# Jaber Vasquez Malca

## Implementación de un sistema de gestión de seguridad de la información para la gestión de riesgos en SENATI – Yurimagu...

Revisión Repositorio Institucional de la UNSM

### Detalles del documento

Identificador de la entrega
**trn:oid:::3117:524152528**

Fecha de entrega
**6 nov 2025, 16:31 GMT-5**

Fecha de descarga
**6 nov 2025, 16:36 GMT-5**

Nombre del archivo
**Informes de Tesis de Gestion de Riesgos 21-09-2025 ultimo.pdf**

Tamaño del archivo
**1.4 MB**

**75 páginas**

**13.370 palabras**

**83.664 caracteres**

# 16% Similitud general

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

## Filtrado desde el informe

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

## Fuentes principales

14% Fuentes de Internet
8% Publicaciones
14% Trabajos entregados (trabajos del estudiante)

## Marcas de integridad

**N.º de alertas de integridad para revisión**

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

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

## Fuentes principales

14% Fuentes de Internet
8% Publicaciones
14% Trabajos entregados (trabajos del estudiante)

## Fuentes principales

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

1 Internet
tesis.unsm.edu.pe 4%

2 Internet
hdl.handle.net 3%

3 Internet
repositorio.unsm.edu.pe 1%

4 Trabajos del estudiante
Universidad Nacional de San Martín on 2024-06-04 1%

5 Internet
www.coursehero.com <1%

6 Trabajos del estudiante
Universidad Internacional de la Rioja on 2018-07-26 <1%

7 Trabajos del estudiante
Universidad Nacional de Trujillo on 2025-01-03 <1%

8 Trabajos del estudiante
Universidad Cesar Vallejo on 2016-03-11 <1%

9 Internet
repositorio.usmp.edu.pe <1%

10 Internet
repositorio.utp.edu.pe <1%

11 Trabajos del estudiante
Corporación Universitaria Minuto de Dios, UNIMINUTO on 2022-12-07 <1%

| | | |
|---|---|---|
| 12 | Trabajos del estudiante<br>Universidad Nacional de San Martín on 2024-03-12 | <1% |
| 13 | Trabajos del estudiante<br>Morgan Park High School on 2023-01-03 | <1% |
| 14 | Internet<br>cdn.www.gob.pe | <1% |
| 15 | Publicación<br>Erick Flores-Chacón, Alex Pacheco, Yvett Gonzales-Ortiz, Lenin Moreno-Vega, Fior... | <1% |
| 16 | Trabajos del estudiante<br>Pontificia Universidad Catolica del Peru on 2025-06-05 | <1% |
| 17 | Trabajos del estudiante<br>Universidad Internacional de la Rioja on 2022-02-09 | <1% |
| 18 | Trabajos del estudiante<br>Universidad Tecnologica del Peru on 2025-07-20 | <1% |
| 19 | Internet<br>repositorio.unprg.edu.pe | <1% |
| 20 | Internet<br>ciencialatina.org | <1% |
| 21 | Internet<br>estrategia.gobiernoenlinea.gov.co | <1% |
| 22 | Internet<br>repositorio.undac.edu.pe | <1% |
| 23 | Internet<br>www.fluidsignal.com | <1% |
| 24 | Publicación<br>Fernández Coronel, Nilda. "Estrategias y logros de aprendizaje en los estudiantes ... | <1% |
| 25 | Trabajos del estudiante<br>consultoriadeserviciosformativos on 2023-11-07 | <1% |

26 Internet
repositorio.uct.edu.pe <1%

27 Trabajos del estudiante
Universidad Cesar Vallejo on 2025-08-01 <1%

28 Publicación
Castañeda Castañeda, Iran Aparicio. "Programa de intervención basado en meto... <1%

29 Publicación
Martino Mendoza, Carmen Patricia | Solórzano Pérez, Evelyn Verónica | Vizcarra ... <1%

30 Trabajos del estudiante
POSGRADO on 2025-09-13 <1%

31 Publicación
Quispe Condori, Rossi Yamillet. "Inteligencia emocional y síndrome de Burnout e... <1%

32 Trabajos del estudiante
Universidad Internacional de la Rioja on 2022-02-10 <1%

33 Trabajos del estudiante
Universidad Mariano Gálvez de Guatemala on 2024-05-01 <1%

34 Trabajos del estudiante
Universidad Nacional de Cajamarca on 2025-09-03 <1%

35 Trabajos del estudiante
Universidad Nacional de Cajamarca on 2025-10-03 <1%

36 Trabajos del estudiante
Universidad Nacional de San Martín on 2022-12-05 <1%

37 Trabajos del estudiante
Universidad Nacional del Centro del Peru on 2025-02-24 <1%

38 Trabajos del estudiante
ufidelitas on 2025-02-07 <1%

**ESCUELA DE POSGRADO**
**UNIDAD DE POSGRADO DE LA FACULTAD DE INGENIERIA DE SISTEMAS E INFORMÁTICA**
**PROGRAMA DE MAESTRIA EN CIENCIAS CON MENCIÓN EN TECNOLOGÍA DE LA INFORMACIÓN**

Tesis

# Implementación de un sistema de gestión de seguridad de la información para la gestión de riesgos en SENATI – Yurimaguas, 2024.

Para optar el grado académico de Maestro en Ciencias con mención en Tecnologías de la Información

**Autor:**
Jaber Vasquez Malca
https://orcid.org/0009-0007-9182-4361

**Asesor:**
Ing. Dr. Alberto Alva Arévalo
https://orcid.org/0000-0002-8392-3542

**Coasesor:**
Lic. Dra. Milagros Zevallos Ruiz
https://orcid.org/0000-0002-6030-0676

**Tarapoto, Perú**

**2025**

**ESCUELA DE POSGRADO**
**UNIDAD DE POSGRADO DE LA FACULTAD DE INGENIERIA DE SISTEMAS E INFORMÁTICA**
**PROGRAMA DE MAESTRIA EN CIENCIAS CON MENCIÓN EN TECNOLOGÍA DE LA INFORMACIÓN**

Tesis

# Implementación de un sistema de gestión de seguridad de la información para la gestión de riesgos en SENATI – Yurimaguas, 2024.

Para optar el grado académico de Maestro en Ciencias con mención en Tecnologías de la Información

**Autor:**
Jaber Vasquez Malca
https://orcid.org/0009-0007-9182-4361

**Asesor:**
Ing. Dr. Alberto Alva Arévalo
https://orcid.org/0000-0002-8392-3542

**Coasesor:**
Lic. Dra. Milagros Zevallos Ruiz
https://orcid.org/0000-0002-6030-0676

**Tarapoto, Perú**

**2025**

**ESCUELA DE POSGRADO**
**UNIDAD DE POSGRADO DE LA FACULTAD DE INGENIERIA DE SISTEMAS E INFORMÁTICA**
**PROGRAMA DE MAESTRIA EN CIENCIAS CON MENCIÓN EN TECNOLOGÍA DE LA INFORMACIÓN**

Tesis

# Implementación de un sistema de gestión de seguridad de la información para la gestión de riesgos en SENATI – Yurimaguas, 2024

Para optar el grado académico de Maestro en Ciencias con Mención en Tecnología de la Información

**Autor**

Jaber Vasquez Malca

Sustentado y aprobado el 15 de setiembre de 2025, por los siguientes jurados:

**Presidente de Jurado**
Ing. Dr. Elmer Ruiz Trigozo

**Secretario de Jurado**
Ing. Dr. Angel Cárdenas García

**Vocal de Jurado**
Ing. Mg. Segundo Roger Ramírez Shupingahua

**Asesor**
Ing. Dr. Alberto Alva Arévalo

**Coasesor**
Lic. Dra. Milagros Zevallos Ruiz

**Tarapoto, Perú**

**2025**

**ESCUELA DE POSGRADO**
**UNIDAD DE POSGRADO DE LA FACULTAD DE INGENIERIA DE SISTEMAS E INFORMÁTICA**
**PROGRAMA DE MAESTRIA EN CIENCIAS CON MENCIÓN EN TECNOLOGÍA DE LA INFORMACIÓN**

Tesis

# Implementación de un sistema de gestión de seguridad de la información para la gestión de riesgos en SENATI – Yurimaguas, 2024.

Para optar el grado académico de Maestro en Ciencias con Mención en Tecnología de la Información

Los suscritos declaran que el presente Trabajo de tesis es original, en su contenido y forma.

**Ejecutor**
Jaber Vasquez Malca

**Asesor**
Ing. Dr. Alberto Alva Arévalo

**Coasesor**
Lic. Dra. Milagros Zevallos Ruiz

**Tarapoto, Perú**

**2025**

# Ficha de identificación

| | |
|---|---|
| **Título:**<br>Implementación de un sistema de gestión de seguridad de la información para la gestión de riesgos en SENATI – Yurimaguas, 2024 | **Área de investigación:** Maestría en Ciencias con mención en Tecnología de la Información.<br>**Línea de investigación:** Ciencias en Tecnología de la Información.<br>**Sublínea de investigación:** Seguridad de la Información.<br>**Grupo de investigación** Ciencias en Tecnología de la Información (Resolución N° 228-2023-UNSM/EPG-CD).<br>**Tipo de investigación:**<br>Básica ☐, Aplicada ☒, Desarrollo experimental ☐ |

| | |
|---|---|
| **Autor:**<br>Jaber Vasquez Malca | Facultad de Ingeniería de Sistemas e Informática<br>Escuela Profesional de Ingeniería de Sistemas e Informática<br>https://orcid.org/0009-0007-9182-4361 |

| | |
|---|---|
| **Asesor:**<br>Ing. Dr. Alberto Alva Arévalo | **Dependencia local de soporte:**<br>Facultad de Ingeniería de Sistemas e Informática<br>Escuela Profesional de Ingeniería de Sistemas e Informática<br>Unidad o Laboratorio Ingeniería de Sistemas e Informática<br>https://orcid.org/0000-0002-8392-3542 |

| | |
|---|---|
| **Coasesor:**<br>Lic. Dra. Milagros Zevallos Ruiz | **Dependencia local de soporte**<br>Programa de doctorado en Gestión Universitaria<br>Escuela de Posgrado<br>Unidad o Laboratorio Escuela de Posgrado<br>https://orcid.org/0000-0002-6030-0676 |

# Dedicatoria

A mi querida esposa Mariluz, a mi hija Mayeline y a mi hijo Kendrick, gracias por su amor, incondicional apoyo y sacrificios, que me han proporcionado la fuerza para llegar hasta este punto. Agradezco que me hayan enseñado que la tenacidad y el esfuerzo son fundamentales para lograr las metas.

**Jaber**

# Agradecimientos

Deseo manifestar mi gratitud más sincera a mis profesores y asesores por su sabiduría, paciencia y guía. Le agradezco por darme su apoyo en todo momento y por orientarme a lo largo de todo este proceso. Estoy profundamente agradecido al coordinador de SENATI Yurimaguas por brindarme su apoyo y permitirme realizar la investigación en su reconocida institución.

**El autor**

# Índice general

# Índice de tablas

# Índice de figuras

# RESUMEN

Implementación de un sistema de gestión de seguridad de la información para la gestión de riesgos en SENATI – Yurimaguas, 2024.

Hablar sobre la gestión de riesgos de información en la actualidad es un tema muy importante en las organizaciones y con el aumento de nuevas tecnologías se generan brechas de seguridad. Por tal razón esta investigación tuvo como objeto principal determinar la incidencia del sistema de gestión de seguridad de la información en la gestión del riesgo en la institución educativa superior SENATI – Yurimaguas, 2024 El estudio se enmarcó en un enfoque cuantitativo, de tipo aplicado, con un diseño preexperimental de nivel explicativo. La muestra constituida por 30 colaboradores de la sede SENATI – Yurimaguas, seleccionados de manera intencionada debido a su relación directa con los activos de información. Se aplicó una encuesta en dos momentos: pretest y postest. Los resultados evidenciaron que, antes de la intervención, los niveles de identificación, análisis, evaluación y tratamiento del riesgo se situaban entre bajos y medios. Sin embargo, luego de implementar el SGSI, estos indicadores alcanzaron niveles altos. Asimismo, la validación del software reveló una alta percepción de efectividad en cuanto a los pilares de confidencialidad (100%), integridad (97%) y disponibilidad (93%). Se concluye que la implementación del SGSI tuvo una incidencia positiva y significativa en la gestión de riesgos de información, lo cual se corroboró mediante la prueba estadística de Wilcoxon (p-valor < 0,05).

***Palabras clave***: SGSI, Gestión de Riesgo, Confidencialidad, Integridad, Disponibilidad.

# ABSTRACT

Implementation of an information security management system for risk management at SENATI – Yurimaguas, 2024.

Talking about information risk management is currently a very important topic in organizations, especially with the rise of new technologies that create security gaps. For this reason, the main objective of this research was to determine the impact of the information security management system on risk management at the SENATI – Yurimaguas higher education institution, 2024. The study was based on a quantitative, applied approach, with a pre-experimental design at an explanatory level. The sample consisted of 30 employees from the SENATI – Yurimaguas headquarters, selected intentionally due to their direct relationship with information assets. A survey was administered at two points in time: pretest and posttest. The results showed that, prior to the intervention, risk identification, analysis, assessment, and treatment levels were low to medium. However, after implementing the ISMS, these indicators reached high levels. Furthermore, the validation of the software revealed a high perception of effectiveness in terms of the pillars of confidentiality (100%), integrity (97%), and availability (93%). It was concluded that the implementation of the ISMS had a positive and significant impact on information risk management, which was corroborated by the Wilcoxon statistical test (p-value < 0.05).

***Keywords***: ISMS, Risk Management, Confidentiality, Integrity, Availability.

# CAPÍTULO I
# INTRODUCCIÓN A LA INVESTIGACIÓN

Administrar los riesgos de información es tema crucial en el entorno actual de las organizaciones, incluyendo las instituciones educativas superiores. La dependencia de los sistemas de información y el avance tecnológico, los riesgos y las vulnerabilidades con referencia a la protección de la información sin duda aumentaron.

A nivel global, se ha observado un aumento notable en acontecimientos de seguridad informática no deseables, como vulneraciones de datos, ciberataques y robos de información confidencial. Estos incidentes pueden tener un impacto devastador en las organizaciones, tanto en términos económicos como en su reputación.

Según (Check Point Research Team, 2023) indica que en el segundo trimestre del año 2023 hay un 8% de ataques más semanalmente en comparación con el año 2022 a nivel general, y en relación a las regiones en incremento de un 23% en África, 22% en Asia del Pacifico, 18% en Norte América; con respecto a los sectores, el educativo e investigación sufrió 2179 ataques, gubernamental y militar 1772 ataques, atención sanitaria 1744 ataques.

En Latinoamérica la pandemia acelero la transformación digital de los gobiernos, organizaciones, industrias e instituciones; se aplicó el teletrabajo sin muchas veces tener en cuenta los riesgos y robos de información tanto personal como empresarial. El informe para Latinoamérica de (ESET, 2022) indica lo siguiente El país con la mayor cantidad de detecciones es Perú (18%), seguido inmediatamente por México (17%), Colombia (12%), Argentina (11%) y Ecuador (9%).

En un informe con N° 001-2023-DP/ADHPD la institución pública autónoma en Perú Defensoría del Pueblo, (2023) menciona que, desde enero a setiembre del 2021, la Policía Nacional del Perú registró 11985 denuncias por delitos informáticos, además menciona que el 70% de las denuncias corresponden a fraude informático.

En el ámbito de institutos educativos superiores, la administración de riesgos de información se vuelve aún más crítica por la numerosa cantidad de datos sensibles que gestionan. Estas instituciones alojan información personal de alumnos, profesores, colaboradores, además propiedad intelectual y datos de investigación. La pérdida o violación de esta información puede dar lugar a consecuencias graves, como el robo de identidad, el daño a la reputación institucional y el Infracción de las regulaciones que protegen los datos.

Específicamente en el ámbito de SENATI sede Yurimaguas, se enfrenta a desafíos únicos en cuanto a la administración correcta de vulnerabilidades de información. La institución ya presentó diversas situaciones como suplantación de credenciales, hurtos de hardware entre otras incidencias, de lo expuesto se logró subsanar, pero no se tiene ninguna herramienta o marco que permita gestionar adecuadamente los riesgos y prevenir o reducir el impacto que provocaría situaciones de mayor escala.

El problema general y cuatro problemas específicos se presentan, conforme a las bases previamente discutidas sobre el problema. Por consiguiente, el problema general formulado dice así ¿Cuál es la incidencia del sistema de gestión de seguridad de la información en la gestión del riesgo en la institución educativa superior SENATI – Yurimaguas, 2024?, A partir de lo anterior, se derivan los siguientes problemas específicos; PE1. ¿Cuál es la incidencia del sistema de gestión de seguridad de la información en la identificación del riesgo en la institución educativa superior SENATI – Yurimaguas, 2024?, PE2. ¿Cuál es la incidencia del sistema de gestión de seguridad de la información en el análisis del riesgo en la institución educativa superior SENATI – Yurimaguas, 2024?, PE3. ¿Cuál es la incidencia del sistema de gestión de seguridad de la información en la evaluación del riesgo en la institución educativa superior SENATI – Yurimaguas, 2024?, PE4. ¿Cuál es la incidencia del sistema de gestión de seguridad de la información en el tratamiento del riesgo en la institución educativa superior SENATI – Yurimaguas, 2024?

Esta investigación plantea la siguiente hipótesis general, El sistema de gestión de seguridad de la información incide de forma positiva en la gestión del riesgo en la institución educativa superior SENATI – Yurimaguas, 2024. Con sus respectivas hipótesis específicas; HE1. El sistema de gestión de seguridad de la información incide de forma positiva en la identificación del riesgo en la institución educativa superior SENATI – Yurimaguas, 2024, HE2. El sistema de gestión de seguridad de la información incide de forma positiva en el análisis del riesgo en la institución educativa superior SENATI – Yurimaguas, 2024, HE3. El sistema de gestión de seguridad de la información incide de forma positiva en la evaluación del riesgo en la institución educativa superior SENATI – Yurimaguas, 2024, HE4. El sistema de gestión de seguridad de la información incide de forma positiva en el tratamiento del riesgo en la institución educativa superior SENATI – Yurimaguas, 2024.

Del mismo modo la finalidad principal de la investigación es Determinar la incidencia del sistema de gestión de seguridad de la información en la gestión del riesgo en la institución educativa superior SENATI – Yurimaguas, 2024. Con sus respectivos

objetivos específicos; OE1: Determinar la incidencia del sistema de gestión de seguridad de la información en la identificación del riesgo en la institución educativa superior SENATI – Yurimaguas, 2024, OE2: Determinar la incidencia del sistema de gestión de seguridad de la información en el análisis del riesgo en la institución educativa superior SENATI – Yurimaguas, 2024, OE3: Determinar la incidencia del sistema de gestión de seguridad de la información en la evaluación del riesgo en la institución educativa superior SENATI – Yurimaguas, 2024, OE4: Determinar la incidencia del sistema de gestión de seguridad de la información en el tratamiento del riesgo en la institución educativa superior SENATI – Yurimaguas, 2024.

# CAPÍTULO II
# MARCO TEÓRICO

## 2.1. Antecedentes de la investigación

**Internacional:**

(Hernández, 2020). Propuso un “Plan director para la implementación del SGSI”, El propósito principal fue garantizar los pilares fundamentales del aseguramiento de la información mediante el SGSI. Esta investigación utilizo una perspectiva descriptivo y analítico, utilizando auditorías internas y evaluaciones de riesgo como herramientas centrales para diagnosticar vulnerabilidades y definir los controles necesarios. Para el trabajo de campo y recojo de datos se seleccionó de manera aleatoria de las distintas áreas de la organización una muestra de 30 trabajadores, al cual se aplicó cuestionarios y entrevistas dirigidas. Los resultados revelan que el 95% de los participantes reconoció la necesidad urgente de reforzar los controles de seguridad, mientras que el 85% admitió no tener claro qué políticas de seguridad estaban vigentes. Además, el 80% expresó interés en recibir formación en esta materia. La investigación finalizo mencionando que la implementación de un SGSI no solo es esencial para reducir los riesgos informáticos, sino que también resalta la necesidad de instaurar políticas de seguridad definidas y comprensibles, además se debe preparar y capacitar al personal.

Según (Álava & Choez, 2023). Propusieron en su investigación “Desarrollo de un SGSI para Invimedic S.A., siguiendo las pautas establecidas por la norma ISO 27001”. Su meta fue diseñar un SGSI a medida, basado en ISO 27001. La investigación partió de la perspectiva de un enfoque descriptivo y analítico, utilizando encuestas y entrevistas aplicadas a un total de 50 trabajadores pertenecientes a distintas áreas de la organización. Antes de la implementación del SGSI, el 75% de los empleados declaró no tener conocimiento suficiente sobre buenas prácticas en seguridad informática. Sin embargo, tras la implementación, se evidenció una mejora del 60% en la adhesión a las políticas de seguridad. Como conclusión la cultura organizacional cambió positivamente, la conciencia creció y la información se aseguró.

**Nacional:**

(Sanchez, 2023). Ejecuto un estudio titulado “La gestión de la seguridad electrónica en el campo de las TI y el SGSI en una compañía aérea”. El propósito de esta investigación tuvo como objetivo comprender en profundidad el impacto real de un SGSI dentro del entorno dinámico que presentan las TI. Para tal fin, optó un diseño no experimental, de

tipo básico, correlacional y transversal, así como un enfoque cuantitativo. El trabajo de campo convocó a 50 profesionales del área, quienes respondieron encuestas tipo Likert: ese instrumento que pretende traducir opiniones complejas en escalas de uno al cinco, el cuestionario fue validado por especialistas y logró una respetable confiabilidad estadística, con un α de 0.816 para el SGSI y un 0.926 para la gestión de seguridad electrónica. En otras palabras, los datos no sólo hablaron; hablaron con coherencia. En el proceso de análisis, se empleó el software SPSS v25. Primero, se empleó la evaluación de normalidad Kolmogorov-Smirnov, en previsión de que sean suficientemente obedientes los datos como para seguir una distribución normal. Luego, se aplicó la correlación de Pearson, ese método que nos dice si dos variables caminan de la mano o van por senderos opuestos. Claramente, había una conexión significativa y positiva entre la implementación del SGSI y la gestión de la seguridad electrónica. Es decir, cuando uno mejora, el otro no se queda atrás. Una relación que, en tiempos de ciber amenazas crecientes, no es sólo conveniente, es vital.

Por su parte (Guizado, 2024). En su estudio sobre el “El impacto de un SGSI basado en la norma ISO 27001:2022 en la protección de la información en una municipalidad distrital”. El objetivo principal fue analizar en una municipalidad distrital el impacto de la protección de información aplicando un SGSI. Se utilizó un diseño no experimental y un enfoque cuantitativo correlacional-causal en el estudio, que fue de tipo aplicado. La investigación de campo incluyó a una muestra de 132 expertos en el sector tecnológico. Con un total de 200 profesionales en población y una muestra por conveniencia. Se aplicaron dos cuestionarios validados por especialistas, cuyos niveles de confiabilidad fueron 0.842 y 0.885, respectivamente. Logrando que la implementación del SGSI muestre un nivel ideal y respecto a la protección de la información un nivel intermedio, identificando una correlación estadísticamente significativa ($r = 0.611$; $p = 0.032$). De esta forma, se evidenció que un SGSI correctamente implementado tiene una consecuencia importante en el aseguramiento de la información institucional.

En otro estudio, (Coronado, 2024). Exploró el uso de un “Establecimiento de un SGSI, en línea con la ISO 27001:2022, para proteger los activos informativos de una institución pública del sector defensa ubicada en Lima”. El propósito de este estudio fue salvaguardar los activos de información institucional. El trabajo se estructuró bajo un diseño preexperimental y enfoque cuantitativo-aplicado, adoptando métodos deductivo, analítico e hipotético. Puso la lupa sobre 30 controles clave en el proceso central de la institución como población. A través de guías de observación, el estudio evaluó aspectos tan críticos como los controles de accesos, continuidad operativa y protección de redes. Siguiendo las directrices del anexo A de la norma ISO 27002:2022, se implementaron

dichos controles; como resultados los incidentes disminuyeron en disponibilidad un 86.70%, en integridad un 77.81%, en confidencialidad un 87.66%. Dichos hallazgos respaldan la eficacia del SGSI para resguardar la información crítica en entornos de alta sensibilidad operativa.

(Castro, 2022). centró su atención en la "La administración de riesgos y la protección de datos en una institución del sistema electoral". Determinar si la administración de riesgos guarda relación con el aseguramiento de información fue la finalidad del estudio. El enfoque fue básico y no experimental, pero no por eso menos revelador el 42% de los trabajadores encuestados admitieron que una gestión de riesgos adecuada fortalece la seguridad digital; el 58% restante, más escéptico, consideró que aún había mucho por hacer. La conclusión fue clara mencionando que hay una relación significativa, y fortalecerla es cuestión de voluntad y método.

(Narro, 2021). Investigó sobre "La gestión de riesgos y el SGSI en el departamento informático de una universidad estatal situada en la región cajamarquina". La finalidad fue que, en el departamento de informática del centro superior estatal ubicada en la región cajamarquina, reconocer la correlación entre la administración de riesgo y el SGSI. Se utilizó enfoque aplicado, método deductivo-inductivo, diseño que no manipula las variables de tipo transaccional con correlación. El muestro consistió en 10 colaboradores del área tecnológica, quienes respondieron un cuestionario tipo Likert con tres niveles de respuesta para desentrañar vínculos entre 65 ítems del SGSI y 18 sobre riesgos. El estudio arrojó una conclusión contundente que existe una relación positiva entre ambas variables, incluso en contextos académicos de ámbito universitario.

(Panaqué et al., 2022). Optaron por una ruta más panorámica. Realizaron una revisión sistemática de literatura y a su investigación lo titularon "Impacto que tiene la implementación de un SGSI basado en la norma ISO 27001 sobre las entidades". El objetivo fue evaluar los efectos derivados en distintas organizaciones luego de implementar el aseguramiento de información apoyado en el marco ISO 27001. Utilizando el método PRISMA, seleccionaron 20 estudios clave entre 2015 y 2021 publicados en repositorios académicas como Alicia, Dialnet Plus, Redalyc y Scielo, y examinando los efectos de implementar SGSI basados en la norma ISO 27001. Aunque los resultados no se expresaron en porcentajes, el resultado fue claro afirmando que la mejora de la seguridad de la información es un beneficio recurrente y prácticamente garantizado. Los autores concluyen que la implementación de dicha norma una correcta protección de los datos de las organizaciones. En un mundo donde los bytes crecen

más rápido que las certezas, contar con una norma internacional como guía parece, al menos, una forma decente de no perderse del todo.

**Regional:**

Paredes & Romero (2021). La investigación titulada “Gestión de riesgos vinculados a los productos que el Gobierno Regional de San Martín ofreció a la población en 2020” evidenció en sus resultados cuantitativos que se identificaron y se priorizaron cuatro áreas clave. En la ejecución de los planes, se implementó en los plazos establecidos al 100% las 9 medidas de remediación, mientras que de las 27 medidas de control solo se lograron implementar 13 (48%), quedando pendientes aquellas vinculadas al producto de reducción de vulnerabilidad. La evaluación realizada mediante el aplicativo de la Contraloría General reportó un puntaje de cumplimiento de 67% y un grado de madurez de 58.77%, lo que refleja avances parciales pero significativos en la gestión de riesgos, mostrando un impacto positivo en el cumplimiento de los objetivos del GORESAM durante el 2020

Velásquez et al. (2025). La investigación “Sistema de gestión de la seguridad y confidencialidad de la información en el Hospital II-1 Moyobamba, 2024”. La finalidad del estudio en el ámbito hospitalario fue identificar la relación de la confidencialidad de información y un SGSI; la metodología aplicada con un enfoque cuantitativo, empleando un método deductivo y teniendo un alcance relacional con una configuración no experimental transversal, usando una muestra censal de 16 empleados, encuestas y dos cuestionarios como técnica de recolección de datos, procesamiento en Excel y SPSS, pruebas de normalidad y correlación Rho de Spearman ante datos no normales; los resultados cuantitativos muestran que el SGSI fue valorado como eficiente por 62,5% (regular 25,0%; deficiente 12,5%), con mayor eficiencia en gestión 68,8%, seguida de seguridad 62,5% e implantación 56,3%; la confidencialidad fue percibida como alta por 56,3% (media 31,3%; baja 12,5%), destacando la dimensión cultural-organizacional 68,8% en nivel alto, mientras que tecnológica y procesos-políticas alcanzaron 50,0% cada una en nivel alto; estadísticamente se confirmó una correlación positiva fuerte y significativa entre SGSI y confidencialidad (Rho = 0,757; p = 0,001), con asociaciones significativas del SGSI con las dimensiones tecnológica y procesos-políticas, mas no con la cultural-organizacional.

Tuanama (2024). La investigación titulada “Gestión de calidad y administración de los servicios tecnológicos en el SAT-Tarapoto, 2022”. Se planteó la idea de analizar cómo se relacionan los dos sistemas. Para realizar el estudio, con un total de 35 colaboradores, se implementó una investigación no experimental, descriptivo-

correlacional y transversal, utilizando cuestionarios estructurados. Los resultados cuantitativos muestran la percepción en un 51.4% de nivel medio y un 31.4% en nivel alto sobre la administración de calidad, una percepción en 57.1% nivel medio y 25.7% nivel alto en la gestión de servicios de TI. Por dimensiones, liderazgo, procesos y participación del personal oscilaron entre 48% y 54% en nivel medio, mientras que seguridad informática, procesamiento de datos y conectividad se situaron en promedios similares. Las pruebas estadísticas confirmaron una correlación fuerte y una relación positiva entre la administración de calidad y los servicios tecnológicos, según los coeficientes de Pearson (r=0.833) y Spearman (ρ=0.827), lo que evidencia que una mejor calidad de gestión se asocia directamente con la eficiencia en los servicios tecnológicos del SAT-Tarapoto.

## 2.2. Fundamentos teóricos

### 2.2.1. Sistema de Gestión de Seguridad de la Información

No solamente es el manual de buenas intenciones ni una colección de protocolos escritos en lenguaje críptico; representa una estructura ordenada que combina procedimientos, políticas y controles, todos ellos orientados a proteger la información dentro de una entidad con efectividad y propósito (ISO/IEC 27001, 2022). Más que un marco normativo, el SGSI funciona como una estrategia integral, donde convergen recursos humanos, tecnológicos y administrativos en defensa de uno de los activos más vulnerables y codiciados de nuestro tiempo: los datos. Según la (Plataforma del Estado Peruano, 2024), este tipo de sistema se construye sobre un enfoque estructurado, guiado por la evaluación constante de riesgos y la implementación de controles pertinentes. Todo esto en alineación con los objetivos institucionales, como quien afina una brújula antes de salir a navegar por aguas repletas de amenazas. Porque eso es, precisamente, lo que busca minimizar los peligros que puedan comprometer el aseguramiento de información, sin dejar nunca de lado el enfoque de la estrategia global.

### 2.2.2. Seguridad de la Información

En ese escenario, el aseguramiento de información ha emergido como un factor fundamental e imprescindible. Se entiende, en esencia, como el conjunto de medidas destinadas a impedir accesos no autorizados, alteraciones indebidas o destrucciones malintencionadas de datos críticos. Dicho de otro modo, proteger la confidencialidad, la integridad y la disponibilidad; la famosa tríada CID ya no es un ideal abstracto, sino el eje central sobre el que gira cualquier estrategia de protección de la información (PAIS, 2020). De acuerdo con (Whitman & Mattord, 2018), coinciden al señalar que esta disciplina abarca un espectro de prácticas destinadas no solo a proteger la información,

sino también a asegurar los sistemas encargados de procesarla, almacenarla o transmitirla. En sintonía, (Stallings & Brown, 2024) subrayan que su implementación requiere la integración de mecanismos técnicos, organizativos y procedimentales, todos diseñados con un fin común que es prevenir y mitigar las amenazas que acechan los sistemas de información desde las sombras, los errores humanos, o desde una simple red Wi-Fi mal protegida.


**Figura 1**
*Dimensiones de Seguridad de la Información.*
***Fuente:*** (Martínez Ramirez, 2020)

## Dimensiones

**Confidencialidad.** Pilar esencial de la tríada CID, la confidencialidad busca algo tan simple y difícil en la práctica como restringir el acceso a la información exclusivamente a quienes están debidamente autorizados. Para (Pfleeger et al., 2015), este principio se garantiza mediante políticas diseñadas para limitar la disponibilidad de datos a usuarios previamente definidos. (Tipton & Krause, 2007) coinciden al afirmar que la confidencialidad supone un control riguroso sobre quién puede ver qué, cuándo y cómo. Asimismo, la (U.S. Government Publishing Office, 2011) amplía la noción, incorporando además salvaguardas de información confidencial o propietaria y datos personales. A su vez, (Jason, 2011) introduce una distinción clave: aunque la confidencialidad y la privacidad suelen caminar juntas, esta última trasciende lo técnico y toca fibras éticas y legales relacionadas con el uso y la divulgación de los datos personales.

**Integridad**. Aquí hablamos de precisión, coherencia y resistencia frente a alteraciones no autorizadas. Para (Stallings & Brown, 2024) la integridad se orienta a prevenir cualquier modificación indebida. (Whitman & Mattord, 2018) hacen hincapié en la importancia de preservar la confiabilidad de la información, mientras (Jason, 2011)

subraya que las amenazas no siempre son maliciosas; también hay errores accidentales que comprometen los datos. Además, este principio abarca elementos como el no repudio y la autenticidad, lo que implica garantizar que la información provenga de fuentes legítimas y no haya sido manipulada (U.S. Government Publishing Office, 2011b). Según (Pfleeger et al., 2015) un sistema íntegro garantiza que solo los individuos o sistemas autorizados de manera explícita puedan modificar los activos informáticos.

**Disponibilidad**. En este caso, lo importante no es sólo proteger los datos, sino asegurarse de que estén ahí cuando se necesiten. La disponibilidad implica que los usuarios legítimos puedan acceder a la información de forma oportuna y continua, sin obstáculos técnicos ni cuellos de botella innecesarios (Pfleeger et al., 2015). Desde una mirada gubernamental, esta dimensión también garantiza que la información esté disponible para facilitar decisiones críticas y sostener el funcionamiento operativo (U.S. Government Publishing Office, 2011b). (Jason, 2011) complementa esta idea destacando que la disponibilidad no es simplemente estar “en línea”, sino estarlo justo en el momento clave, sin barreras administrativas o fallos de infraestructura.

**SGSI basado en la Norma ISO 27001**

Se ha afirmado como uno de los estándares globales más sólidos y confiables en lo que respecta a la administración de la seguridad informativa. No es un conjunto de normas inmutables, sino un marco normativo sólido que posibilita la estructuración, implementación y mejora continua de un SGSI, todo bajo la lógica de la administración de riesgos (ISO/IEC 27001, 2022). Esta perspectiva no solo resguarda los activos informáticos, sino que además los ajusta a las metas estratégicas y operativas de la entidad, transformando la seguridad en un beneficio competitivo.

Según (Calder & Watkins, 2008), la norma sirve como una guía sistemática para implementar controles efectivos para cada entidad que se ajustan a según lo requieran, independientemente del tamaño o sector. El modelo PHVA (Planificar, Hacer, Verificar, Actuar) proporciona la agilidad necesaria para adaptarse a cambios tecnológicos, nuevas amenazas y transformaciones internas. Así, ISO/IEC 27001 deja de ser un simple estándar técnico para convertirse en una herramienta estratégica que mejora la gobernanza, refuerza la confianza del cliente y potencia la reputación institucional.

### 2.2.3. Gestión de Riesgo de Información

Gestionar el riesgo en materia de información no es una formalidad administrativa, sino un proceso crítico que permite identificar y neutralizar amenazas antes de que se transformen en daños. De acuerdo con la normativa (ISO/IEC 27005, 2022), se trata de

un proceso que consta de actividades sistemáticas dirigidas a identificar, examinar, analizar y gestionar los riesgos que amenazan la disponibilidad, confidencialidad e integridad de los datos. Y no, no se trata únicamente de instalar firewalls. La gestión del riesgo exige una mirada integral que considere factores humanos, organizacionales y tecnológicos. Su correcta implementación no sólo reduce vulnerabilidades, sino que optimiza los recursos y permite una toma de decisiones más informada y eficaz.

**Dimensiones**

**Identificación del Riesgo**. El primer paso es siempre mirar de frente al problema: ¿qué activos están expuestos?, ¿qué amenazas pueden afectarlos? De acuerdo con la (ISO/IEC 27005, 2022), esta fase exige un inventario detallado de los recursos físicos, humanos y tecnológicos, así como una clasificación precisa de los riesgos potenciales. (Stoneburner et al., 2002) subrayan la importancia de identificar eventos que puedan afectar negativamente los sistemas informáticos, mientras que (Peltier, 2016) propone un enfoque que no se limite a documentar, sino que analice las relaciones entre activos, amenazas y vulnerabilidades para obtener una visión clara y contextualizada del entorno de riesgo.

**Análisis del Riesgo**. Aquí se profundiza; ya no se trata sólo de ver el riesgo, sino de entenderlo. Este análisis del valor de las consecuencias que podría tener ocurriera, ya sea desde un enfoque cualitativo o cuantitativo (ISO/IEC 27005, 2022b). El (NIST, 2012) considera este paso clave para comprender la magnitud del riesgo, mientras que (Peltier, 2016) sugiere tener en cuenta la criticidad de los activos y el historial de incidentes. El objetivo es claro, separar el ruido de las verdaderas amenazas y priorizar lo que realmente importa.

**Evaluación del Riesgo**. Una vez analizado, toca decidir. ¿Qué hacer con ese riesgo? (Whitman & Mattord, 2018) explican que esta etapa implica determinar si se acepta el riesgo, se transfiere (por ejemplo, mediante seguros), se mitiga con controles o se elimina. Es una fase estratégica que permite asignar esfuerzos de manera inteligente y concentrarse en los peligros más urgentes para la organización.

**Tratamiento del Riesgo**. Aquí es donde el plan se convierte en acción. El tratamiento del riesgo supone seleccionar e implementar medidas concretas: desde controles técnicos hasta políticas organizativas, capacitaciones o rediseños en la infraestructura tecnológica. (Humphreys, 2016) destaca que estas acciones deben estar alineadas con los recursos y contexto de la organización, y no basta con implementarlas: deben documentarse y revisarse con frecuencia para evaluar su eficacia a largo plazo.

**Gestión de riesgo basado en la Norma ISO 27005**

La norma ISO 27005 es el complemento metodológico perfecto de la ISO 27001, ya que se enfoca en el manejo de riesgos. No es solo un manual técnico: es una guía que afina el análisis y tratamiento de amenazas, mejorando la precisión y efectividad del SGSI. Según Humphreys (2016), su enfoque permite tomar decisiones estratégicas bien fundamentadas, elevando la capacidad de respuesta institucional frente a eventos adversos.

(Whitman & Mattord, 2018) coinciden en que este marco no sólo ayuda a anticipar amenazas emergentes, sino que refuerza la postura general de seguridad, cultivando una verdadera cultura de prevención y resiliencia. En ese sentido, ISO 27005 es fundamental para las entidades que quieren incluir en todos los niveles operativos la administración de riesgos, realizando un compromiso transversal y no solo una inquietud del área de TI el aseguramiento de información.

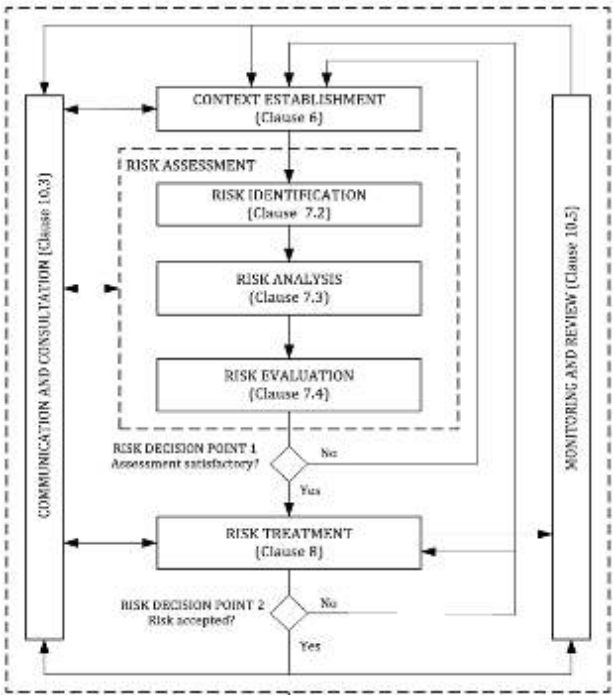



**Figura 2**
*Procedimiento de manejo de riesgos para la salvaguarda de la información.*
**Fuente:** (ISO/IEC 27005, 2022b)

# CAPÍTULO III
# MATERIALES Y MÉTODOS

## 3.1. Ámbito y condiciones de la investigación

### 3.1.1. Contexto de la investigación

Esta tesis se realizó en la unidad de formación profesional de SENATI Yurimaguas, ubicado Av. 15 de agosto Mz A Lt 1 en el distrito de Yurimaguas de la provincia de Alto Amazonas región de Loreto en Perú; el giro del negocio de dicha institución privada se basa en la enseñanza, formación y capacitación de profesionales técnicos y público en general.

### 3.1.2. Periodo de ejecución

EL estudio fue desarrollado desde agosto de 2024 hasta julio de 2025.

### 3.1.3. Autorizaciones y permisos

Se recibió el consentimiento de la coordinación de SENATI Yurimaguas para la elaboración y ejecución de la investigación, véase en el anexo 1.

### 3.1.4. Control ambiental y protocolos de bioseguridad

No es pertinente.

### 3.1.5. Aplicación de principios éticos internacionales

La investigación se efectuó con un alto nivel de responsabilidad y profesionalismo, cumpliendo con las normativas nacionales e internacionales que garantizan su validez científica. La administración de los activos de información de SENATI Yurimaguas se realizó con rigor, garantizando la fidelidad de los datos, su uso exclusivo con fines académicos y sin comprometer la confidencialidad institucional ni afectar a personas vinculadas. Se evitó cualquier impacto negativo en el ecosistema organizacional, promoviendo un análisis justo y orientado al beneficio colectivo. Todas las fuentes utilizadas fueron reconocidas conforme a los criterios de citación establecidos en la norma APA séptima edición, asegurando el respeto a la propiedad intelectual.

## 3.2. Sistema de variables

### 3.2.1. Variables principales

**Variable independiente:** Sistema de gestión de seguridad de la información.

**Variable dependiente:** Gestión de Riesgo

**Tabla 1**

*Variables por objetivo general*

"**Objetivo general:** Determinar la incidencia del sistema de gestión de seguridad de la información en la gestión del riesgo en la institución educativa superior SENATI – Yurimaguas, 2024"

| V. abstracta | V. concreta | M. registro | U. medida |
|---|---|---|---|
| Sistema de gestión de seguridad de la información | **Confidencialidad**<br>Control de acceso físico<br>Control de acceso lógico<br>Protección contra accesos no autorizados<br>Políticas de confidencialidad<br>**Integridad**<br>Registro de cambios<br>Protección contra alteraciones<br>Respaldo de información<br>Verificación de integridad<br>**Disponibilidad**<br>Redundancia o respaldo<br>Protección ante fallas<br>Tiempo de recuperación<br>Disponibilidad continua | Cuestionario | Cualitativo - Ordinal |
| **V. abstracta** | **V. concreta** | **M. registro** | **U. medida** |
| Gestión de Riesgo | **Identificación**<br>Registro de activos<br>Valoración del activo<br>Reconocimiento de amenazas<br>Reconocimiento de vulnerabilidades<br>**Análisis**<br>Estimación de impacto<br>Estimación de probabilidad<br>Nivel de riesgo<br>**Evaluación**<br>Criterios de aceptación<br>Priorización de riesgos<br>Registro de decisiones<br>**Tratamiento**<br>Medidas de mitigación<br>Controles aplicados<br>Seguimiento | Cuestionario | Cualitativo - Ordinal |

Fuente: Elaboración propia

### 3.2.2. Variables secundarias

No aplicable.

## 3.3. Procedimientos de la investigación

### Tipo y nivel de investigación

Esta investigación utilizó un enfoque cuantitativo porque, a través de instrumentos y estadísticas, posibilita la medición, el análisis y la verificación objetiva de las relaciones entre variables. La investigación es de tipo aplicada, dado que tiene como propósito resolver una problemática específica relacionada con la gestión de riesgos en SENATI Yurimaguas, mediante la implementación de un SGSI, generando así beneficios prácticos y mejoras operativas en el contexto institucional. En cuanto al nivel de investigación, se clasifica como explicativo, ya que intenta establecer cómo la puesta en marcha del SGSI tiee un efecto causal en la optimización de la administración de riesgos. Conforme con (Hernandez Sampieri et al., 2014), la investigación explicativa tiene como objetivo responder a las razones de los hechos y fenómenos. La intención es exponer las razones por las que se produce el fenómeno y en qué circunstancias sucede, o la razón de la relación entre dos o más variables. Igualmente, (Arias Odón, 2016) destacan que este tipo de investigación permite comprobar hipótesis mediante el análisis de relaciones causa-efecto entre variables.

### Diseño de investigación

El diseño preexperimental fue necesario para esta investigación debido a que se intervinieron con la variable independiente (implementación del SGSI) a un conjunto de activos para analizar el impacto en la variable dependiente (gestión de riesgos), (Hernandez Sampieri et al., 2014).

$$Ge: O_1 \text{ ---------- } X \text{ ---------- } O_2$$

Donde:

Ge: Grupo experimental

$O_1$: Pretest

X: estimulo o tratamiento

$O_2$: Postest

### Población

La totalidad de los activos de información del centro SENATI – Yurimaguas constituye la población del estudio, identificados en la matriz de activos de acuerdo con la norma ISO/IEC 27002. Esta población incluye activos de tipo humano (personal clave), tecnológico (hardware y software), físico (infraestructura), lógico (datos e información) y servicios (conectividad, energía, etc.), todos ellos importantes para manejar riesgos y proteger la información en la entidad. Es importante subrayar que el término población

no solo incluye a personas, sino a cualquier conjunto homogéneo que sea pertinente para la investigación. (Saucedo Vega, 2025)

**Muestra**

La muestra estuvo compuesta por los activos críticos de información seleccionados con base en el nivel de impacto, vulnerabilidad y exposición identificados en la matriz de valoración. Entre estos activos se incluyen plataformas digitales, redes, dispositivos, documentos críticos, servicios esenciales y, especialmente, el componente humano vinculado directamente a estos activos.

Para medir el efecto de la implementación del sistema, un pretest–postest como encuesta fue necesario aplicar a los 30 trabajadores del SENATI – Yurimaguas. El número corresponde a los trabajadores identificados en la sede, verificado mediante consulta directa a la institución, y seleccionados intencionadamente por su relación con los activos de información esenciales. Estas personas son la unidad de observación, dado que se examinan sus conocimientos, prácticas y percepciones relacionadas con la administración del aseguramiento de la información antes y después de la intervención. De acuerdo con (Alaminos & Castejón, 2006) la muestra intencional constituye una estrategia metodológica válida para la recolección de datos, particularmente eficaz en estudios que requieren poblaciones reducidas y con características altamente específicas.

### 3.3.1. Objetivo específico 1

Determinar la incidencia del sistema de gestión de seguridad de la información en la identificación del riesgo en la institución educativa superior SENATI – Yurimaguas, 2024.

- Diseño y validación de herramientas para recopilar datos.
- Recolección de datos a través del cuestionario pretest.
- Definición del contexto organizacional y el ámbito del SGSI.
- Elaboración de normativas de protección de la información.
- Elaboración de inventario de los activos.
- Clasificación de los activos por confidencialidad, integridad y disponibilidad.
- Establecimiento de las vulnerabilidades y amenazas vinculadas a los activos.
- Elaboración de una herramienta para la identificación de riesgos.

### 3.3.2. Objetivo específico 2

Determinar la incidencia del sistema de gestión de seguridad de la información en el análisis del riesgo en la institución educativa superior SENATI – Yurimaguas, 2024.

- Asignar valores de impacto y probabilidad a los riesgos identificados.

- Determinar los grados de riesgo.
- Representar los riesgos en un mapa de calor.

### 3.3.3. Objetivo específico 3

Determinar la incidencia del sistema de gestión de seguridad de la información en la evaluación del riesgo en la institución educativa superior SENATI – Yurimaguas, 2024.

- Definir criterios para la aceptación de riesgos.
- Evaluar la eficacia de los controles existentes.

### 3.3.4. Objetivo específico 4

Determinar la incidencia del sistema de gestión de seguridad de la información en el tratamiento del riesgo en la institución educativa superior SENATI – Yurimaguas, 2024.

- Elección de las alternativas de tratamiento para cada riesgo.
- Aplicación de controles de seguridad correspondientes.
- Recojo de datos mediante el cuestionario postest.
- Análisis estadístico descriptivo e inferencial haciendo uso de las herramientas de Excel y SPSS v.27.
- Exposición de los resultados

# CAPÍTULO IV

# RESULTADOS Y DISCUSIÓN

## 4.1. Resultados descriptivos de la variable SGSI

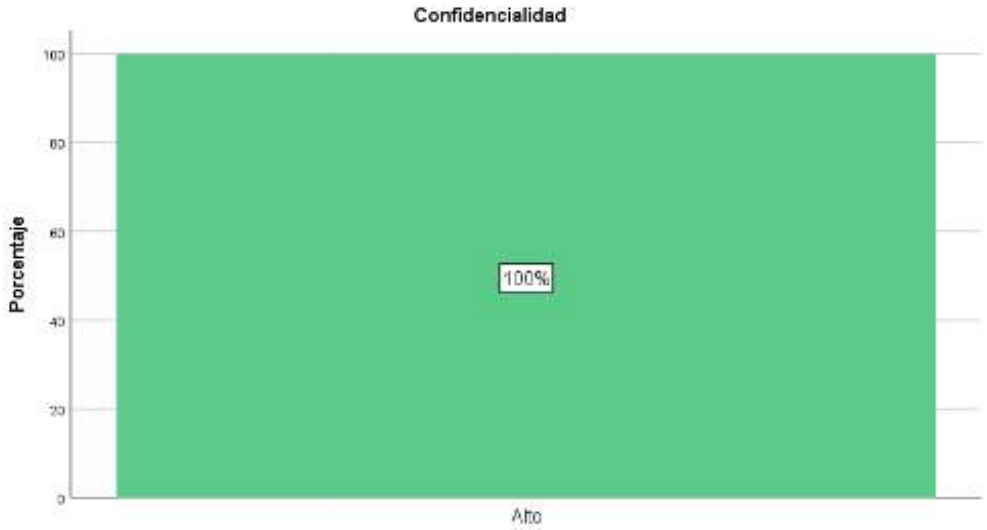



**Figura 3**
*Nivel de confidencialidad en la administración de riesgos de la institución educativa superior SENATI – Yurimaguas, 2024.*
Fuente: Elaboración propia

**Interpretación:** De los 30 encuestados en la institución educativa superior SENATI Yurimaguas en relación a los activos de información, se puede decir que el 100% detecta un alto nivel de confidencialidad.

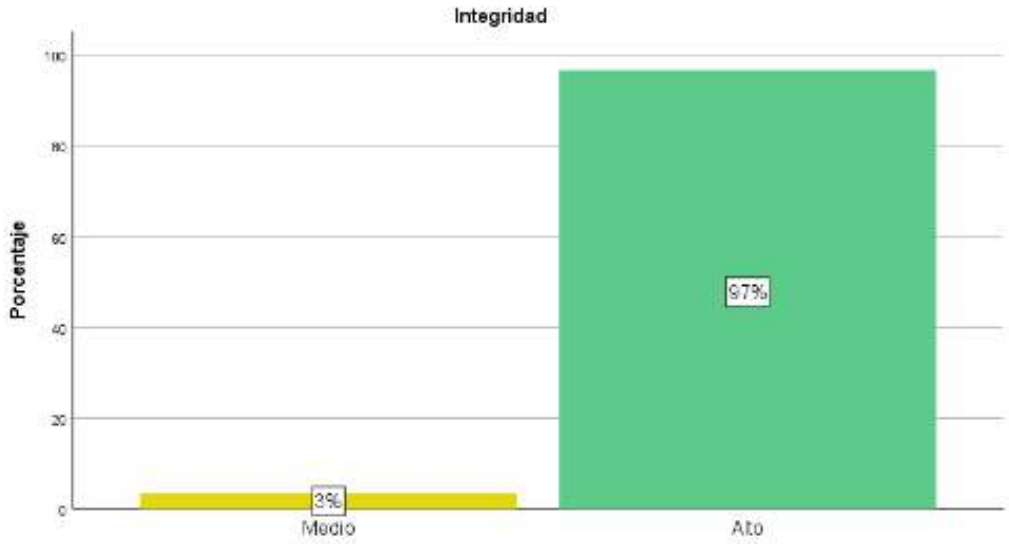



**Figura 4**
*Nivel de integridad en la gestión de riesgos en la institución educativa superior SENATI – Yurimaguas, 2024.*
Fuente: Elaboración propia

**Interpretación:** De los 30 encuestados en la institución educativa superior SENATI, respecto a los activos de información de la entidad educativa superior SENATI – Yurimaguas, 2024; el 97% percibe un nivel de integridad alto y el 3% un nivel medio.

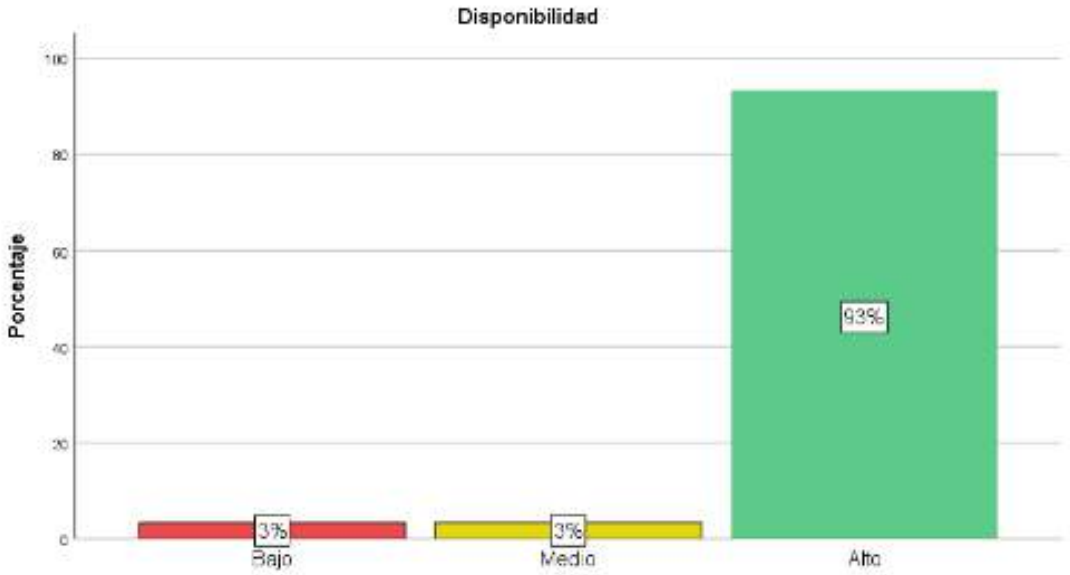



**Figura 5**
*Nivel de disponibilidad en la administración de riesgos en la institución educativa superior SENATI – Yurimaguas, 2024.*
***Fuente:*** Elaboración propia

**Interpretación:** De los 30 encuestados en la institución educativa superior SENATI, percibe respecto a la disponibilidad en un nivel alto de 93%, en un nivel medio de 3% y nivel bajo en 3%, respecto a los activos de información de la institución educativa superior SENATI – Yurimaguas, 2024.

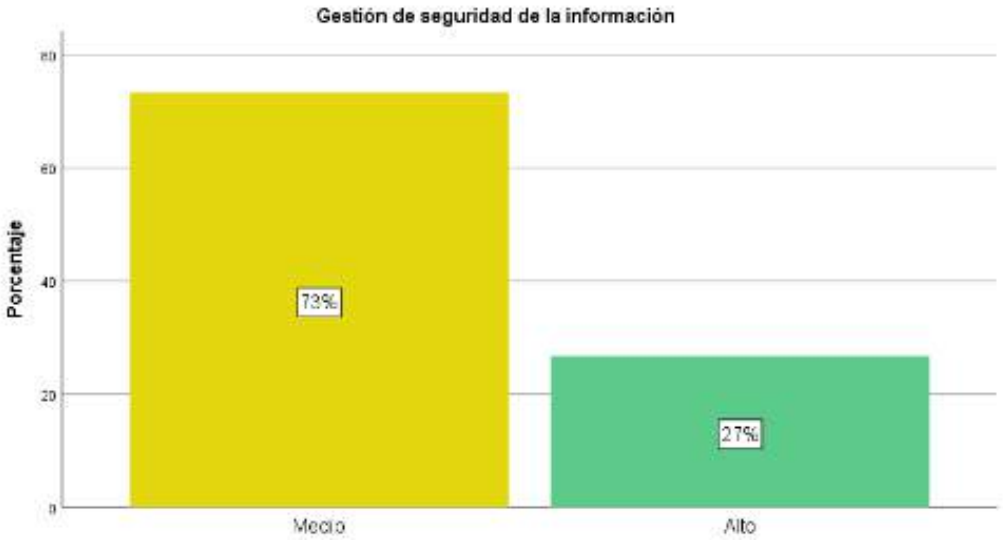



**Figura 6**
*Nivel de gestión de seguridad de la información en la institución educativa superior SENATI – Yurimaguas, 2024.*
Fuente: Elaboración propia

**Interpretación:** De los 30 encuestados en la institución educativa superior SENATI, respecto a los activos de información de la institución educativa superior SENATI – Yurimaguas, 2024; la percepción sobre la gestión del aseguramiento de información es en un nivel medio de 73%, y un nivel alto de 27%.

## 4.2. Resultados descriptivos de la variable Gestión del riesgo

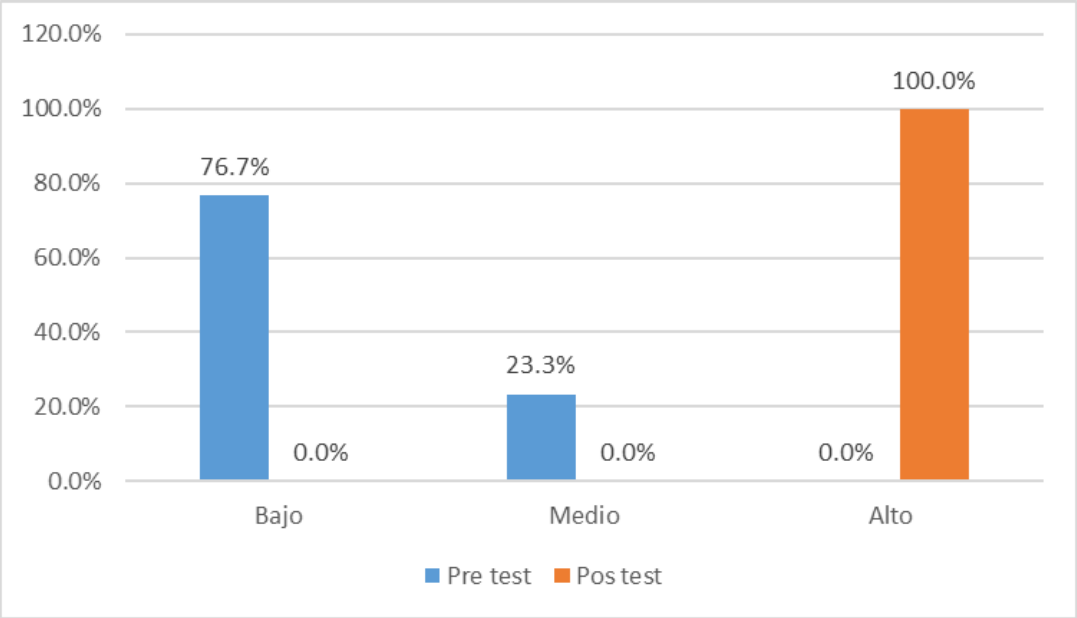



**Figura 7**
*Nivel de Identificación del riesgo en la institución educativa superior SENATI - Yurimaguas, 2024.*
***Fuente:*** Elaboración propia

**Interpretación:** En la institución educativa superior SENATI – Yurimaguas, según los resultados obtenidos del pretest aplicado a 30 participantes, el 76.7% percibía un nivel bajo de identificación del riesgo, mientras que el 23.3% reportaba un nivel medio. Después de implementar la administración del aseguramiento de información, se nota un cambio importante en el postest, donde el 100% de los encuestados percibe un nivel alto de identificación del riesgo respecto a los activos de información institucionales, evidenciando una mejora sustancial en esta dimensión.

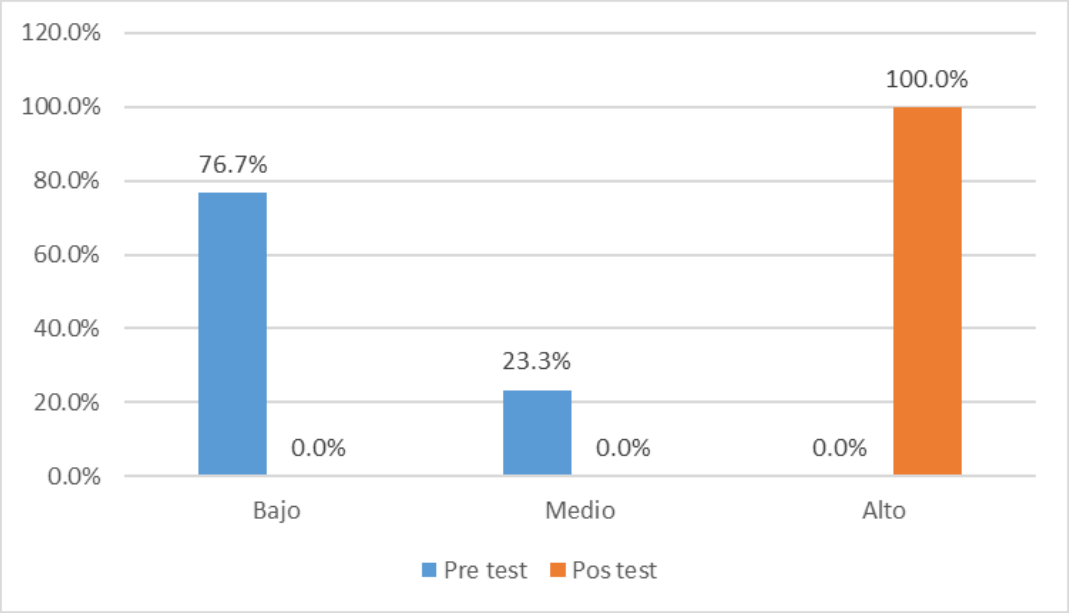



**Figura 8**
*Nivel de Análisis del riesgo en la institución educativa superior SENATI - Yurimaguas, 2024.*
Fuente: Elaboración propia

**Interpretación:** En la institución educativa superior SENATI – Yurimaguas, según los resultados obtenidos del pretest aplicado a 30 participantes, el 76.7% evidenciaba un nivel bajo de análisis del riesgo, mientras que el 23.3% reportaba un nivel medio. Después de implementar la administración del aseguramiento de información, se nota un cambio importante en el postest, donde el 100% de los encuestados evidencia un nivel alto de análisis del riesgo respecto a los activos de información institucionales, evidenciando una mejora sustancial en esta dimensión.

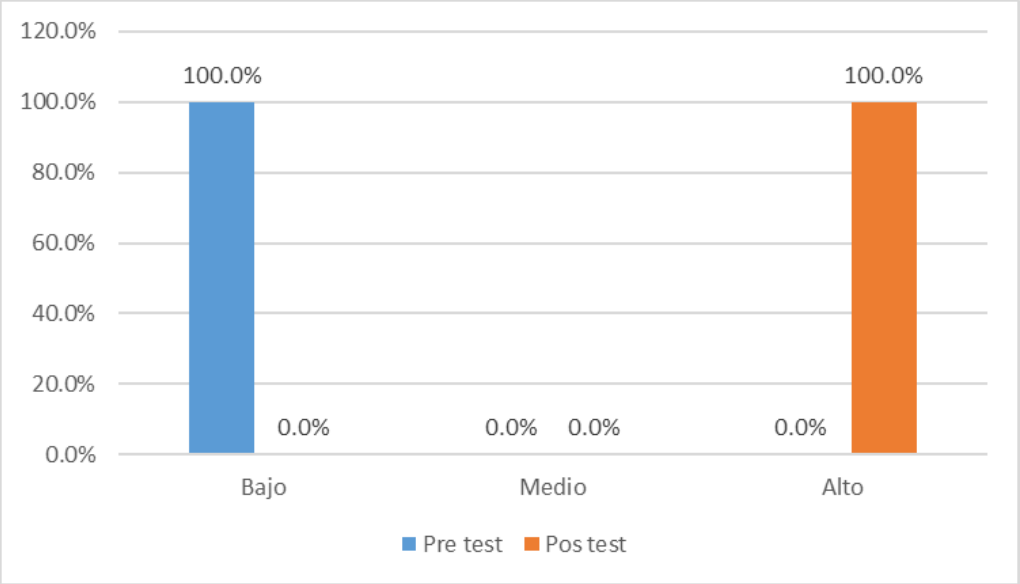



**Figura 9**
*Nivel de Evaluación del riesgo en la institución educativa superior SENATI - Yurimaguas, 2024.*
Fuente: Elaboración propia

**Interpretación:** En la institución educativa superior SENATI – Yurimaguas, según los resultados obtenidos del pretest aplicado a 30 participantes, el 100% evidenciaba un nivel bajo de evaluación del riesgo. Después de implementar la administración del aseguramiento de información, se nota un cambio importante en el postest, donde el 100% de los encuestados evidencia un nivel alto de evaluación del riesgo respecto a los activos de información institucionales, evidenciando una mejora sustancial en esta dimensión.

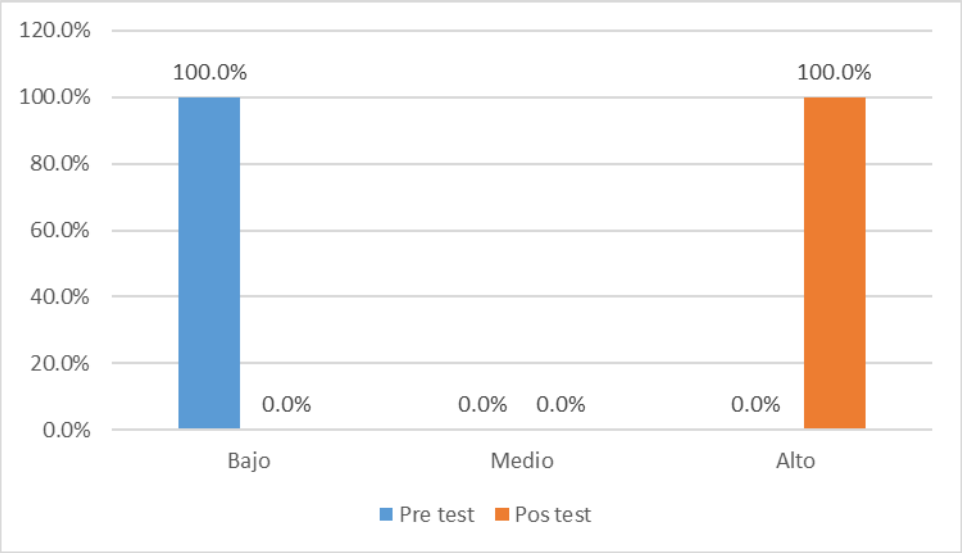



**Figura 10**
*Nivel de Tratamiento del riesgo en la institución educativa superior SENATI - Yurimaguas, 2024.*
Fuente: Elaboración propia

**Interpretación:** En la institución educativa superior SENATI – Yurimaguas, según los resultados obtenidos del pretest aplicado a 30 participantes, el 100% evidenciaba un nivel bajo de tratamiento del riesgo. Después de implementar la administración del aseguramiento de información, se nota un cambio importante en el postest, donde el 100% de los encuestados evidencia un nivel alto de tratamiento del riesgo respecto a los activos de información institucionales, evidenciando una mejora sustancial en esta dimensión.

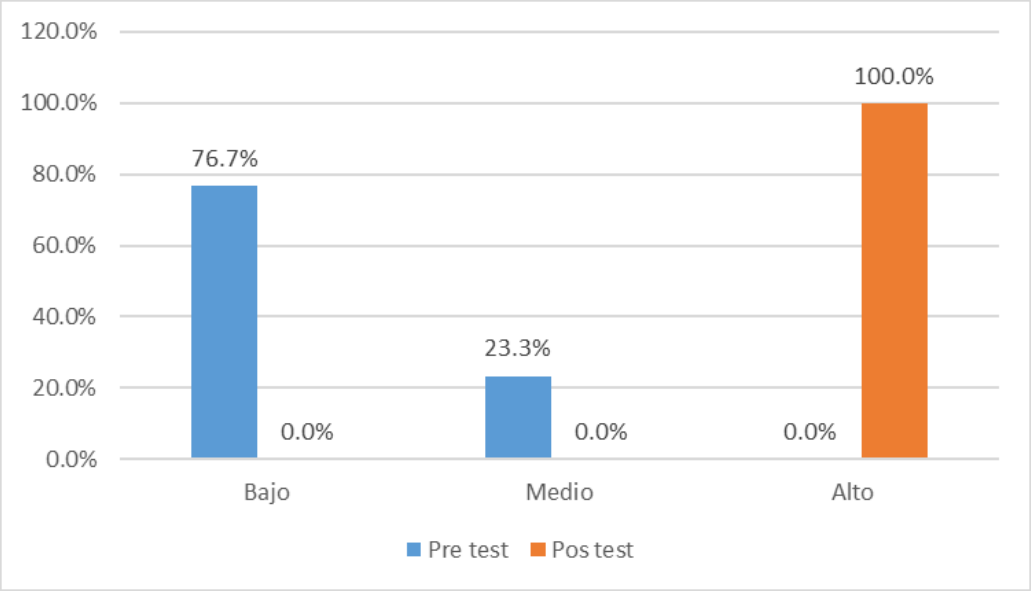



**Figura 11**
*Nivel de Gestión del riesgo en la institución educativa superior SENATI - Yurimaguas, 2024.*
Fuente: Elaboración propia

**Interpretación:** En la institución educativa superior SENATI – Yurimaguas, según los resultados obtenidos del pretest aplicado a 30 participantes, el 76.7% evidenciaba un nivel bajo de gestión del riesgo, mientras que el 23.3% reportaba un nivel medio. Después de implementar la administración del aseguramiento de información, se nota un cambio importante en el postest, donde el 100% de los encuestados demuestran un alto nivel de gestión de riesgos en relación con los activos informativos institucionales, evidenciando una mejora sustancial en esta variable.

## 4.3. Resultados inferenciales – Prueba de hipótesis

### Resultado general

**Ho:** El sistema de gestión de seguridad de la información no incide de forma positiva en la gestión del riesgo en la institución educativa superior SENATI – Yurimaguas, 2024.

**H1**: El sistema de gestión de seguridad de la información incide de forma positiva en la gestión del riesgo en la institución educativa superior SENATI – Yurimaguas, 2024.

**Tabla 2**

*Prueba de hipótesis general*

**Estadísticos de prueba[a]**

| | Gestión del Riesgo - Postest - Gestión del Riesgo - Pretest |
|---|---|
| Z | -4,864[b] |
| Sig. asintótica(bilateral) | ,000 |

a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos negativos.

Fuente: Elaboración propia

**Interpretación:** Los hallazgos del análisis de rangos con signo de Wilcoxon indican que Z = -4.864 y una significación asintótica bilateral p = 0.000. La hipótesis nula se rechaza porque p < 0.05, lo cual señala que hay diferencias significativas a nivel estadístico entre los resultados del pretest y el postest en relación con la variable Gestión del Riesgo.

Esto indica que la puesta en marcha del Sistema de Gestión de Seguridad de la Información (SGSI) tuvo un impacto positivo relevante, ya que la percepción y el desempeño en cuanto a la gestión del riesgo por parte de los miembros del Instituto SENATI – Yurimaguas mejoraron.

## 4.4. Resultado específico 1

**Ho:** El sistema de gestión de seguridad de la información no incide de forma positiva en la identificación del riesgo en la institución educativa superior SENATI – Yurimaguas, 2024.

**H1:** El sistema de gestión de seguridad de la información incide de forma positiva en la identificación del riesgo en la institución educativa superior SENATI – Yurimaguas, 2024.

**Tabla 3**

*Prueba de hipótesis específica 1*

**Estadísticos de prueba[a]**

| | Identificación del Riesgo - Pos test - Identificación del Riesgo - Pre test |
|---|---|
| Z | -5,069[b] |
| Sig. asintótica(bilateral) | ,000 |

a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos negativos.

Fuente: Elaboración propia

**Interpretación:** Para la dimensión de Identificación del Riesgo, los rangos con signo de Wilcoxon mostraron un valor Z = -5.069 y una significancia asintótica bilateral p = 0.000.

Como p < 0.05, se descarta la hipótesis nula y se concluye que hay distinciones estadísticamente significativas entre los resultados del pretest y el postest.

Este descubrimiento señala que la aplicación del Sistema de Gestión de Seguridad de la Información (SGSI) tuvo un efecto positivo y considerable en el reconocimiento del riesgo, ya que aumentó la habilidad de los participantes para detectar, estimar y entender los riesgos vinculados a los activos informativos en el Instituto SENATI – Yurimaguas.

**Discusión:** En relación con el objetivo específico 1, Los resultados logrados demuestran una mejora significativa en la detección del riesgo tras la puesta en práctica del Sistema de Gestión de Seguridad de la Información (SGSI). Antes de la intervención, la mayoría de los encuestados percibía un nivel bajo de identificación de riesgos; después del uso del SGSI, sin embargo, el 100 % reportó una percepción alta en este aspecto. Este descubrimiento no solo tiene un valor estadístico, sino que también muestra un fortalecimiento de la cultura organizacional enfocada en el manejo preventivo, en línea con los principios de la norma ISO/IEC 27002, que establece la necesidad de clasificar e inventariar los activos de información para su adecuada protección. Este resultado coincide con lo reportado por MENDELEY CITATION PLACEHOLDER 47, quien afirma que, utilizando los controles del SGSI según el Anexo A de la norma ISO 27001:2022, se disminuye de manera considerable la cantidad de incidentes relacionados con la seguridad, permitiendo una identificación más precisa y oportuna de amenazas.

## 4.5. Resultado específico 2

**Ho:** El sistema de gestión de seguridad de la información no incide de forma positiva en el análisis del riesgo en la institución educativa superior SENATI – Yurimaguas, 2024.

**H1:** El sistema de gestión de seguridad de la información incide de forma positiva en el análisis del riesgo en la institución educativa superior SENATI – Yurimaguas, 2024.

**Tabla 4**

*Prueba de hipótesis específica 2*

**Estadísticos de prueba[a]**

| | Análisis del Riesgo - Pos test - Análisis del Riesgo - Pre test |
|---|---|
| Z | -5,069[b] |
| Sig. asintótica(bilateral) | ,000 |

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

Fuente: Elaboración propia

**Interpretación:** El análisis de la dimensión de Análisis del Riesgo mediante la prueba de Wilcoxon mostró un estadístico Z = -5.069 y una significancia bilateral p = 0.000, lo que muestra que los resultados previos a la intervención y posteriores a esta difieren significativamente (p < 0.05).

Se puede asegurar que el análisis de riesgo mejoró de manera importante gracias a la implementación del Sistema de Gestión de Seguridad de la Información (SGSI), según este resultado, fortaleciendo la capacidad del personal para identificar amenazas, evaluar vulnerabilidades y comprender los posibles impactos sobre los activos de información en el Instituto SENATI – Yurimaguas.

**Discusión:** Respecto al objetivo específico 2, Se notó un avance significativo en el análisis del riesgo. La prueba de Wilcoxon corroboró las diferencias importantes entre el pretest y el postest, lo que demuestra que la aplicación del sistema contribuyó directamente a una mayor capacidad para reconocer y evaluar amenazas, vulnerabilidades y sus posibles consecuencias. Este descubrimiento está relacionado con lo propuesto por la teoría de Deming sobre el ciclo de mejora continua, que subraya la importancia de la planificación basada en evidencia para la toma de decisiones informadas. En este sentido, el SGSI no solo actúa como un marco de control, sino como un catalizador para el análisis sistemático y el juicio crítico sobre los riesgos que enfrentan los activos institucionales. Así lo corroboran también los hallazgos de MENDELEY CITATION PLACEHOLDER 48 y MENDELEY CITATION PLACEHOLDER 49, quienes encontraron que la implementación de un SGSI genera mayor conciencia sobre la importancia del análisis riguroso para proteger la información organizacional.

## 4.6. Resultado específico 3

**Ho:** El sistema de gestión de seguridad de la información no incide de forma positiva en la evaluación del riesgo en la institución educativa superior SENATI – Yurimaguas, 2024.

**H1**: El sistema de gestión de seguridad de la información incide de forma positiva en la evaluación del riesgo en la institución educativa superior SENATI – Yurimaguas, 2024.

**Tabla 5**
*Prueba de hipótesis específica 3*

**Estadísticos de prueba[a]**

| | Evaluación del Riesgo - Pos test - Evaluación del Riesgo - Pre test |
|---|---|
| Z | -5,477[b] |
| Sig. asintótica(bilateral) | ,000 |

a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos negativos.

Fuente: Elaboración propia

**Interpretación:** La aplicación de la prueba de rangos con signo de Wilcoxon a la dimensión Evaluación del Riesgo, produjo un resultado de Z = -5.477 y una significancia p = 0.000 en ambos sentidos, lo que señala que existe una diferencia estadísticamente significativa entre las calificaciones del pretest y el postest ($p < 0.05$).

Este hallazgo evidencia que el establecimiento del Sistema de Gestión de Seguridad de la Información (SGSI) produjo un notable avance en la valoración del riesgo, reforzando la habilidad institucional para determinar el impacto y la probabilidad de que las amenazas contra los activos informativos sucedan dentro del Instituto SENATI – Yurimaguas.

**Discusión:** En cuanto al objetivo específico 3, los resultados confirman que la evaluación del riesgo mejoró significativamente luego de la implementación del SGSI. Esta dimensión, que implica valorar el impacto y la probabilidad de ocurrencia en acontecimientos desfavorables, se fortaleció gracias a la estandarización de procesos y a la adopción de criterios técnicos establecidos por las normas internacionales ISO/IEC 27001 y 27005. Desde una perspectiva teórica, esto se puede interpretar a la luz del enfoque sistémico de Bertalanffy, en el que una organización se concibe como un sistema interconectado, donde la evaluación de riesgos permite priorizar intervenciones y optimizar recursos. Los resultados hallados son coherentes con los estudios de MENDELEY CITATION PLACEHOLDER 50 y MENDELEY CITATION PLACEHOLDER 51, quienes resaltan que la adecuada implementación del SGSI incide en el fortalecimiento del análisis y evaluación de amenazas, promoviendo una toma de decisiones más eficiente.

## 4.7. Resultado específico 4

**Ho:** El sistema de gestión de seguridad de la información no incide de forma positiva en el tratamiento del riesgo en la institución educativa superior SENATI – Yurimaguas, 2024.

**H1**: El sistema de gestión de seguridad de la información incide de forma positiva en el tratamiento del riesgo en la institución educativa superior SENATI – Yurimaguas, 2024.

**Tabla 6**

*Prueba de hipótesis específica 4*

**Estadísticos de prueba[a]**

| | Tratamiento del Riesgo - Pos test - Tratamiento del Riesgo - Pre test |
|---|---|
| Z | -5,477[b] |
| Sig. asintótica(bilateral) | ,000 |

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

Fuente: Elaboración propia

**Interpretación:** El examen de rangos con signo de Wilcoxon, realizado en la dimensión Tratamiento del Riesgo, resultó en un valor Z = -5.477 y una significancia asintótica bilateral de p = 0.000, lo que señala una diferencia estadísticamente relevante entre los puntajes del pretest y el postest ($p < 0.05$).

En el Instituto SENATI – Yurimaguas, la puesta en marcha de la administración del aseguramiento de Información tuvo un impacto positivo importante en el manejo del riesgo, al propiciar que se identificaran, priorizaran y aplicaran medidas correctivas o preventivas para los riesgos informáticos.

**Discusión:** Finalmente, respecto al objetivo específico 4, se evidencia que el tratamiento del riesgo también experimentó una mejora estadísticamente significativa. Esta dimensión incluye acciones como la implementación de controles, la aceptación de ciertos niveles de riesgo, y el monitoreo continuo de las decisiones tomadas. La teoría de administración del riesgo que propone la ISO 31000, la cual pone énfasis en la necesidad de respuestas estratégicas ante situaciones inciertas, puede explicar el avance. Asimismo, la teoría del capital humano de Becker permite entender cómo la capacitación y empoderamiento del personal —como ocurrió en este estudio con los 30 colaboradores evaluados— eleva la capacidad institucional de respuesta frente al riesgo. Estos hallazgos se respaldan en investigaciones como las de MENDELEY CITATION PLACEHOLDER 52 y MENDELEY CITATION PLACEHOLDER 53, quienes

demostraron que un SGSI fortalece las decisiones de tratamiento del riesgo mediante políticas claras, controles técnicos y administrativos, y seguimiento oportuno.

En conjunto, los resultados obtenidos en este estudio corroboran la eficacia del SGSI como herramienta de gestión integral de riesgos en contextos educativos, particularmente en instituciones técnicas como SENATI – Yurimaguas. Los avances registrados en cada una de las dimensiones permiten llegar a la conclusión de que el sistema no solo tiene un impacto favorable en el aseguramiento de información, sino que además fomenta una cultura organizacional más activa, resistente y acorde con los estándares internacionales.

# CONCLUSIONES

1. Respecto al objetivo específico 1, Se llega a la conclusión de que la puesta en marcha del SGSI en SENATI - Yurimaguas tiene un impacto positivo en la detección de riesgos. Después de la intervención, el personal demuestra un reconocimiento más sistemático y explícito de los activos de información, además de las amenazas vinculadas a ellos. Esto representa un primer paso firme en la gestión integral de riesgos.
2. En relación con el objetivo específico 2, se determina que el SGSI favorece sustancialmente el análisis de riesgos, al mejorar la capacidad del personal para estimar tanto la probabilidad de ocurrencia como el impacto de posibles incidentes sobre los activos de información. Este avance fortalece la toma de decisiones basada en evidencia, promoviendo una visión crítica frente a los factores de vulnerabilidad.
3. En función del objetivo específico 3, Se llega a la conclusión de que el SGSI colabora de forma importante con una evaluación del riesgo más estricta y coherente, posibilitando la clasificación y priorización de los riesgos en función de criterios técnicos y objetivos. Esta práctica disminuye la incertidumbre en la planificación institucional y fortalece el uso eficaz de los recursos destinados a garantizar la seguridad de la información.
4. Conforme al objetivo específico 4, Se establece que el SGSI mejora considerablemente la gestión de los riesgos a través de la aplicación de medidas apropiadas para prevenir, corregir y mitigar. Asimismo, promueve el establecimiento de políticas internas sostenibles y procedimientos de supervisión que aseguran la persistencia de la seguridad informativa a largo plazo.
5. En términos generales, Se concluye que el Sistema de Gestión de Seguridad de la Información es un instrumento eficaz para perfeccionar la administración del riesgo en entidades educativas superiores. La implementación de esto fomenta no solo el cumplimiento de las normas internacionales, sino también una cultura organizativa más consciente, madura y capaz de resistir frente a los riesgos que ponen en peligro los activos informativos.

# RECOMENDACIONES

1. Respecto al objetivo específico 1, Se aconseja mejorar los programas de formación continua para los empleados, con un enfoque en identificar los activos de información y riesgos relacionados. Esto garantizará una mayor conciencia organizacional sobre la criticidad de los activos y fomentará una cultura preventiva frente a amenazas emergentes.
2. En función del objetivo específico 2, se aconseja implementar herramientas digitales complementarias que automaticen parte del análisis de riesgos, permitiendo evaluar con mayor precisión la probabilidad e impacto de las amenazas. Asimismo, se sugiere estandarizar las matrices de análisis para mantener criterios homogéneos en toda la organización.
3. En relación con el objetivo específico 3, se recomienda establecer protocolos institucionales claros para la evaluación de riesgos, basados en indicadores medibles que orienten la toma de decisiones estratégicas. Además, se recomienda que un comité de seguridad de la información revise periódicamente esta evaluación.
4. Conforme al objetivo específico 4, Es imprescindible elaborar y poner en práctica un plan formal de tratamiento de riesgos que contenga responsables, cronogramas, recursos y procedimientos de seguimiento. La alta dirección debe aprobar este plan y coordinarlo con los planes de continuidad operativa del SENATI.
5. A nivel general, se recomienda institucionalizar el Sistema de Gestión de Seguridad de la Información (SGSI) como política transversal en todos los procesos administrativos y tecnológicos del centro SENATI – Yurimaguas. Esta medida permitirá garantizar la sostenibilidad del modelo propuesto, su mejora continua y su adaptación frente a nuevos desafíos tecnológicos y normativos.

# REFERENCIAS BIBLIOGRÁFICAS

Alaminos Chica, A., & Castejón Costa, J. L. (2006). *ELABORACIÓN, ANÁLISIS E INTERPRETACIÓN DE ENCUESTAS, CUESTIONARIOS Y ESCALAS DE OPINIÓN CORE View metadata, citation and similar papers at core* (S. A. Editorial Marfil, Ed.).

Álava Cuadra, M. E., & Choez Salazar, H. A. (2023). *Diseño de un SGSI basado en el estándar ISO 27001 para la empresa Invimedic S.A.* Universidad Politécnica Salesiana.

Arias Odón, F. G. (2016). *El Proyecto de Investigación Introducción a la metodología científica* (E. Episreme, Ed.; 7th ed.).

Calder, A., & Watkins, S. (2008). *IT Governance A Managers Guide to Data Security and ISO 27001/ISO 27002* (4th ed.).

Castro Ríos, H. (2022). Seguridad de la información y gestión del riesgo en una entidad del sistema electoral, año 2021. In *Universidad César Vallejo*. Universidad César Vallejo.

Check Point Research Team. (2023). *Average Weekly Global Cyberattacks peak with the highest number in 2 years, marking an 8% growth year over year, according to Check Point Research*. Check Point. https://blog.checkpoint.com/security/average-weekly-global-cyberattacks-peak-with-the-highest-number-in-2-years-marking-an-8-growth-year-over-year-according-to-check-point-research/

Coronado Farroñan, G. L. (2024). *SGSI basado en ISO/IEC_27001:2022 para la protección de activos de información de una entidad pública del Sector Defensa, Lima 2024*. Universidad Cesar Vallejo.

Defensoría del Pueblo. (2023). *La ciberdelincuencia en el Perú: Estrategias y retos del Estado*.

ESET. (2022). *ESET Security Report LATAM 2022*.

Guizado Castillo, J. M. (2024). *SGSI según ISO/IEC 27001:2022 y su incidencia en la protección de información en una municipalidad distrital, Lima 2023*. Universidad Cesar Vallejo.

Hernández Ladino, C. S. (2020). *Plan director para la implementación del sistema de gestión de seguridad de la información*. Universitat Oberta de Catalunya.

Hernandez Sampieri, R., Fernandez Collado, C., & Baptisa Lucio, M. del P. (2014). *Metodología de la Investigación* (6th ed.).

Humphreys, E. (2016). *Implementing the ISO/IEC 27001 ISMS Standard, Second Edition* (Artech House, Ed.; 2nd ed.).

ISO/IEC 27001. (2022). *Information security, cybersecurity and privacy protection — Information security management systems — Requirements*.

ISO/IEC 27005. (2022a). *Information security, cybersecurity and privacy protection — Guidance on managing information security risks*.

ISO/IEC 27005. (2022b). *Information security, cybersecurity and privacy protection — Guidance on managing information security risks*.

Jason, A. (2011a). *The Basics of Information Security*.

Jason, A. (2011b). *The Basics of Information Security*.

Martinez Ramirez, C. A. (2020). *Confidencialidad, integridad y disponibilidad*. https://es.linkedin.com/pulse/confidencialidad-integridad-y-disponibilidad-martinez-ramirez

Narro Mestanza, S. M. (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.* Universidad Privada del Norte.

NIST. (2012). Guide for Conducting Risk Assessments (SP 800-30 Rev.1). *NIST Guide for Conducting Risk Assessments*, 95.

PAIS. (2020). *SGSI: Sistema de Gestión de Seguridad de la Información, según la Norma Técnica Peruana NTP ISO/IEC 27001:2014*. https://www.pais.gob.pe/sgsi/sgsi.html

Panaqué Dominguez, J. A., Lizárraga Caipo, Y. G., & Mendoza De los Santos, A. (2022). Efectos de la implementación de un SGSI basado en la norma ISO 27001 para las organizaciones. *Perfiles de Ingeniería*, *18*(18), 67–74. https://doi.org/https://doi.org/10.31381/perfilesingenieria.v18i18.5399

Paredes Sanchez, S., & Romero Lozano, M. (2021). *Gestión de riesgos de los productos que se proveen a la ciudadanía por el Gobierno Regional de San Martín, 2020.* https://repositorio.unsm.edu.pe/backend/api/core/bitstreams/88500d2a-98b8-4514-b7ca-ae995e614a28/content

Peltier, T. R. (2016a). Information Security Policies, Procedures, and Standards: guidelines for effective information security management. CRC press. In *Information Security Policies, Procedures, and Standards*.

Peltier, T. R. (2016b). Information Security Policies, Procedures, and Standards: guidelines for effective information security management. CRC press. In *Information Security Policies, Procedures, and Standards*.

Pfleeger, C. P., Pfleeger, S. L., & Margulies, J. (2015). *Security in Computing* (5th ed.).

Plataforma del Estado Peruano. (2024). *Sistema de gestión de seguridad de la información*. Gob.Pe. https://www.gob.pe/14086-sistema-de-gestion-de-seguridad-de-la-informacion

Sanchez Rios, J. (2023). *SGSI y la gestión de seguridad electrónica del área TI en una empresa de servicios aéreos, Lima 2023*. Universidad César Vallejo.

Saucedo Vega, W. (2025). *Estadistica Descriptiva* (Universidad César Vallejo SAC, Ed.; 1st ed.). https://doi.org/https://doi.org/10.18050/estadisdescrip

Stallings, W., & Brown, L. (2024). Computer Security: Principles and Practice. In *Journal of Information Privacy and Security* (5th ed.). https://doi.org/10.1080/15536548.2013.10845680

Stoneburner, G., Goguen, A., & Feringa, A. (2002). Risk Management Guide for Information Technology Systems Recommendations. *Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg*, 55.

Tipton, H. F., & Krause, M. (2007). *Information.Security.Management.Handbook.* (6th ed.).

Tuanama Guevara, C. W. (2024). *Sistema de gestión de calidad y la gestión de servicios de tecnología de la información en el SAT-Tarapoto 2022.* https://repositorio.unsm.edu.pe/backend/api/core/bitstreams/94d426b7-87fc-48c3-a454-64a61b8e1e7b/content

U.S. Government Publishing Office. (2011a). *U.S.C. Title 44 - PUBLIC PRINTING AND DOCUMENTS*.

U.S. Government Publishing Office. (2011b). *U.S.C. Title 44 - PUBLIC PRINTING AND DOCUMENTS*.

Velásquez, M. H. H., Arévalo, A. A., & Ruiz, M. M. Z. (2025). *Sistema de gestión para la seguridad de la información y la confidencialidad de la información, Hospital II-1 Moyobamba, 2024.* . https://repositorio.unsm.edu.pe/backend/api/core/bitstreams/86280e6a-cfb1-4d0f-96f1-e157a010428f/content

Whitman, M. E., & Mattord, H. J. (2018). Principles of Information Security. In *Cengage Learning* (6th ed.).

# ANEXOS

## Anexo 1: Autorización y permiso.

SENATI

Yurimaguas, 01 de octubre de 2024

RE) 1.006. 2024 ETIY

**SR. JABER VASQUEZ MALCA**
**Instructor U.C.P Iquitos - Yurimaguas**
Estudiante de la Maestría en Ciencias con mención en Tecnología de la Información.
UNIVERSIDAD NACIONAL DE SAN MARTIN

**Ref. Respuesta a solicitud de permiso para realizar Trabajo de Investigación.**

De mi especial Consideración.

Por medio del presente me dirijo a usted con el debido respeto que se merece y al mismo tiempo darle la **AUTORIZACIÓN** correspondiente al documento que usted ha solicitado para la realización de su trabajo de investigación sobre "Implementación de un sistema de gestión de seguridad de la información para la gestión de riesgos en SENATI – Yurimaguas, 2024", le hago llegar mis deseos para que así puedan alcanzar sus metas y anhelos planificados de poder lograr obtener el grado de magister en Ciencias con mención en Tecnología de la Información.

Una vez más deseándoles lo mejor de los éxitos, me despido de usted, reiterándole mi especial consideración.

Atentamente;

SENATI UCP YURIMAGUAS NACIONAL LORETO

Ing. JUAN MOISES HURTADO GORDON
Coordinador de la
Escuela de Tecnologías de la Información
SENATI UCP Iquitos - Yurimaguas

SGS SGS SGS

Av. 15 de Agosto Mz. A Lt. 1, Yurimaguas, Loreto
eti-yurimaguas@senati.edu.pe www.senati.edu.pe
Telefax: 065-352084

## Anexo 2: Matriz de consistencia.

| Titulo: Implementación de un sistema de gestión de seguridad de la información para la gestión de riesgos en SENATI – Yurimaguas, 2024. | | | | | |
|---|---|---|---|---|---|
| **Problemas de investigación** | **Objetivos de Investigación** | **Hipótesis de Investigación** | **Definición Operacional** | | **Metodología y diseño** |
| **Problema General** | **Objetivo General** | **Hipótesis General** | **Variables** | **Dimensiones** | |
| ¿Cuál es la incidencia del sistema de gestión de seguridad de la información en la gestión del riesgo en la institución educativa superior SENATI – Yurimaguas, 2024? | Determinar la incidencia del sistema de gestión de seguridad de la información en la gestión del riesgo en la institución educativa superior SENATI – Yurimaguas, 2024. | El sistema de gestión de seguridad de la información incide de forma positiva en la gestión del riesgo en la institución educativa superior SENATI – Yurimaguas, 2024. | X: Sistema de Gestión de Seguridad de la Información | Confidencialidad | **Metodología:**<br>Cuantitativo<br>**Tipo:**<br>-Investigación Aplicada<br>**Diseño:**<br>-Pre experimental<br>**Población:**<br>- Activos de SENATI Yurimaguas.<br>**Muestra:**<br>Muestreo intencional a 30 trabajadores de SENATI Yurimaguas por su vínculo directo con los activos de información críticos de la gestión institucional.<br>**Instrumento:**<br>- Cuestionario. |
| | | | | Integridad | |
| | | | | Disponibilidad | |
| **Problema Especifico** | **Objetivos Especificos** | **Hipótesis Especificos** | **Variables** | **Dimensiones** | |
| ¿Cuál es la incidencia del sistema de gestión de seguridad de la información en la identificación del riesgo en la institución educativa superior SENATI – Yurimaguas, 2024? | Determinar la incidencia del sistema de gestión de seguridad de la información en la identificación del riesgo en la institución educativa superior SENATI – Yurimaguas, 2024. | El sistema de gestión de seguridad de la información incide de forma positiva en la identificación del riesgo en la institución educativa superior SENATI – Yurimaguas, 2024. | Y: Gestión de Riesgos | Identificación del riesgo | |
| ¿Cuál es la incidencia del sistema de gestión de seguridad de la información en el análisis del riesgo en la institución educativa superior SENATI – Yurimaguas, 2024? | Determinar la incidencia del sistema de gestión de seguridad de la información en el análisis del riesgo en la institución educativa superior SENATI – Yurimaguas, 2024. | El sistema de gestión de seguridad de la información incide de forma positiva en el análisis del riesgo en la institución educativa superior SENATI – Yurimaguas, 2024. | | Análisis del riesgo | |
| ¿Cuál es la incidencia del sistema de gestión de seguridad de la información en la evaluación del riesgo en la institución educativa superior SENATI – Yurimaguas, 2024? | Determinar la incidencia del sistema de gestión de seguridad de la información en la evaluación del riesgo en la institución educativa superior SENATI – Yurimaguas, 2024. | El sistema de gestión de seguridad de la información incide de forma positiva en la evaluación del riesgo en la institución educativa superior SENATI – Yurimaguas, 2024. | | Evaluación del riesgo | |
| ¿Cuál es la incidencia del sistema de gestión de seguridad de la información en el tratamiento del riesgo en la institución educativa superior SENATI – Yurimaguas, 2024? | Determinar la incidencia del sistema de gestión de seguridad de la información en el tratamiento del riesgo en la institución educativa superior SENATI – Yurimaguas, 2024. | El sistema de gestión de seguridad de la información incide de forma positiva en el tratamiento del riesgo en la institución educativa superior SENATI – Yurimaguas, 2024. | | Tratamiento del riesgo | |

## Anexo 3: Instrumentos de recolección de datos.

**CUESTIONARIO: "*Sistema de Gestión de Seguridad de la Información*"**

El presente cuestionario tiene como objeto medir el nivel de la variable de **GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN** de la investigación **"*Implementación de un sistema de gestión de seguridad de la información para la gestión de riesgos en SENATI – Yurimaguas*"**. Los datos recopilados serán tratados de manera confidencial.

| | |
|---|---|
| **Activo** | |
| **Código** | |
| **Fecha** | |
| **Hora** | |

Niveles de escala:

| 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|
| Nunca se cumple | Se cumple parcialmente | Se cumple moderadamente | Se cumple casi completamente | Se cumple completamente y está documentado |

| Dimensiones | | indicador | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| Confidencialidad | 1 | ¿El activo está en un lugar con acceso restringido? | | | | | |
| | 2 | ¿Requiere autenticación (usuario/contraseña)? | | | | | |
| | 3 | ¿Tiene cifrado o restricciones de permisos? | | | | | |
| | 4 | ¿Existen políticas documentadas de confidencialidad? | | | | | |
| Integridad | 5 | ¿Se registran las modificaciones al activo? | | | | | |
| | 6 | ¿Tiene protección contra modificaciones no autorizadas? | | | | | |
| | 7 | ¿Se realizan respaldos periódicos de la información? | | | | | |
| | 8 | ¿Se verifica la consistencia de la información almacenada? | | | | | |
| Disponibilidad | 9 | ¿Tiene sistemas redundantes o respaldo activo? | | | | | |
| | 10 | ¿El activo Cuenta con protección ante fallos (UPS, backup, etc.)? | | | | | |
| | 11 | ¿Existe un tiempo máximo de recuperación establecido? | | | | | |
| | 12 | ¿El activo estuvo disponible sin interrupciones críticas? | | | | | |

## CUESTIONARIO: *"Gestión de Riesgo"*

El presente cuestionario tiene como objeto medir el nivel de la variable de GESTION DE RIESGO de la investigación "***Implementación de un sistema de gestión de seguridad de la información para la gestión de riesgos en SENATI – Yurimaguas***". Los datos recopilados serán tratados de manera confidencial.

| | |
|---|---|
| **Activo** | |
| **Código** | |
| **Fecha** | |
| **Hora** | |

Niveles de escala:

| 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|
| Nunca se cumple | Se cumple parcialmente | Se cumple moderadamente | Se cumple casi completamente | Se cumple completamente y está documentado |

| Dimensiones | | Criterios o indicadores de medición | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|---|
| **Identificación de Riesgos** | 1 | ¿El activo está inventariado formalmente? | | | | | |
| | 2 | ¿Se ha valorado el activo según su criticidad? | | | | | |
| | 3 | ¿Se han identificado amenazas relevantes? | | | | | |
| | 4 | ¿Se han detectado vulnerabilidades asociadas? | | | | | |
| **Análisis de Riesgos** | 5 | ¿Se ha estimado el impacto de las amenazas? | | | | | |
| | 6 | ¿Se ha estimado la probabilidad de ocurrencia? | | | | | |
| | 7 | ¿Se ha calculado el nivel de riesgo? | | | | | |
| **Evaluación de Riesgos** | 8 | ¿Se definen criterios para aceptar o rechazar riesgos? | | | | | |
| | 9 | ¿Se priorizan los riesgos detectados? | | | | | |
| | 10 | ¿Se registran las decisiones sobre tratamiento o aceptación? | | | | | |
| **Tratamiento de Riesgos** | 11 | ¿Se aplican medidas para reducir riesgos? | | | | | |
| | 12 | ¿Existen controles técnicos o administrativos definidos? | | | | | |
| | 13 | ¿Se realiza seguimiento al tratamiento del riesgo? | | | | | |

## Ficha de Evaluación de Activos Críticos – SENATI Yurimaguas

Institución: SENATI – Yurimaguas

Fecha de aplicación: 2024

Responsable de la evaluación: Área de Tecnologías de la Información (TI) y Coordinación Académica de SENATI – Yurimaguas.

| Código | Activo crítico | Tipo | Responsable | Confidencialidad (1-3) | Integridad (1-3) | Disponibilidad (1-3) | Valor total | Nivel de criticidad | Amenazas / Vulnerabilidades | Controles aplicados |
|---|---|---|---|---|---|---|---|---|---|---|
| A1 | Servidor académico principal | Tecnológico | Área TI | 3 | 3 | 3 | 9 | Crítico | Fallas eléctricas, ciberataques, sobrecarga | UPS, firewall, copias de seguridad |
| A2 | Base de datos de alumnos (matrícula y notas) | Lógico | Registro Académico | 3 | 3 | 2 | 8 | Crítico | Accesos no autorizados, malware | Políticas de acceso, cifrado, antivirus |
| A3 | Red de conectividad institucional | Servicio | Área TI | 2 | 2 | 3 | 7 | Alto | Saturación, interrupción de internet | Redundancia, monitoreo de red |
| A4 | Documentos críticos (expedientes académicos) | Físico | Secretaría Académica | 3 | 2 | 2 | 7 | Alto | Pérdida física, incendios, manipulación indebida | Archivadores seguros, digitalización |
| A5 | Personal administrativo clave | Humano | Dirección | 2 | 2 | 3 | 7 | Alto | Suplantación de identidad, error humano | Capacitación, autenticación multifactor |

**Leyenda de valoración:** 1 = Bajo | 2 = Medio | 3 = Alto

# Anexo 4: Validación de los instrumentos de investigación

## INFORME DE OPINIÓN SOBRE INSTRUMENTO DE INVESTIGACIÓN CIENTÍFICA

### I. DATOS GENERALES

Apellidos y nombres del experto : Ing. MSc. Héctor Hernán Henríquez Taboada
Institución donde labora : UPN / UTP
Especialidad : Docente en Metodología
Instrumento de evaluación : **Cuestionario SGSI**
Autor del instrumento : Jaber Vasquez Malca

### II. ASPECTOS DE VALIDACIÓN

**MUY DEFICIENTE (1) DEFICIENTE (2) ACEPTABLE (3) BUENA (4) EXCELENTE (5)**

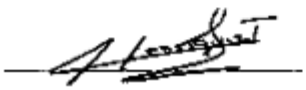
| CRITERIOS | INDICADORES | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| CLARIDAD | Los ítems están redactados con lenguaje apropiado y libre de ambigüedades acorde con los sujetos muestrales. | | | | | X |
| OBJETIVIDAD | Las instrucciones y los ítems del instrumento permiten recoger la información objetiva sobre la variable, en todas sus dimensiones en indicadores conceptuales y operacionales. | | | | | X |
| ACTUALIDAD | El instrumento demuestra vigencia acorde con el conocimiento científico, tecnológico, innovación y legal inherente a la variable. | | | | | X |
| ORGANIZACIÓN | Los ítems del instrumento reflejan organicidad lógica entre la definición operacional y conceptual respecto a la variable, de manera que permiten hacer inferencias en función a las hipótesis, problema y objetivos de la investigación. | | | | | X |
| SUFICIENCIA | Los ítems del instrumento son suficientes en cantidad y calidad acorde con la variable, dimensiones e indicadores. | | | | | X |
| INTENCIONALIDAD | Los ítems del instrumento son coherentes con el tipo de investigación y responden a los objetivos, hipótesis y variable de estudio. | | | | | X |
| CONSISTENCIA | La información que se recoja a través de los ítems del instrumento, permitirá analizar, describir y explicar la realidad, motivo de la investigación. | | | | | X |
| COHERENCIA | Los ítems del instrumento expresan relación con los indicadores de cada dimensión de la variable. | | | | | X |
| METODOLOGÍA | La relación entre la técnica y el instrumento propuestos responden al propósito de la investigación, desarrollo tecnológico e innovación. | | | | | X |
| PERTINENCIA | La redacción de los ítems concuerda con la escala valorativa del instrumento. | | | | | X |
| **PUNTAJE TOTAL** | | **50** | | | | |

(Nota: Tener en cuenta que el instrumento es válido cuando se tiene un puntaje mínimo de 41 "Excelente"; sin embargo, un puntaje menor al anterior se considera al instrumento no válido ni aplicable)

### III. OPINIÓN DE APLICACIÓN

APLICA

### IV. PROMEDIO DE EVALUACIÓN: 5.0



Ing. MSc. Héctor Hernán Henríquez Taboada

Lima, 01 de noviembre del 2024

# INFORME DE OPINIÓN SOBRE INSTRUMENTO DE INVESTIGACIÓN CIENTÍFICA

## I. DATOS GENERALES

Apellidos y nombres del experto : Ing. MSc. Héctor Hernán Henríquez Taboada
Institución donde labora : UPN / UTP
Especialidad : Docente en Metodología
Instrumento de evaluación : **Cuestionario Gestión de Riesgos**
Autor del instrumento : Jaber Vasquez Malca

## II. ASPECTOS DE VALIDACIÓN

**MUY DEFICIENTE (1) DEFICIENTE (2) ACEPTABLE (3) BUENA (4) EXCELENTE (5)**

| CRITERIOS | INDICADORES | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| CLARIDAD | Los ítems están redactados con lenguaje apropiado y libre de ambigüedades acorde con los sujetos muestrales. | | | | | X |
| OBJETIVIDAD | Las instrucciones y los ítems del instrumento permiten recoger la información objetiva sobre la variable, en todas sus dimensiones en indicadores conceptuales y operacionales. | | | | | X |
| ACTUALIDAD | El instrumento demuestra vigencia acorde con el conocimiento científico, tecnológico, innovación y legal inherente a la variable. | | | | | X |
| ORGANIZACIÓN | Los ítems del instrumento reflejan organicidad lógica entre la definición operacional y conceptual respecto a la variable, de manera que permiten hacer inferencias en función a las hipótesis, problema y objetivos de la investigación. | | | | | X |
| SUFICIENCIA | Los ítems del instrumento son suficientes en cantidad y calidad acorde con la variable, dimensiones e indicadores. | | | | | X |
| INTENCIONALIDAD | Los ítems del instrumento son coherentes con el tipo de investigación y responden a los objetivos, hipótesis y variable de estudio. | | | | | X |
| CONSISTENCIA | La información que se recoja a través de los ítems del instrumento, permitirá analizar, describir y explicar la realidad, motivo de la investigación. | | | | | X |
| COHERENCIA | Los ítems del instrumento expresan relación con los indicadores de cada dimensión de la variable. | | | | | X |
| METODOLOGÍA | La relación entre la técnica y el instrumento propuestos responden al propósito de la investigación, desarrollo tecnológico e innovación. | | | | | X |
| PERTINENCIA | La redacción de los ítems concuerda con la escala valorativa del instrumento. | | | | | X |
| **PUNTAJE TOTAL** | | | | **50** | | |

(Nota: Tener en cuenta que el instrumento es válido cuando se tiene un puntaje mínimo de 41 "Excelente"; sin embargo, un puntaje menor al anterior se considera al instrumento no válido ni aplicable)

## III. OPINIÓN DE APLICACIÓN

APLICA

## IV. PROMEDIO DE EVALUACIÓN: 5.0

Lima, 01 de noviembre del 2024

Ing. MSc. Héctor Hernán
Henríquez Taboada

# INFORME DE OPINIÓN SOBRE INSTRUMENTO DE INVESTIGACIÓN CIENTÍFICA

## I. DATOS GENERALES

Apellidos y nombres del experto : Dr. Santiago Raúl Gonzales Sánchez
Institución donde labora : Universidad Tecnológica del Perú
Especialidad : Docente en Metodología
Instrumento de evaluación : **Cuestionario Gestión de Riesgos**
Autor del instrumento : Jaber Vasquez Malca

## II. ASPECTOS DE VALIDACIÓN

**MUY DEFICIENTE (1) DEFICIENTE (2) ACEPTABLE (3) BUENA (4) EXCELENTE (5)**

| CRITERIOS | INDICADORES | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| CLARIDAD | Los ítems están redactados con lenguaje apropiado y libre de ambigüedades acorde con los sujetos muestrales. | | | | | X |
| OBJETIVIDAD | Las instrucciones y los ítems del instrumento permiten recoger la información objetiva sobre la variable, en todas sus dimensiones en indicadores conceptuales y operacionales. | | | | | X |
| ACTUALIDAD | El instrumento demuestra vigencia acorde con el conocimiento científico, tecnológico, innovación y legal inherente a la variable. | | | X | | |
| ORGANIZACIÓN | Los ítems del instrumento reflejan organicidad lógica entre la definición operacional y conceptual respecto a la variable, de manera que permiten hacer inferencias en función a las hipótesis, problema y objetivos de la investigación. | | | | | X |
| SUFICIENCIA | Los ítems del instrumento son suficientes en cantidad y calidad acorde con la variable, dimensiones e indicadores. | | | | | X |
| INTENCIONALIDAD | Los ítems del instrumento son coherentes con el tipo de investigación y responden a los objetivos, hipótesis y variable de estudio. | | | | | X |
| CONSISTENCIA | La información que se recoja a través de los ítems del instrumento, permitirá analizar, describir y explicar la realidad, motivo de la investigación. | | | | X | |
| COHERENCIA | Los ítems del instrumento expresan relación con los indicadores de cada dimensión de la variable. | | | | X | |
| METODOLOGÍA | La relación entre la técnica y el instrumento propuestos responden al propósito de la investigación, desarrollo tecnológico e innovación. | | | | | X |
| PERTINENCIA | La redacción de los ítems concuerda con la escala valorativa del instrumento. | | | | X | |
| **PUNTAJE TOTAL** | | **45** | | | | |

(Nota: Tener en cuenta que el instrumento es válido cuando se tiene un puntaje mínimo de 41 "Excelente"; sin embargo, un puntaje menor al anterior se considera al instrumento no válido ni aplicable)

## III. OPINIÓN DE APLICACIÓN

APLICA

## IV. PROMEDIO DE EVALUACIÓN: 4.5

Dr. Santiago Raúl Gonzales Sánchez

Lima, 01 de noviembre del 2024

# INFORME DE OPINIÓN SOBRE INSTRUMENTO DE INVESTIGACIÓN CIENTÍFICA

## I. DATOS GENERALES

Apellidos y nombres del experto : Dr. Santiago Raúl Gonzales Sánchez
Institución donde labora : Universidad Tecnológica del Perú
Especialidad : Docente en Metodología
Instrumento de evaluación : **Cuestionario SGSI**
Autor del instrumento : Jaber Vasquez Malca

## II. ASPECTOS DE VALIDACIÓN

**MUY DEFICIENTE (1) DEFICIENTE (2) ACEPTABLE (3) BUENA (4) EXCELENTE (5)**

| CRITERIOS | INDICADORES | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| CLARIDAD | Los ítems están redactados con lenguaje apropiado y libre de ambigüedades acorde con los sujetos muestrales. | | | | | X |
| OBJETIVIDAD | Las instrucciones y los ítems del instrumento permiten recoger la información objetiva sobre la variable, en todas sus dimensiones en indicadores conceptuales y operacionales. | | | | | X |
| ACTUALIDAD | El instrumento demuestra vigencia acorde con el conocimiento científico, tecnológico, innovación y legal inherente a la variable. | | | X | | |
| ORGANIZACIÓN | Los ítems del instrumento reflejan organicidad lógica entre la definición operacional y conceptual respecto a la variable, de manera que permiten hacer inferencias en función a las hipótesis, problema y objetivos de la investigación. | | | | | X |
| SUFICIENCIA | Los ítems del instrumento son suficientes en cantidad y calidad acorde con la variable, dimensiones e indicadores. | | | | | X |
| INTENCIONALIDAD | Los ítems del instrumento son coherentes con el tipo de investigación y responden a los objetivos, hipótesis y variable de estudio. | | | | | X |
| CONSISTENCIA | La información que se recoja a través de los ítems del instrumento, permitirá analizar, describir y explicar la realidad, motivo de la investigación. | | | | X | |
| COHERENCIA | Los ítems del instrumento expresan relación con los indicadores de cada dimensión de la variable. | | | | X | |
| METODOLOGÍA | La relación entre la técnica y el instrumento propuestos responden al propósito de la investigación, desarrollo tecnológico e innovación. | | | | | X |
| PERTINENCIA | La redacción de los ítems concuerda con la escala valorativa del instrumento. | | | | X | |
| **PUNTAJE TOTAL** | | **45** | | | | |

(Nota: Tener en cuenta que el instrumento es válido cuando se tiene un puntaje mínimo de 41 "Excelente"; sin embargo, un puntaje menor al anterior se considera al instrumento no válido ni aplicable)

## III. OPINIÓN DE APLICACIÓN

APLICA

## IV. PROMEDIO DE EVALUACIÓN: 4.5

Dr. Santiago Raúl Gonzales Sánchez

Lima, 01 de noviembre del 2024

# INFORME DE OPINIÓN SOBRE INSTRUMENTO DE INVESTIGACIÓN CIENTÍFICA

## I. DATOS GENERALES

Apellidos y nombres del experto : Dr. Walter Saucedo Vega
Institución donde labora : UNSM / UCV
Especialidad : Docente en Metodología
Instrumento de evaluación : **Cuestionario SGSI**
Autor del instrumento : Jaber Vasquez Malca

## II. ASPECTOS DE VALIDACIÓN

**MUY DEFICIENTE (1) DEFICIENTE (2) ACEPTABLE (3) BUENA (4) EXCELENTE (5)**

| CRITERIOS | INDICADORES | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| CLARIDAD | Los ítems están redactados con lenguaje apropiado y libre de ambigüedades acorde con los sujetos muestrales. | | | | | X |
| OBJETIVIDAD | Las instrucciones y los ítems del instrumento permiten recoger la información objetiva sobre la variable, en todas sus dimensiones en indicadores conceptuales y operacionales. | | | | X | |
| ACTUALIDAD | El instrumento demuestra vigencia acorde con el conocimiento científico, tecnológico, innovación y legal inherente a la variable. | | | | | X |
| ORGANIZACIÓN | Los ítems del instrumento reflejan organicidad lógica entre la definición operacional y conceptual respecto a la variable, de manera que permiten hacer inferencias en función a las hipótesis, problema y objetivos de la investigación. | | | | | X |
| SUFICIENCIA | Los ítems del instrumento son suficientes en cantidad y calidad acorde con la variable, dimensiones e indicadores. | | | | X | |
| INTENCIONALIDAD | Los ítems del instrumento son coherentes con el tipo de investigación y responden a los objetivos, hipótesis y variable de estudio. | | | | | X |
| CONSISTENCIA | La información que se recoja a través de los ítems del instrumento, permitirá analizar, describir y explicar la realidad, motivo de la investigación. | | | | X | |
| COHERENCIA | Los ítems del instrumento expresan relación con los indicadores de cada dimensión de la variable. | | | | | X |
| METODOLOGÍA | La relación entre la técnica y el instrumento propuestos responden al propósito de la investigación, desarrollo tecnológico e innovación. | | | | | X |
| PERTINENCIA | La redacción de los ítems concuerda con la escala valorativa del instrumento. | | | | | X |
| **PUNTAJE TOTAL** | | **47** | | | | |

(Nota: Tener en cuenta que el instrumento es válido cuando se tiene un puntaje mínimo de 41 "Excelente"; sin embargo, un puntaje menor al anterior se considera al instrumento no válido ni aplicable)

## III. OPINIÓN DE APLICACIÓN

APLICA

## IV. PROMEDIO DE EVALUACIÓN: 4.7

Dr. Walter Saucedo Vega

Tarapoto, 01 de noviembre del 2024

# INFORME DE OPINIÓN SOBRE INSTRUMENTO DE INVESTIGACIÓN CIENTÍFICA

## I. DATOS GENERALES

Apellidos y nombres del experto : Dr. Walter Saucedo Vega
Institución donde labora : UNSM / UCV
Especialidad : Docente en Metodología
Instrumento de evaluación : **Cuestionario Gestión de Riesgos**
Autor del instrumento : Jaber Vasquez Malca

## II. ASPECTOS DE VALIDACIÓN

**MUY DEFICIENTE (1) DEFICIENTE (2) ACEPTABLE (3) BUENA (4) EXCELENTE (5)**

| CRITERIOS | INDICADORES | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| CLARIDAD | Los ítems están redactados con lenguaje apropiado y libre de ambigüedades acorde con los sujetos muestrales. | | | | | X |
| OBJETIVIDAD | Las instrucciones y los ítems del instrumento permiten recoger la información objetiva sobre la variable, en todas sus dimensiones en indicadores conceptuales y operacionales. | | | | X | |
| ACTUALIDAD | El instrumento demuestra vigencia acorde con el conocimiento científico, tecnológico, innovación y legal inherente a la variable. | | | | | X |
| ORGANIZACIÓN | Los ítems del instrumento reflejan organicidad lógica entre la definición operacional y conceptual respecto a la variable, de manera que permiten hacer inferencias en función a las hipótesis, problema y objetivos de la investigación. | | | | | X |
| SUFICIENCIA | Los ítems del instrumento son suficientes en cantidad y calidad acorde con la variable, dimensiones e indicadores. | | | | X | |
| INTENCIONALIDAD | Los ítems del instrumento son coherentes con el tipo de investigación y responden a los objetivos, hipótesis y variable de estudio. | | | | | X |
| CONSISTENCIA | La información que se recoja a través de los ítems del instrumento, permitirá analizar, describir y explicar la realidad, motivo de la investigación. | | | | X | |
| COHERENCIA | Los ítems del instrumento expresan relación con los indicadores de cada dimensión de la variable. | | | | | X |
| METODOLOGÍA | La relación entre la técnica y el instrumento propuestos responden al propósito de la investigación, desarrollo tecnológico e innovación. | | | | | X |
| PERTINENCIA | La redacción de los ítems concuerda con la escala valorativa del instrumento. | | | | | X |
| **PUNTAJE TOTAL** | | **47** | | | | |

(Nota: Tener en cuenta que el instrumento es válido cuando se tiene un puntaje mínimo de 41 "Excelente"; sin embargo, un puntaje menor al anterior se considera al instrumento no válido ni aplicable)

## III. OPINIÓN DE APLICACIÓN

APLICA

## IV. PROMEDIO DE EVALUACIÓN: 4.7

Dr. Walter Saucedo Vega

Tarapoto, 01 de noviembre del 2024

## Anexo 5: Datos para el análisis descriptivo de la variable independiente

| | C | I | D | G |
|---|---|---|---|---|
| 1 | 3 | 3 | 3 | 3 |
| 2 | 3 | 3 | 3 | 3 |
| 3 | 3 | 3 | 3 | 3 |
| 4 | 3 | 3 | 3 | 3 |
| 5 | 3 | 3 | 3 | 3 |
| 6 | 3 | 3 | 3 | 3 |
| 7 | 3 | 3 | 3 | 3 |
| 8 | 3 | 3 | 3 | 3 |
| 9 | 3 | 2 | 2 | 2 |
| 10 | 3 | 3 | 3 | 2 |
| 11 | 3 | 3 | 3 | 2 |
| 12 | 3 | 3 | 3 | 2 |
| 13 | 3 | 3 | 1 | 2 |
| 14 | 3 | 3 | 3 | 2 |
| 15 | 3 | 3 | 3 | 2 |
| 16 | 3 | 3 | 3 | 2 |
| 17 | 3 | 3 | 3 | 2 |
| 18 | 3 | 3 | 3 | 2 |
| 19 | 3 | 3 | 3 | 2 |
| 20 | 3 | 3 | 3 | 2 |
| 21 | 3 | 3 | 3 | 2 |
| 22 | 3 | 3 | 3 | 2 |
| 23 | 3 | 3 | 3 | 2 |
| 24 | 3 | 3 | 3 | 2 |
| 25 | 3 | 3 | 3 | 2 |
| 26 | 3 | 3 | 3 | 2 |
| 27 | 3 | 3 | 3 | 2 |
| 28 | 3 | 3 | 3 | 2 |
| 29 | 3 | 3 | 3 | 2 |
| 30 | 3 | 3 | 3 | 2 |

## Anexo 6: Datos para el análisis descriptivo de la variable dependiente

| | Pre_I | Pre_A | Pre_E | Pre_T | Pre | Pos_I | Pos_A | Pos_E | Pos_T | Pos |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 2 | 1 | 1 | 2 | 3 | 3 | 3 | 3 | 3 |
| 2 | 2 | 2 | 1 | 1 | 2 | 3 | 3 | 3 | 3 | 3 |
| 3 | 2 | 2 | 1 | 1 | 2 | 3 | 3 | 3 | 3 | 3 |
| 4 | 2 | 2 | 1 | 1 | 2 | 3 | 3 | 3 | 3 | 3 |
| 5 | 2 | 2 | 1 | 1 | 2 | 3 | 3 | 3 | 3 | 3 |
| 6 | 2 | 2 | 1 | 1 | 2 | 3 | 3 | 3 | 3 | 3 |
| 7 | 2 | 2 | 1 | 1 | 2 | 3 | 3 | 3 | 3 | 3 |
| 8 | 1 | 1 | 1 | 1 | 1 | 3 | 3 | 3 | 3 | 3 |
| 9 | 1 | 1 | 1 | 1 | 1 | 3 | 3 | 3 | 3 | 3 |
| 10 | 1 | 1 | 1 | 1 | 1 | 3 | 3 | 3 | 3 | 3 |
| 11 | 1 | 1 | 1 | 1 | 1 | 3 | 3 | 3 | 3 | 3 |
| 12 | 1 | 1 | 1 | 1 | 1 | 3 | 3 | 3 | 3 | 3 |
| 13 | 1 | 1 | 1 | 1 | 1 | 3 | 3 | 3 | 3 | 3 |
| 14 | 1 | 1 | 1 | 1 | 1 | 3 | 3 | 3 | 3 | 3 |
| 15 | 1 | 1 | 1 | 1 | 1 | 3 | 3 | 3 | 3 | 3 |
| 16 | 1 | 1 | 1 | 1 | 1 | 3 | 3 | 3 | 3 | 3 |
| 17 | 1 | 1 | 1 | 1 | 1 | 3 | 3 | 3 | 3 | 3 |
| 18 | 1 | 1 | 1 | 1 | 1 | 3 | 3 | 3 | 3 | 3 |
| 19 | 1 | 1 | 1 | 1 | 1 | 3 | 3 | 3 | 3 | 3 |
| 20 | 1 | 1 | 1 | 1 | 1 | 3 | 3 | 3 | 3 | 3 |
| 21 | 1 | 1 | 1 | 1 | 1 | 3 | 3 | 3 | 3 | 3 |
| 22 | 1 | 1 | 1 | 1 | 1 | 3 | 3 | 3 | 3 | 3 |
| 23 | 1 | 1 | 1 | 1 | 1 | 3 | 3 | 3 | 3 | 3 |
| 24 | 1 | 1 | 1 | 1 | 1 | 3 | 3 | 3 | 3 | 3 |
| 25 | 1 | 1 | 1 | 1 | 1 | 3 | 3 | 3 | 3 | 3 |
| 26 | 1 | 1 | 1 | 1 | 1 | 3 | 3 | 3 | 3 | 3 |
| 27 | 1 | 1 | 1 | 1 | 1 | 3 | 3 | 3 | 3 | 3 |
| 28 | 1 | 1 | 1 | 1 | 1 | 3 | 3 | 3 | 3 | 3 |
| 29 | 1 | 1 | 1 | 1 | 1 | 3 | 3 | 3 | 3 | 3 |
| 30 | 1 | 1 | 1 | 1 | 1 | 3 | 3 | 3 | 3 | 3 |

# Anexo 7: Implementación del SGSI – SENATI Yurimaguas

## I. Contexto y Alcance

### Contexto Organizacional

La sede SENATI – Yurimaguas es una institución educativa superior que maneja información crítica vinculada a procesos académicos, administrativos y tecnológicos. En su operación diaria gestiona datos personales de estudiantes, registros académicos, expedientes administrativos, así como la infraestructura tecnológica que permite el soporte a la enseñanza y a la gestión institucional. La ausencia de un sistema formal de seguridad de la información genera exposición a riesgos como accesos no autorizados, pérdida de datos, fallas de red o errores humanos.

### Objetivo del SGSI

El SGSI se implementa con el propósito de **proteger los activos de información críticos** de la sede, asegurando su **confidencialidad, integridad y disponibilidad (C-I-D)**, y de este modo garantizar la continuidad operativa y la confianza de estudiantes, docentes y personal administrativo.

### Alcance del SGSI

El alcance del SGSI en SENATI – Yurimaguas se definió de acuerdo a los criterios de la norma ISO/IEC 27001 y 27005, considerando:

- **Activos tecnológicos:** servidores, equipos de cómputo, redes internas, software académico.
- **Activos lógicos:** bases de datos de matrícula, notas, expedientes digitales.
- **Activos físicos:** documentos impresos, archivadores, infraestructura administrativa.
- **Activos humanos:** personal académico, administrativo y de soporte TI vinculado a la gestión de información.
- **Activos de servicios:** conectividad a internet, energía eléctrica y plataformas digitales de soporte académico.

### Justificación del Alcance

El alcance se limita a los procesos académicos y administrativos esenciales, debido a que en estos recae la mayor criticidad institucional. La delimitación permite focalizar los esfuerzos de seguridad en las áreas de mayor riesgo y factibilidad de control,

garantizando la viabilidad de la implementación dentro del contexto de un proyecto académico.

## II. Política de Seguridad de la Información

### Introducción

La política de seguridad de la información constituye el pilar fundamental del SGSI, estableciendo las directrices que orientan la protección de los activos de información del SENATI – Yurimaguas. Este documento formaliza el compromiso institucional con la gestión de riesgos, la prevención de incidentes y la mejora continua.

### Objetivo

Garantizar la confidencialidad, integridad y disponibilidad (C-I-D) de la información académica y administrativa, reduciendo los riesgos asociados a amenazas internas y externas, y promoviendo una cultura de seguridad en toda la comunidad educativa.

### Alcance

La política es aplicable a:

- Personal académico, administrativo y de soporte TI.
- Activos tecnológicos, lógicos, físicos, humanos y de servicios identificados como críticos.
- Procesos académicos (matrícula, notas, expedientes) y administrativos (gestión documental, conectividad).

### Principios

1. Confidencialidad: Solo el personal autorizado puede acceder a la información crítica.
2. Integridad: Toda modificación de datos debe ser controlada y trazable.
3. Disponibilidad: Los sistemas deben estar disponibles en los horarios operativos.
4. Cumplimiento: Adecuación a normas ISO/IEC 27001 y 27005, así como a la legislación peruana vigente en materia de protección de datos.
5. Mejora continua: El SGSI será revisado y actualizado periódicamente.

### Responsabilidades

- Área de Tecnologías de la Información (TI): Implementar controles técnicos (firewall, cifrado, backups).
- Coordinación Académica: Custodiar la integridad y seguridad de registros académicos y expedientes.
- Personal administrativo: Cumplir lineamientos y reportar incidentes de seguridad.
- Dirección de SENATI Yurimaguas: Aprobar y supervisar el cumplimiento de la política.

**Compromisos**

- Capacitar anualmente al personal en buenas prácticas de seguridad.
- Garantizar medidas de respaldo y recuperación ante desastres.
- Monitorear periódicamente los incidentes de seguridad.
- Asegurar la participación de todo el personal en el cumplimiento de esta política.

## III. Inventario y Clasificación de Activos

**Introducción**

El inventario de activos constituye la base del SGSI, ya que permite identificar y organizar todos los recursos de información que requieren protección. En SENATI – Yurimaguas se clasificaron los activos de acuerdo con la norma ISO/IEC 27002, en categorías humanas, tecnológicas, lógicas, físicas y de servicios.

**Inventario de Activos**

Los activos identificados en la institución se distribuyen de la siguiente manera:

- Humanos: personal académico, administrativo y de soporte TI vinculado al uso y gestión de la información.
- Tecnológicos: servidores, computadoras, routers, equipos de red y software de gestión académica.
- Lógicos: bases de datos de alumnos (matrícula y notas), expedientes digitales, aplicaciones y plataformas digitales.
- Físicos: expedientes académicos impresos, documentos administrativos, archivadores.

- Servicios: red de conectividad institucional, internet, energía eléctrica y sistemas de respaldo.

### Clasificación por Criticidad

Cada activo fue evaluado en función de los criterios de Confidencialidad, Integridad y Disponibilidad (C-I-D), aplicando una escala de 1 (bajo), 2 (medio) y 3 (alto). El valor total determina el nivel de criticidad del activo.

Ejemplo de clasificación:

| Código | Activo | Tipo | Confidencialidad | Integridad | Disponibilidad | Valor total | Nivel de criticidad |
|---|---|---|---|---|---|---|---|
| A1 | Servidor académico principal | Tecnológico | 3 | 3 | 3 | 9 | Crítico |
| A2 | Base de datos de alumnos (matrícula y notas) | Lógico | 3 | 3 | 2 | 8 | Crítico |
| A3 | Red de conectividad institucional | Servicio | 2 | 2 | 3 | 7 | Alto |
| A4 | Documentos físicos (expedientes académicos) | Físico | 3 | 2 | 2 | 7 | Alto |
| A5 | Personal administrativo clave | Humano | 2 | 2 | 3 | 7 | Alto |

### Justificación

La clasificación permite priorizar los esfuerzos de seguridad en los activos con mayor criticidad (valor ≥ 8), dado que su compromiso representaría un alto impacto en la continuidad académica y administrativa de SENATI – Yurimaguas.

## IV. Gestión de Riesgos de la Información

### Introducción

La gestión de riesgos es un proceso sistemático que permite identificar, analizar, evaluar y tratar las amenazas que pueden comprometer la seguridad de los activos de

información. En SENATI – Yurimaguas se aplicó la metodología de ISO/IEC 27005, tomando como referencia los activos críticos previamente clasificados.

**Identificación de Riesgos**

Se analizaron las posibles amenazas y vulnerabilidades de cada activo crítico. Ejemplos:

- Servidor académico principal: fallas eléctricas, ciberataques, sobrecargas.
- Base de datos de alumnos: accesos no autorizados, corrupción de datos, malware.
- Red de conectividad institucional: saturación, corte de internet, ataques de denegación de servicio.
- Documentos físicos (expedientes académicos): pérdida por incendio, robo, manipulación indebida.
- Personal administrativo clave: error humano, suplantación de identidad, falta de capacitación.

**Análisis de Riesgos**

Cada riesgo fue evaluado en términos de probabilidad de ocurrencia y impacto en la organización, con valores de 1 (bajo), 2 (medio) y 3 (alto).

Ejemplo de matriz simplificada:

| Activo | Amenaza/Vulnerabilidad | Probabilidad | Impacto | Nivel de Riesgo (PxI) |
|---|---|---|---|---|
| Servidor académico | Ciberataque | 3 | 3 | 9 (Crítico) |
| Base de datos alumnos | Acceso no autorizado | 2 | 3 | 6 (Alto) |
| Red institucional | Corte de internet | 2 | 2 | 4 (Medio) |
| Documentos académicos | Incendio | 1 | 3 | 3 (Medio) |
| Personal clave | Error humano | 2 | 2 | 4 (Medio) |

**Evaluación de Riesgos**

Con base en los valores obtenidos, se construyó un mapa de calor de riesgos que permitió priorizar:

- Nivel Crítico (≥ 7): Servidor académico, base de datos de alumnos.
- Nivel Alto (5–6): Red institucional, personal administrativo clave.
- Nivel Medio (3–4): Documentos físicos.

**Resultado de la Evaluación**

El análisis evidenció que los activos tecnológicos y lógicos presentan la mayor exposición a riesgos, lo que exige implementar controles técnicos y administrativos robustos. Por otro lado, aunque los documentos físicos y el personal clave tienen riesgos moderados, requieren medidas de mitigación para evitar incidentes.

## V. Plan de Tratamiento de Riesgos

**Introducción**

El plan de tratamiento de riesgos constituye la fase de acción del SGSI. Una vez identificados y evaluados los riesgos, se definen estrategias y controles para mitigarlos, transferirlos, aceptarlos o evitarlos, garantizando la continuidad de los procesos académicos y administrativos.

**Estrategias de Tratamiento**

De acuerdo con la norma ISO/IEC 27005, se adoptaron las siguientes opciones:

- Mitigar: Reducir la probabilidad o impacto mediante controles preventivos.
- Transferir: Delegar parte del riesgo (ej. contratación de seguros o proveedores externos).
- Aceptar: Reconocer el riesgo y asumirlo, en caso de que su costo de control sea mayor al posible impacto.
- Evitar: Eliminar la actividad que genera el riesgo.

**Plan de Tratamiento aplicado a los activos críticos**

| Activo | Riesgo identificado | Nivel | Estrategia | Control propuesto | Responsable |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| Servidor académico | Ciberataque, fallas eléctricas | Crítico | Mitigar | Firewall, UPS, respaldos automáticos | Área TI |
| Base de datos de alumnos | Acceso no autorizado | Crítico | Mitigar | Políticas de acceso, cifrado, doble autenticación | Área TI y Coordinación Académica |
| Red de conectividad institucional | Saturación, corte de internet | Alto | Mitigar/Transferir | Redundancia de enlaces, monitoreo, soporte ISP | Área TI |
| Documentos físicos | Pérdida por incendio o manipulación indebida | Medio | Mitigar | Digitalización, archivadores ignífugos | Secretaría Académica |
| Personal administrativo clave | Error humano, suplantación | Alto | Mitigar/Aceptar | Capacitación, autenticación multifactor | Dirección y Coordinación Académica |

**Justificación del Plan**

El plan asegura que los activos con nivel crítico reciban prioridad en controles técnicos y administrativos, mientras que los activos de nivel alto y medio se gestionan con medidas proporcionales a su impacto. Así se optimizan recursos y se garantiza la protección integral de la información institucional.

## VI. Controles de Seguridad Implementados

**Introducción**

Los controles de seguridad son las medidas concretas aplicadas para reducir la probabilidad o el impacto de los riesgos identificados en el SGSI. Su implementación busca garantizar la confidencialidad, integridad y disponibilidad de la información institucional, evitando que los activos críticos queden expuestos a amenazas internas o externas.

En SENATI – Yurimaguas, los controles se organizaron en tres grandes categorías: técnicos, administrativos y físicos, siguiendo las directrices de la norma ISO/IEC 27002.

Esta clasificación permite abordar la seguridad desde un enfoque integral, combinando tecnología, gestión y protección del entorno físico.

**Controles Técnicos**

Los controles técnicos son aquellos basados en soluciones tecnológicas para proteger los sistemas y datos:

- Firewall perimetral y antivirus corporativo: instalados para filtrar accesos no autorizados y proteger los servidores de malware, phishing y ataques de red. Estos mecanismos actúan como la primera línea de defensa frente a amenazas externas.
- Copias de seguridad automáticas: programadas en los servidores y bases de datos críticos. Esto asegura que, en caso de pérdida de información o incidente, los datos puedan recuperarse sin afectar los procesos académicos y administrativos.
- Cifrado de datos sensibles: aplicado a bases de datos de matrícula y expedientes digitales, de modo que solo usuarios autorizados puedan acceder a la información.
- Políticas de acceso con doble autenticación (2FA): implementadas para el personal que maneja información crítica, reduciendo el riesgo de suplantación de credenciales.
- Monitoreo de red en tiempo real: que permite detectar patrones anómalos de tráfico, caídas de servicio o intentos de saturación de la red institucional.

Estos controles fortalecen la infraestructura tecnológica y aseguran que la información académica y administrativa esté protegida frente a ataques cibernéticos o fallos del sistema.

**Controles Administrativos**

Los controles administrativos se centran en la gestión de procesos y en el factor humano, considerado uno de los eslabones más vulnerables en la seguridad de la información:

- Política institucional de seguridad de la información: documento que fija lineamientos y responsabilidades claras para todo el personal.

- Capacitación en buenas prácticas de seguridad: talleres periódicos donde se instruye al personal sobre manejo de contraseñas, protección de datos, prevención de ingeniería social y correcta manipulación de documentos.
- Protocolos de respuesta a incidentes: procedimientos escritos que guían al personal sobre qué hacer ante intentos de intrusión, pérdida de información o interrupciones en los servicios digitales.
- Cláusulas de confidencialidad: incluidas en los contratos de trabajo y reglamentos internos, para asegurar el compromiso de los trabajadores en el resguardo de datos sensibles.
- Auditorías internas periódicas: revisiones semestrales que verifican el cumplimiento de la política, los planes de tratamiento y la efectividad de los controles implementados.

Estos controles aseguran que los procesos administrativos y el comportamiento del personal estén alineados con los principios del SGSI, reduciendo la incidencia de errores humanos y fortaleciendo la cultura de seguridad.

**Controles Físicos**

Los controles físicos protegen los espacios e infraestructuras donde se almacenan y gestionan los activos de información:

- Acceso restringido a salas de servidores: solo el personal del área de TI puede ingresar, mediante llaves o tarjetas de control.
- Archivadores ignífugos y con cerradura: donde se guardan expedientes académicos y documentos administrativos sensibles, reduciendo el riesgo de pérdida por incendios, robos o manipulación indebida.
- Sistemas de respaldo eléctrico (UPS): instalados en equipos críticos para garantizar la continuidad de los servicios frente a cortes de energía.
- Videovigilancia en áreas sensibles: cámaras instaladas en salas de servidores y oficinas administrativas para disuadir accesos indebidos.
- Política de uso de dispositivos externos: restricción del uso de memorias USB o discos duros externos en computadoras institucionales, con el fin de prevenir fugas de información o infecciones de malware.

Con estos controles se refuerza la seguridad física del entorno, minimizando vulnerabilidades que no dependen únicamente de la tecnología.

**Justificación**

La combinación de controles técnicos, administrativos y físicos garantiza un modelo de protección basado en el principio de defensa en profundidad, que implica establecer múltiples capas de seguridad para que, si una falla, las demás continúen protegiendo los activos críticos.

Gracias a la implementación de estos controles, SENATI – Yurimaguas ha fortalecido de manera tangible su capacidad de prevenir, detectar y responder ante incidentes de seguridad, consolidando una gestión integral de la información que sustenta los objetivos institucionales.

## VII. Seguimiento y Mejora Continua

**Introducción**

El seguimiento y la mejora continua constituyen la fase más estratégica del SGSI, ya que permiten verificar la eficacia real de las medidas implementadas y garantizar que el sistema se mantenga alineado con la evolución de los riesgos y con las necesidades institucionales. Sin un proceso permanente de control, el SGSI corre el riesgo de volverse obsoleto frente a nuevas amenazas tecnológicas, cambios en la organización o variaciones en el entorno académico-administrativo.

En el caso de SENATI – Yurimaguas, el seguimiento del SGSI busca no solo confirmar la validez de las políticas y controles, sino también generar un **ciclo de retroalimentación** que fortalezca la cultura de seguridad de la información en toda la comunidad educativa.

**Actividades de Seguimiento**

1. Monitoreo de incidentes: se lleva un registro detallado de eventos relacionados con la seguridad, tales como intentos de acceso no autorizado, fallas en la red, pérdida de documentos físicos o errores humanos. Este registro permite identificar patrones y anticipar riesgos emergentes.
2. Evaluación periódica de controles: cada trimestre se revisa la eficacia de los controles implementados (firewall, backups, cifrado, autenticación) para verificar que cumplen con los objetivos de mitigación planteados en el plan de tratamiento de riesgos.
3. Auditorías internas: se programan revisiones semestrales para comprobar el grado de cumplimiento de la política de seguridad, la correcta aplicación de los

procedimientos y la responsabilidad de cada área en la protección de los activos críticos.

4. Revisión documental: se actualizan inventarios de activos, matrices de riesgos y planes de tratamiento conforme se detectan cambios en la infraestructura tecnológica o en los procesos administrativos.
5. Retroalimentación del personal: se aplican encuestas y entrevistas breves al personal académico y administrativo para medir la percepción sobre la seguridad de la información y su compromiso con las políticas establecidas.

**Actividades de Mejora Continua**

1. Revisión anual del SGSI: cada año se actualizan formalmente la política de seguridad, el inventario de activos y la matriz de riesgos, asegurando que el sistema responda a los nuevos desafíos tecnológicos y organizacionales.
2. Acciones correctivas y preventivas: cuando se detectan incidentes o fallas en los controles, se implementan acciones inmediatas (ejemplo: reforzar capacitación, actualizar software de seguridad, cambiar protocolos de respaldo).
3. Capacitación constante: el personal participa en talleres y cursos de actualización sobre ciberseguridad, gestión documental y buenas prácticas de protección de datos, fortaleciendo la conciencia institucional en seguridad.
4. Integración de nuevas tecnologías: se promueve la adopción gradual de soluciones avanzadas como autenticación biométrica, monitoreo centralizado (SIEM) y protocolos de encriptación de última generación.
5. Comparación con estándares internacionales: se contrastan periódicamente los resultados del SGSI con los lineamientos de ISO/IEC 27001 y 27005, así como con las tendencias globales en gestión de seguridad de la información.

**Justificación**

La seguridad de la información no es un estado estático, sino un proceso dinámico que evoluciona al ritmo de los riesgos y de los avances tecnológicos. Por ello, el seguimiento y la mejora continua garantizan que el SGSI del SENATI – Yurimaguas no quede limitado a una implementación inicial, sino que se consolide como un sistema vivo, sostenible y adaptable. De este modo, se asegura la protección de los activos críticos en el largo plazo, se minimiza la probabilidad de incidentes graves y se fortalece la

confianza de estudiantes, docentes y personal administrativo en los procesos institucionales.