J-40402082-9

Fundación Aula Virtual

Aula Virtual

Generando Conocimiento

http://www.aulavirtual.web.ve

ISSN: 2665-0398

Deposito Legal: LA2020000026

Vol. 6 Nº 13 Año 2025

Periodicidad Continua

AulaVirtual
Generando Conocimiento

ISSN: 2665-0398

REVISTA CIENTÍFICA AULA VIRTUAL

Revista Científica Arbitrada de Fundación Aula Virtual

Email: revista@aulavirtual.web.ve
URL: http://aulavirtual.web.ve/revista

Generando Conocimiento

ISSN: 2665-0398
Depósito Legal: LA2020000026
País: Venezuela
Año de Inicio: 2020
Periodicidad: Continua
Sistema de Arbitraje: Revisión por pares. "Doble Ciego"
Licencia: **Creative Commons** CC BY NC ND
Volumen: 6
Número: 13
Año: 2025
Período: Continua-2025
Dirección Fiscal: Av. Libertador, Arca del Norte, Nro. 52D, Barquisimeto estado Lara, Venezuela, C.P. 3001

La Revista seriada Científica Arbitrada e Indexada **Aula Virtual**, es de acceso abierto y en formato electrónico; la misma está orientada a la divulgación de las producciones científicas creadas por investigadores en diversas áreas del conocimiento. Su cobertura temática abarca Tecnología, Ciencias de la Salud, Ciencias Administrativas, Ciencias Sociales, Ciencias Jurídicas y Políticas, Ciencias Exactas y otras áreas afines. Su publicación es **CONTINUA**, indexada y arbitrada por especialistas en el área, bajo la modalidad de doble ciego. Se reciben las producciones tipo: *Artículo Científico* en las diferentes modalidades cualitativas y cuantitativas, *Avances Investigativos*, *Ensayos, Reseñas Bibliográficas, Ponencias o publicaciones derivada de eventos*, y cualquier otro tipo de investigación orientada al tratamiento y profundización de la información de los campos de estudios de las diferentes ciencias. La Revista **Aula Virtual,** busca fomentar la divulgación del conocimiento científico y el pensamiento crítico reflexivo en el ámbito investigativo.

ISSN: 2665-0398

PLAN DE SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA MEJORAR LA ADMINISTRACIÓN DE RIESGO

INFORMATION SECURITY MANAGEMENT SYSTEM PLAN TO IMPROVE RISK MANAGEMENT

Tipo de Publicación: Artículo Científico
Recibido: 07/10/2025
Aceptado: 27/11/2025
Publicado: 28/12/2025
Código Único AV: e580
Páginas: 1(2367-2382)
DOI: https://doi.org/10.5281/zenodo.18076040

Autores:
Freddy Elar Ferrari Fernández
Ingeniero de Sistemas
Magister en Docencia Universitaria y Gestión Educativa
https://orcid.org/0000-0002-6878-648X
E-mail: freddy_ferrari@unu.edu.pe
Afiliación: Universidad Nacional de Ucayali
País: Republica del Perú

Jorge Luis Hilario Rivas
Ingeniero Industrial
Doctor en Ingeniería de Sistemas
https://orcid.org/0000-0003-1283-5630
E-mail: dr@jorgeluishilario.com
Afiliación: Universidad Nacional de Ucayali
País: República del Perú

Resumen

La investigación Plan de Sistema de Gestión de Seguridad de la Información (SGSI) para mejorar la Administración de Riesgo tuvo como objetivo demostrar si la aplicación de un plan de SGSI contribuye significativamente a optimizar la gestión de riesgos en organizaciones. Se desarrolló un estudio aplicado, de nivel descriptivo, con un diseño pre test – post test, aplicado a 49 estudiantes de Ingeniería de Sistemas de la Universidad Nacional de Ucayali, organizados en 12 equipos distribuidos en Entidades/Procesos. La recolección de datos se realizó mediante encuestas validadas estadísticamente, considerando las dimensiones de confidencialidad, integridad, disponibilidad, identificación y tasación de activos, así como el análisis de riesgos, de acuerdo con las normas NTP-ISO/IEC 17799 y NTP-ISO/IEC 27001:2014. Los resultados evidencian una mejora significativa en la administración de riesgos tras la implementación del plan, con un promedio de diferencia $\bar{D} = 1.4967$, confirmado mediante prueba t ($Tc = 13.576 > Tt = 1.761$; Sig. bilateral < 0.05) y un nivel de confianza del 95 %. En las dimensiones específicas se registraron mejoras en confidencialidad ($\bar{D} = 1.6100$), integridad ($\bar{D} = 1.2860$) y disponibilidad ($\bar{D} = 1.5940$). Asimismo, se identificaron 220 activos, de los cuales se gestionaron 204; en el análisis de riesgos se evaluaron 141 activos, 594 amenazas y 594 vulnerabilidades. Se concluye que la implementación de un plan de SGSI no solo produce mejoras estadísticamente significativas en la gestión de riesgos, sino que también fortalece la seguridad organizacional al proteger la confidencialidad, integridad y disponibilidad de la información. En consecuencia, constituye una estrategia esencial para garantizar la continuidad operativa, reducir vulnerabilidades y responder de manera efectiva a los desafíos de entornos digitales cada vez más complejos.

Palabras Clave Administración de riesgos, seguridad de la información, SGSI, ISO/IEC 27001

Abstract

The research Information Security Management System (ISMS) Plan to Improve Risk Management aimed to demonstrate whether the implementation of an ISMS plan significantly contributes to optimizing risk management in organizations. An applied, descriptive-level study was conducted using a pre-test–post-test design with 49 Systems Engineering students from the National University of Ucayali, organized into 12 teams distributed across Entities/Processes. Data collection was carried out through statistically validated surveys, assessing the dimensions of confidentiality, integrity, availability, asset identification and valuation, and risk analysis, in accordance with NTP-ISO/IEC 17799 and NTP-ISO/IEC 27001:2014 standards. The results show a significant improvement in risk management after the implementation of the plan, with an average difference of $\bar{D} = 1.4967$, confirmed by a t-test ($Tc = 13.576 > Tt = 1.761$; Sig. bilateral < 0.05) and a 95% confidence level. Specific improvements were recorded in confidentiality ($\bar{D} = 1.6100$), integrity ($\bar{D} = 1.2860$), and availability ($\bar{D} = 1.5940$). A total of 220 assets were identified, of which 204 were managed; in the risk analysis, 141 assets, 594 threats, and 594 vulnerabilities were evaluated. It is concluded that implementing an ISMS plan not only leads to statistically significant improvements in risk management but also strengthens organizational security by protecting the confidentiality, integrity, and availability of information. Consequently, it constitutes an essential strategy to ensure operational continuity, reduce vulnerabilities, and effectively respond to the challenges of increasingly complex digital environments.

Keywords Risk management, information security, ISMS, ISO/IEC 27001

ISSN: 2665-0398

Introducción

La gestión de la seguridad de la información se ha convertido en un desafío prioritario para las organizaciones, tanto públicas como privadas, debido al incremento de amenazas, vulnerabilidades y riesgos asociados al uso intensivo de las Tecnologías de la Información y la Comunicación (TIC). La protección de los activos informacionales resulta esencial para garantizar la confidencialidad, integridad y disponibilidad de los datos, pilares reconocidos en las normas internacionales de seguridad (International Organization for Standardization, 2015a); (Betancourt, 2016).

En el contexto actual, caracterizado por la acelerada obsolescencia del conocimiento y la transformación digital, las instituciones se ven obligadas a adoptar sistemas formales y estandarizados que fortalezcan sus capacidades de prevención y respuesta frente a incidentes de seguridad (Panaqué Domínguez, Lizárraga Caipo & Mendoza de los Santos, 2022).

La implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), en concordancia con la norma ISO/IEC 27001 (Norma Técnica Peruana (NTP), 2016), permite establecer un marco de mejora continua orientado a identificar, evaluar y mitigar riesgos de manera sistemática (Solano Quincho, Horna Maguiña & Mendoza de los Santos, 2023).

En el ámbito universitario, la integración de prácticas de auditoría y seguridad informática en la formación académica contribuye no solo a fortalecer las competencias profesionales, sino también a generar propuestas de mejora aplicables en entornos reales. Bajo esta perspectiva, la presente investigación plantea el diseño e implementación de un Plan de SGSI con el propósito de evaluar su impacto en la administración de riesgos de seguridad de la información en la Escuela Profesional de Ingeniería de Sistemas de la Universidad Nacional de Ucayali.

La contribución esencial de este estudio consiste en evidenciar, a través de resultados comprobados, la efectividad de un Plan de SGSI aplicado en 12 entidades y procesos organizacionales, demostrando su alcance e impacto más allá del entorno académico. Desde el punto de vista metodológico, al emplear un diseño cuasi experimental con evaluaciones antes y después de la intervención, se refuerza el enfoque de gestión de riesgos de seguridad de la información, en concordancia con los lineamientos establecidos por las normas NTP-ISO/IEC 17799 y NTP-ISO/IEC 27001:2014.

De igual manera, la investigación aporta una alternativa práctica y aplicable, susceptible de ser adoptada por organizaciones públicas o privadas para fortalecer la protección de sus activos

Revista Aula Virtual, ISSN: 2665-0398; Periodicidad: Continua
Volumen: 6, Número: 13, Año: 2025 (Continua-2025)

informacionales y consolidar una cultura institucional orientada a la seguridad digital.

Desarrollo

Fundamentos de la Seguridad de la Información

Para garantizar que la seguridad de la información es gestionada correctamente se debe identificar inicialmente su ciclo de vida y los aspectos relevantes adoptados para certificar la confidencialidad, integridad y disponibilidad.

> La confidencialidad garantiza que la información solo sea accesible o divulgada a personas, procesos o entidades debidamente autorizadas. La integridad implica asegurar la exactitud, consistencia y totalidad de los datos, así como la correcta operación de los mecanismos que los procesan. Por su parte, la disponibilidad asegura que los recursos informáticos y la información estén accesibles y utilizables por los usuarios autorizados en el momento que se requiera.
>
> Con base en el entendimiento del ciclo de vida de cada activo informacional, es esencial implementar un enfoque sistemático, formalizado y difundido en toda la organización para su gestión, priorizando la evaluación y tratamiento de los riesgos inherentes. Este conjunto estructurado de actividades y políticas constituye el Sistema de Gestión de Seguridad de la Información (SGSI), el cual permite proteger los activos de información dentro de un marco de mejora continua (Betancourt, 2016).

El estudio y administración de los riesgos fundamentado en procesos empresariales/servicios de Tecnologías de la Información es un instrumento eficaz para valorar y manejar una organización en relación a los peligros de los sistemas de datos. Así, los procesos comerciales/servicios de Tecnología de la Información (TI) se basan en los activos de las TIC que respaldan los procesos comerciales/servicios de TI.

Esto requiere un estudio y administración de los riesgos en los sistemas de información realista y dirigido a las metas de la organización. Una vez evaluado el riesgo y aplicados los controles apropiados de la Norma Técnica Peruana (NTP), (2016) norma ISO/IEC 27002:2014 o de otras normas, nos queda un riesgo residual que la gerencia de la empresa acepta.

Análisis y Gestión de Riesgos

El análisis de riesgos en seguridad de la información se entiende como el proceso sistemático de identificar amenazas, vulnerabilidades y el nivel de exposición de los activos organizacionales, a fin de estimar la probabilidad e impacto de incidentes (International Organization for Standardization, 2015a). Este análisis permite fundamentar decisiones sobre las medidas de protección más adecuadas, asegurando que la información crítica esté resguardada de manera proporcional a su valor y nivel de riesgo.

La gestión de riesgos, por su parte, implica la selección e implementación de controles técnicos, administrativos y organizativos orientados a prevenir, reducir o contener los riesgos detectados.

ISSN: 2665-0398

Su finalidad es mantener los niveles de riesgo dentro de parámetros aceptables definidos por la organización, garantizando la confidencialidad, integridad y disponibilidad de la información (Solano Quincho, Horna Maguiña & Mendoza de los Santos, 2023).

Ambos procesos conforman un ciclo continuo: primero, el análisis permite identificar y evaluar los riesgos; posteriormente, la gestión define e implementa las estrategias de tratamiento, que pueden incluir mitigación, transferencia, aceptación o eliminación del riesgo. Este enfoque, alineado a la (Norma Técnica Peruana (NTP), 2016) norma ISO/IEC 27001, asegura que la administración de riesgos de seguridad de la información no sea una acción aislada, sino parte de una estrategia integral de mejora continua (Panaqué Domínguez, Lizárraga Caipo & Mendoza de los Santos, 2022) (Ver Figura 1).

EVALUACION DEL NIVEL DE RIESGO (NR)

NR = I x P x R

Apetito y tolerancia al riesgo de seguridad de información

Resultado (NR = I x P x R)	Nivel de Riesgo	Opción de tratamiento
1, 2, 3, 4, 5, 6	Muy bajo	Apetito al Riesgo (Riesgos aceptados)
8, 9, 10, 12, 15, 16	Bajo	
18, 20, 24, 25, 27, 30	Medio	Tolerancia al Riesgo (tratados, por acuerdo del Comité de Seguridad de Información)
32, 36, 40, 45, 48, 50 60, 64, 75, 80, 100, 125	Alto Muy Alto	Tratamiento de Riesgos

Figura 1: Matriz de Análisis de Riesgo
Fuente. Elaboración propia

ISO 27001

La norma técnica peruana NTP-ISO/IEC 17799, al igual que el estándar internacional ISO/IEC 27001, establece directrices orientadas a garantizar la protección adecuada de los activos de información dentro de una organización. Para ello, todos los activos deben ser debidamente inventariados y contar con un responsable formalmente designado. Es imprescindible identificar a los encargados de cada activo crítico, quienes asumirán la responsabilidad de asegurar la implementación y mantenimiento de los controles de seguridad correspondientes.

Si bien las tareas operativas relacionadas con la aplicación de dichos controles pueden ser delegadas, la responsabilidad final sobre la seguridad del activo recae en su propietario designado, quien deberá velar por la integridad y eficacia de las medidas adoptadas (International Organization for Standardization, 2015a).

Inventario De Activos

De acuerdo con la norma ISO/IEC 27001, todos los activos de información deben ser claramente identificados, manteniendo un inventario actualizado que registre aquellos elementos que resulten críticos para la operación de la organización. Este inventario debe clasificar y documentar los activos en función de su relevancia para el negocio, incluyendo aspectos clave como tipo, formato, ubicación física o digital, copias de respaldo, licenciamiento y su valor estratégico.

La administración de este inventario debe evitar redundancias innecesarias; sin embargo, es fundamental asegurar

Revista Aula Virtual, ISSN: 2665-0398; Periodicidad: Continua
Volumen: 6, Número: 13, Año: 2025 (Continua-2025)

su coherencia con otros registros de activos existentes dentro de la organización. Este control contribuye directamente a los procesos de recuperación ante desastres y a la gestión integral de la seguridad de la información (International Organization for Standardization, 2015a).

Métodos

Diseño de la Investigación

La investigación fue de tipo aplicada, con un nivel descriptivo, empleando un diseño cuasi–experimental pre test – post test con un solo grupo. Este diseño permitió evaluar los cambios en la variable dependiente (administración de riesgos) antes y después de la implementación del Plan de SGSI, comparando los resultados obtenidos en ambas mediciones (Hernández & Mendoza, 2018).

Técnicas e Instrumentos

La técnica principal de recolección de datos fue la encuesta estructurada, diseñada con base en las dimensiones: confidencialidad, integridad, disponibilidad, identificación y tasación de activos, y análisis de riesgos. El cuestionario estuvo conformado por 15 ítems en escala Likert (1 a 5), elaborados a partir de criterios de la norma NTP-ISO/IEC 27001:2014.

Confiabilidad del Instrumento

La consistencia interna del cuestionario se verificó mediante el coeficiente alfa de Cronbach, alcanzando un valor superior a 0.80. Según Ruiz Bolívar, (2010), este rango corresponde a un nivel alto de confiabilidad, lo que indica homogeneidad en los ítems y estabilidad de las mediciones.

Procedimiento

1. Aplicación del pre test para medir la percepción inicial de la administración de riesgos.
2. Implementación del Plan de SGSI en cada equipo, incluyendo identificación de activos, análisis de amenazas y vulnerabilidades, y diseño de controles de seguridad.
3. Aplicación del post test, con el mismo cuestionario, para medir los cambios tras la implementación.
4. Análisis estadístico mediante la prueba t de muestras relacionadas, con un nivel de significancia de 0.05, para determinar diferencias significativas entre pre y post test.

Operacionalización de Variables

1. Variable I

Sistema de Gestión de Seguridad de la Información (SGSI).

a. Definición Conceptual

Un Sistema de Gestión de Seguridad de Información (SGSI) es un sistema gerencial general basado en un enfoque de riesgos para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información.

b. Definición Operacional

Dimensiones

ISSN: 2665-0398

- Confidencialidad
- Integridad
- Disponibilidad

2. Variable II

Administración de Riesgo.

a. Definición Conceptual

Es reconocer, medir y gestionar los riesgos vinculados a la seguridad de la información para cumplir con las metas empresariales a través de una serie de actividades que demandan el conocimiento del gerente de seguridad de la información acerca del método esencial de administración de riesgos.

b. Definición Operacional

Para efectuar la Operacionalización de esta variable se ha elaborado un cuestionario basado en las dimensiones:

- Identificación y Tasación de Activos
- Análisis de Riesgos.

Población y Muestra de la Investigación

1. Población

El experimento se ha desarrollado en la Carrera Profesional de Ingeniería de Sistemas de la Universidad Nacional de Ucayali, Semestre Académico 2022-II, y consideramos como población, a todos los alumnos matriculados Asignatura: Auditoria y Seguridad en Informática, X Ciclo, que en total son 49 alumnos que integran los 12 equipos distribuidos en "Entidades/Procesos".

2. Muestra

El tamaño de muestra utilizando es el Tipo No Probabilístico que según Hernández & Mendoza, (2018) "Subgrupo de la población en la que la elección de los elementos no depende de la probabilidad sino de las características de la investigación" bajo el diseño de muestreo intencional o de conveniencia El caso más frecuente de este procedimiento el utilizar como muestra los individuos a los que se tiene fácil acceso (los docentes de universidad emplean con mucha frecuencia a sus propios alumnos), donde se tomará a los 49 alumnos que integran los 12 equipos distribuidos en "Entidades/Procesos" de investigación de la Escuela Profesional de Ingeniería de Sistemas.

Técnicas e Instrumentos de la Recolección de Datos

1. Técnica

La técnica que se aplicará es:

- Encuesta

2. Instrumentos

La validez del instrumento se realizará mediante el análisis de Alfa de Cronbach.

> Dicho coeficiente determina la consistencia interna de una prueba, analizando la correlación media de una variable con todas las demás que la

Revista Aula Virtual, ISSN: 2665-0398; Periodicidad: Continua
Volumen: 6, Número: 13, Año: 2025 (Continua-2025)

integran. Por lo general, toma valores dentro del intervalo [0,1], donde un valor próximo al límite inferior indica una consistencia escasa, es decir, con una gran variabilidad de los temas tratados, y, por el contrario, un valor próximo a la unidad conllevaría a un alto de grado de consistencia. No obstante, pudiera tomar valores negativos, lo que indicaría que en el cuestionario hay preguntas que recogen temas opuestos al resto (Hernández & Mendoza, 2018).

Como criterio general, Ruiz Bolívar, (2010, p.39) sugiere las recomendaciones siguientes para evaluar los coeficientes de Alfa de Cronbach:

Escala	Descripción - Nivel
0.01 α 0.20	Muy Baja
0.21 α 0.40	Baja
0.41 α 0.60	Moderada
0.61 α 0,80	Alta
0.81 α 1	Muy Alta

Tabla 1. Escala de Alfa de Cronbach
Fuente: Construcción de Instrumentos de Medición en Ciencias Sociales

3. Elementos

Formulario de encuestas para alumnos

4. Fuentes

La fuente primaria, se obtiene de la información por contacto directo con el sujeto de estudio, documental, percepción de los implicados, alumnos y la técnica cuantitativa: tales como encuestas.

Resultados

El diagnóstico inicial permitió identificar 220 activos de información, de los cuales 204 fueron valorados y gestionados según la norma NTP-ISO/IEC 17799. En la fase de análisis de riesgos se evaluaron 141 activos críticos, identificándose 594 amenazas y un número equivalente de 594 vulnerabilidades. Estos hallazgos muestran la amplitud de factores de riesgo presentes en los procesos evaluados, evidenciando la necesidad de contar con un SGSI que sistematice la identificación, clasificación y priorización de riesgos.

Los resultados del diseño pre test – post test confirmaron que la implementación del Plan de SGSI produjo mejoras significativas en la administración de riesgos, con un promedio de diferencia $\bar{D} = 1.4967$, validado mediante prueba t ($Tc = 13.576 > Tt = 1.761$; $p < 0.05$) y un nivel de confianza del 95%. Estas mejoras se distribuyeron en las dimensiones de confidencialidad ($\bar{D} = 1.6100$), integridad ($\bar{D} = 1.2860$) y disponibilidad ($\bar{D} = 1.5940$), lo que refleja un impacto positivo tanto en la protección de los datos como en la continuidad de los procesos organizacionales.

El análisis estadístico no solo confirma la efectividad del plan, sino que también revela la existencia de áreas críticas que requieren atención prioritaria. La alta cantidad de amenazas y vulnerabilidades identificadas indica que las

ISSN: 2665-0398

organizaciones evaluadas se encuentran en escenarios de riesgo considerable, donde la ausencia de controles sistemáticos podría comprometer la operación. En este sentido, los resultados coinciden con estudios previos que destacan la utilidad del SGSI como marco para reducir la exposición y garantizar la seguridad de la información (Merino, 2021; Gómez Ángeles, 2024) (Ver Figura 2).

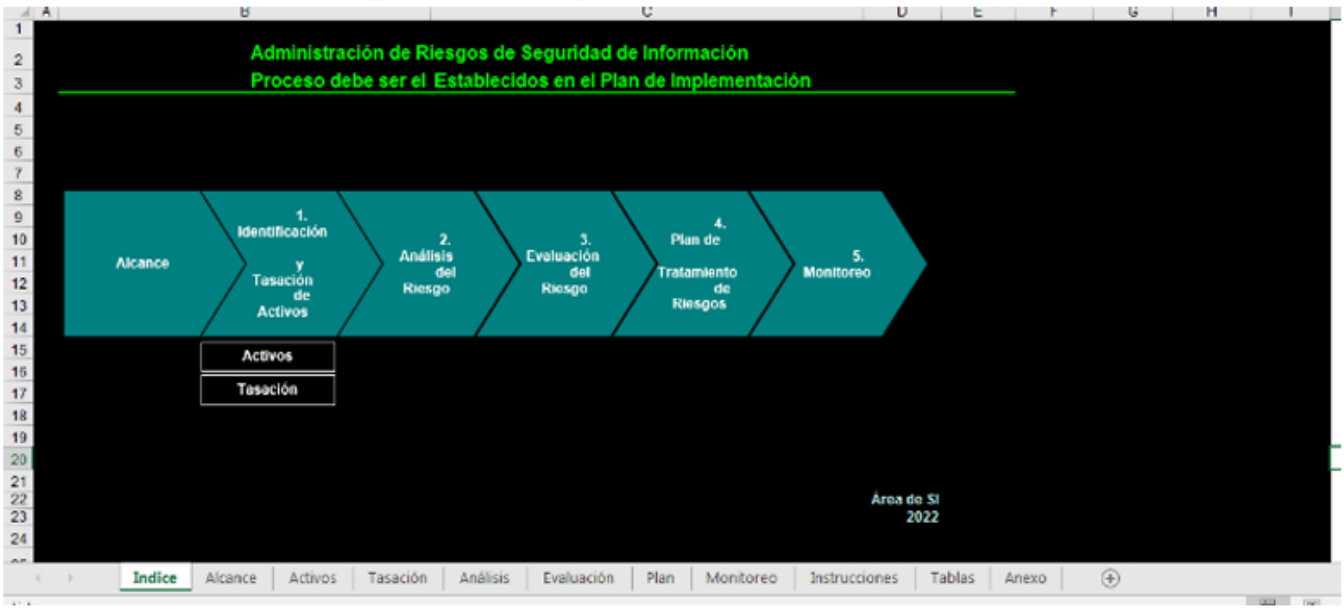

Figura 2. Seguridad de la Información
Fuente. Elaboración propia

Revista Aula Virtual, ISSN: 2665-0398; Periodicidad: Continua
Volumen: 6, Número: 13, Año: 2025 (Continua-2025)

						Numero de Análisis de Riesgos		
EQUIPO	**ENTIDAD/PROCESO**	**COMPRENDE**	**Número de Identificación Activos**	**Numero de Tasación de Activos**	**Numero de Activos Analizados**	**Numero de Amenazas**	**Numero de Vulnerabilidad**	**FUENTE DE INFORMACION**
1	PROCESO DE ALMACENAMIENTO EN LA EMPRESA OTIFARMA S.A.C	Comprende: 1. Recepción de productos 2. Control de vencimiento de productos 3. Gestión de inventario de productos	11	11	5	21	21	Administración de Riesgos de Seguridad de Información Proceso de GESTION DE ALMACEN EN LA EMPRESA OTIFARMA S.A.C
2	SISTEMA COMERCIAL DE "GRUPO YUCRA"	Comprende: 1. Realizar pedidos 2. Entrada y salida de productos 3. Realizar informes	14	8	8	32	32	Administración de Riesgos de Seguridad de Información Proceso debe ser el Establecidos en el Plan de Implementación
3	ÁREA DE LOGÍSTICA DE LA EMPRESA "CREDIVARGAS"	Comprende: 1. Compra 2. Transferencia 3. Transacción	11	11	9	35	35	Administración de Riesgos de Seguridad de Información Gestión Logística de la Empresa CrediVargas
4	EMPRESA DE FACTURACIÓN ELECTRÓNICA LORITO SOFT	Comprende: 1. Gestión de Comprobante de pago 2. Gestión de Ventas 3. Gestión de T. I	15	5	5	21	21	Administración de Riesgos de Seguridad de Información Proceso debe ser el SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN LA EMPRESA DE FACTURACIÓN ELECTRÓNICA LORITO SOFT
5	PARA LA COMUNICACIÓN SERVIDOR – COMPUTADORA EN EL ÁREA DE SERVIDORES EN LA MUNICIPALIDAD PROVINCIAL DE CORONEL PORTILLO	Comprende: 1. Validación de equipo 2. Conexión al servidor para extracción de datos (software)	19	19	9	51	51	Administración de Riesgos de Seguridad de Información Proceso debe ser la COMUNICACIÓN SERVIDOR – COMPUTADORA EN EL ÁREA DE SERVIDORES EN LA MUNICIPALIDAD PROVINCIAL DE CORONEL PORTILLO
6	EMPRESA MOLINO EL IMPERIO SAC	Comprende: 1. Proceso de gestión de salida de producto 2. Proceso de gestión de entrada de producto 3. Proceso de control de empleados 4. Proceso de Gestión de Pilado	25	25	21	131	131	Administración de Riesgos de Seguridad de Información Proceso debe ser el SISTEMA DE LA EMPRESA MOLINO EL IMPERIO SAC

ISSN: 2665-0398

7	"Vista Cinema" de Cineplanet Pucallpa	Comprende: 1. Entrada y salida de productos e inventario 2. Generar reportes diarios por ventas	9	9	8	32	32	Administración de Riesgos de Seguridad de Información Proceso de "VISTA CINEMA" de CINEPLANET - PUCALLPA
8	RESERVAS DEL HOSPEDAJE AEROPUERTO	Comprende: 1. Proceso de reserva de habitación 2. Proceso de facturación de caja	7	7	7	27	27	Administración de Riesgos de Seguridad de Información Proceso debe ser el SISTEMA DE RESERVAS DEL HOSPEDAJE AEROPUERTO
9	DEL AREA DE SOPORTE TECNICO - UNU	Comprende: 1. Mantenimiento y reparación de los equipos 2. Instalación y configuración de software 3. Atender Asistencias Técnicas	17	17	13	52	52	Administración de Riesgos de Seguridad de Información Proceso debe ser el Establecidos en el Plan de Implementación
10	INNOVACIÓN TECNOLOGICA DE LA EMPRESA LEX & IUS.	Comprende: 1. Recopilación de datos e información 2. Procesamiento de datos 3. Presentación de información 4. Gestión de la información y su seguridad 5. Almacenamiento y uso eficiente de la información 6. Monitoreo y control del rendimiento (Toma de decisiones)	56	56	23	92	92	Administración de Riesgos de Seguridad de Información Proceso de la GERENCIA DE INNOVACIÓN TECNOLOGICA DE LA EMPRESA LEX & IUS
11	PROCESO DE SISTEMAS WEB PARA LA EMPRESA CAOTEC E.I.R.L	Comprende: 1. Asesoramiento en T.I 2. Desarrollo de software	27	27	24	64	64	Administración de Riesgos de Seguridad de Información Proceso debe ser el Establecidos en el Plan de Implementación
12	ÁREA DE PRESUPUESTO Y ADMINISTRACIÓN EN LA EMPRESA INMOBILIARIA JOSUE E.I.R.L	Comprende: 1. proceso de licitaciones 2. administración del bien	9	9	9	36	36	Administración de Riesgos de Seguridad de Información Proceso debe ser EMPRESA INMOBILIARIA JOSUE E.I.R.L.
		TOTAL	**220**	**204**	**141**	**594**	**594**	

Tabla 2. Resumen de Administración de Riesgos del SGSI
Fuente: Elaboración Propia

Revista Aula Virtual, ISSN: 2665-0398; Periodicidad: Continua
Volumen: 6, Número: 13, Año: 2025 (Continua-2025)

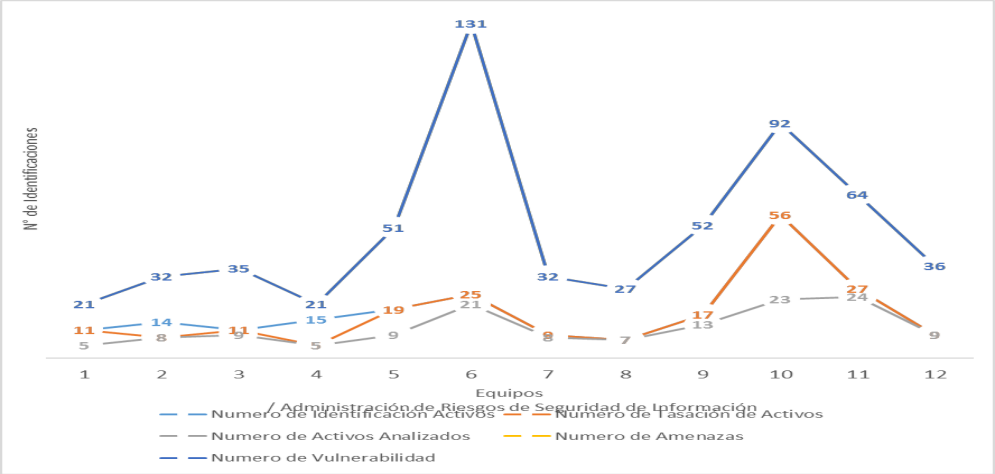

Figura 3. Resumen de Administración de Riesgos del SGSI
Fuente: Elaboración Propia

Hipótesis General

Planteo De Hipótesis

Ho: Un Plan de Sistema de Gestión de Seguridad de la Información no mejora de manera significativa la Administración de Riesgo.

Ha: Un Plan de Sistema de Gestión de Seguridad de la Información mejora de manera significativa la Administración de Riesgo.

Regla de Decisión Estadística

Si el Valor Sig. ≥ 0.05, se acepta Ho. Si el valor Sig. < 0.05, se acepta Ha.

Determinación Del Valor Crítico (Tt)

Para el cálculo del valor critico se ha empleado la tabla de distribución normal

$Tt\ (1-\alpha)\ (n-1)$

$Tt\ (1-0.05)\ (15-1)$

$Tt\ (0.95)\ (14) = 1.761$

Cálculo de la Función Prueba (Tc)

Se ha utilizado el programa estadístico para calcular la función de prueba, SPPS, insertando los valores promedios de los resultados del cuestionario aplicado (Ver Tabla 3).

ISSN: 2665-0398

	PRE TEST	POS TEST	$\bar{D}$
PREG1	2.8000	4.3700	1.570
PREG2	2.7100	4.0600	1.350
PREG3	2.7100	4.2200	1.510
PREG4	2.2000	4.1000	1.900
PREG5	2.6900	4.4100	1.720
PREG6	3.5700	4.4700	0.900
PREG7	2.6900	4.1600	1.470
PREG8	2.1600	3.0800	0.920
PREG9	2.4500	4.0800	1.630
PREG10	2.6100	4.1200	1.510
PREG11	2.6500	4.3900	1.740
PREG12	2.7100	3.2200	0.510
PREG13	2.6900	4.4100	1.720
PREG14	2.2000	4.2900	2.090
PREG15	2.2700	4.1800	1.910
PROMEDIO	2.6073	4.1040	1.4967

Tabla 3. Análisis Pre y Pos Test
Fuente: Elaboración Propia

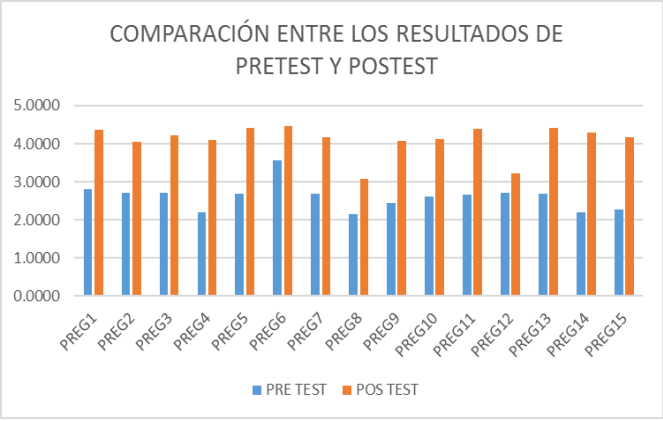

Figura 4. Secciones del ISO 27001
Fuente: Elaboración Propia

A continuación, se presenta la fórmula para el estadístico de prueba:

$$Tc = \frac{\bar{d}}{S_d/\sqrt{n}} = 13.576$$

Prueba de muestras relacionadas									
		Diferencias relacionadas					t	gl	Sig. (bilateral)
		Media	Desviación típ.	Error típ. de la media	95% Intervalo de confianza para la diferencia				
					Inferior	Superior			
Par 1	POTEST - PRETEST	1,49667	,42698	,11025	1,26021	1,73312	**13,576**	14	,000

Tabla 4. Prueba de muestras seleccionadas
Fuente: Elaboración Propia

Toma de Decisiones

Como Tc=13.576 es mayor Tt=1.7610, se rechaza la Ho y se acepta la Ha. Luego de ejecutar el diseño de investigación y aplicar cálculos estadísticos, se determina que un Plan de Sistema de Gestión de Seguridad de la Información mejora de manera significativa la Administración de Riesgo, con un nivel de confianza del 95%.

Discusión

Los resultados obtenidos confirman que la implementación de un Plan de SGSI produce mejoras significativas en la administración de riesgos, con evidencias estadísticas que respaldan avances en confidencialidad, integridad y disponibilidad de la información. Este hallazgo concuerda con lo reportado por Merino (2021), quien mostró beneficios similares al aplicar la norma ISO/IEC 27001 en una empresa comercial, y con Gómez Ángeles (2024), quien evidenció

Revista Aula Virtual, ISSN: 2665-0398; Periodicidad: Continua
Volumen: 6, Número: 13, Año: 2025 (Continua-2025)

mejoras sustanciales en una municipalidad limeña. Sin embargo, a diferencia de estos estudios centrados en organizaciones consolidadas, el presente trabajo se aplicó en un contexto académico, lo que amplía la comprensión del SGSI como herramienta tanto de formación como de gestión.

El análisis de riesgos permitió identificar 594 amenazas y 594 vulnerabilidades en el total de procesos evaluados, lo que refleja un panorama de riesgo considerable. Este resultado coincide con lo señalado por Solano Quincho, Horna Maguiña & Mendoza de los Santos (2023), quienes destacan la necesidad de integrar la seguridad informática en la estrategia global de gestión de servicios. Sin embargo, el hecho de que este volumen de riesgos se detecte incluso en procesos académicos y administrativos universitarios problematiza la idea de que las instituciones educativas enfrentan una exposición menor frente al sector privado o gubernamental.

El aporte innovador de este estudio radica en la aplicación práctica del SGSI en un entorno académico real, sustentada con un diseño cuasi–experimental que demuestra de manera cuantitativa su efectividad. Esto no solo fortalece la formación profesional de los estudiantes, sino que también ofrece un modelo replicable en organizaciones que carecen de políticas estructuradas de seguridad.

En conclusión, los hallazgos confirman que el SGSI constituye un marco estratégico adaptable a distintos contextos, capaz de reducir vulnerabilidades, priorizar riesgos y garantizar la continuidad de los procesos en entornos organizacionales diversos.

Conclusiones

1. Los resultados del diseño pre test – post test confirmaron que la implementación del Plan de SGSI mejora de manera estadísticamente significativa la administración de riesgos ($\bar{D}$ = 1.4967; Tc = 13.576 > Tt = 1.761; p < 0.05), con un nivel de confianza del 95%. Este hallazgo demuestra avances en las dimensiones de confidencialidad ($\bar{D}$ = 1.6100), integridad ($\bar{D}$ = 1.2860) y disponibilidad ($\bar{D}$ = 1.5940).
2. La identificación de 220 activos, de los cuales 204 fueron gestionados, evidencia que el Plan de SGSI facilita la clasificación y control de activos informacionales críticos. Este resultado confirma el segundo objetivo, mostrando que el SGSI es una herramienta estratégica para proteger los recursos más sensibles de la organización y garantizar la continuidad de los procesos.
3. De acuerdo con el resumen de administración de riesgos del SGSI, se gestionaron 141 activos, identificándose 594 amenazas y 594 vulnerabilidades en el total de procesos

ISSN: 2665-0398

evaluados, conforme a la norma NTP ISO/IEC 27001:2014. Este hallazgo evidencia la magnitud de los riesgos presentes y confirma que el SGSI constituye un marco eficaz para su identificación, priorización y tratamiento, contribuyendo a reducir la exposición de la organización y fortaleciendo la seguridad de la información.

Referencias

Betancourt, A. (2016). Diseño de un prototipo de software para aplicar análisis GAP a los controles descritos en el Anexo A de la norma ISO 27001:2013 [Tesis de pregrado, Universidad Tecnológica de Pereira]. Repositorio UTP. Documento en línea. Disponible https://repositorio.utp.edu.co/server/api/core/bitstreams/a15d27ff-d674-4e89-a22a-42d61c2403e6/content

Gómez Ángeles, M. P. (2024). Implementación de un SGSI bajo la ISO/27001 para mejorar la seguridad informática en una municipalidad de Lima [Tesis de licenciatura, Universidad Tecnológica del Perú]. Repositorio UTP. Documento en línea. Disponible https://hdl.handle.net/20.500.12867/12467

Hernández Sampieri, R., & Mendoza Torres, C. (2018). Metodología de la investigación: Las rutas cuantitativa, cualitativa y mixta (5.ª ed.). McGraw-Hill Interamericana.

International Organization for Standardization. (2015a). ISO/IEC 27001:2013 – Information technology – Security techniques – Information security management systems – Requirements. ISO.

Merino, C. (2021). Implementación de un plan de seguridad informática con la norma ISO/IEC 27001 en la empresa Ransa Comercial S.A. – Piura [Tesis de licenciatura, Universidad Católica Los Ángeles de Chimbote]. Repositorio ULADECH. Documento en línea. Disponible https://repositorio.uladech.edu.pe/handle/20.500.13032/24698

Norma Técnica Peruana (NTP). (2016). NTP-ISO/IEC 27001:2014 – Tecnología de la información – Técnicas de seguridad – Sistemas de gestión de seguridad de la información – Requisitos. Instituto Nacional de Calidad (INACAL).

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

Ruiz Bolívar, C. (2010). Construcción de instrumentos de medición en ciencias sociales. Universidad Pedagógica Experimental Libertador.

Solano Quincho, L. M., Horna Maguiña, M. M., & Mendoza De los Santos, A. C. (2023). Garantía de seguridad de la información empresarial a través de la gestión de servicios. Innovación y Software, 4(2), 96–106. Documento en línea. Disponible https://doi.org/10.48168/innosoft.s12.a95