente al 95% y 5% de límite para el error.

Test de normalidad

Si n > 50 se aplica Kolmogorov–Smirnov

Si n <= 50 se aplica Shapiro–Wilk

Criterio de decisión

Si p-valor < 0.05 se desestima la H0

Si p-valor >= 0.05 se acepta la H0 y se desestima la H1

Resultados de la prueba

Tabla 7

Prueba de normalidad – Nivel de Probabilidad

	Kolmogorov-Smirnov[a]		
	Estadístico	gl	Sig.
Nivel de Probabilidad - Pre Test	0,451	74	**0,000**
Nivel de Probabilidad - Post Test			

Fuente: Elaboración propia

Como se muestra en el cuadro 7, el indicador nivel de probabilidad, cuenta con un tamaño de muestra superior a 50 (n>50), por lo cual, se usó Kolmogorov-Smirnov. Por otro lado, se visualiza que el p-valor, para el indicador, es igual a 0.000, es decir, es menor a 0.05 (p-valor<0.05), por lo tanto, se afirma con un grado de significancia del 5% que los data cuenta con una distribución libre.

Tabla 8

Prueba de normalidad – Nivel de Riesgo

	Kolmogorov-Smirnov[a]		
	Estadístico	gl	Sig.
Nivel de Riesgo - Pre Test	0,481	74	**0,000**
Nivel de Riesgo - Post Test			

Fuente: Elaboración propia

Como se muestra en el cuadro 8, el indicador nivel de riesgo cuenta con un tamaño de muestra superior a 50 (n>50), por lo cual, se usó Kolmogorov-Smirnov. Por otro lado, se visualiza que el p-valor, para el indicador, es igual a 0.000, es decir, es menor a 0.05 (p-valor<0.05), por lo tanto, se afirma con un grado de significancia del 5% que los data cuenta con una distribución libre.

Tabla 9

Prueba de normalidad – Número de controles

	Kolmogorov-Smirnov[a]		
	Estadístico	gl	Sig.
Número de controles - Pre Test	0,494	114	**0,000**
Número de controles - Post Test			

Fuente: Elaboración propia

Como se muestra en el cuadro 9, el indicador número de controles, cuentan con un tamaño de muestra superior a 50 (n>50), por lo cual, se usó Kolmogorov-Smirnov. Por otro lado, se visualiza que el p-valor, para el indicador, es igual a 0.000, es decir, es menor a 0.05 (p-valor<0.05), por lo tanto, se afirma con un grado de significancia del 5% que los data cuenta con una distribución libre. Finalmente, para la prueba de hipótesis se usó el test de Wilcoxon, para cada indicador respectivamente.

Prueba de hipótesis

Hipótesis general

H0: La aplicabilidad de un SGSI no mejora la Gestión de Riesgos en el área de Infraestructura y Operaciones en una entidad pública, Callao 2023

H1: La aplicabilidad de un SGSI mejora la Gestión de Riesgos en el área de Infraestructura y Operaciones en una entidad pública, Callao 2023

Nivel de significancia

Grado de confianza equivalente al 95% y 5% de límite para el error.

Prueba estadística

Dado que las muestras son relacionadas y los datos no son paramétricos, se usó el test de Wilcoxon.

Pauta de resolución

Si p-valor < 0.05 se desestima la H0

Si p-valor >= 0.05 se r desestima la H1

Hipótesis Especifica 1

HE0: La aplicación de un SGSI no influye positivamente reduciendo el nivel de probabilidad en la Gestión de Riesgos en el área de Infraestructura y Operaciones en una entidad pública, 2023.

HE1: La aplicación de un SGSI influye positivamente reduciendo el nivel de probabilidad en la Gestión de Riesgos en el área de Infraestructura y Operaciones en una entidad pública, 2023.

Nivel de significancia

Grado de confianza equivalente al 95% y 5% de límite para el error.

Prueba estadística

Dado que las muestras son relacionadas y los datos no son paramétricos, se usó el test de Wilcoxon.

Pauta de resolución

Si p-valor < 0.05 se desestima la HE0

Si p-valor >= 0.05 se desestima la HE1

Tabla 10

Prueba de hipótesis de Nivel de Probabilidad

Estadísticos de prueba[a]	
	Nivel de Probabilidad (Pre Test) Nivel de Probabilidad (Post Test)
Z	-8,006[b]
Sig. asintótica(bilateral)	**0,000**

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

Fuente: Elaboración propia

Como se muestra en el cuadro 8, el valor **sig.** es inferior a **0.05**, en virtud de lo cual se desestima la hipótesis HE0 y se acepta la hipótesis HE1 con un grado de confianza equivalente al 95%, concluyendo que: La aplicación de un SGSI influye positivamente reduciendo el nivel de probabilidad en la Gestión de Riesgos en el área de Infraestructura y Operaciones en una entidad pública, 2023.

Hipótesis Especifica 2

HE0: La aplicación de un SGSI no influye positivamente reduciendo el nivel de riesgo en la Gestión de Riesgos en el área de Infraestructura y Operaciones en una entidad pública, 2023.

HE2: La aplicación de un SGSI influye positivamente reduciendo el nivel de riesgo en la Gestión de Riesgos en el área de Infraestructura y Operaciones en una entidad pública, 2023.

Nivel de significancia

Grado de confianza equivalente al 95% y 5% de límite para el error.

Prueba estadística

Dado que las muestras son relacionadas y los datos no son paramétricos, se usó el test de Wilcoxon.

Pauta de resolución

Si p-valor < 0.05 se desestima la HE0

Si p-valor >= 0.05 se desestima la HE2

Tabla 11

Prueba de hipótesis de Nivel de Riesgo

Estadísticos de prueba[a]	
	Nivel de Riesgo (Pre Test) Nivel de Riesgo (Post Test)
Z	-8,185[b]
Sig. asintótica(bilateral)	**0,000**

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

Fuente: Elaboración propia

Como se muestra en el cuadro 9, el valor **sig.** es inferior a **0.05**, en virtud de lo cual se desestima la hipótesis HE0 y se acepta la hipótesis HE2 con un grado de confianza equivalente al 95%, concluyendo que: La aplicación de un SGSI influye positivamente reduciendo el nivel de riesgo en la Gestión de Riesgos en el área de Infraestructura y Operaciones en una entidad pública, 2023.

Hipótesis Especifica 3

HE0: La aplicación del SGSI no influye de manera positiva incrementando el número de controles en la Gestión de Riesgos en el área de Infraestructura y Operaciones en una entidad pública, 2023.

HE3: La aplicación del SGSI influye de manera positiva incrementando el número de controles en la Gestión de Riesgos en el área de Infraestructura y Operaciones en una entidad pública, 2023.

Nivel de significancia

Grado de confianza equivalente al 95% y 5% de límite para el error.

Prueba estadística

Dado que las muestras son relacionadas y los datos no son paramétricos, se usó el test de Wilcoxon.

Pauta de resolución

Si p-valor < 0.05 se desestima la HE0

Si p-valor >= 0.05 se desestima la HE3

Tabla 12

Prueba de hipótesis de Número de controles aplicados

Estadísticos de prueba[a]	
	Número de controles aplicados (Pre Test) Número de controles aplicados (Post Test)
Z	-4,690[b]
Sig. asintótica(bilateral)	**0,000**

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

Fuente: Elaboración propia

Como se muestra en el cuadro 10, el valor **sig.** es inferior a **0.05**, en virtud de lo cual se desestima la hipótesis HE0 y se acepta la hipótesis HE3 con un grado de confianza equivalente al 95%, concluyendo que: La aplicación del SGSI influye de manera positiva incrementando el número de controles en la Gestión de Riesgos en el área de Infraestructura y Operaciones en una entidad pública, 2023.

V.DISCUSIÓN

Como objetivo general de este estudio, se planteó determinar de qué manera influye un SGSI en la gestión de riesgos en el área de infraestructura y operaciones en una entidad pública, Callao 2023, se determina que por medio de los resultados obtenidos con respecto a las hipótesis específicas planteadas en su momento, se observó un nivel de significancia estadística cuyo valor es igual a 0.000, él es inferior a 0.05, en contraste a lo establecido en la pauta de resolución, nos permitió desestimar la hipótesis nula y aceptar la hipótesis general, demostrando estadísticamente, con nivel de confianza equivalente al 95% y 5% como límite al error, que la aplicabilidad de un SGSI mejora la Gestión de Riesgos en el área de Infraestructura y Operaciones en una entidad pública, gracias a este estándar se identificó, evaluó y cuantificó el nivel de los riesgo con respecto a las amenazas y vulnerabilidades, permitiendo elaborar un plan para el tratamiento para la mitigación de los mismos.

En este sentido, con los objetivos planteados lineas arriba, coincidimos con Lopes et al (2019) que en su estudio concluye que existe un consenso en que la aplicación del estándar ISO 27001 identifica la data personal como un activo de seguridad de la información y así mismo se considera un factor facilitador para que las organizaciones cumplan de manera efectiva el reglamento que brinda las directrices para proteger los datos personales propuesto por la UE, ya que salvaguarda la seguridad en la información sensible. En esa misma línea, Martinez (2020) en su estudio, concluye que luego de explicar a las empresas los beneficios aplicar metodologías para un SGSI, la más votada fue la ISO 27001 con un 24% y que el 84% de las empresas se encuentran interesadas en la implementación, mientras que el 16% restante no cuenta con el presupuesto necesario.

Igualmente, Mirtsch et al., (2021) concluyeron que la implementación de la norma SGSI es un buen punto de partida para aumentar el nivel general de seguridad y que las empresas se ven beneficiadas sin necesidad de certificarse. De igual forma, Cuenca (2023) concluyó en su estudio que tras la introducción del SGSI, el 35% y el 40% del personal encuestado tienen un nivel medio y óptimo de

conocimientos sobre seguridad de la información respectivamente, lo cual reflejó una mejora significativa en la organización.

Por otro lado, para Atencio (2019) llegó a la conclusión de que un plan de seguridad mejora tras la implementación y aplicación del SGSI, ya que los resultados demostraron que el cumplimiento de la norma aumentó de manera significativa del 35% al 41%. Finalmente, Narro (2021) en su estudio concluye que, con el SGSI y el respectivo cumplimiento de este, mayor será el nivel de seguridad en la gestión de riesgos.

Al estudiar cómo influye un SGSI en el nivel de probabilidad en la gestión de riesgos en el área de infraestructura y operaciones en una entidad pública, los resultados fueron analizados por la prueba estadística test de Wilcoxon, arrojando un p-valor inferior a 0.05, en contraste a lo establecido en la pauta de resolución, nos permite negar la hipótesis nula y aceptar la primera hipótesis específica definida en su momento, con grado de confianza equivalente al 95% y 5% como límite al error, que la aplicación de un SGSI influye positivamente reduciendo el nivel de probabilidad en la Gestión de Riesgos en el área de Infraestructura y Operaciones en una entidad pública, debido a que, en un primer momento de la evaluación, el nivel de probabilidad mostraba un nivel de 2.54 puntos, luego de la aplicación de un SGSI el nivel de probabilidad bajo a 1.47 puntos, mostrando una clara reducción de 1.07 puntos, lo que equivale a un 21.4%.

Para el indicador nivel de probabilidad, los resultados concuerdan con Achmadi et al., (2018) en su estudio abordó que el centro de datos debe estar protegido física y lógicamente para proteger el sistema informático de ataques a la seguridad. Cualquier violación, como el robo de información, la denegación de servicio y el acceso no autorizado, puede tener consecuencias negativas para la empresa, como la pérdida de ingresos, reputación y confianza de los clientes. Implantar un SGSI puede ayudar a identificar, gestionar y mitigar las amenazas de seguridad de la información. Aplicó un marco SGSI desarrollado específicamente para que los centros de datos y se gestionan la disponibilidad, confidencialidad e integridad de la seguridad de la información. Este estudio ayudó a demostrar que

mediante la aplicabilidad de este marco SGSI, la dirección redujo el nivel de probabilidad de las amenazas en el centro de datos en un 17.8%.

Así mismo, se coincide con Guardia (2020) quien realizó una investigación aplicada correlacional de enfoque cuantitativo, cuyo objetivo fue desarrollar un SGSI y que los riesgos informáticos sean minimizados. Como resultado se observa que el porcentaje de colaboradores con conocimiento de tratamiento de riesgos, asciende al 99%, por lo que la probabilidad de los riesgos frente a un ataque se minimizó.

En ese sentido, Sánchez (2021) en su estudio afirma que una entidad que no cuenta con SGSI implementado, se encuentra muy expuesta su seguridad de la información, a todos tipos de ciberataques, provocando pérdidas a la entidad. Su estudio fue experimental descriptivo, de enfoque cuantitativo. Los resultados revelan que un 90% considera que es importante la seguridad de la información y que no se cuenta con estrategias para proteger la información, en cuanto a las vulnerabilidades se encuentra que el 14% es vulnerable, 48% medianamente vulnerable y 38% muy vulnerable. Concluyó que implementar un SGSI en cooperativa, mejora y reduce el nivel en la exposición al riesgo en la información y su seguridad.

Finalmente, Razikin y Soewito (2022) en su trabajo propusieron un modelo para el diseño de sistemas de seguridad informática basado en el análisis de riesgos y el marco de ciberseguridad ISO/IEC 27001. El objetivo del modelo propuesto es encontrar el mejor sistema de seguridad para mitigar las amenazas a la seguridad. El modelo construido es capaz de vincular el valor de prioridad de reducción de amenazas basado en la puntuación relativa de amenazas con la puntuación relativa de cumplimiento del estándar ISO 27001. El valor de prioridad de reducción de amenazas es clave para priorizar las recomendaciones para construir un sistema de seguridad informática basado en el marco ISO/IEC 27001. Los resultados arrojan una puntuación media de conformidad con estándar ISO 27001 aumentó del 36,27% al 82,37%. Además, la puntuación media de criticidad de la amenaza basada en 12 tipos de amenazas disminuyó de 8,75 a 4,00. Los

resultados de la evaluación de la relación entre la aplicación de las recomendaciones del sistema de seguridad y la mitigación de los ciberataques muestran un aumento de la eficacia de la mitigación de los ciberataques de una puntuación media del 18,32% al 40,74%.

Al estudiar cómo influye un SGSI en el nivel de riesgo en la gestión de riesgos en el área de infraestructura y operaciones en una entidad pública, los resultados fueron analizados por la prueba estadística test de Wilcoxon, arrojando un p-valor inferior a 0.05, en contraste a lo establecido en la pauta de resolución, nos permite desestima la hipótesis nula y aceptar la segunda hipótesis específica definida en su momento, con nivel de confianza equivalente al 95% y 5% como límite al error, que la aplicación de un SGSI influye positivamente reduciendo el nivel de riesgo en la Gestión de Riesgos en el área de Infraestructura y Operaciones en una entidad pública, ya que en un primer momento de la evaluación, el nivel de riesgo mostraba un nivel de 10.30 puntos, luego de la aplicación de un SGSI el nivel de probabilidad bajo a 5.98 puntos, mostrando una clara reducción de 4.32 puntos, lo que equivale a un 17.28%.

Para el indicador nivel de riesgo, estos resultados coinciden con Jara (2018) ya que, en su estudio, una entidad pública que no contaba con un SGSI en los procesos del negocio y el nivel de seguridad de la información era bajo, por ello implementó un SGSI. En la población y muestra, se consideraron 31 activos y 114 controles. Por lo cual, se utilizó una investigación de tipo aplicada, pre-experimental. Para la evaluación de los resultados, se utiliza un enfoque cuantitativo. Como resultado, el promedio del nivel del riesgo se redujo en 4.06 puntos. Por lo que concluyó, que un SGSI mejora la gestión de riesgos en una entidad pública.

Al estudiar cómo influye un SGSI en el número de controles aplicado en la gestión de riesgos en el área de infraestructura y operaciones en una entidad pública, los resultados fueron analizados por la prueba estadística test de Wilcoxon, arrojando un p-valor inferior a 0.05, en contraste a lo establecido en la pauta de resolución, nos permite desestima la hipótesis nula y aceptar la tercera

hipótesis específica definida en su momento, con nivel de confianza equivalente al 95% y 5% como límite al error, que la aplicación de un SGSI influye positivamente incrementando el número de controles aplicados en la Gestión de Riesgos en el área de Infraestructura y Operaciones en una entidad pública, ya que en un primer momento de la evaluación, el número de controles aplicados mostraba un cumplimiento de 79.82% (91 controles), luego de la aplicación de un SGSI el cumplimiento subió a 99.12% (113 controles), mostrando un claro incremento de 12 controles, lo que equivale a un 17.28%.

Para el indicador número de controles, se concuerda con Huerta (2019) en su estudio evidenció que la implementación de un SGSI mejora la gestión de riesgos. Para la muestra se consideraron 24 activos críticos y 114 controles del anexo A, los cuales fueron registrados en fichas de observación. Para ello, utilizó una investigación de tipo aplicada, pre-experimental. Los resultados fueron validados mediante un enfoque cuantitativo y demostró que los controles aplicados antes de implementar un SGSI eran 11, lo que equivale a un 9.6%, luego de la aplicación del SGSI aumentaron a 104 controles, lo que equivale a 91.2%, elevando el número de controles en 93, lo que muestra una clara mejoría en el nivel de seguridad en un 81.6%. Por lo que concluyó, que la implementación de un SGSI mejora la gestión de riesgos en una entidad privada.

Del mismo modo, se concuerda con Aquino (2020) en una entidad pública no cuenta con alguna norma o directiva que indique cómo se debe proteger la información. En su investigación se plantea aplicar un SGSI en base ISO 27001. Por ello utilizó una investigación de tipo aplicada, pre-experimental. Los resultados revelaron que los riesgos de seguridad respecto a los controles tenían un nivel de 86.15%, el cual se redujo a un 11.15%; mostrando claramente una reducción del 75%. Por otro lado, se incrementó el número de controles de seguridad, ya que antes solo eran 18 lo cual representa un 15,78%, estos incrementaron a 65 controles lo que representa un 57,01%; lo cual refleja un crecimiento de 41,23%. Agregando a lo anterior, Izquierdo (2021) en su estudio realizó la uniformización de los estándares respecto a la gestión de la seguridad de la información con la finalidad de preparar un marco adecuado a los procesos relacionados a cada

farmacia de los hospitales en la región Amazonas. Gracias al estudio se encontró en los controles una mejora de un 31% de eficiencia. En ese mismo sentido, el control de acceso muestra una mejora del 70%.

En contraste con Fonseca et al., (2021) en su estudio considera que un SGSI es una herramienta importante para gestionar y controlar la seguridad de la información, ya que permite preservar y garantizar los pilares de seguridad de los activos y reducir el nivel del riesgo, ya sea mitigando, transfiriendo o controlándolos. Es por ello, que se decidió aplicar un modelo de SGSI a un caso real. Como resultado satisfactorio, se identificaron activos de información, las vulnerabilidades técnicas y los riesgos aplicados. Así mismo se observa la necesidad de añadir un plan de continuidad para actualizar el SGSI. Los resultados demuestran que se llega a un 21% de cumplimientos de los requisitos mínimos, 49% el cumplimiento de los controles del Anexo A. Como conclusión se afirma que el aplicar un modelo de SGSI es crucial dentro de una organización ya que permite obtener un valor diferencial en las operaciones de los servicios, mejorando los procesos.

Finalmente, es similar con Alsahafi et al., (2022) en su investigación analizó el cumplimiento del marco NCA-ECC por parte de las organizaciones saudíes en relación con la implantación de un SGSI. Se seleccionaron como muestra tres universidades públicas sauditas certificadas con un SGSI y se evaluó su cumplimiento del NCA-ECC en cuanto a la aplicación de los controles esenciales de un SGSI (29 controles en total). Se observa que, de los 29 controles esenciales, sólo 12 se aplican (41%), 13 se aplican parcialmente (45%), 3 no se aplican y, por último, (4%) no se aplican en las universidades. Puede concluirse que las organizaciones con certificación ISO/IEC 27001 sólo cumplen los requisitos de NCA-ECC en el 64% de los casos.

VI.CONCLUSIONES

Primera: La aplicabilidad de un SGSI mejoró la gestión de riesgos en el área de infraestructura y operaciones en una entidad pública, Callao 2023. Debido a que se redujo el nivel de probabilidad de riesgo en un 21.4%, de igual manera se redujo el nivel de riesgo en 17.28% y por último los controles aplicados se incrementaron en 17.28%.

Segunda: Un SGSI influyó de manera positiva reduciendo el nivel de probabilidad en la gestión de riesgos en el área de infraestructura y operaciones en una entidad pública, Callao 2023. Debido a que, en un primer momento de la evaluación, el nivel de probabilidad de riesgo mostraba un nivel de 2.54 puntos, luego de la aplicación de un SGSI el nivel de probabilidad de riesgo bajo a 1.47 puntos, mostrando una clara reducción de 1.07 puntos, lo que equivale a un 21.4%.

Tercera: Un SGSI influyó de manera positiva reduciendo en el nivel de riesgo en la gestión de riesgos en el área de infraestructura y operaciones en una entidad pública, Callao 2023. Debido a que, en un primer momento de la evaluación, el nivel de riesgo mostraba un nivel de 10.30 puntos, luego de la aplicación de un SGSI el nivel de probabilidad bajo a 5.98 puntos, mostrando una clara reducción de 4.32 puntos, lo que equivale a un 17.28%.

Cuarta: Un SGSI influyó de manera positiva incrementando el número de controles aplicados en la gestión de riesgos en el área de infraestructura y operaciones en una entidad pública, Callao 2023. Debido a que, en un primer momento de la evaluación, el número de controles aplicados mostraba un cumplimiento de 79.82% (91 controles), luego de la aplicación de un SGSI el cumplimiento subió a 99.12% (113 controles), mostrando un claro incremento de 12 controles, lo que equivale a un 17.28%.

VII.RECOMENDACIONES

Primera: Se recomienda al líder del comité de gobierno digital programar auditorías de manera regular al proceso de infraestructura y operaciones para ayudar en la mejora continua de la aplicabilidad del SGS, mejorando la gestión de riesgos y minimizando la paralización de las operaciones, lo cual repercutirá en pérdidas económicas y de reputación.

Segunda: Se recomienda al Oficial de Seguridad de la Información, realizar charlas de concientización y sensibilización de manera frecuente, incrementando el nivel de conocimiento, de manera que se reduzca la probabilidad de eventos e incidentes por parte de los empleados.

Tercera: Se recomienda al Oficial de Seguridad de la Información implementar la plataforma nacional de incidentes de seguridad digital y la plataforma nacional de alertas de seguridad digital, de manera que pueda prevenir y reducir el riesgo en los incidentes potenciales a nivel nacional e internacional.

Cuarta: Se recomienda al Oficial de Seguridad de la Información analizar la posibilidad de apoyar el SGSI con otros marcos de seguridad, como el framework NIST, de manera que se puede aprovechar lo mejor de ambos en cuanto a controles de ciberseguridad en las infraestructuras críticas e importantes. Así mismo, revisar la aplicabilidad de los controles el Anexo A, revisar la pertinencia y si estas agregan valor.

REFERENCIAS

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

Alvaro, A. (2009) “Sicherheit in der Informationsgesellschaft,” in Freiheit: gefühlt–gedacht–gelebt, Springer, pp. 214–227.

Aquino Cruz, M., Huallpa Laguna, J. N., Huillcen Baca, H. A., Carpio Vargas, E. E., & Palomino Valdivia, F. D. L. (2020). Implementation of an Information Security Management System based on the ISO/IEC 27001: 2013 standard for the information technology division. In The International Conference on Advances in Emerging Trends and Technologies (pp. 264-272). Springer, Cham.

Atencio, E. (2019). Diseño de un sistema de gestión de seguridad de la información basado en la NTP-ISO/IEC 27001:2014 para la dirección general de informática y estadística de la Universidad Nacional Daniel Alcides Carrión Pasco Perú. Universidad Nacional Daniel Alcides Carrión, Cerro de Pasco – Perú.

Araujo, T. (2017). Evaluación de Riesgo, Supervisión y Monitoreo en el Logro de Objetivos, en el Fondo de Aseguramiento Saludpol – Perú.http://repositorio.ucv.edu.pe/bitstream/handle/UCV/4360/Araujo_BTA.pdf?sequence=1&isAllowed=y

Bekerman, Uriel, La gestión de riesgos cibernéticos en la Union Europea (The Cyber Risk Management in the European Union) (June 22, 2020). Diario DPI Suplemento Derecho y Tecnologías Nro. 64 - 22.06.2020, Available at SSRN: https://ssrn.com/abstract=3636178

Boehmer, W. (2008) “Appraisal of the Effectiveness and Efficiency of an Information Security Management System Based on ISO 27001,” Securware, vol. 8, pp. 224–231.

Borek, A., Parlikad, A. K., Webb, J., & Woodall, P. (2013). Total information risk management: maximizing the value of data and information assets. Massachusetts, Estados Unidos de América. Elsevier.

Breier J. and Schindler, F. (2014) Assets Dependencies Model in Information Security Risk Management. In: Linawati, Mahendra M.S., Neuhold E.J., Tjoa A.M., You I. (eds) Information and Communication Technology. ICT-EurAsia 2014. Lecture Notes in Computer Science, vol 8407. Springer, Berlin, Heidelberg

Brenner, J. (2007). "ISO 27001: Risk management and compliance," Risk Management Magazine, vol. 54, no. 1, p. 24.

Calder, A. (2009). Information Security Based on ISO 27001/ISO 27002: A Management Guide. Van Haren Publishing.

Castro, F. (2003). El proyecto de investigación y su esquema de elaboración /por Fernando Castro Márquez. Caracas, Venezuela: Editorial Uyapar.

Cerezo. J (2022) Aplicación de la norma ISO 27001 para la gestión de la seguridad de la información en la empresa Plataforma Buscador Académico BUSAC. S.A. en Ecuador, Trujillo 2022. Tesis, Universidad César Vallejo, Lima. https://repositorio.ucv.edu.pe/handle/20.500.12692/102607

Correa (2019). APA: Introducción a la Estadística Bayesiana, Editorial ITM pag (11) https://books.google.com.pe/books?id=9wynDwAAQBAJ&pg=PR2&dq=estadistica&hl=es-419&sa=X&ved=2ahUKEwiDysOa69zzAhW9JrkGHbqlBIIQ6AF6BAgHEAI#v=onepage&q=estadistica&f=false

Cuenca Neyra, E. E. (2023). SGSI según ISO/IEC 27001:2013 para el control de activos de TI en una empresa privada de Outsourcing, Lima 2023. Tesis, Universidad César Vallejo. https://repositorio.ucv.edu.pe/handle/20.500.12692/109516

Chinyemba, M. K., & Phiri, J. (2018). An investigation into information security threats from insiders and how to mitigate them: A case study of zambian

public sector. Journal of Computer Science, 14(10), 1389-1400. https://doi.org/10.3844/jcssp.2018.1389.1400

D. Achmadi, Y. Suryanto and K. Ramli, "On Developing Information Security Management System (ISMS) Framework for ISO 27001-based Data Center," 2018 International Workshop on Big Data and Information Security (IWBIS), Jakarta, Indonesia, 2018, pp. 149-157. https://ieeexplore.ieee.org/abstract/document/8471700/metrics#metrics

Dutton, J. (2016). Identifying assets for conducting an asset-based information security risk assessment. Londres, Reino Unido. Portal Vigilant Software.

Fonseca, O., Rojas, A., & Flores, H. (junio de 2021). A Model of an Information Security Management System Based on NTC-ISO/IEC 27001 Standard. IAENG International Journal of Computer Science, 10. Obtenido de https://www.researchgate.net/profile/Alix-E-Rojas/publication/362062660_A_Model_of_an_Information_Security_Management_System_Based_on_NTC-ISOIEC_27001_Standard/links/62d485bcd351bd24f51fa7c5/A-Model-of-an-Information-Security-Management-System-Based-on-NT

Fakhri, B., Fahimah, N. and Ibrahim, J. (2015). “Information Security Aligned To Enterprise Management,” Middle East Journal of Business, vol. 10, no. 1.

Galindo (2020). APA: Estadística para no estadísticos una guía básica sobre la metodología cuantitativa de trabajos académicos. pag 56 https://www.3ciencias.com/wp-content/uploads/2020/03/Estad%C3%ADstica-para-no-estad%C3%ADsticos-Una-gu%C3%ADa-b%C3%A1sica-sobre-la-metodolog%C3%ADa-cuantitativa-de-trabajos-acad%C3%A9micos-2

Guardia. R (2020) Diseño de un modelo de seguridad de la información para minimizar los riesgos informáticos en la gestión académica del Instituto de Educación Superior Tecnológico público. Huaraz 2020. Universidad Nacional Santiago Antúnez de Mayolo. Huaraz. https://repositorio.unasam.edu.pe/handle/UNASAM/4212

Guerra, Erick, Neira, Harold, Díaz, Jorge L., & Patiño, Janns. (2021). Desarrollo de un sistema de gestión para la seguridad de la información basado en

metodología de identificación y análisis de riesgo en bibliotecas universitarias. Información tecnológica, 32(5), 145-156. https://dx.doi.org/10.4067/S0718-07642021000500145

Halvorson, N. (2008). Information Risk Management: A Process Approach to Risk Diagnosis and Treatment. USA: Auerbach Publications.

Hernández-Sampieri, R., & Mendoza, C. (2020). Metodología de la investigación: las rutas cuantitativa, cualitativa y mixta. Mcgraw-hill.

Hernández, R., Fernández, C., & Baptista, M. (2014). Metodología de la investigación. México: McGRAW-HILL / Interamericana Editores, S.A. de C.V. https://eticainvestigativa.wordpress.com/2016/03/29/aspectos-eticos-en-lainvestigacion-cientifica/

Huerta. C (2019) Sistema de gestión de seguridad de la información para mejorar el proceso de gestión del riesgo de Coopsol Consultoría, Lima 2019. Tesis, Universidad César Vallejo, Lima. https://repositorio.ucv.edu.pe/handle/20.500.12692/46037

ISO/IEC 27001 (2013). ISO/IEC 27001:2013 Information Technology. Security techniques. Information security management systems, Requirements. Génova, Suiza: ISO/IEC.

ISO 31000 (2009). ISO 31000:2009 Risk Management - Principles and Guide lines. Geneva. Suiza: International Standards Organisation.

ISO 31000 (2018). ISO 31000:2018 Risk Management - Principles and Guide lines. Geneva. Suiza: International Standards Organisation.

ISOTools (2019), Gestión de riesgos de seguridad de la información. Recuperado de: https://www.isotools.org/2019/08/20/gestion-de-riesgos-de-seguridad-de-lainformacion-un-aspecto-clave-en-las-organizaciones-actuales

Izquierdo, J. (2021). Modelo basado en la gestión de seguridad de la información para contribuir en los procesos de las farmacias de los hospitales II-I en la región amazonas. Universidad Católica Santo Toribio de Mogrovejo. http://hdl.handle.net/20.500.12423/4193

Jara. O (2018) Sistema de gestión de seguridad de la información para mejorar el proceso de gestión del riesgo en un gobierno, Lima 2018. Tesis, Universidad César Vallejo, Lima. https://repositorio.ucv.edu.pe/handle/20.500.12692/31209

Joyanes, L. (2015). Sistemas de Información en la Empresa. (1a ed.). México: Alfaomega.

Lopes, I. M., Guarda, T., & Oliveira, P. (2019). Implementation of ISO 27001 standards as GDPR compliance facilitator. Journal of Information Systems Engineering and Management, 4(2) https://doi.org/10.29333/jisem/5888

M. Mirtsch, J. Kinne and K. Blind, "Exploring the Adoption of the International Information Security Management System Standard ISO/IEC 27001: A Web Mining-Based Analysis," in IEEE Transactions on Engineering Management, vol. 68, no. 1, pp. 87-100, Feb. 2021. https://ieeexplore.ieee.org/abstract/document/9082865

Martínez, W. Y. S. (2020). Beneficios de utilizar metodologías para la implantación de Sistemas de Gestión de Seguridad de la Información. INF-FCPN-PGI Revista PGI, 104-107. https://ojs.umsa.bo/ojs/index.php/inf_fcpn_pgi/article/view/121

Merino, F. y Cañizares, D. (2011). Implantación de un Sistema de Gestión de Seguridad de la Información según la ISO 27001. (1a ed.). Bogotá, Colombia: Ediciones de la U.

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

Nancylia, M., Mudjtabar, E., Sutikno, S. and Rosmansyah, Y. (2014) The measurement design of information security management system. 8th International Conference on Telecommunication Systems Services and Applications (TSSA).

Narro, S. (2021). El sistema de gestión de seguridad de la información y la gestión de riesgos en el área informática de una universidad pública, región Cajamarca 2020. Cajamarca 2021. Tesis, Universidad Privada del Norte. https://repositorio.upn.edu.pe/handle/11537/30041

National Institute of Standards and Technology Special Publication 800-30, Guide for Conducting Risk Assessments, September 2012

NTP ISO/IEC 17799 (2007). NTP ISO/IEC 17799:2007 Tecnología de la información. Código de buenas prácticas para la gestión de la seguridad de la información. Lima, Perú: ISO/IEC.

NTP ISO/IEC 27001. (2014). INFORMATION TECHNOLOGY. Security techniques. Information security management systems - Requirements. Lima

NTP ISO/IEC 27005 (2018). NTP ISO/IEC 27005:2018 Tecnología de la información. Técnicas de seguridad. Gestión de riesgos de la seguridad de la información. Lima, Perú: ISO/IEC.

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

Sánchez, C. (2021) Modelo de Gestión de la Seguridad de la Información adaptado a las Cooperativas de Ahorro y Crédito de la ciudad de Guayaquil. Guayaquil 2021. Tesis, Universidad Tecnológica Empresarial de Guayaquil. http://biblioteca.uteg.edu.ec/xmlui/handle/123456789/1533

Olaf, P. & Publishing, V. (2010). Enterprise Risk Management. London, ISBM

Peltier, T. (2013). Information security fundamentals. CRC Press.

Peltier, T. (2014). Information Security Fundamentals. 2da. Edición. Florida, CRC Press.

Pritchard, C. (2015) Risk Management Concepts and Guidance. 5ª edición. Boca Raton. Florida, ISBN

Valderrama, S. (2013). Pasos para elaborar proyectos y tesis de investigación. Lima-Perú: San Marcos.

Vidal (2018). APA: La educación en ética, ciencia y espiritualidad Bogotá: Ediciones USTA. Pag (200) https://repository.usta.edu.co/handle/11634/16166

Whitman, M. and Mattord, H. (2013). Management of information security. Cengage Learning.

ANEXOS

Anexo 1: Matriz de Operacionalización de variables

Título: SGSI en la Gestión de Riesgos en el área de Infraestructura y Operaciones de una entidad pública, 2023

Variable de Estudio	Definición Conceptual	Definición Operacional	Dimensión	Indicadores	Escala
SGSI	El estándar nacional NTP-IO/IEC 27001 (2014) constituye que un SGSI mantiene el aspecto confidencial, íntegro y disponible de la información por medio del establecimiento de procedimientos de gestión de riesgos y proporciona garantía de que los riesgos se gestionan adecuadamente.	La R.M. Nº 004-2016-PCM autoriza la implementación obligatoria de la NTP ISO/IEC 27001:2014 sobre el SGSI en las instituciones públicas que son parte del sistema nacional de información. El SGSI implica el establecimiento de un plan para diseñar, implementar y mantener un conjunto de políticas, directivas, manuales, instructivos, actividades e indicadores para la gestión eficaz de la información que garantice el aspecto íntegro, confidencial y disponible con respecto a la información. Al emplear el método de gestión de riesgos fundamentado en la ISO 27005 en el área infraestructura y operaciones de una organización pública proporciona una seguridad a los 3 pilares, mediante la implementación de diversas actividades.			
Gestion de Riesgos	Para Peltier (2014), el procedimiento de la gestión de riesgos implica definir el riesgo, tasar la posibilidad de ocurrencia y tomar medidas para mitigar los riesgos potenciales.	La gestión de riesgos se encuadra en 3 dimensiones: análisis del riesgo, evaluación del riesgo y tratamiento del riesgo. El riesgo se puntualiza como la probabilidad de sufrir daños o pérdidas (ISOTools, 2019). El control de riesgos es uno de los pasos en el procedimiento de gestión de riesgos, trae consigo la desarrollar y poner en práctica un plan de reacción a los riesgos, el seguimiento y la activación de eventos, la aplicación de planes de preventivos y/o reactivos, y el seguimiento de los riesgos emergentes (Olaf y Pebbling, 2010).	Análisis de Riesgo	Nivel de Probabilidad	Razón
			Evaluación de Riesgo	Nivel de Riesgo	Razón
			Tratamiento de Riesgo	Numero de controles	Ordinal

Anexo 2: Juicio de Expertos

Dimensiones del instrumento:

- **Primera dimensión**: Análisis de riesgos
- Medir el nivel de la probabilidad el riesgo

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Código de activo	1	4	4	4	
Amenaza	2	4	4	4	
Vulnerabilidad	3	4	4	4	
Degradación	4	4	4	4	
Impacto	5	4	4	4	
Probabilidad	6	4	4	4	

- **Segunda dimensión**: Evaluación de riesgos
- Medir el nivel de riesgo

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Código de activo	1	4	4	4	
Amenaza	2	4	4	4	
Vulnerabilidad	3	4	4	4	
Degradación	4	4	4	4	
Impacto	5	4	4	4	
Probabilidad	6	4	4	4	
Riesgo	7	4	4	4	

- **Tercera dimensión**: Tratamiento de riesgos
- Medir el número de controles aplicados

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Clausula	1	4	4	4	
Sección	2	4	4	4	
Objetivo	3	4	4	4	
Aplicación	4	4	4	4	
Existencia	5	4	4	4	
Justificación	6	4	4	4	

Observaciones (precisar si hay suficiencia):

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

Apellidos y nombres del juez validador: Dr. ACUÑA BENITES, MARLON FRANK

Especialidad del validador: Ing. Sistemas / Investigador

18 de mayo del 2023

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

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

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

Firma del Experto validador

Dimensiones del instrumento:

- **Primera dimensión**: Análisis de riesgos
- Medir el nivel de la probabilidad el riesgo

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Código de activo	1	4	4	4	
Amenaza	2	4	4	4	
Vulnerabilidad	3	4	4	4	
Degradación	4	4	4	4	
Impacto	5	4	4	4	
Probabilidad	6	4	4	4	

- **Segunda dimensión**: Evaluación de riesgos
- Medir el nivel de riesgo

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Código de activo	1	4	4	4	
Amenaza	2	4	4	4	
Vulnerabilidad	3	4	4	4	
Degradación	4	4	4	4	
Impacto	5	4	4	4	
Probabilidad	6	4	4	4	
Riesgo	7	4	4	4	

- **Tercera dimensión**: Tratamiento de riesgos
- Medir el número de controles aplicados

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Clausula	1	4	4	4	
Sección	2	4	4	4	
Objetivo	3	4	4	4	
Aplicación	4	4	4	4	
Existencia	5	4	4	4	
Justificación	6	4	4	4	

Observaciones (precisar si hay suficiencia):

_____

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

Apellidos y nombres del juez validador: Mg. MUÑOZ LA RIVA, WALDIR ADHEMIR

Especialidad del validador: Lic. Administración

16 de mayo del 2023

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

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

Firma del Experto validador

Dimensiones del instrumento:

- **Primera dimensión**: Análisis de riesgos
- Medir el nivel de la probabilidad el riesgo

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Código de activo	1	4	4	4	
Amenaza	2	4	4	4	
Vulnerabilidad	3	4	4	4	
Degradación	4	4	4	4	
Impacto	5	4	4	4	
Probabilidad	6	4	4	4	

- **Segunda dimensión**: Evaluación de riesgos
- Medir el nivel de riesgo

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Código de activo	1	4	4	4	
Amenaza	2	4	4	4	
Vulnerabilidad	3	4	4	4	
Degradación	4	4	4	4	
Impacto	5	4	4	4	
Probabilidad	6	4	4	4	
Riesgo	7	4	4	4	

- **Tercera dimensión**: Tratamiento de riesgos
- Medir el número de controles aplicados

Indicadores	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
Clausula	1	4	4	4	
Sección	2	4	4	4	
Objetivo	3	4	4	4	
Aplicación	4	4	4	4	
Existencia	5	4	4	4	
Justificación	6	4	4	4	

Observaciones (precisar si hay suficiencia):

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

Apellidos y nombres del juez validador: Dr. LEZAMA GONZALES, PEDRO

Especialidad del validador: Ingeniero de Sistemas

15 de mayo del 2023

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

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

Firma del Experto validador

Anexo 3: Fichas de Observación

PERÚ APN	**FICHA DE OBSERVACIÓN N° 01** **INDICADOR: NIVEL DE PROBABILIDAD** **FASE: PRE-TEST**		
CODIGO:	SGSI-FO-001-PT	**VERSIÓN:**	V1
CLASIFICACIÓN:	CONFIDENCIAL	**FECHA DIESÑO:**	Mar-23
PROCESO:	GESTIÓN DE RIESGOS		
INVESTIGADOR:	HENRY FRANK HUAMANTECA DAMIAN		
FECHA DE RECOLECCIÓN:	6 al 10 de marzo		
PUESTO:			

IDENTIFICACION DE RIESGOS							**ANÁLISIS DE RIESGOS**		**PROBABILIDAD PROMEDIO**
CODIGO ACTIVO	**AMENAZA**	**VULNERABI|LIDAD**	**DEGRADACIÓN**				**IMPACTO**	**PROBABILIDAD**	
			C	**I**	**D**	**DREGADACIÓN MAXIMA**			
Activo 1	AM97 - Falla del sistema operativo	VU15 - Falta de evidencia de auditoria	2	2	3	Significativo	4	3	3
	AM97 - Falla del sistema operativo	VU21 - Seteo incorrecto de parámetros|	2	2	3	Significativo	4	3	
	AM13 - Pérdida del suministro de electricidad	VU3 - Susceptibilidad a la humedad, al polvo y a la suciedad	2	2	3	Significativo	4	3	
	AM30 - Mal funcionamiento del equipo	VU10 - Equipo desfasado por vigencia tecnológica	2	1	3	Significativo	4	3	
	AM30 - Mal funcionamiento del equipo	VU100 - Fallas conocidas del hardware	2	2	3	Significativo	4	3	
Activo 2	AM29 - Falla de equipo	VU3 - Susceptibilidad a la humedad, al polvo y a la suciedad	1	1	3	Significativo	4	3	2,75
	AM29 - Falla de equipo	VU10 - Equipo desfasado por vigencia tecnológica	2	1	3	Significativo	4	3	
	AM86 - No soporta nuevas tecnologías de hardware y software	VU10 - Equipo desfasado por vigencia tecnológica	2	1	3	Significativo	4	2	

	AM13 - Pérdida del suministro de electricidad	VU3 - Susceptibilidad a la humedad, al polvo y a la suciedad	2	2	3	Significativo	4	3	
Activo 3	AM30 - Mal funcionamiento del equipo	VU100 - Fallas conocidas del hardware	2	2	3	Significativo	4	3	3
Activo 4	AM30 - Mal funcionamiento del equipo	VU100 - Fallas conocidas del hardware	2	2	3	Significativo	4	3	3
Activo 5	AM30 - Mal funcionamiento del equipo	VU100 - Fallas conocidas del hardware	2	2	3	Significativo	4	3	3
Activo 6	AM30 - Mal funcionamiento del equipo	VU100 - Fallas conocidas del hardware	2	2	3	Significativo	4	3	3
Activo 7	AM29 - Falla de equipo	VU3 - Susceptibilidad a la humedad, al polvo y a la suciedad	1	1	3	Significativo	4	3	2,75
	AM29 - Falla de equipo	VU10 - Equipo desfasado por vigencia tecnológica	2	1	3	Significativo	4	3	
	AM86 - No soporta nuevas tecnologías de hardware y software	VU10 - Equipo desfasado por vigencia tecnológica	2	1	3	Significativo	4	2	
	AM13 - Pérdida del suministro de electricidad	VU3 - Susceptibilidad a la humedad, al polvo y a la suciedad	2	2	3	Significativo	4	3	
Activo 8	AM30 - Mal funcionamiento del equipo	VU100 - Fallas conocidas del hardware	2	2	3	Significativo	4	3	3
Activo 9	AM30 - Mal funcionamiento del equipo	VU100 - Fallas conocidas del hardware	2	2	3	Significativo	4	3	3
Activo 10	AM30 - Mal funcionamiento del equipo	VU100 - Fallas conocidas del hardware	2	2	3	Significativo	4	3	3
Activo 11	AM30 - Mal funcionamiento del equipo	VU100 - Fallas conocidas del hardware	2	2	3	Significativo	4	3	3
Activo 12	AM32 - Mal funcionamiento del software	VU115 - Falta de actualización de parches	2	2	3	Significativo	4	3	3
Activo 13	AM97 - Falla del sistema operativo	VU21 - Seteo incorrecto de parámetros	2	2	3	Significativo	4	3	3
Activo 14	AM88 - Instalación de software sin autorización, sin licencia	VU105 - Uso no controlado de licencias	1	1	3	Significativo	4	2	2
Activo 15	AM13 - Pérdida del suministro de electricidad	VU3 - Susceptibilidad a la humedad, al polvo y a la suciedad	2	2	3	Significativo	4	2	2
Activo 16	AM30 - Mal funcionamiento del equipo	VU100 - Fallas conocidas del hardware	3	2	2	Significativo	4	2	2

Activo 17	AM29 - Falla de equipo	VU124 - La aplicación, el soporte, registro de incidentes, mantenimiento servidores y otros equipos, servicio de backups lo realiza el proveedor del servicio ante una finalización de contrato la entidad quedaría sin este servicio	2	2	3	Significativo	4	2	2
Activo 18	AM99 - Ciberataques	VU96 - No se realiza la Identificación y Gestión de Vulnerabilidades	2	2	3	Significativo	4	2	2
Activo 19	AM13 - Pérdida del suministro de electricidad	VU3 - Susceptibilidad a la humedad, al polvo y a la suciedad	3	3	2	Catastrófico	5	3	3
Activo 20	AM99 - Ciberataques	VU96 - No se realiza la Identificación y Gestión de Vulnerabilidades	2	3	3	Catastrófico	5	3	3
Activo 21	AM6 - Polvo, corrosión, congelación	VU1 - Mantenimiento insuficiente / instalación fallida de medios de almacenamiento / Asignación Insuficiente de recursos	2	2	3	Significativo	4	3	3
Activo 22	AM72 - Disfunciones del sistema (bugs)	VU12 - Errores conocidos en el software	2	2	3	Significativo	4	3	3
Activo 23	AM29 - Falla de equipo	VU124 - La aplicación, el soporte, registro de incidentes, mantenimiento servidores y otros equipos, servicio de backups lo realiza el proveedor del servicio ante una finalización de contrato la entidad quedaría sin este servicio	2	2	3	Significativo	4	3	3
Activo 24	AM6 - Polvo, corrosión, congelación	VU1 - Mantenimiento insuficiente / instalación fallida de medios de almacenamiento / Asignación Insuficiente de recursos	2	2	3	Significativo	4	3	3
Activo 25	AM72 - Disfunciones del sistema (bugs)	VU12 - Errores conocidos en el software	2	2	3	Significativo	4	2	2
Activo 26	AM98 - Recortes presupuestales que afecta la adquisición de bienes y/o servicios	VU100 - Fallas conocidas del hardware	2	2	3	Significativo	4	2	2

	tecnológicos para la mejora del SGSI.								
Activo 27	AM72 - Disfunciones del sistema (bugs)	VU12 - Errores conocidos en el software	2	2	3	Significativo	4	2	2
Activo 28	AM72 - Disfunciones del sistema (bugs)	VU12 - Errores conocidos en el software	2	2	3	Significativo	4	2	2
Activo 29	AM72 - Disfunciones del sistema (bugs)	VU12 - Errores conocidos en el software	2	2	3	Significativo	4	2	2
Activo 30	AM32 - Mal funcionamiento del software	VU106 - Falta de renovación de licencias	2	2	3	Significativo	4	2	2
Activo 31	AM43 - Hacking	VU96 - No se realiza la Identificación y Gestión de Vulnerabilidades	2	2	3	Significativo	4	3	3
Activo 32	AM32 - Mal funcionamiento del software	VU106 - Falta de renovación de licencias	3	2	2	Significativo	4	2	2
Activo 33	AM32 - Mal funcionamiento del software	VU106 - Falta de renovación de licencias	2	2	3	Significativo	4	2	2
Activo 34	AM97 - Falla del sistema operativo	VU115 - Falta de actualización de parches	2	2	3	Significativo	4	2	2
Activo 35	AM97 - Falla del sistema operativo	VU115 - Falta de actualización de parches	2	2	3	Significativo	4	2	2
Activo 36	AM97 - Falla del sistema operativo	VU115 - Falta de actualización de parches	2	2	3	Significativo	4	2	2
Activo 37	AM97 - Falla del sistema operativo	VU115 - Falta de actualización de parches	2	2	3	Significativo	4	2	2
Activo 38	AM97 - Falla del sistema operativo	VU115 - Falta de actualización de parches	2	2	3	Significativo	4	2	2
Activo 39	AM72 - Disfunciones del sistema (bugs)	VU12 - Errores conocidos en el software	2	2	3	Significativo	4	3	3
Activo 40	AM99 - Ciberataques	VU96 - No se realiza la Identificación y Gestión de Vulnerabilidades	2	2	3	Significativo	4	3	3
Activo 41	AM99 - Ciberataques	VU96 - No se realiza la Identificación y Gestión de Vulnerabilidades	2	2	3	Significativo	4	3	3
Activo 42	AM46 - Acceso no autorizado al sitema	VU144 - Falta de un procedimiento formal o su actualización, para el registro y baja de usuarios	2	2	3	Significativo	4	2	2
Activo 43	AM29 - Falla de equipo	VU3 - Susceptibilidad a la humedad, al polvo y a la suciedad	2	2	3	Significativo	4	2	2
Activo 44	AM13 - Pérdida del suministro de electricidad	VU6 - Susceptibilidad a variación de voltaje	2	2	3	Significativo	4	2	2

Activo 45	AM29 - Falla de equipo	VU96 - No se realiza la Identificación y Gestión de Vulnerabilidades	2	2	3	Significativo	4	2	2
Activo 46	AM99 - Ciberataques	VU1 - Mantenimiento insuficiente / instalación fallida de medios de almacenamiento / Asignación Insuficiente de recursos	2	2	3	Significativo	4	2	2
Activo 47	AM99 - Ciberataques	VU1 - Mantenimiento insuficiente / instalación fallida de medios de almacenamiento / Asignación Insuficiente de recursos	2	2	3	Significativo	4	2	2
Activo 48	AM35 - Uso de software falsificado o copiado	VU46 - Uso incorrecto del software y hardware	2	3	1	Significativo	4	2	2
Activo 49	AM43 - Hacking	VU46 - Uso incorrecto del software y hardware	2	3	1	Significativo	4	2	2
Activo 50	AM21 - Robo de medios o documentos	VU125 - Eventos e incidentes que afecten a la seguridad de la información mal gestionados	3	3	2	Catastrófico	5	3	3
Activo 51	AM29 - Falla de equipo	VU10 - Equipo desfasado por vigencia tecnológica	2	2	3	Significativo	4	2	2,5
	AM13 - Pérdida del suministro de electricidad	VU6 - Susceptibilidad a variación de voltaje	2	2	3	Significativo	4	2	
	AM6 - Polvo, corrosión, congelación	VU3 - Susceptibilidad a la humedad, al polvo y a la suciedad	2	2	3	Significativo	4	3	
	AM12 - Fallas del sistema de aire acondicionado o del suministro de agua	VU6 - Susceptibilidad a variación de voltaje	2	2	3	Significativo	4	3	
Activo 52	AM12 - Fallas del sistema de aire acondicionado o del suministro de agua	VU6 - Susceptibilidad a variación de voltaje	2	2	3	Significativo	4	2	2
Activo 53	AM5 - Destrucción del equipo o los medios	VU41 - Gestión inadecuada de la red (capacidad de recuperación del ruteo)	2	2	3	Significativo	4	2	2
Activo 54	AM5 - Destrucción del equipo o los medios	VU41 - Gestión inadecuada de la red (capacidad de recuperación del ruteo)	2	2	3	Significativo	4	2	2
Activo 55	AM5 - Destrucción del equipo o los medios	VU41 - Gestión inadecuada de la red (capacidad de recuperación del ruteo)	2	2	3	Significativo	4	2	2

Activo 56	AM91 - Indisponibilidad del Servicio de Help Desk	VU124 - La aplicación, el soporte, registro de incidentes, mantenimiento servidores y otros equipos, servicio de backups lo realiza el proveedor del servicio ante una finalización de contrato la ENTIDAD quedaría sin este servicio	2	2	3	Significativo	4	2	2
Activo 57	AM29 - Falla de equipo	VU124 - La aplicación, el soporte, registro de incidentes, mantenimiento servidores y otros equipos, servicio de backups lo realiza el proveedor del servicio ante una finalización de contrato la ENTIDAD quedaría sin este servicio	2	2	3	Significativo	4	3	3
Activo 58	AM29 - Falla de equipo	VU124 - La aplicación, el soporte, registro de incidentes, mantenimiento servidores y otros equipos, servicio de backups lo realiza el proveedor del servicio ante una finalización de contrato la entidad quedaría sin este servicio	2	2	3	Significativo	4	3	3
Activo 59	AM29 - Falla de equipo	VU124 - La aplicación, el soporte, registro de incidentes, mantenimiento servidores y otros equipos, servicio de backups lo realiza el proveedor del servicio ante una finalización de contrato la ENTIDAD quedaría sin este servicio	2	2	3	Significativo	4	3	3
Activo 60	AM42 - Ruptura en la disponibilidad del personal	VU43 - Ausencia del personal	2	2	3	Significativo	4	3	3
Activo 61	AM42 - Ruptura en la disponibilidad del personal	VU43 - Ausencia del personal	2	2	3	Significativo	4	3	3

Activo 62	AM42 - Ruptura en la disponibilidad del personal	VU43 - Ausencia del personal	2	2	3	Significativo	4	3	3
Activo 63	AM42 - Ruptura en la disponibilidad del personal	VU43 - Ausencia del personal	2	2	3	Significativo	4	3	3
Activo 64	AM13 - Pérdida del suministro de electricidad	VU6 - Susceptibilidad a variación de voltaje	2	2	3	Significativo	4	3	3
Activo 65	AM22 - Robo de equipos o partes	VU54 - Falta de protección física del edificio, puertas, ventanas	2	2	3	Significativo	4	3	3
	AM13 - Pérdida del suministro de electricidad	VU6 - Susceptibilidad a variación de voltaje	2	2	3	Significativo	4	3	
	AM1 - Incendio	VU131 - Ausencia de sistema contraincendios con propiedades dieléctricas	3	3	3	Catastrófico	5	3	
Activo 66	AM72 - Disfunciones del sistema (bugs)	VU12 - Errores conocidos en el software	2	2	3	Significativo	4	3	3
Activo 67	AM70 - Códigos maliciosos (ej. Virus, bomba lógica, troyano)	VU115 - Falta de actualización de parches	2	2	3	Significativo	4	3	3
Activo 68	AM30 - Mal funcionamiento del equipo	VU100 - Fallas conocidas del hardware	2	2	3	Significativo	4	3	3
Activo 69	AM43 - Hacking	VU96 - No se realiza la Identificación y Gestión de Vulnerabilidades	2	2	3	Significativo	4	3	3
Activo 70	AM80 - Pérdida de información	VU130 - Ausencia de un mecanismo de control del ingreso/acceso a la infraestructura informática (léase Active Directory, servidor de archivos), que compare la presencia del usuario legítimo versus su propósito laboral	2	2	3	Significativo	4	3	3
Activo 71	AM72 - Disfunciones del sistema (bugs)	VU12 - Errores conocidos en el software	3	3	3	Catastrófico	5	2	2
Activo 72	AM22 - Robo de equipos o partes	VU54 - Falta de protección física del edificio, puertas, ventanas	3	3	2	Catastrófico	5	2	2
Activo 73	AM14 - Falla del equipo de telecomunicaciones	VU10 - Equipo desfasado por vigencia tecnológica	2	3	3	Catastrófico	5	2	2
Activo 74	AM72 - Disfunciones del sistema (bugs)	VU12 - Errores conocidos en el software	2	2	3	Significativo	4	3	3

FICHA DE OBSERVACIÓN N° 01

INDICADOR: NIVEL DE PROBABILIDAD

FASE: POST-TEST

CODIGO:	SGSI-FO-001-PT	**VERSIÓN:**	V1
CLASIFICACIÓN:	CONFIDENCIAL	**FECHA DIESÑO:**	Mar-23
PROCESO:	GESTIÓN DE RIESGOS		
INVESTIGADOR:	HENRY FRANK HUAMANTECA DAMIAN		
FECHA DE RECOLECCIÓN:	3 al 7 de abril		
PUESTO:			

IDENTIFICACION DE RIESGOS							ANÁLISIS DE RIESGOS		PROBABILIDAD PROMEDIO
CODIGO ACTIVO	AMENAZA	VULNERABI|LIDAD	DEGRADACIÓN				IMPACTO	PROBABILIDAD	
			C	I	D	DREGADACIÓN MAXIMA			
Activo 1	AM97 - Falla del sistema operativo	VU15 - Falta de evidencia de auditoria	2	2	3	Significativo	4	2	1,80
	AM97 - Falla del sistema operativo	VU21 - Seteo incorrecto de parámetros|	2	2	3	Significativo	4	2	
	AM13 - Pérdida del suministro de electricidad	VU3 - Susceptibilidad a la humedad, al polvo y a la suciedad	2	2	3	Significativo	4	2	
	AM30 - Mal funcionamiento del equipo	VU10 - Equipo desfasado por vigencia tecnológica	2	1	3	Significativo	4	1	
	AM30 - Mal funcionamiento del equipo	VU100 - Fallas conocidas del hardware	2	2	3	Significativo	4	2	
Activo 2	AM29 - Falla de equipo	VU3 - Susceptibilidad a la humedad, al polvo y a la suciedad	1	1	3	Significativo	4	2	1,75
	AM29 - Falla de equipo	VU10 - Equipo desfasado por vigencia tecnológica	2	1	3	Significativo	4	2	
	AM86 - No soporta nuevas tecnologías de hardware y software	VU10 - Equipo desfasado por vigencia tecnológica	2	1	3	Significativo	4	1	
	AM13 - Pérdida del suministro de	VU3 - Susceptibilidad a la humedad, al polvo y a la	2	2	3	Significativo	4	2	

	electricidad	suciedad							
Activo 3	AM30 - Mal funcionamiento del equipo	VU100 - Fallas conocidas del hardware	2	2	3	Significativo	4	2	2,00
Activo 4	AM30 - Mal funcionamiento del equipo	VU100 - Fallas conocidas del hardware	2	2	3	Significativo	4	2	2,00
Activo 5	AM30 - Mal funcionamiento del equipo	VU100 - Fallas conocidas del hardware	2	2	3	Significativo	4	2	2,00
Activo 6	AM30 - Mal funcionamiento del equipo	VU100 - Fallas conocidas del hardware	2	2	3	Significativo	4	2	2,00
Activo 7	AM29 - Falla de equipo	VU3 - Susceptibilidad a la humedad, al polvo y a la suciedad	1	1	3	Significativo	4	2	1,75
	AM29 - Falla de equipo	VU10 - Equipo desfasado por vigencia tecnológica	2	1	3	Significativo	4	2	
	AM86 - No soporta nuevas tecnologías de hardware y software	VU10 - Equipo desfasado por vigencia tecnológica	2	1	3	Significativo	4	1	
	AM13 - Pérdida del suministro de electricidad	VU3 - Susceptibilidad a la humedad, al polvo y a la suciedad	2	2	3	Significativo	4	2	
Activo 8	AM30 - Mal funcionamiento del equipo	VU100 - Fallas conocidas del hardware	2	2	3	Significativo	4	2	2,00
Activo 9	AM30 - Mal funcionamiento del equipo	VU100 - Fallas conocidas del hardware	2	2	3	Significativo	4	2	2,00
Activo 10	AM30 - Mal funcionamiento del equipo	VU100 - Fallas conocidas del hardware	2	2	3	Significativo	4	2	2,00
Activo 11	AM30 - Mal funcionamiento del equipo	VU100 - Fallas conocidas del hardware	2	2	3	Significativo	4	2	2,00
Activo 12	AM32 - Mal funcionamiento del software	VU115 - Falta de actualización de parches	2	2	3	Significativo	4	2	2,00
Activo 13	AM97 - Falla del sistema operativo	VU21 - Seteo incorrecto de parámetros	2	2	3	Significativo	4	2	2,00
Activo 14	AM88 - Instalación de software sin autorización, sin licencia	VU105 - Uso no controlado de licencias	1	1	3	Significativo	4	1	1,00
Activo 15	AM13 - Pérdida del suministro de electricidad	VU3 - Susceptibilidad a la humedad, al polvo y a la suciedad	2	2	3	Significativo	4	1	1,00
Activo 16	AM30 - Mal funcionamiento del equipo	VU100 - Fallas conocidas del hardware	3	2	2	Significativo	4	1	1,00

Activo 17	AM29 - Falla de equipo	VU124 - La aplicación, el soporte, registro de incidentes, mantenimiento servidores y otros equipos, servicio de backups lo realiza el proveedor del servicio ante una finalización de contrato la ENTIDAD quedaría sin este servicio	2	2	3	Significativo	4	1	1,00
Activo 18	AM99 - Ciberataques	VU96 - No se realiza la Identificación y Gestión de Vulnerabilidades	2	2	3	Significativo	4	1	1,00
Activo 19	AM13 - Pérdida del suministro de electricidad	VU3 - Susceptibilidad a la humedad, al polvo y a la suciedad	3	3	2	Catastrófico	5	1	1,00
Activo 20	AM99 - Ciberataques	VU96 - No se realiza la Identificación y Gestión de Vulnerabilidades	2	3	3	Catastrófico	5	1	1,00
Activo 21	AM6 - Polvo, corrosión, congelación	VU1 - Mantenimiento insuficiente / instalación fallida de medios de almacenamiento / Asignación Insuficiente de recursos	2	2	3	Significativo	4	2	2,00
Activo 22	AM72 - Disfunciones del sistema (bugs)	VU12 - Errores conocidos en el software	2	2	3	Significativo	4	2	2,00
Activo 23	AM29 - Falla de equipo	VU124 - La aplicación, el soporte, registro de incidentes, mantenimiento servidores y otros equipos, servicio de backups lo realiza el proveedor del servicio ante una finalización de contrato la ENTIDAD quedaría sin este servicio	2	2	3	Significativo	4	2	2,00
Activo 24	AM6 - Polvo, corrosión, congelación	VU1 - Mantenimiento insuficiente / instalación fallida de medios de almacenamiento / Asignación Insuficiente de recursos	2	2	3	Significativo	4	2	2,00
Activo 25	AM72 - Disfunciones del sistema (bugs)	VU12 - Errores conocidos en el software	2	2	3	Significativo	4	1	1,00
Activo 26	AM98 - Recortes presupuestales que afecta la adquisición de bienes y/o servicios	VU100 - Fallas conocidas del hardware	2	2	3	Significativo	4	1	1,00

	tecnológicos para la mejora del SGSI.								
Activo 27	AM72 - Disfunciones del sistema (bugs)	VU12 - Errores conocidos en el software	2	2	3	Significativo	4	1	1,00
Activo 28	AM72 - Disfunciones del sistema (bugs)	VU12 - Errores conocidos en el software	2	2	3	Significativo	4	1	1,00
Activo 29	AM72 - Disfunciones del sistema (bugs)	VU12 - Errores conocidos en el software	2	2	3	Significativo	4	1	1,00
Activo 30	AM32 - Mal funcionamiento del software	VU106 - Falta de renovación de licencias	2	2	3	Significativo	4	1	1,00
Activo 31	AM43 - Hacking	VU96 - No se realiza la Identificación y Gestión de Vulnerabilidades	2	2	3	Significativo	4	2	2,00
Activo 32	AM32 - Mal funcionamiento del software	VU106 - Falta de renovación de licencias	3	2	2	Significativo	4	1	1,00
Activo 33	AM32 - Mal funcionamiento del software	VU106 - Falta de renovación de licencias	2	2	3	Significativo	4	1	1,00
Activo 34	AM97 - Falla del sistema operativo	VU115 - Falta de actualización de parches	2	2	3	Significativo	4	1	1,00
Activo 35	AM97 - Falla del sistema operativo	VU115 - Falta de actualización de parches	2	2	3	Significativo	4	1	1,00
Activo 36	AM97 - Falla del sistema operativo	VU115 - Falta de actualización de parches	2	2	3	Significativo	4	1	1,00
Activo 37	AM97 - Falla del sistema operativo	VU115 - Falta de actualización de parches	2	2	3	Significativo	4	1	1,00
Activo 38	AM97 - Falla del sistema operativo	VU115 - Falta de actualización de parches	2	2	3	Significativo	4	1	1,00
Activo 39	AM72 - Disfunciones del sistema (bugs)	VU12 - Errores conocidos en el software	2	2	3	Significativo	4	2	2,00
Activo 40	AM99 - Ciberataques	VU96 - No se realiza la Identificación y Gestión de Vulnerabilidades	2	2	3	Significativo	4	2	2,00
Activo 41	AM99 - Ciberataques	VU96 - No se realiza la Identificación y Gestión de Vulnerabilidades	2	2	3	Significativo	4	2	2,00
Activo 42	AM46 - Acceso no autorizado al sitema	VU144 - Falta de un procedimiento formal o su actualización, para el registro y baja de usuarios	2	2	3	Significativo	4	1	1,00
Activo 43	AM29 - Falla de equipo	VU3 - Susceptibilidad a la humedad, al polvo y a la suciedad	2	2	3	Significativo	4	1	1,00
Activo 44	AM13 - Pérdida del suministro de electricidad	VU6 - Susceptibilidad a variación de voltaje	2	2	3	Significativo	4	1	1,00

Activo 45	AM29 - Falla de equipo	VU96 - No se realiza la Identificación y Gestión de Vulnerabilidades	2	2	3	Significativo	4	1	1,00
Activo 46	AM99 - Ciberataques	VU1 - Mantenimiento insuficiente / instalación fallida de medios de almacenamiento / Asignación Insuficiente de recursos	2	2	3	Significativo	4	1	1,00
Activo 47	AM99 - Ciberataques	VU1 - Mantenimiento insuficiente / instalación fallida de medios de almacenamiento / Asignación Insuficiente de recursos	2	2	3	Significativo	4	1	1,00
Activo 48	AM35 - Uso de software falsificado o copiado	VU46 - Uso incorrecto del software y hardware	2	3	1	Significativo	4	1	1,00
Activo 49	AM43 - Hacking	VU46 - Uso incorrecto del software y hardware	2	3	1	Significativo	4	1	1,00
Activo 50	AM21 - Robo de medios o documentos	VU125 - Eventos e incidentes que afecten a la seguridad de la información mal gestionados	3	3	2	Catastrófico	5	1	1,00
Activo 51	AM29 - Falla de equipo	VU10 - Equipo desfasado por vigencia tecnológica	2	2	3	Significativo	4	1	1,50
	AM13 - Pérdida del suministro de electricidad	VU6 - Susceptibilidad a variación de voltaje	2	2	3	Significativo	4	1	
	AM6 - Polvo, corrosión, congelación	VU3 - Susceptibilidad a la humedad, al polvo y a la suciedad	2	2	3	Significativo	4	2	
	AM12 - Fallas del sistema de aire acondicionado o del suministro de agua	VU6 - Susceptibilidad a variación de voltaje	2	2	3	Significativo	4	2	
Activo 52	AM12 - Fallas del sistema de aire acondicionado o del suministro de agua	VU6 - Susceptibilidad a variación de voltaje	2	2	3	Significativo	4	1	1,00
Activo 53	AM5 - Destrucción del equipo o los medios	VU41 - Gestión inadecuada de la red (capacidad de recuperación del ruteo)	2	2	3	Significativo	4	1	1,00
Activo 54	AM5 - Destrucción del equipo o los medios	VU41 - Gestión inadecuada de la red (capacidad de recuperación del ruteo)	2	2	3	Significativo	4	1	1,00
Activo 55	AM5 - Destrucción del equipo o los medios	VU41 - Gestión inadecuada de la red (capacidad de recuperación del ruteo)	2	2	3	Significativo	4	1	1,00

Activo 56	AM91 - Indisponibilidad del Servicio de Help Desk	VU124 - La aplicación, el soporte, registro de incidentes, mantenimiento servidores y otros equipos, servicio de backups lo realiza el proveedor del servicio ante una finalización de contrato la ENTIDAD quedaría sin este servicio	2	2	3	Significativo	4	1	1,00
Activo 57	AM29 - Falla de equipo	VU124 - La aplicación, el soporte, registro de incidentes, mantenimiento servidores y otros equipos, servicio de backups lo realiza el proveedor del servicio ante una finalización de contrato la ENTIDAD quedaría sin este servicio	2	2	3	Significativo	4	2	2,00
Activo 58	AM29 - Falla de equipo	VU124 - La aplicación, el soporte, registro de incidentes, mantenimiento servidores y otros equipos, servicio de backups lo realiza el proveedor del servicio ante una finalización de contrato la ENTIDAD quedaría sin este servicio	2	2	3	Significativo	4	2	2,00
Activo 59	AM29 - Falla de equipo	VU124 - La aplicación, el soporte, registro de incidentes, mantenimiento servidores y otros equipos, servicio de backups lo realiza el proveedor del servicio ante una finalización de contrato la ENTIDAD quedaría sin este servicio	2	2	3	Significativo	4	2	2,00
Activo 60	AM42 - Ruptura en la disponibilidad del personal	VU43 - Ausencia del personal	2	2	3	Significativo	4	2	2,00
Activo 61	AM42 - Ruptura en la disponibilidad del personal	VU43 - Ausencia del personal	2	2	3	Significativo	4	2	2,00

Activo 62	AM42 - Ruptura en la disponibilidad del personal	VU43 - Ausencia del personal	2	2	3	Significativo	4	2	2,00
Activo 63	AM42 - Ruptura en la disponibilidad del personal	VU43 - Ausencia del personal	2	2	3	Significativo	4	2	2,00
Activo 64	AM13 - Pérdida del suministro de electricidad	VU6 - Susceptibilidad a variación de voltaje	2	2	3	Significativo	4	2	2,00
Activo 65	AM22 - Robo de equipos o partes	VU54 - Falta de protección física del edificio, puertas, ventanas	2	2	3	Significativo	4	2	2,00
	AM13 - Pérdida del suministro de electricidad	VU6 - Susceptibilidad a variación de voltaje	2	2	3	Significativo	4	2	
	AM1 - Incendio	VU131 - Ausencia de sistema contraincendios con propiedades dieléctricas	3	3	3	Catastrófico	5	2	
Activo 66	AM72 - Disfunciones del sistema (bugs)	VU12 - Errores conocidos en el software	2	2	3	Significativo	4	2	2,00
Activo 67	AM70 - Códigos maliciosos (ej. Virus, bomba lógica, troyano)	VU115 - Falta de actualización de parches	2	2	3	Significativo	4	2	2,00
Activo 68	AM30 - Mal funcionamiento del equipo	VU100 - Fallas conocidas del hardware	2	2	3	Significativo	4	2	2,00
Activo 69	AM43 - Hacking	VU96 - No se realiza la Identificación y Gestión de Vulnerabilidades	2	2	3	Significativo	4	2	2,00
Activo 70	AM80 - Pérdida de información	VU130 - Ausencia de un mecanismo de control del ingreso/acceso a la infraestructura informática (léase Active Directory, servidor de archivos), que compare la presencia del usuario legítimo versus su propósito laboral	2	2	3	Significativo	4	2	2,00
Activo 71	AM72 - Disfunciones del sistema (bugs)	VU12 - Errores conocidos en el software	3	3	3	Catastrófico	5	1	1,00
Activo 72	AM22 - Robo de equipos o partes	VU54 - Falta de protección física del edificio, puertas, ventanas	3	3	2	Catastrófico	5	1	1,00
Activo 73	AM14 - Falla del equipo de telecomunicaciones	VU10 - Equipo desfasado por vigencia tecnológica	2	3	3	Catastrófico	5	1	1,00
Activo 74	AM72 - Disfunciones del sistema (bugs)	VU12 - Errores conocidos en el software	2	2	3	Significativo	4	1	1,00

TABLA RESUMEN

INDICADOR: NIVEL DE PROBABILIDAD

CODIGO ACTIVO	PRE TEST	POST TEST
ACTIVO 1	3,00	1,80
ACTIVO 2	2,75	1,75
ACTIVO 3	3,00	2,00
ACTIVO 4	3,00	2,00
ACTIVO 5	3,00	2,00
ACTIVO 6	3,00	2,00
ACTIVO 7	2,75	1,75
ACTIVO 8	3,00	2,00
ACTIVO 9	3,00	2,00
ACTIVO 10	3,00	2,00
ACTIVO 11	3,00	2,00
ACTIVO 12	3,00	2,00
ACTIVO 13	3,00	2,00
ACTIVO 14	3,00	1,00
ACTIVO 15	2,00	1,00
ACTIVO 16	2,00	1,00
ACTIVO 17	2,00	1,00
ACTIVO 18	2,00	1,00
ACTIVO 19	2,00	1,00
ACTIVO 20	3,00	1,00
ACTIVO 21	3,00	2,00
ACTIVO 22	3,00	2,00
ACTIVO 23	3,00	2,00
ACTIVO 24	3,00	2,00
ACTIVO 25	3,00	1,00
ACTIVO 26	2,00	1,00
ACTIVO 27	2,00	1,00
ACTIVO 28	2,00	1,00
ACTIVO 29	2,00	1,00
ACTIVO 30	2,00	1,00

ACTIVO 31	2,00	2,00
ACTIVO 32	3,00	1,00
ACTIVO 33	2,00	1,00
ACTIVO 34	2,00	1,00
ACTIVO 35	2,00	1,00
ACTIVO 36	2,00	1,00
ACTIVO 37	2,00	1,00
ACTIVO 38	2,00	1,00
ACTIVO 39	2,00	2,00
ACTIVO 40	3,00	2,00
ACTIVO 41	3,00	2,00
ACTIVO 42	3,00	1,00
ACTIVO 43	2,00	1,00
ACTIVO 44	2,00	1,00
ACTIVO 45	2,00	1,00
ACTIVO 46	2,00	1,00
ACTIVO 47	2,00	1,00
ACTIVO 48	2,00	1,00
ACTIVO 49	2,00	1,00
ACTIVO 50	2,00	1,00
ACTIVO 51	2,50	1,50
ACTIVO 52	3,00	1,00
ACTIVO 53	2,00	1,00
ACTIVO 54	2,00	1,00
ACTIVO 55	2,00	1,00
ACTIVO 56	2,00	1,00
ACTIVO 57	2,00	2,00
ACTIVO 58	3,00	2,00
ACTIVO 59	3,00	2,00
ACTIVO 60	3,00	2,00
ACTIVO 61	3,00	2,00
ACTIVO 62	3,00	2,00
ACTIVO 63	3,00	2,00
ACTIVO 64	3,00	2,00
ACTIVO 65	3,00	2,00
ACTIVO 66	3,00	2,00
ACTIVO 67	3,00	2,00
ACTIVO 68	3,00	2,00
ACTIVO 69	3,00	2,00

ACTIVO 70	3,00	2,00
ACTIVO 71	3,00	1,00
ACTIVO 72	2,00	1,00
ACTIVO 73	2,00	1,00
ACTIVO 74	2,00	1,00
PROMEDIO	**2,53**	**1,47**

FICHA DE OBSERVACIÓN N° 02

INDICADOR: NIVEL DE RIESGO

FASE: PRE-TEST

CODIGO:	SGSI-FO-002-PT	**VERSIÓN:**	V1
CLASIFICACIÓN:	CONFIDENCIAL	**FECHA DIESÑO:**	Mar-23
PROCESO:	GESTIÓN DE RIESGOS		
INVESTIGADOR:	HENRY FRANK HUAMANTECA DAMIAN		
FECHA DE RECOLECCIÓN:	6 al 10 de marzo		
PUESTO:			

IDENTIFICACIÓN DE RIESGOS			**DEGRADACIÓN**				**ANÁLISIS DE RIESGOS**			**RIESGO PROMEDIO**
CÓDIGO ACTIVO	**AMENAZA**	**VULNERABILIDAD**	**C**	**I**	**D**	**DEGRADACIÓN MAXIMA**	IMPACTO	PROBABILIDAD	RIESGO	
Activo 1	AM97 - Falla del sistema operativo	VU15 - Falta de evidencia de auditoria	2	2	3	Significativo	4	3	12	12,00
	AM97 - Falla del sistema operativo	VU21 - Seteo incorrecto de parámetros	2	2	3	Significativo	4	3	12	
	AM13 - Pérdida del suministro de electricidad	VU3 - Susceptibilidad a la humedad, al polvo y a la suciedad	2	2	3	Significativo	4	3	12	
	AM30 - Mal funcionamiento del equipo	VU10 - Equipo desfasado por vigencia tecnológica	2	1	3	Significativo	4	3	12	
	AM30 - Mal funcionamiento del equipo	VU100 - Fallas conocidas del hardware	2	2	3	Significativo	4	3	12	
Activo 2	AM29 - Falla de equipo	VU3 - Susceptibilidad a la humedad, al polvo y a la suciedad	1	1	3	Significativo	4	3	12	11,00
	AM29 - Falla de equipo	VU10 - Equipo desfasado por vigencia tecnológica	2	1	3	Significativo	4	3	12	
	AM86 - No soporta nuevas tecnologías de hardware y software	VU10 - Equipo desfasado por vigencia tecnológica	2	1	3	Significativo	4	2	8	
	AM13 - Pérdida del suministro de electricidad	VU3 - Susceptibilidad a la humedad, al polvo y a la suciedad	2	2	3	Significativo	4	3	12	

Activo 3	AM30 - Mal funcionamiento del equipo	VU100 - Fallas conocidas del hardware	2	2	3	Significativo	4	3	12	12,00
Activo 4	AM30 - Mal funcionamiento del equipo	VU100 - Fallas conocidas del hardware	2	2	3	Significativo	4	3	12	12,00
Activo 5	AM30 - Mal funcionamiento del equipo	VU100 - Fallas conocidas del hardware	2	2	3	Significativo	4	3	12	12,00
Activo 6	AM30 - Mal funcionamiento del equipo	VU100 - Fallas conocidas del hardware	2	2	3	Significativo	4	3	12	12,00
Activo 7	AM29 - Falla de equipo	VU3 - Susceptibilidad a la humedad, al polvo y a la suciedad	1	1	3	Significativo	4	3	12	11,00
	AM29 - Falla de equipo	VU10 - Equipo desfasado por vigencia tecnológica	2	1	3	Significativo	4	3	12	
	AM86 - No soporta nuevas tecnologías de hardware y software	VU10 - Equipo desfasado por vigencia tecnológica	2	1	3	Significativo	4	2	8	
	AM13 - Pérdida del suministro de electricidad	VU3 - Susceptibilidad a la humedad, al polvo y a la suciedad	2	2	3	Significativo	4	3	12	
Activo 8	AM30 - Mal funcionamiento del equipo	VU100 - Fallas conocidas del hardware	2	2	3	Significativo	4	3	12	12,00
Activo 9	AM30 - Mal funcionamiento del equipo	VU100 - Fallas conocidas del hardware	2	2	3	Significativo	4	3	12	12,00
Activo 10	AM30 - Mal funcionamiento del equipo	VU100 - Fallas conocidas del hardware	2	2	3	Significativo	4	3	12	12,00
Activo 11	AM30 - Mal funcionamiento del equipo	VU100 - Fallas conocidas del hardware	2	2	3	Significativo	4	3	12	12,00
Activo 12	AM32 - Mal funcionamiento del software	VU115 - Falta de actualización de parches	2	2	3	Significativo	4	3	12	12,00
Activo 13	AM97 - Falla del sistema operativo	VU21 - Seteo incorrecto de parámetros	2	2	3	Significativo	4	3	12	12,00
Activo 14	AM88 - Instalación de software sin autorización, sin licencia	VU105 - Uso no controlado de licencias	1	1	3	Significativo	4	2	8	8,00
Activo 15	AM13 - Pérdida del suministro de electricidad	VU3 - Susceptibilidad a la humedad, al polvo y a la suciedad	2	2	3	Significativo	4	2	8	8,00
Activo 16	AM30 - Mal funcionamiento del equipo	VU100 - Fallas conocidas del hardware	3	2	2	Significativo	4	2	8	8,00

Activo 17	AM29 - Falla de equipo	VU124 - La aplicación, el soporte, registro de incidentes, mantenimiento servidores y otros equipos, servicio de backups lo realiza el proveedor del servicio ante una finalización de contrato la ENTIDAD quedaría sin este servicio	2	2	3	Significativo	4	2	8	8,00
Activo 18	AM99 - Ciberataques	VU96 - No se realiza la Identificación y Gestión de Vulnerabilidades	2	2	3	Significativo	4	2	8	8,00
Activo 19	AM13 - Pérdida del suministro de electricidad	VU3 - Susceptibilidad a la humedad, al polvo y a la suciedad	3	3	2	Catastrófico	5	3	15	15,00
Activo 20	AM99 - Ciberataques	VU96 - No se realiza la Identificación y Gestión de Vulnerabilidades	2	3	3	Catastrófico	5	3	15	15,00
Activo 21	AM6 - Polvo, corrosión, congelación	VU1 - Mantenimiento insuficiente / instalación fallida de medios de almacenamiento / Asignación Insuficiente de recursos	2	2	3	Significativo	4	3	12	12,00
Activo 22	AM72 - Disfunciones del sistema (bugs)	VU12 - Errores conocidos en el software	2	2	3	Significativo	4	3	12	12,00
Activo 23	AM29 - Falla de equipo	VU124 - La aplicación, el soporte, registro de incidentes, mantenimiento servidores y otros equipos, servicio de backups lo realiza el proveedor del servicio ante una finalización de contrato la ENTIDAD quedaría sin este servicio	2	2	3	Significativo	4	3	12	12,00
Activo 24	AM6 - Polvo, corrosión, congelación	VU1 - Mantenimiento insuficiente / instalación fallida de medios de almacenamiento / Asignación Insuficiente de recursos	2	2	3	Significativo	4	3	12	12,00
Activo 25	AM72 - Disfunciones del sistema (bugs)	VU12 - Errores conocidos en el software	2	2	3	Significativo	4	2	8	8,00

Activo 26	AM98 - Recortes presupuestales que afecta la adquisición de bienes y/o servicios tecnológicos para la mejora del SGSI.	VU100 - Fallas conocidas del hardware	2	2	3	Significativo	4	2	8	8,00
Activo 27	AM72 - Disfunciones del sistema (bugs)	VU12 - Errores conocidos en el software	2	2	3	Significativo	4	2	8	8,00
Activo 28	AM72 - Disfunciones del sistema (bugs)	VU12 - Errores conocidos en el software	2	2	3	Significativo	4	2	8	8,00
Activo 29	AM72 - Disfunciones del sistema (bugs)	VU12 - Errores conocidos en el software	2	2	3	Significativo	4	2	8	8,00
Activo 30	AM32 - Mal funcionamiento del software	VU106 - Falta de renovación de licencias	2	2	3	Significativo	4	2	8	8,00
Activo 31	AM43 - Hacking	VU96 - No se realiza la Identificación y Gestión de Vulnerabilidades	2	2	3	Significativo	4	3	12	12,00
Activo 32	AM32 - Mal funcionamiento del software	VU106 - Falta de renovación de licencias	3	2	2	Significativo	4	2	8	8,00
Activo 33	AM32 - Mal funcionamiento del software	VU106 - Falta de renovación de licencias	2	2	3	Significativo	4	2	8	8,00
Activo 34	AM97 - Falla del sistema operativo	VU115 - Falta de actualización de parches	2	2	3	Significativo	4	2	8	8,00
Activo 35	AM97 - Falla del sistema operativo	VU115 - Falta de actualización de parches	2	2	3	Significativo	4	2	8	8,00
Activo 36	AM97 - Falla del sistema operativo	VU115 - Falta de actualización de parches	2	2	3	Significativo	4	2	8	8,00
Activo 37	AM97 - Falla del sistema operativo	VU115 - Falta de actualización de parches	2	2	3	Significativo	4	2	8	8,00
Activo 38	AM97 - Falla del sistema operativo	VU115 - Falta de actualización de parches	2	2	3	Significativo	4	2	8	8,00
Activo 39	AM72 - Disfunciones del sistema (bugs)	VU12 - Errores conocidos en el software	2	2	3	Significativo	4	3	12	12,00
Activo 40	AM99 - Ciberataques	VU96 - No se realiza la Identificación y Gestión de Vulnerabilidades	2	2	3	Significativo	4	3	12	12,00
Activo 41	AM99 - Ciberataques	VU96 - No se realiza la Identificación y Gestión de	2	2	3	Significativo	4	3	12	12,00

		Vulnerabilidades								
Activo 42	AM46 - Acceso no autorizado al sitema	VU144 - Falta de un procedimiento formal o su actualización, para el registro y baja de usuarios	2	2	3	Significativo	4	2	8	8,00
Activo 43	AM29 - Falla de equipo	VU3 - Susceptibilidad a la humedad, al polvo y a la suciedad	2	2	3	Significativo	4	2	8	8,00
Activo 44	AM13 - Pérdida del suministro de electricidad	VU6 - Susceptibilidad a variación de voltaje	2	2	3	Significativo	4	2	8	8,00
Activo 45	AM29 - Falla de equipo	VU96 - No se realiza la Identificación y Gestión de Vulnerabilidades	2	2	3	Significativo	4	2	8	8,00
Activo 46	AM99 - Ciberataques	VU1 - Mantenimiento insuficiente / instalación fallida de medios de almacenamiento / Asignación Insuficiente de recursos	2	2	3	Significativo	4	2	8	8,00
Activo 47	AM99 - Ciberataques	VU1 - Mantenimiento insuficiente / instalación fallida de medios de almacenamiento / Asignación Insuficiente de recursos	2	2	3	Significativo	4	2	8	8,00
Activo 48	AM35 - Uso de software falsificado o copiado	VU46 - Uso incorrecto del software y hardware	2	3	1	Significativo	4	2	8	8,00
Activo 49	AM43 - Hacking	VU46 - Uso incorrecto del software y hardware	2	3	1	Significativo	4	2	8	8,00
Activo 50	AM21 - Robo de medios o documentos	VU125 - Eventos e incidentes que afecten a la seguridad de la información mal gestionados	3	3	2	Catastrófico	5	3	15	15,00
Activo 51	AM29 - Falla de equipo	VU10 - Equipo desfasado por vigencia tecnológica	2	2	3	Significativo	4	2	8	10,00
	AM13 - Pérdida del suministro de electricidad	VU6 - Susceptibilidad a variación de voltaje	2	2	3	Significativo	4	2	8	
	AM6 - Polvo, corrosión, congelación	VU3 - Susceptibilidad a la humedad, al polvo y a la suciedad	2	2	3	Significativo	4	3	12	
	AM12 - Fallas del sistema de aire acondicionado o del	VU6 - Susceptibilidad a variación de voltaje	2	2	3	Significativo	4	3	12	

	suministro de agua									
Activo 52	AM12 - Fallas del sistema de aire acondicionado o del suministro de agua	VU6 - Susceptibilidad a variación de voltaje	2	2	3	Significativo	4	2	8	8,00
Activo 53	AM5 - Destrucción del equipo o los medios	VU41 - Gestión inadecuada de la red (capacidad de recuperación del ruteo)	2	2	3	Significativo	4	2	8	8,00
Activo 54	AM5 - Destrucción del equipo o los medios	VU41 - Gestión inadecuada de la red (capacidad de recuperación del ruteo)	2	2	3	Significativo	4	2	8	8,00
Activo 55	AM5 - Destrucción del equipo o los medios	VU41 - Gestión inadecuada de la red (capacidad de recuperación del ruteo)	2	2	3	Significativo	4	2	8	8,00
Activo 56	AM91 - Indisponibilidad del Servicio de Help Desk	VU124 - La aplicación, el soporte, registro de incidentes, mantenimiento servidores y otros equipos, servicio de backups lo realiza el proveedor del servicio ante una finalización de contrato la ENTIDAD quedaría sin este servicio	2	2	3	Significativo	4	2	8	8,00
Activo 57	AM29 - Falla de equipo	VU124 - La aplicación, el soporte, registro de incidentes, mantenimiento servidores y otros equipos, servicio de backups lo realiza el proveedor del servicio ante una finalización de contrato la ENTIDAD quedaría sin este servicio	2	2	3	Significativo	4	3	12	12,00
Activo 58	AM29 - Falla de equipo	VU124 - La aplicación, el soporte, registro de incidentes, mantenimiento servidores y otros equipos, servicio de backups lo realiza el proveedor del servicio ante una finalización	2	2	3	Significativo	4	3	12	12,00

		de contrato la ENTIDAD quedaría sin este servicio								
Activo 59	AM29 - Falla de equipo	VU124 - La aplicación, el soporte, registro de incidentes, mantenimiento servidores y otros equipos, servicio de backups lo realiza el proveedor del servicio ante una finalización de contrato la ENTIDAD quedaría sin este servicio	2	2	3	Significativo	4	3	12	12,00
Activo 60	AM42 - Ruptura en la disponibilidad del personal	VU43 - Ausencia del personal	2	2	3	Significativo	4	3	12	12,00
Activo 61	AM42 - Ruptura en la disponibilidad del personal	VU43 - Ausencia del personal	2	2	3	Significativo	4	3	12	12,00
Activo 62	AM42 - Ruptura en la disponibilidad del personal	VU43 - Ausencia del personal	2	2	3	Significativo	4	3	12	12,00
Activo 63	AM42 - Ruptura en la disponibilidad del personal	VU43 - Ausencia del personal	2	2	3	Significativo	4	3	12	12,00
Activo 64	AM13 - Pérdida del suministro de electricidad	VU6 - Susceptibilidad a variación de voltaje	2	2	3	Significativo	4	3	12	12,00
Activo 65	AM22 - Robo de equipos o partes	VU54 - Falta de protección física del edificio, puertas, ventanas	2	2	3	Significativo	4	3	12	13,00
	AM13 - Pérdida del suministro de electricidad	VU6 - Susceptibilidad a variación de voltaje	2	2	3	Significativo	4	3	12	
	AM1 - Incendio	VU131 - Ausencia de sistema contraincendios con propiedades dieléctricas	3	3	3	Catastrófico	5	3	15	
Activo 66	AM72 - Disfunciones del sistema (bugs)	VU12 - Errores conocidos en el software	2	2	3	Significativo	4	3	12	12,00
Activo 67	AM70 - Códigos maliciosos (ej. Virus, bomba lógica, troyano)	VU115 - Falta de actualización de parches	2	2	3	Significativo	4	3	12	12,00
Activo 68	AM30 - Mal funcionamiento del equipo	VU100 - Fallas conocidas del hardware	2	2	3	Significativo	4	3	12	12,00

Activo 69	AM43 - Hacking	VU96 - No se realiza la Identificación y Gestión de Vulnerabilidades	2	2	3	Significativo	4	3	12	12,00
Activo 70	AM80 - Pérdida de información	VU130 - Ausencia de un mecanismo de control del ingreso/acceso a la infraestructura informática (léase Active Directory, servidor de archivos), que compare la presencia del usuario legítimo versus su propósito laboral	2	2	3	Significativo	4	3	12	12,00
Activo 71	AM72 - Disfunciones del sistema (bugs)	VU12 - Errores conocidos en el software	3	3	3	Catastrófico	5	2	10	10,00
Activo 72	AM22 - Robo de equipos o partes	VU54 - Falta de protección física del edificio, puertas, ventanas	3	3	2	Catastrófico	5	2	10	10,00
Activo 73	AM14 - Falla del equipo de telecomunicaciones	VU10 - Equipo desfasado por vigencia tecnológica	2	3	3	Catastrófico	5	2	10	10,00
Activo 74	AM72 - Disfunciones del sistema (bugs)	VU12 - Errores conocidos en el software	2	2	3	Significativo	4	3	12	12,00

FICHA DE OBSERVACIÓN N° 02

INDICADOR: NIVEL DE RIESGO

FASE: POST-TEST

CODIGO:	SGSI-FO-002-PT	**VERSIÓN:**	V1
CLASIFICACIÓN:	CONFIDENCIAL	**FECHA DIESÑO:**	Mar-23
PROCESO:	GESTIÓN DE RIESGOS		
INVESTIGADOR:	HENRY FRANK HUAMANTECA DAMIAN		
FECHA DE RECOLECCIÓN:	3 al 7 de abril		
PUESTO:			

IDENTIFICACIÓN DE RIESGOS			**DEGRADACIÓN**				**ANÁLISIS DE RIESGOS**			**RIESGO PROMEDIO**
CÓDIGO ACTIVO	**AMENAZA**	**VULNERABILIDAD**	**C**	**I**	**D**	**DEGRADACIÓN MAXIMA**	IMPACTO	PROBABILIDAD	RIESGO	
Activo 1	AM97 - Falla del sistema operativo	VU15 - Falta de evidencia de auditoria	2	2	3	Significativo	4	2	8	7,20
	AM97 - Falla del sistema operativo	VU21 - Seteo incorrecto de parámetros	2	2	3	Significativo	4	2	8	
	AM13 - Pérdida del suministro de electricidad	VU3 - Susceptibilidad a la humedad, al polvo y a la suciedad	2	2	3	Significativo	4	2	8	
	AM30 - Mal funcionamiento del equipo	VU10 - Equipo desfasado por vigencia tecnológica	2	1	3	Significativo	4	1	4	
	AM30 - Mal funcionamiento del equipo	VU100 - Fallas conocidas del hardware	2	2	3	Significativo	4	2	8	
Activo 2	AM29 - Falla de equipo	VU3 - Susceptibilidad a la humedad, al polvo y a la suciedad	1	1	3	Significativo	4	2	8	7,00
	AM29 - Falla de equipo	VU10 - Equipo desfasado por vigencia tecnológica	2	1	3	Significativo	4	2	8	
	AM86 - No soporta nuevas tecnologías de hardware y software	VU10 - Equipo desfasado por vigencia tecnológica	2	1	3	Significativo	4	1	4	
	AM13 - Pérdida del suministro de electricidad	VU3 - Susceptibilidad a la humedad, al polvo y a la suciedad	2	2	3	Significativo	4	2	8	

Activo 3	AM30 - Mal funcionamiento del equipo	VU100 - Fallas conocidas del hardware	2	2	3	Significativo	4	2	8	8,00
Activo 4	AM30 - Mal funcionamiento del equipo	VU100 - Fallas conocidas del hardware	2	2	3	Significativo	4	2	8	8,00
Activo 5	AM30 - Mal funcionamiento del equipo	VU100 - Fallas conocidas del hardware	2	2	3	Significativo	4	2	8	8,00
Activo 6	AM30 - Mal funcionamiento del equipo	VU100 - Fallas conocidas del hardware	2	2	3	Significativo	4	2	8	8,00
Activo 7	AM29 - Falla de equipo	VU3 - Susceptibilidad a la humedad, al polvo y a la suciedad	1	1	3	Significativo	4	2	8	7,00
	AM29 - Falla de equipo	VU10 - Equipo desfasado por vigencia tecnológica	2	1	3	Significativo	4	2	8	
	AM86 - No soporta nuevas tecnologías de hardware y software	VU10 - Equipo desfasado por vigencia tecnológica	2	1	3	Significativo	4	1	4	
	AM13 - Pérdida del suministro de electricidad	VU3 - Susceptibilidad a la humedad, al polvo y a la suciedad	2	2	3	Significativo	4	2	8	
Activo 8	AM30 - Mal funcionamiento del equipo	VU100 - Fallas conocidas del hardware	2	2	3	Significativo	4	2	8	8,00
Activo 9	AM30 - Mal funcionamiento del equipo	VU100 - Fallas conocidas del hardware	2	2	3	Significativo	4	2	8	8,00
Activo 10	AM30 - Mal funcionamiento del equipo	VU100 - Fallas conocidas del hardware	2	2	3	Significativo	4	2	8	8,00
Activo 11	AM30 - Mal funcionamiento del equipo	VU100 - Fallas conocidas del hardware	2	2	3	Significativo	4	2	8	8,00
Activo 12	AM32 - Mal funcionamiento del software	VU115 - Falta de actualización de parches	2	2	3	Significativo	4	2	8	8,00
Activo 13	AM97 - Falla del sistema operativo	VU21 - Seteo incorrecto de parámetros	2	2	3	Significativo	4	2	8	8,00
Activo 14	AM88 - Instalación de software sin autorización, sin licencia	VU105 - Uso no controlado de licencias	1	1	3	Significativo	4	1	4	4,00
Activo 15	AM13 - Pérdida del suministro de electricidad	VU3 - Susceptibilidad a la humedad, al polvo y a la suciedad	2	2	3	Significativo	4	1	4	4,00
Activo 16	AM30 - Mal funcionamiento del equipo	VU100 - Fallas conocidas del hardware	3	2	2	Significativo	4	1	4	4,00

Activo 17	AM29 - Falla de equipo	VU124 - La aplicación, el soporte, registro de incidentes, mantenimiento servidores y otros equipos, servicio de backups lo realiza el proveedor del servicio ante una finalización de contrato la ENTIDAD quedaría sin este servicio	2	2	3	Significativo	4	1	4	4,00
Activo 18	AM99 - Ciberataques	VU96 - No se realiza la Identificación y Gestión de Vulnerabilidades	2	2	3	Significativo	4	1	4	4,00
Activo 19	AM13 - Pérdida del suministro de electricidad	VU3 - Susceptibilidad a la humedad, al polvo y a la suciedad	3	3	2	Catastrófico	5	1	5	5,00
Activo 20	AM99 - Ciberataques	VU96 - No se realiza la Identificación y Gestión de Vulnerabilidades	2	3	3	Catastrófico	5	1	5	5,00
Activo 21	AM6 - Polvo, corrosión, congelación	VU1 - Mantenimiento insuficiente / instalación fallida de medios de almacenamiento / Asignación Insuficiente de recursos	2	2	3	Significativo	4	2	8	8,00
Activo 22	AM72 - Disfunciones del sistema (bugs)	VU12 - Errores conocidos en el software	2	2	3	Significativo	4	2	8	8,00
Activo 23	AM29 - Falla de equipo	VU124 - La aplicación, el soporte, registro de incidentes, mantenimiento servidores y otros equipos, servicio de backups lo realiza el proveedor del servicio ante una finalización de contrato la ENTIDAD quedaría sin este servicio	2	2	3	Significativo	4	2	8	8,00
Activo 24	AM6 - Polvo, corrosión, congelación	VU1 - Mantenimiento insuficiente / instalación fallida de medios de almacenamiento / Asignación Insuficiente de recursos	2	2	3	Significativo	4	2	8	8,00
Activo 25	AM72 - Disfunciones del sistema (bugs)	VU12 - Errores conocidos en el software	2	2	3	Significativo	4	1	4	4,00

Activo 26	AM98 - Recortes presupuestales que afecta la adquisición de bienes y/o servicios tecnológicos para la mejora del SGSI.	VU100 - Fallas conocidas del hardware	2	2	3	Significativo	4	1	4	4,00
Activo 27	AM72 - Disfunciones del sistema (bugs)	VU12 - Errores conocidos en el software	2	2	3	Significativo	4	1	4	4,00
Activo 28	AM72 - Disfunciones del sistema (bugs)	VU12 - Errores conocidos en el software	2	2	3	Significativo	4	1	4	4,00
Activo 29	AM72 - Disfunciones del sistema (bugs)	VU12 - Errores conocidos en el software	2	2	3	Significativo	4	1	4	4,00
Activo 30	AM32 - Mal funcionamiento del software	VU106 - Falta de renovación de licencias	2	2	3	Significativo	4	1	4	4,00
Activo 31	AM43 - Hacking	VU96 - No se realiza la Identificación y Gestión de Vulnerabilidades	2	2	3	Significativo	4	2	8	8,00
Activo 32	AM32 - Mal funcionamiento del software	VU106 - Falta de renovación de licencias	3	2	2	Significativo	4	1	4	4,00
Activo 33	AM32 - Mal funcionamiento del software	VU106 - Falta de renovación de licencias	2	2	3	Significativo	4	1	4	4,00
Activo 34	AM97 - Falla del sistema operativo	VU115 - Falta de actualización de parches	2	2	3	Significativo	4	1	4	4,00
Activo 35	AM97 - Falla del sistema operativo	VU115 - Falta de actualización de parches	2	2	3	Significativo	4	1	4	4,00
Activo 36	AM97 - Falla del sistema operativo	VU115 - Falta de actualización de parches	2	2	3	Significativo	4	1	4	4,00
Activo 37	AM97 - Falla del sistema operativo	VU115 - Falta de actualización de parches	2	2	3	Significativo	4	1	4	4,00
Activo 38	AM97 - Falla del sistema operativo	VU115 - Falta de actualización de parches	2	2	3	Significativo	4	1	4	4,00
Activo 39	AM72 - Disfunciones del sistema (bugs)	VU12 - Errores conocidos en el software	2	2	3	Significativo	4	2	8	8,00
Activo 40	AM99 - Ciberataques	VU96 - No se realiza la Identificación y Gestión de Vulnerabilidades	2	2	3	Significativo	4	2	8	8,00
Activo 41	AM99 - Ciberataques	VU96 - No se realiza la Identificación y Gestión de	2	2	3	Significativo	4	2	8	8,00

		Vulnerabilidades								
Activo 42	AM46 - Acceso no autorizado al sitema	VU144 - Falta de un procedimiento formal o su actualización, para el registro y baja de usuarios	2	2	3	Significativo	4	1	4	4,00
Activo 43	AM29 - Falla de equipo	VU3 - Susceptibilidad a la humedad, al polvo y a la suciedad	2	2	3	Significativo	4	1	4	4,00
Activo 44	AM13 - Pérdida del suministro de electricidad	VU6 - Susceptibilidad a variación de voltaje	2	2	3	Significativo	4	1	4	4,00
Activo 45	AM29 - Falla de equipo	VU96 - No se realiza la Identificación y Gestión de Vulnerabilidades	2	2	3	Significativo	4	1	4	4,00
Activo 46	AM99 - Ciberataques	VU1 - Mantenimiento insuficiente / instalación fallida de medios de almacenamiento / Asignación Insuficiente de recursos	2	2	3	Significativo	4	1	4	4,00
Activo 47	AM99 - Ciberataques	VU1 - Mantenimiento insuficiente / instalación fallida de medios de almacenamiento / Asignación Insuficiente de recursos	2	2	3	Significativo	4	1	4	4,00
Activo 48	AM35 - Uso de software falsificado o copiado	VU46 - Uso incorrecto del software y hardware	2	3	1	Significativo	4	1	4	4,00
Activo 49	AM43 - Hacking	VU46 - Uso incorrecto del software y hardware	2	3	1	Significativo	4	1	4	4,00
Activo 50	AM21 - Robo de medios o documentos	VU125 - Eventos e incidentes que afecten a la seguridad de la información mal gestionados	3	3	2	Catastrófico	5	1	5	5,00
Activo 51	AM29 - Falla de equipo	VU10 - Equipo desfasado por vigencia tecnológica	2	2	3	Significativo	4	1	4	6,00
	AM13 - Pérdida del suministro de electricidad	VU6 - Susceptibilidad a variación de voltaje	2	2	3	Significativo	4	1	4	
	AM6 - Polvo, corrosión, congelación	VU3 - Susceptibilidad a la humedad, al polvo y a la suciedad	2	2	3	Significativo	4	2	8	
	AM12 - Fallas del sistema de aire acondicionado o del	VU6 - Susceptibilidad a variación de voltaje	2	2	3	Significativo	4	2	8	

	suministro de agua									
Activo 52	AM12 - Fallas del sistema de aire acondicionado o del suministro de agua	VU6 - Susceptibilidad a variación de voltaje	2	2	3	Significativo	4	1	4	4,00
Activo 53	AM5 - Destrucción del equipo o los medios	VU41 - Gestión inadecuada de la red (capacidad de recuperación del ruteo)	2	2	3	Significativo	4	1	4	4,00
Activo 54	AM5 - Destrucción del equipo o los medios	VU41 - Gestión inadecuada de la red (capacidad de recuperación del ruteo)	2	2	3	Significativo	4	1	4	4,00
Activo 55	AM5 - Destrucción del equipo o los medios	VU41 - Gestión inadecuada de la red (capacidad de recuperación del ruteo)	2	2	3	Significativo	4	1	4	4,00
Activo 56	AM91 - Indisponibilidad del Servicio de Help Desk	VU124 - La aplicación, el soporte, registro de incidentes, mantenimiento servidores y otros equipos, servicio de backups lo realiza el proveedor del servicio ante una finalización de contrato la ENTIDAD quedaría sin este servicio	2	2	3	Significativo	4	1	4	4,00
Activo 57	AM29 - Falla de equipo	VU124 - La aplicación, el soporte, registro de incidentes, mantenimiento servidores y otros equipos, servicio de backups lo realiza el proveedor del servicio ante una finalización de contrato la ENTIDAD quedaría sin este servicio	2	2	3	Significativo	4	2	8	8,00
Activo 58	AM29 - Falla de equipo	VU124 - La aplicación, el soporte, registro de incidentes, mantenimiento servidores y otros equipos, servicio de backups lo realiza el proveedor del servicio ante una finalización	2	2	3	Significativo	4	2	8	8,00

		de contrato la ENTIDAD quedaría sin este servicio								
Activo 59	AM29 - Falla de equipo	VU124 - La aplicación, el soporte, registro de incidentes, mantenimiento servidores y otros equipos, servicio de backups lo realiza el proveedor del servicio ante una finalización de contrato la ENTIDAD quedaría sin este servicio	2	2	3	Significativo	4	2	8	8,00
Activo 60	AM42 - Ruptura en la disponibilidad del personal	VU43 - Ausencia del personal	2	2	3	Significativo	4	2	8	8,00
Activo 61	AM42 - Ruptura en la disponibilidad del personal	VU43 - Ausencia del personal	2	2	3	Significativo	4	2	8	8,00
Activo 62	AM42 - Ruptura en la disponibilidad del personal	VU43 - Ausencia del personal	2	2	3	Significativo	4	2	8	8,00
Activo 63	AM42 - Ruptura en la disponibilidad del personal	VU43 - Ausencia del personal	2	2	3	Significativo	4	2	8	8,00
Activo 64	AM13 - Pérdida del suministro de electricidad	VU6 - Susceptibilidad a variación de voltaje	2	2	3	Significativo	4	2	8	8,00
Activo 65	AM22 - Robo de equipos o partes	VU54 - Falta de protección física del edificio, puertas, ventanas	2	2	3	Significativo	4	2	8	8,67
	AM13 - Pérdida del suministro de electricidad	VU6 - Susceptibilidad a variación de voltaje	2	2	3	Significativo	4	2	8	
	AM1 - Incendio	VU131 - Ausencia de sistema contraincendios con propiedades dieléctricas	3	3	3	Catastrófico	5	2	10	
Activo 66	AM72 - Disfunciones del sistema (bugs)	VU12 - Errores conocidos en el software	2	2	3	Significativo	4	2	8	8,00
Activo 67	AM70 - Códigos maliciosos (ej. Virus, bomba lógica, troyano)	VU115 - Falta de actualización de parches	2	2	3	Significativo	4	2	8	8,00
Activo 68	AM30 - Mal funcionamiento del equipo	VU100 - Fallas conocidas del hardware	2	2	3	Significativo	4	2	8	8,00

Activo 69	AM43 - Hacking	VU96 - No se realiza la Identificación y Gestión de Vulnerabilidades	2	2	3	Significativo	4	2	8	8,00
Activo 70	AM80 - Pérdida de información	VU130 - Ausencia de un mecanismo de control del ingreso/acceso a la infraestructura informática (léase Active Directory, servidor de archivos), que compare la presencia del usuario legítimo versus su propósito laboral	2	2	3	Significativo	4	2	8	8,00
Activo 71	AM72 - Disfunciones del sistema (bugs)	VU12 - Errores conocidos en el software	3	3	3	Catastrófico	5	1	5	5,00
Activo 72	AM22 - Robo de equipos o partes	VU54 - Falta de protección física del edificio, puertas, ventanas	3	3	2	Catastrófico	5	1	5	5,00
Activo 73	AM14 - Falla del equipo de telecomunicaciones	VU10 - Equipo desfasado por vigencia tecnológica	2	3	3	Catastrófico	5	1	5	5,00
Activo 74	AM72 - Disfunciones del sistema (bugs)	VU12 - Errores conocidos en el software	2	2	3	Significativo	5	1	5	5,00

TABLA RESUMEN

INDICADOR: NIVEL DE RIESGO

CODIGO ACTIVO	PRE TEST	POST TEST
ACTIVO 1	12,00	7,20
ACTIVO 2	11,00	7,00
ACTIVO 3	12,00	8,00
ACTIVO 4	12,00	8,00
ACTIVO 5	12,00	8,00
ACTIVO 6	12,00	8,00
ACTIVO 7	11,00	7,00
ACTIVO 8	12,00	8,00
ACTIVO 9	12,00	8,00
ACTIVO 10	12,00	8,00
ACTIVO 11	12,00	8,00
ACTIVO 12	12,00	8,00
ACTIVO 13	12,00	8,00
ACTIVO 14	8,00	4,00
ACTIVO 15	8,00	4,00
ACTIVO 16	8,00	4,00
ACTIVO 17	8,00	4,00
ACTIVO 18	8,00	4,00
ACTIVO 19	15,00	5,00
ACTIVO 20	15,00	5,00
ACTIVO 21	12,00	8,00
ACTIVO 22	12,00	8,00
ACTIVO 23	12,00	8,00
ACTIVO 24	12,00	8,00
ACTIVO 25	8,00	4,00
ACTIVO 26	8,00	4,00
ACTIVO 27	8,00	4,00
ACTIVO 28	8,00	4,00
ACTIVO 29	8,00	4,00
ACTIVO 30	8,00	4,00

ACTIVO 31	12,00	8,00
ACTIVO 32	8,00	4,00
ACTIVO 33	8,00	4,00
ACTIVO 34	8,00	4,00
ACTIVO 35	8,00	4,00
ACTIVO 36	8,00	4,00
ACTIVO 37	8,00	4,00
ACTIVO 38	8,00	4,00
ACTIVO 39	12,00	8,00
ACTIVO 40	12,00	8,00
ACTIVO 41	12,00	8,00
ACTIVO 42	8,00	4,00
ACTIVO 43	8,00	4,00
ACTIVO 44	8,00	4,00
ACTIVO 45	8,00	4,00
ACTIVO 46	8,00	4,00
ACTIVO 47	8,00	4,00
ACTIVO 48	8,00	4,00
ACTIVO 49	8,00	4,00
ACTIVO 50	15,00	5,00
ACTIVO 51	10,00	6,00
ACTIVO 52	8,00	4,00
ACTIVO 53	8,00	4,00
ACTIVO 54	8,00	4,00
ACTIVO 55	8,00	4,00
ACTIVO 56	8,00	4,00
ACTIVO 57	12,00	8,00
ACTIVO 58	12,00	8,00
ACTIVO 59	12,00	8,00
ACTIVO 60	12,00	8,00
ACTIVO 61	12,00	8,00
ACTIVO 62	12	8,00
ACTIVO 63	12	8,00
ACTIVO 64	12	8,00
ACTIVO 65	13	8,67
ACTIVO 66	12	8,00
ACTIVO 67	12	8,00
ACTIVO 68	12	8,00
ACTIVO 69	12	8,00

ACTIVO 70	12	8,00
ACTIVO 71	10	5,00
ACTIVO 72	10	5,00
ACTIVO 73	10	5,00
ACTIVO 74	10	5,00
PROMEDIO	**10,30**	**5,98**

PERÚ APN	**FICHA DE OBSERVACIÓN N° 03** **INDICADOR: NÚMERO DE CONTROLES** **FASE: PRE-TEST**		
CODIGO:	SGSI-FO-003-PT	**VERSIÓN:**	V1
CLASIFICACIÓN:	CONFIDENCIAL	**FECHA DIESÑO:**	Mar-23
PROCESO:	GESTIÓN DE RIESGOS		
INVESTIGADOR:	HENRY FRANK HUAMANTECA DAMIAN		
FECHA DE RECOLECCIÓN:	6 al 10 de marzo		
PUESTO:			

DECLARACIÓN DE APLICABILIDAD

Criterios

- **LR: Requerimientos legales**
- **CO: Obligaciones contractuales**
- **BR/BP: Requerimientos del negocio/mejores prácticas adoptadas**
- **RRA: Resultado de la valoración de riesgos**

CLÁUSULA N°	SECCIÓN	OBJETIVOS DE CONTROL	APLICA	EXISTE	JUSTIFICACIÓN			
					LR	CO	BR/BP	RRA
A.5	**POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN**							
	A.5.1 Dirección de Gestión para la Seguridad de Información	A.5.1.1 Políticas de seguridad de información	SI	SI			X	
		A.5.1.2 Revisión de las políticas de seguridad de información	SI	SI			X	
A.6	**ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**							
	A.6.1 Organización Interna	A.6.1.1 Funciones de seguridad de información y responsabilidades	SI	SI			X	
		A.6.1.2 Separación de deberes	SI	SI			X	
		A.6.1.3 Contacto con autoridades	SI	SI				

		A.6.1.4 Contacto con grupos de interés especial	SI	SI				
		A.6.1.5 Seguridad de información en gerencia de proyectos	SI	SI			X	
	A.6.2 Equipos Móviles y trabajo a distancia	A.6.2.1 Política de los equipos móviles	SI	SI			X	
		A.6.2.2 Trabajo a distancia	SI	SI				
A.7	**SEGURIDAD LIGADA A LOS RECURSOS HUMANOS**							
	A.7.1 Antes del Empleo	A.7.1.1 Evaluación	SI	SI				X
		A.7.1.2 Términos y condiciones de empleo	SI	SI				X
	A.7.2 Durante el Empleo	A.7.2.1 Responsabilidades de gestión	SI	SI			X	
		A.7.2.2 Conciencia de seguridad de información, educación y capacitación	SI	SI				X
		A.7.2.3 Proceso disciplinario	SI	SI			X	
	A.7.3 Términos y Cambio de Empleo	A.7.3.1 Término o cambio de las responsabilidades de empleo	SI	SI			X	
A.8	**GESTIÓN DE ACTIVOS**							
	A.8.1 Responsabilidad por Activos	A.8.1.1 Inventario de activos	SI	SI				X
		A.8.1.2 Propiedad de activos	SI	SI				X
		A.8.1.3 Uso aceptable de activos	SI	SI			X	
		A.8.1.4 Retorno de activos	SI	SI			X	
	A.8.2 Clasificación de la Información	A.8.2.1 Clasificación de información	SI	SI				X
		A.8.2.2 Etiquetado de información	SI	SI				X
		A.8.2.3 Manejo de activos	SI	SI			X	
	A.8.3 Manejo de Medios	A.8.3.1 Gestión de medios removibles	SI	SI				X
		A.8.3.2 Desecho de los medios	SI	SI				X
		A.8.3.3 Transferencia de medios físicos	SI	SI				X
A.9	**CONTROL DE ACCESOS**							

	A.9.1 Requisitos de Negocio para el Control de Acceso	A.9.1.1 Política de control de acceso	SI	SI				X
		A.9.1.2 Acceso a redes y servicios de red	SI	SI				X
	A.9.2 Gestión de Acceso de Usuario	A.9.2.1 Registro y cancelación de registro de usuarios	SI	SI				X
		A.9.2.2 Provisión del acceso de usuario	SI	SI				X
		A.9.2.3 Gestión de derechos de acceso privilegiados	SI	SI				X
		A.9.2.4 Gestión de la información de autenticación secreta de los usuarios	SI	SI				X
		A.9.2.5 Revisión de derechos de acceso de usuarios	SI	SI				X
		A.9.2.6 Eliminación o ajuste de derechos de acceso	SI	SI				X
	A.9.3 Responsabilidades de Usuarios	A.9.3.1 Uso de información de autenticación secreta	SI	SI			X	
	A.9.4 Control de Acceso de Aplicación y Sistema	A.9.4.1 Restricción de acceso a la información	SI	SI				X
		A.9.4.2 Procedimientos seguros de inicio de sesión	SI	SI				X
		A.9.4.3 Sistema de gestión de contraseña	SI	SI				X
		A.9.4.4 Uso de programas de utilidad privilegiada	SI	SI			X	
		A.9.4.5 Control de acceso al código fuente del programa	SI	SI				X
A.10	**CIFRADO**							
	A.10.1 Controles criptográficos	A.10.1.1 Política de uso de los controles criptográficos	SI	NO				X
		A.10.1.2 Gestión de claves	SI	SI			X	
A.11	**SEGURIDAD FÍSICA Y DEL AMBIENTE**							
	A.11.1 Áreas de Seguridad	A.11.1.1 Perímetro de seguridad física	SI	SI				X
		A.11.1.2 Controles de entrada física	SI	SI			X	
		A.11.1.3 Seguridad de oficinas, salas	SI	SI			X	
		A.11.1.4 Protección contra amenazas externas y ambientales	SI	SI			X	

		A.11.1.5 Trabajo en zonas seguras	SI	SI			X	
		A.11.1.6 Area de Despacho y Carga	SI	SI			X	
	A.11.2 Equipos	A.11.2.1 Situar los equipo y protección	SI	SI			X	
		A.11.2.2 Servicios públicos de apoyo	SI	SI			X	X
		A.11.2.3 Seguridad del cableado	SI	NO				X
		A.11.2.4 Mantenimiento de los equipos	SI	SI			X	
		A.11.2.5 Retiro de los activos	SI	SI			X	
		A.11.2.6 Seguridad de los equipos y de los activos fuera de las instalaciones	SI	NO			X	
		A.11.2.7 Eliminación segura o reúso de equipos	SI	SI			X	
		A.11.2.8 Equipos de usuarios no atendidos	SI	SI			X	
		A.11.2.9 Política de escritorio y pantalla limpia	SI	SI				X
A.12	**SEGURIDAD DE LAS OPERACIONES**							
	A.12.1 Procedimientos Operacionales y Responsabilidades	A.12.1.1 Procedimientos de operación documentados	SI	SI				X
		A.12.1.2 Gestión de cambio	SI	SI				X
		A.12.1.3 Gestión de capacidad	SI	SI				X
		A.12.1.4 Separación de evaluaciones de desarrollo y entornos operacionales	SI	NO				X
	A.12.2 Protección contra Malware	A.12.2.1 Control contra malware	SI	SI				X
	A.12.3 Copia	A.12.3.1 Copia de información	SI	SI				X
	A.12.4 Registro y Monitoreo	A.12.4.1 Registro de eventos	SI	SI			X	
		A.12.4.2 Protección de información de registro	SI	SI			X	
		A.12.4.3 Registros de administrador y operador	SI	SI			X	
		A.12.4.4 Sincronización de reloj	SI	SI			X	

	A.12.5 Control del Software Operativo	A.12.5.1 Instalación de software en sistemas operacionales	SI	SI			X	
	A.12.6 Gestión de Vulnerabilidad Técnica	A.12.6.1 Gestión de vulnerabilidades técnicas	SI	SI				X
		A.12.6.2 Restricciones en la instalación de software	SI	SI				X
	A.12.7 Consideraciones de Auditoría de Sistemas de Información	A.12.7.1 Controles de auditoría de sistemas de información	SI	NO			X	
A.13	**SEGURIDAD DE LAS COMUNICACIONES**							
	A.13.1 Gestión de Seguridad de Redes	A.13.1.1 Controles de redes	SI	SI			X	
		A.13.1.2 Seguridad de los servicios de redes	SI	SI				X
		A.13.1.3 Separación en redes	SI	SI				X
	A.13.2 Transferencia de Información	A.13.2.1 Procedimientos y políticas de transferencia de información	SI	SI			X	
		A.13.2.2 Acuerdos sobre transferencia de información	SI	SI			X	
		A.13.2.3 Mensajería electrónica	SI	SI			X	
		A.13.2.4 Acuerdo de confidencialidad o de no divulgación	SI	SI			X	
A.14	**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS**							
	A.14.1 Requisitos de Seguridad de los Sistemas de Información	A.14.1.1 Análisis y especificaciones de los requisitos de seguridad de la información	SI	SI			X	
		A.14.1.2 Asegurar los servicios de aplicaciones en redes públicas	SI	SI			X	
		A.14.1.3 Protección de las transacciones de servicios de aplicaciones	SI	SI			X	
	A.14.2 Seguridad en los Procesos de Desarrollo y el Apoyo	A.14.2.1 Política de desarrollo de seguridad	SI	SI			X	
		A.14.2.2 Procedimientos de control de cambios de sistema	SI	SI			X	
		A.14.2.3 Revisión técnica de las aplicaciones después de los cambios de la plataforma de operación	SI	SI			X	
		A.14.2.4 Restricciones a los cambios en los paquetes de software	SI	SI			X	
		A.14.2.5 Principios de ingeniería de sistemas seguros	SI	SI			X	

		A.14.2.6 Entorno de desarrollo seguro	SI	SI			X	
		A.14.2.7 Desarrollo de externalización	SI	SI			X	
		A.14.2.8 Pruebas de seguridad del sistema	SI	SI			X	
		A.14.2.9 Pruebas de aceptación del sistema	SI	SI			X	
	A.14.3 Datos de Pruebas	A.14.3.1 Protección de datos de prueba	SI	SI			X	
A.15	**RELACIONES CON LOS PROVEEDORES**							
	A.15.1 Seguridad de la Información en la Relación con los Proveedores	A.15.1.1 Política de seguridad de información para la relación con los proveedores	SI	SI		X		
		A.15.1.2 Abordar la seguridad dentro de acuerdos con proveedores	SI	SI		X		
		A.15.1.3 Cadena de suministro de tecnología de información y comunicaciones	SI	SI			X	
	A.15.2 Gestión de la Prestación de Servicios de Proveedor	A.15.2.1 Monitoreo y revisión de los servicios de proveedores	SI	SI		X		
		A.15.2.2 Gestión de cambios de los servicios del proveedor	SI	SI		X		
A.16	**GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN**							
	A.16.1 Gestión de Incidentes de Seguridad de la Información y Mejoras	A.16.1.1 Responsabilidades y procedimientos	SI	SI			X	
		A.16.1.2 Informe de eventos de seguridad de información	SI	SI			X	
		A.16.1.3 Informes de debilidades de seguridad de información	SI	SI			X	
		A.16.1.4 Evaluación y decisión sobre los eventos de seguridad de información	SI	SI			X	
		A.16.1.5 Respuesta a los incidentes de seguridad de información	SI	SI			X	
		A.16.1.6 Aprendiendo de los incidentes de seguridad de la información	SI	SI			X	
		A.16.1.7 Recolección de evidencia	SI	SI			X	
A.17	**SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO**							
	A.17.1 Continuidad de Seguridad de Información	A.17.1.1 Planeando la continuidad de seguridad de información	SI	SI				X
		A.17.1.2 Implementación de la continuidad de seguridad de información	SI	SI				X

		A.17.1.3 Verificar, revisar y evaluar la continuidad de seguridad de la información	SI	SI				X
	A.17.2 Redundancias	A.17.2.1 Disponibilidad de instalaciones de procesamiento de información	SI	SI			X	
A.18	**CUMPLIMIENTO**							
	A.18.1 Cumplimiento de los Requisitos Legales y Contractuales	A.18.1.1 Identificación de la legislación aplicable y los requisitos contractuales	SI	SI	X			
		A.18.1.2 Derechos de propiedad intelectual	SI	SI	X			
		A.18.1.3 Protección de registros	SI	SI	X			
		A.18.1.4 Privacidad y protección de datos personales	SI	SI	X			
		A.18.1.5 Regulación de los Controles Criptográficos	SI	NO			X	
	A.18.2 Revisiones de Seguridad de Información	A.18.2.1 Revisión independiente de seguridad de la información	SI	SI			X	
		A.18.2.2 Cumplimiento de las políticas y normas de seguridad	SI	SI			X	
		A.18.2.3 Revisión de cumplimiento técnico	SI	SI			X	

	FICHA DE OBSERVACIÓN N° 03 **INDICADOR: NÚMERO DE CONTROLES** **FASE: POST-TEST**		
CODIGO:	SGSI-FO-003-PT	**VERSIÓN:**	V1
CLASIFICACIÓN:	CONFIDENCIAL	**FECHA DIESÑO:**	Mar-23
PROCESO:	GESTIÓN DE RIESGOS		
INVESTIGADOR:	HENRY FRANK HUAMANTECA DAMIAN		
FECHA DE RECOLECCIÓN:	3 al 7 de abril		
PUESTO:			

DECLARACIÓN DE APLICABILIDAD

Criterios

- **LR: Requerimientos legales**
- **CO: Obligaciones contractuales**
- **BR/BP: Requerimientos del negocio/mejores prácticas adoptadas**
- **RRA: Resultado de la valoración de riesgos**

CLÁUSULA N°	SECCIÓN	OBJETIVOS DE CONTROL	APLICA	EXISTE	JUSTIFICACIÓN			
					LR	CO	BR/BP	RRA
A.5	**POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN**							
	A.5.1 Dirección de Gestión para la Seguridad de Información	A.5.1.1 Políticas de seguridad de información	SI	SI			X	
		A.5.1.2 Revisión de las políticas de seguridad de información	SI	SI			X	
A.6	**ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**							
	A.6.1 Organización Interna	A.6.1.1 Funciones de seguridad de información y responsabilidades	SI	SI			X	
		A.6.1.2 Separación de deberes	SI	SI			X	
		A.6.1.3 Contacto con autoridades	SI	SI				

		A.6.1.4 Contacto con grupos de interés especial	SI	SI				
		A.6.1.5 Seguridad de información en gerencia de proyectos	SI	SI			X	
	A.6.2 Equipos Móviles y trabajo a distancia	A.6.2.1 Política de los equipos móviles	SI	SI			X	
		A.6.2.2 Trabajo a distancia	SI	SI				
A.7	**SEGURIDAD LIGADA A LOS RECURSOS HUMANOS**							
	A.7.1 Antes del Empleo	A.7.1.1 Evaluación	SI	SI				X
		A.7.1.2 Términos y condiciones de empleo	SI	SI				X
	A.7.2 Durante el Empleo	A.7.2.1 Responsabilidades de gestión	SI	SI			X	
		A.7.2.2 Conciencia de seguridad de información, educación y capacitación	SI	SI				X
		A.7.2.3 Proceso disciplinario	SI	SI			X	
	A.7.3 Términos y Cambio de Empleo	A.7.3.1 Término o cambio de las responsabilidades de empleo	SI	SI			X	
A.8	**GESTIÓN DE ACTIVOS**							
	A.8.1 Responsabilidad por Activos	A.8.1.1 Inventario de activos	SI	SI				X
		A.8.1.2 Propiedad de activos	SI	SI				X
		A.8.1.3 Uso aceptable de activos	SI	SI			X	
		A.8.1.4 Retorno de activos	SI	SI			X	
	A.8.2 Clasificación de la Información	A.8.2.1 Clasificación de información	SI	SI				X
		A.8.2.2 Etiquetado de información	SI	SI				X
		A.8.2.3 Manejo de activos	SI	SI			X	
	A.8.3 Manejo de Medios	A.8.3.1 Gestión de medios removibles	SI	SI				X
		A.8.3.2 Desecho de los medios	SI	SI				X
		A.8.3.3 Transferencia de medios físicos	SI	SI				X
A.9	**CONTROL DE ACCESOS**							

	A.9.1 Requisitos de Negocio para el Control de Acceso	A.9.1.1 Política de control de acceso	SI	SI				X
		A.9.1.2 Acceso a redes y servicios de red	SI	SI				X
	A.9.2 Gestión de Acceso de Usuario	A.9.2.1 Registro y cancelación de registro de usuarios	SI	SI				X
		A.9.2.2 Provisión del acceso de usuario	SI	SI				X
		A.9.2.3 Gestión de derechos de acceso privilegiados	SI	SI				X
		A.9.2.4 Gestión de la información de autenticación secreta de los usuarios	SI	SI				X
		A.9.2.5 Revisión de derechos de acceso de usuarios	SI	SI				X
		A.9.2.6 Eliminación o ajuste de derechos de acceso	SI	SI				X
	A.9.3 Responsabilidades de Usuarios	A.9.3.1 Uso de información de autenticación secreta	SI	SI			X	
	A.9.4 Control de Acceso de Aplicación y Sistema	A.9.4.1 Restricción de acceso a la información	SI	SI				X
		A.9.4.2 Procedimientos seguros de inicio de sesión	SI	SI				X
		A.9.4.3 Sistema de gestión de contraseña	SI	SI				X
		A.9.4.4 Uso de programas de utilidad privilegiada	SI	SI			X	
		A.9.4.5 Control de acceso al código fuente del programa	SI	SI				X
A.10	**CIFRADO**							
	A.10.1 Controles criptográficos	A.10.1.1 Política de uso de los controles criptográficos	SI	SI				X
		A.10.1.2 Gestión de claves	SI	SI			X	
A.11	**SEGURIDAD FÍSICA Y DEL AMBIENTE**							
	A.11.1 Áreas de Seguridad	A.11.1.1 Perímetro de seguridad física	SI	SI				X
		A.11.1.2 Controles de entrada física	SI	SI			X	
		A.11.1.3 Seguridad de oficinas, salas	SI	SI			X	
		A.11.1.4 Protección contra amenazas externas y ambientales	SI	SI			X	

		A.11.1.5 Trabajo en zonas seguras	SI	SI			X	
		A.11.1.6 Area de Despacho y Carga	SI	SI			X	
	A.11.2 Equipos	A.11.2.1 Situar los equipo y protección	SI	SI			X	
		A.11.2.2 Servicios públicos de apoyo	SI	SI			X	X
		A.11.2.3 Seguridad del cableado	SI	SI				X
		A.11.2.4 Mantenimiento de los equipos	SI	SI			X	
		A.11.2.5 Retiro de los activos	SI	SI			X	
		A.11.2.6 Seguridad de los equipos y de los activos fuera de las instalaciones	SI	SI			X	
		A.11.2.7 Eliminación segura o reúso de equipos	SI	SI			X	
		A.11.2.8 Equipos de usuarios no atendidos	SI	SI			X	
		A.11.2.9 Política de escritorio y pantalla limpia	SI	SI				X
A.12	**SEGURIDAD DE LAS OPERACIONES**							
	A.12.1 Procedimientos Operacionales y Responsabilidades	A.12.1.1 Procedimientos de operación documentados	SI	SI				X
		A.12.1.2 Gestión de cambio	SI	SI				X
		A.12.1.3 Gestión de capacidad	SI	SI				X
		A.12.1.4 Separación de evaluaciones de desarrollo y entornos operacionales	SI	SI				X
	A.12.2 Protección contra Malware	A.12.2.1 Control contra malware	SI	SI				X
	A.12.3 Copia	A.12.3.1 Copia de información	SI	SI				X
	A.12.4 Registro y Monitoreo	A.12.4.1 Registro de eventos	SI	SI			X	
		A.12.4.2 Protección de información de registro	SI	SI			X	
		A.12.4.3 Registros de administrador y operador	SI	SI			X	
		A.12.4.4 Sincronización de reloj	SI	SI			X	

	A.12.5 Control del Software Operativo	A.12.5.1 Instalación de software en sistemas operacionales	SI	SI			X	
	A.12.6 Gestión de Vulnerabilidad Técnica	A.12.6.1 Gestión de vulnerabilidades técnicas	SI	SI				X
		A.12.6.2 Restricciones en la instalación de software	SI	SI				X
	A.12.7 Consideraciones de Auditoría de Sistemas de Información	A.12.7.1 Controles de auditoría de sistemas de información	SI	SI			X	
A.13	**SEGURIDAD DE LAS COMUNICACIONES**							
	A.13.1 Gestión de Seguridad de Redes	A.13.1.1 Controles de redes	SI	SI			X	
		A.13.1.2 Seguridad de los servicios de redes	SI	SI				X
		A.13.1.3 Separación en redes	SI	SI				X
	A.13.2 Transferencia de Información	A.13.2.1 Procedimientos y políticas de transferencia de información	SI	SI			X	
		A.13.2.2 Acuerdos sobre transferencia de información	SI	SI			X	
		A.13.2.3 Mensajería electrónica	SI	SI			X	
		A.13.2.4 Acuerdo de confidencialidad o de no divulgación	SI	SI			X	
A.14	**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS**							
	A.14.1 Requisitos de Seguridad de los Sistemas de Información	A.14.1.1 Análisis y especificaciones de los requisitos de seguridad de la información	SI	SI			X	
		A.14.1.2 Asegurar los servicios de aplicaciones en redes públicas	SI	SI			X	
		A.14.1.3 Protección de las transacciones de servicios de aplicaciones	SI	SI			X	
	A.14.2 Seguridad en los Procesos de Desarrollo y el Apoyo	A.14.2.1 Política de desarrollo de seguridad	SI	SI			X	
		A.14.2.2 Procedimientos de control de cambios de sistema	SI	SI			X	
		A.14.2.3 Revisión técnica de las aplicaciones después de los cambios de la plataforma de operación	SI	SI			X	
		A.14.2.4 Restricciones a los cambios en los paquetes de software	SI	SI			X	
		A.14.2.5 Principios de ingeniería de sistemas seguros	SI	SI			X	

		A.14.2.6 Entorno de desarrollo seguro	SI	SI			X	
		A.14.2.7 Desarrollo de externalización	SI	SI			X	
		A.14.2.8 Pruebas de seguridad del sistema	SI	SI			X	
		A.14.2.9 Pruebas de aceptación del sistema	SI	SI			X	
	A.14.3 Datos de Pruebas	A.14.3.1 Protección de datos de prueba	SI	SI			X	
A.15	**RELACIONES CON LOS PROVEEDORES**							
	A.15.1 Seguridad de la Información en la Relación con los Proveedores	A.15.1.1 Política de seguridad de información para la relación con los proveedores	SI	SI		X		
		A.15.1.2 Abordar la seguridad dentro de acuerdos con proveedores	SI	SI		X		
		A.15.1.3 Cadena de suministro de tecnología de información y comunicaciones	SI	SI			X	
	A.15.2 Gestión de la Prestación de Servicios de Proveedor	A.15.2.1 Monitoreo y revisión de los servicios de proveedores	SI	SI		X		
		A.15.2.2 Gestión de cambios de los servicios del proveedor	SI	SI		X		
A.16	**GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN**							
	A.16.1 Gestión de Incidentes de Seguridad de la Información y Mejoras	A.16.1.1 Responsabilidades y procedimientos	SI	SI			X	
		A.16.1.2 Informe de eventos de seguridad de información	SI	SI			X	
		A.16.1.3 Informes de debilidades de seguridad de información	SI	SI			X	
		A.16.1.4 Evaluación y decisión sobre los eventos de seguridad de información	SI	SI			X	
		A.16.1.5 Respuesta a los incidentes de seguridad de información	SI	SI			X	
		A.16.1.6 Aprendiendo de los incidentes de seguridad de la información	SI	SI			X	
		A.16.1.7 Recolección de evidencia	SI	SI			X	
A.17	**SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO**							
	A.17.1 Continuidad de Seguridad de Información	A.17.1.1 Planeando la continuidad de seguridad de información	SI	SI				X
		A.17.1.2 Implementación de la continuidad de seguridad de información	SI	SI				X

		A.17.1.3 Verificar, revisar y evaluar la continuidad de seguridad de la información	SI	SI				X
	A.17.2 Redundancias	A.17.2.1 Disponibilidad de instalaciones de procesamiento de información	SI	SI			X	
A.18	**CUMPLIMIENTO**							
	A.18.1 Cumplimiento de los Requisitos Legales y Contractuales	A.18.1.1 Identificación de la legislación aplicable y los requisitos contractuales	SI	SI	X			
		A.18.1.2 Derechos de propiedad intelectual	SI	SI	X			
		A.18.1.3 Protección de registros	SI	SI	X			
		A.18.1.4 Privacidad y protección de datos personales	SI	SI	X			
		A.18.1.5 Regulación de los Controles Criptográficos	SI	NO			X	
	A.18.2 Revisiones de Seguridad de Información	A.18.2.1 Revisión independiente de seguridad de la información	SI	SI			X	
		A.18.2.2 Cumplimiento de las políticas y normas de seguridad	SI	SI			X	
		A.18.2.3 Revisión de cumplimiento técnico	SI	SI			X	

TABLA RESUMEN				
INDICADOR: NÚMERO DE CONTROLES APLICADOS				
			Momento Experimental	
			Pre Test	Post Test
Control	No existe	Frecuencia	23	1
		%	20,18	0,88
	Si existe	Frecuencia	91	113
		%	79,82	99,12
Total		Frecuencia	114	114
		%	100	100

Anexo 4: Carta de aceptación

PERÚ | Ministerio de Transportes y Comunicaciones | Autoridad Portuaria Nacional

CARTA DE ACEPTACIÓN DE LA AUTORIDAD PORTUARIA NACIONAL

Callao, 03 de enero del 2023

Señor:

Henry Frank Huamanteca Damian

En mi calidad de Oficial de Seguridad de la Información de la Autoridad Portuaria Nacional, visto la solicitud para realizar su trabajo de investigación titulado "SGSI en la Gestion de Riesgos en el área de Infraestructura y Operaciones en una entidad pública, Callao 2023", luego de una evaluación, se resuelve:

Aceptar que se realice el trabajo de investigación en la Autoridad Portuaria Nacional, en el área de Infraestructura y Operaciones. Desde enero del 2023 fecha de inicio, hasta el 03 de agosto del 2023 fecha de término. Reiterando el respeto a los principios éticos de toda investigación científica.

Atte.

RAMOS RAMOS Alex Victor FAU 20509645150 hard
Firmado digitalmente por RAMOS RAMOS Alex Victor FAU 20509645150 hard
Fecha: 2023.05.17 16:42:06 -05'00'

Ramos Ramos, Alex

Anexo 6: ASPECTOS ADMINISTRATIVOS

Recursos y Presupuesto

Para llevar a cabo las actividades de investigación, tratamiento y procesamiento de la data, es necesario contar con el equipo adecuado para cumplir de manera eficaz, los equipos que se utilizarán, se detallan en la siguiente tabla.

Tabla 1 Equipos y bienes duraderos

Medios	Definición	Cantidad Monetaria
Equipo	Laptop Dell	S/. 3 500
	Pantalla Antryx 27”	S/. 1 300
	Teclado Halion	S/. 90
	Mouse Halion	S/. 60
	Total	S/. 6 300

Así mismo, las actividades de recopilación, procesamiento e interpretación de información pertinente a esta investigación, se realizan de manera presencial por el investigador, lo que se considera como costos, los cuales se detallan a continuación.

Tabla 2 Recursos humanos

Medios	Definición	Cantidad Monetaria
Recurso humano	Investigador	S/. 3 500
	Total	S/. 3 500

Por otro lado, para realizar las actividades correspondientes a la investigación se contará con el servicio de internet y para el procesamiento de datos, se utilizará el software SPSS, dichos costos son considerados como materiales e insumos, como se detalla a continuación.

Tabla 3 Materiales e insumos

Medios	Definición	Cantidad Monetaria
Software	SPSS	S/. 100
Servicio	Internet	S/. 160
	Total	S/. 260

Finalmente, todos los presupuestos mencionados líneas arriba, son sumados para obtener el presupuesto total, el cual es requerido para la realización de esta investigación. Los detalles se visualizan en la siguiente tabla**.**

Tabla 4 Presupuesto total

Recursos	**Cantidad monetaria**
Equipos y bienes duraderos	S/. 6 300
Recursos humanos	S/. 3 500
Materiales e insumos	S/. 260
Total	**S/. 10 060**

Financiamiento

Para llevar a cabo la presente investigación, el financiamiento del presupuesto total, mencionado líneas arriba, será cubierto en su totalidad por el tesista, como se muestra a continuación.

Tabla 5 Financiamiento

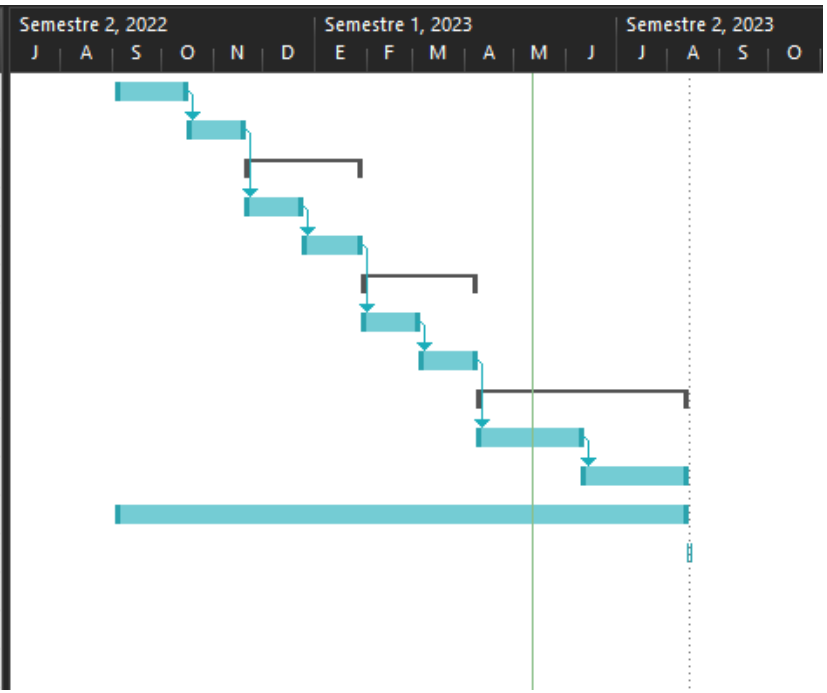
Nombre de la entidad	Cantidad monetaria	Tanto porciento
Autofinanciado	S/. 10 060	100%

Cronograma de Ejecución

Se plasma en un cronograma cada actividad y el tiempo que se le asignará a cada una de ellas, para su cumplimiento. De manera que nos permita llevar el correcto control y seguimiento, ayudando a la realización de esta investigación.

Figura 1 Cronograma de ejecución.

	Nombre de tarea	Dura	Comienzo	Fin
1	Determinacion del problema de investigacion	30 días	lun 05/09/22	vie 14/10/22
2	Marco teorico	25 días	lun 17/10/22	vie 18/11/22
3	**Antecedentes**	**50 días**	**lun 21/11/22**	**vie 27/01/23**
4	Nacionales	25 días	lun 21/11/22	vie 23/12/22
5	Internacionales	25 días	lun 26/12/22	vie 27/01/23
6	**Aplicación de instrumentos**	**50 días**	**lun 30/01/23**	**vie 07/04/23**
7	Coordinaciones con los responsables	25 días	lun 30/01/23	vie 03/03/23
8	Recoleccion de datos	25 días	lun 06/03/23	vie 07/04/23
9	**Resultados**	**90 días**	**lun 10/04/23**	**vie 11/08/23**
10	Procesamiento de datos	45 días	lun 10/04/23	vie 09/06/23
11	Interpretacion de datos	45 días	lun 12/06/23	vie 11/08/23
12	Redaccion del trabajo de investigacion	245 días	lun 05/09/22	vie 11/08/23
13	Sustentacion de tesis	1 día	lun 14/08/23	lun 14/08/23



Anexo 8: Matriz de Consistencia

Título: SGSI en la Gestión de Riesgos en el área de Infraestructura y Operaciones de una entidad pública, 2023

Problemas de Investigación	Objetivos de Investigación	Hipótesis de Investigación	Definición Operacional			Metodología y diseño
Problema General	Objetivo General	Hipótesis General	Variables	Dimensiones	Indicadores	
¿Cómo influye un SGSI en la Gestión de Riesgos en el área de Infraestructura y Operaciones en una entidad pública, 2023?	Determinar la influencia de un SGSI en la Gestión de Riesgos en el área de Infraestructura y Operaciones en una entidad pública, 2023.	La aplicabilidad de un SGSI mejora la Gestión de Riesgos en el área de Infraestructura y Operaciones en una entidad pública, 2023.	X: SGSI			Metodología: SGSI: ISO/IEC 27001:2014 Tipo: Investigación aplicada Diseño: pre-experimental Población: activos de información Instrumento: Ficha de observación
13Problemas Específica	Objetivos Específicos	Hipótesis Específicos	Variables	Dimensiones	Indicadores	
PE1: ¿Cómo influye un SGSI en el nivel de probabilidad en la Gestión de Riesgos en el área de Infraestructura y Operaciones en una entidad pública, 2023?	OE1: Determinar de qué manera influye el SGSI en el nivel de probabilidad en la Gestión de Riesgos en el área de Infraestructura y Operaciones en una entidad pública, 2023.	HE1: La aplicación de un SGSI influye positivamente reduciendo el nivel de probabilidad en la Gestión de Riesgos en el área de Infraestructura y Operaciones en una entidad pública, 2023.	Y: Gestión de Riesgos	Y1: Análisis de Riesgo	Nivel de probabilidad	
PE2: ¿Cómo influye un SGSI en el nivel de riesgo en la Gestión de Riesgos en el área de Infraestructura y Operaciones en una entidad pública, 2023?	OE2: Determinar de qué manera influye el SGSI en el nivel de riesgo en la Gestión de Riesgos en el área de Infraestructura y Operaciones en una entidad pública, 2023.	HE2: La aplicación de un SGSI influye positivamente reduciendo el nivel del riesgo en la Gestión de Riesgos en el área de Infraestructura y Operaciones en una entidad pública, 2023.		Y2: Evaluación de Riesgo	Nivel de riesgo	
PE3: ¿Cómo influye un SGSI en los controles empleados en la Gestión de Riesgos en el área de Infraestructura y Operaciones en una entidad pública, 2023?	OE3: Determinar de qué manera influye el SGSI en los controles aplicados en la Gestión de Riesgos en el área de Infraestructura y Operaciones en una entidad pública, 2023.	HE3: La aplicación del SGSI influye de manera positiva incrementando el número de controles en la Gestión de Riesgos en el área de Infraestructura y Operaciones en una entidad pública, 2023.		Y3: Tratamiento de Riesgo	Número de controles	