ECT | Revista Cientifica Emprendimiento Científico Tecnologico

ISSN: 2810 – 8493
https://revista.ectperu.org.pe/index.php/ect/index

Título Largo: Efecto de la Formación en Seguridad de la Información sobre el Análisis y Evaluación del Riesgo según Normas NTP-ISO/IEC en Contextos Reales

Titulo Corto: Seguridad de la Información para entender Administración de Riesgo

Long Title: Effect of Information Security Training on Risk Analysis and Evaluation According to NTP-ISO/IEC Standards in Real-World Contexts

Short Title: Information Security to Understand Risk Management

Freddy Elar Ferrari-Fernández [1]*, https://orcid.org/0000-0002-6878-648X

[1] Universidad Nacional de Ucayali.

*Autor para la correspondencia. (email) freddy_ferrari@unu.edu.pe

Recibido: 13 Dic 2025 Aceptado: 15 Dic 2025 Publicado:17 Dic 2025

RESUMEN

La Seguridad de la Información constituye un componente esencial para gestionar adecuadamente los riesgos asociados a los activos informacionales. Sin embargo, persisten limitaciones en la comprensión de los procesos de análisis y evaluación del riesgo, especialmente en entornos formativos. El objetivo del estudio fue determinar el efecto de una intervención en Seguridad de la Información sobre la comprensión de la Administración de Riesgos en estudiantes de Ingeniería de Sistemas. Se empleó un diseño preexperimental pretest/postest con una muestra de 21 estudiantes organizados en seis equipos que desarrollaron procesos reales de gestión de riesgos en entidades públicas y privadas. Se aplicó una encuesta validada y se evaluó la diferencia mediante t de Student para muestras relacionadas. Los resultados evidenciaron mejoras significativas en la comprensión de la Administración de Riesgos ($\bar{D} = 2.31520$; $p < 0.001$). Asimismo, las prácticas realizadas permitieron la identificación de 70 activos, la tasación de activos según NTP-ISO/IEC 17799 y el análisis de amenazas y vulnerabilidades conforme a NTP-ISO/IEC 27001:2014. Se concluye que la formación en Seguridad de la Información fortalece significativamente las competencias relacionadas con el análisis y evaluación del riesgo en escenarios organizacionales reales.

Palabras clave: Seguridad de la Información; Administración de Riesgos; Análisis de Riesgos; Evaluación del Riesgo; Formación Profesional; SGSI.

ISSN: 2810 – 8493
https://revista.ectperu.org.pe/index.php/ect/index

ABSTRACT

Information Security is essential for the effective management of risks associated with organizational information assets. However, limitations persist in understanding risk analysis and risk evaluation processes, particularly in educational environments. The objective of this study was to determine the effect of an Information Security training intervention on students' understanding of Risk Management. A pre-experimental pretest–posttest design was applied to a sample of 21 students organized into six teams, who conducted real risk management processes in public and private organizations. A validated survey was applied, and differences were analyzed using the paired-samples t-test. Results showed significant improvements in the understanding of Risk Management ($\bar{D} = 2.31520$; $p < 0.001$). Additionally, the practical activities enabled the identification of 70 assets, the valuation of assets based on NTP-ISO/IEC 17799, and the analysis of threats and vulnerabilities according to NTP-ISO/IEC 27001:2014. It is concluded that Information Security training significantly strengthens competencies related to risk analysis and evaluation in real organizational environments.

Keywords: Information Security; Risk Management; Risk Analysis; Risk Evaluation; Professional Training; ISMS.

INTRODUCCIÓN

La Seguridad de la Información se ha convertido en un componente esencial para garantizar la continuidad y confiabilidad de los procesos en cualquier organización. Proteger los activos informacionales implica comprender y aplicar adecuadamente los principios de Confidencialidad, Integridad y Disponibilidad (CID), así como las directrices establecidas en normas como la NTP-ISO/IEC 17799 y la NTP-ISO/IEC 27001:2014. No obstante, estudios recientes muestran que aún persisten dificultades en la identificación de activos, la valoración de amenazas y la detección de vulnerabilidades, lo que limita la efectividad de los Sistemas de Gestión de Seguridad de la Información (Guevara-Vega et al., 2023; Santos-Olmo et al., 2023).

En los entornos universitarios, esta problemática adquiere una dimensión adicional. Con frecuencia, la formación en Seguridad de la Información enfatiza la teoría, pero ofrece pocas oportunidades para aplicar los marcos normativos en contextos reales. La evidencia

ISSN: 2810 – 8493
https://revista.ectperu.org.pe/index.php/ect/index

científica señala que el aprendizaje significativo en gestión de riesgos requiere experiencias prácticas que permitan al estudiante comprender cómo interactúan los activos, las amenazas y las vulnerabilidades dentro de un proceso organizado (Fajri & Harwahyu, 2024; Hidayatullah et al., 2024). La ausencia de este componente aplicado genera brechas en las competencias profesionales, especialmente en futuros ingenieros responsables de auditar, evaluar y proteger sistemas de información.

En este contexto, el presente estudio tuvo como propósito analizar el efecto de una intervención formativa en Seguridad de la Información sobre la comprensión del proceso de Administración de Riesgos en estudiantes del X Ciclo de Ingeniería de Sistemas de la Universidad Nacional de Ucayali. Para ello, se desarrollaron actividades prácticas en seis entidades reales, tanto privadas como estatales, donde los participantes llevaron a cabo la identificación y tasación de activos, así como la evaluación de amenazas y vulnerabilidades siguiendo lineamientos estandarizados. Esta experiencia permitió contrastar el aprendizaje conceptual con situaciones operativas reales, fortaleciendo la capacidad analítica de los estudiantes.

A partir de esta necesidad formativa, se planteó la pregunta general: ¿En qué medida la formación en Seguridad de la Información influye en la comprensión del proceso de Administración de Riesgos? De ella derivan dos interrogantes específicas: ¿Cómo influye en la comprensión del análisis de riesgos? y ¿Cómo influye en la comprensión de la evaluación del riesgo? En coherencia con ello, el objetivo general fue determinar el efecto de la formación en Seguridad de la Información sobre la comprensión de la Administración de Riesgos, acompañado de objetivos específicos centrados en el análisis y la evaluación del riesgo.

Este estudio integra teoría, práctica y análisis cuantitativo, ofreciendo una mirada formativa que promueve el desarrollo de competencias aplicadas en Seguridad de la Información y responde a la necesidad de vincular el aprendizaje académico con escenarios organizacionales reales.

ISSN: 2810 – 8493
https://revista.ectperu.org.pe/index.php/ect/index

MATERIALES Y MÉTODOS

Tipo y Nivel de investigación

Tipo de investigación

El estudio es de tipo aplicado, pues busca mejorar la comprensión y la capacidad de los estudiantes para utilizar la Seguridad de la Información en el proceso de Administración de Riesgos, resolviendo una necesidad práctica formativa.

Nivel de investigación

El nivel del estudio corresponde a:

- Descriptivo: permitió caracterizar las variables Seguridad de la Información y Administración de Riesgos.
- Experimental (pre–experimental): dado que se aplicó una intervención formativa (X) y se midieron sus efectos en un solo grupo, de acuerdo con Hernández, Fernández y Baptista (2010).

Diseño del estudio

Se empleó un diseño pre–experimental tipo Pretest–Postest con un solo grupo, representado mediante:

$$GE: O_1 \rightarrow X \rightarrow O_2$$

- GE: Grupo Experimental
- O_1: Medición inicial mediante Pretest
- X: Intervención formativa en Seguridad de la Información y aplicación del proceso de Administración de Riesgos
- O_2: Medición final mediante Postest

El diseño permitió evaluar el impacto directo de la intervención educativa en la comprensión de los estudiantes.

Participantes y muestra

La población estuvo conformada por 21 estudiantes matriculados en la asignatura Auditoría y Seguridad Informática, X Ciclo, semestre 2024-II, de la Universidad Nacional de Ucayali.

ISSN: 2810 – 8493
https://revista.ectperu.org.pe/index.php/ect/index

La muestra fue seleccionada bajo un muestreo no probabilístico por conveniencia, integrando a todos los estudiantes del curso, lo cual es adecuado en estudios educativos basados en grupos accesibles.

Participantes y organización del trabajo

Los 21 estudiantes fueron organizados en seis equipos, cada uno asignado a una entidad real del sector privado o estatal. En dichos escenarios, cada equipo ejecutó un proceso completo de Administración de Riesgos de Seguridad de la Información, aplicando las normas NTP-ISO/IEC 17799 y NTP-ISO/IEC 27001:2014.

Los equipos desarrollaron las siguientes actividades:

- Identificación del proceso y sus subprocesos
- Levantamiento del inventario de activos de información
- Clasificación y tasación de activos bajo la triada CID
- Selección de activos críticos
- Identificación de amenazas
- Identificación de vulnerabilidades
- Registro del análisis de riesgos mediante matrices estandarizadas
- Documentación del proceso en informes técnicos

Este esquema garantizó la integración entre teoría y práctica en un entorno organizacional real.

Variables del estudio

Variable Independiente: Seguridad de la Información

- Definición conceptual: Conjunto de mecanismos que garantizan la Confidencialidad, Integridad y Disponibilidad de la información.
- Dimensiones:
    - Confidencialidad
    - Integridad
    - Disponibilidad

Variable Dependiente: Administración de Riesgos

- Definición conceptual: Proceso orientado a identificar, analizar y valorar los riesgos que afectan a los activos de información.
- Dimensiones:

ISSN: 2810 – 8493
https://revista.ectperu.org.pe/index.php/ect/index

- Identificación y tasación de activos
- Análisis de riesgos

Técnicas e instrumentos de recolección de datos

Técnicas

1. Encuesta

Aplicada en dos momentos (Pretest y Postest) para evaluar la comprensión de los estudiantes sobre Seguridad de la Información y su relación con la Administración de Riesgos.

2. Observación documentada y análisis estructurado

Empleada durante el trabajo de campo en las seis entidades reales. Permitió registrar información operativa sobre:

- Procesos y subprocesos
- Activos de información
- Tasación CID
- Amenazas y vulnerabilidades
- Controles existentes
- Flujos documentales

Cada equipo siguió un protocolo uniforme de recolección para asegurar coherencia y comparabilidad.

Instrumentos

1. Cuestionario tipo Likert (13 ítems)

Aplicado en Pretest y Postest, estructurado según las dimensiones:

- Confidencialidad
- Integridad
- Disponibilidad

Escala de 5 puntos (Siempre = 5, Nunca = 1).

La confiabilidad se evaluó mediante Alfa de Cronbach.

2. Matrices de recolección de información en campo

Utilizadas por los seis equipos para sistematizar la información de las entidades:

- Matriz de identificación de procesos y subprocesos

ISSN: 2810 – 8493
https://revista.ectperu.org.pe/index.php/ect/index

- Matriz de inventario de activos de información
- Matriz de tasación CID (Confidencialidad, Integridad, Disponibilidad)
- Matriz de análisis de riesgos (activos críticos, amenazas, vulnerabilidades y controles)

Estas matrices estandarizadas garantizaron la calidad y uniformidad metodológica de la data recolectada.

Fuentes

- **Fuentes primarias:**
  - Respuestas en la encuesta (Pretest–Postest)
  - Información obtenida directamente en las seis entidades reales durante la aplicación del proceso de Administración de Riesgos
- **Fuentes secundarias:**
  - Documentación institucional proporcionada por las entidades
  - Normas: NTP-ISO/IEC 17799 y NTP-ISO/IEC 27001:2014
  - Materiales académicos del curso

Procedimiento

1. Aplicación del Pretest (O_1)
2. Desarrollo de la intervención formativa (X)
3. Trabajo de campo en seis entidades reales
4. Aplicación del Postest (O_2)
5. Sistematización mediante matrices uniformes
6. Preparación de datos para análisis estadístico y triangulación

Análisis de datos

El análisis se realizó en dos niveles complementarios:

1. Análisis estadístico

Procesado en SPSS para:

- Evaluar confiabilidad (Alfa de Cronbach)
- Verificar normalidad (Shapiro–Wilk)
- Aplicar la prueba *t* de Student para muestras relacionadas
- Obtener estadísticos descriptivos

2. Análisis del trabajo de campo

ISSN: 2810 – 8493
https://revista.ectperu.org.pe/index.php/ect/index

La información técnica obtenida en las seis entidades se sistematizó mediante:

- Matrices de activos
- Matrices de amenazas
- Matrices de vulnerabilidades
- Registros de procesos y subprocesos

RESULTADOS

Los resultados obtenidos reflejan el impacto real y medible que tuvo la formación en Seguridad de la Información sobre los estudiantes. La comparación entre el Pretest y el Postest evidencia un cambio sustancial en la comprensión de los principios fundamentales de confidencialidad, integridad y disponibilidad, así como en su capacidad para relacionarlos con la Administración de Riesgos.

Este avance no solo se aprecia en los valores estadísticos, sino también en la experiencia práctica desarrollada por los participantes, quienes trabajaron en entidades reales tanto privadas como estatales aplicando el proceso de Administración de Riesgos para obtener información auténtica sobre: Entidad/Proceso, sub procesos, número de identificación activos, número de tasación de activos, número de activos analizados, número de amenazas, número de vulnerabilidad. Esta articulación entre teoría y práctica brindó un escenario formativo sólido, permitiendo que los estudiantes confrontaran situaciones reales y consolidaran su juicio crítico frente a problemas de seguridad.

Fiabilidad del instrumento

El cuestionario utilizado evidenció estabilidad y consistencia interna:

- Alfa de Cronbach Pretest: 0.780
- Alfa de Cronbach Postest: 0.783

Estos valores confirman que el instrumento fue adecuado para medir la variable relacionada con Seguridad de la Información.

Prueba de normalidad

La prueba de Shapiro–Wilk aplicada a las diferencias de medias mostró:

- **p = 0.512 (> 0.05)**

Lo cual indica que los datos cumplen el supuesto de normalidad y permiten el uso de pruebas paramétricas.

ISSN: 2810 – 8493
https://revista.ectperu.org.pe/index.php/ect/index

Comparación de resultados Pretest y Postest

Los 13 ítems evaluados presentan incrementos entre **2.05 y 2.76 puntos**, lo que demuestra una mejora amplia y consistente.

Los promedios generales fueron:

- Media Pretest: 2.0177
- Media Postest: 4.3338
- Incremento global: 2.3162

Este crecimiento refleja un fortalecimiento notable en la comprensión de conceptos vinculados a confidencialidad, integridad y disponibilidad.

Prueba de hipótesis general

La prueba *t* para muestras relacionadas arrojó:

- **Diferencia media:** 2.3162
- **t calculada:** 18.382
- **gl:** 20
- **p < 0.001**
- **IC 95%:** 2.05231 – 2.57773

Estos resultados demuestran que la intervención en Seguridad de la Información produjo un cambio estadísticamente significativo en la comprensión del proceso de Administración de Riesgos.

Resultados por dimensiones (Hipótesis específicas)

Confidencialidad (Ítems 1–4)

- **Media Pre:** 2.00
- **Media Post:** 4.19
- **Incremento:** 2.20

Se observa un fortalecimiento claro en la percepción de controles y prácticas orientadas a evitar accesos o divulgaciones no autorizadas.

Integridad (Ítems 5–8)

- **Media Pre:** 1.978
- **Media Post:** 4.415
- **Incremento:** 2.437

ISSN: 2810 – 8493
https://revista.ectperu.org.pe/index.php/ect/index

Es la dimensión con mayor crecimiento, particularmente en la protección frente a modificaciones no autorizadas y en la identificación de riesgos asociados.

Disponibilidad (Ítems 9–13)

- **Media Pre:** 2.066
- **Media Post:** 4.382
- **Incremento:** 2.316

Los estudiantes demostraron mayor comprensión sobre planes de contingencia, continuidad y mecanismos para garantizar acceso oportuno a la información.

Evidencia práctica obtenida en las entidades evaluadas

Además del cuestionario, los participantes desarrollaron actividades de campo en entidades reales —privadas y estatales— donde aplicaron el proceso de Administración de Riesgos de Seguridad de la Información. Durante esta experiencia:

- Se identificaron **70 activos de información**.
- Se tasaron **70 activos** según clasificación por CIA.
- Se analizaron **60 activos críticos**.
- Se identificaron **178 amenazas**.
- Se identificaron **178 vulnerabilidades**.

Estos resultados complementan la evidencia estadística y muestran que los participantes lograron aplicar correctamente las metodologías de análisis y evaluación del riesgo basadas en la NTP-ISO/IEC 17799 y la NTP ISO/IEC 27001:2014.

Cuadro N°1. Resumen de Administración de Riesgos del SGSI

						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	Gestión de Productos y Facturación electrónica	1. Gestión de Productos 2. Facturación electrónica 3. Persistencia de datos principal 4. Persistencia de datos sucursal	10	10	8	27	27	Administración de Riesgos de Seguridad de Información Proceso de Gestión de Productos y Facturación electrónica

ISSN: 2810 – 8493
https://revista.ectperu.org.pe/index.php/ect/index

		5. Brindado de servicios principal 6. Brindado de servicios sucursal 7. Generación de archivos xml 8. Acceso al sistema 9. Manuales de usuario 10. Documentación del sistema						
2	Registro de clientes	1. Proceso de registro de cliente 2. Proceso de Gestión Administrativo/almacén	8	8	8	11	11	Administración de Riesgos de Seguridad de Información Proceso de Registro de clientes en la empresa New Cable S.A.C
3	Gestión De Seguridad De Información En OTI	1. Gestión de Servicios 2. Gestión de BackUps 3. Gestión de Redes y Equipo 4. Gestión de Software 5. Gestión de Soporte	21	21	21	57	57	Administración de Riesgos de Seguridad de Información Proceso de Gestión de Seguridad De Información en OTI
4	Gestión de Desarrollo de Software 2024	1. Planificación del proyecto 2.Diseño de Software 3. Codificación 4. Archivos 5. Github 6. Despliegue en producción 7. Manual de usuario	12	12	12	32	32	Administración de Riesgos de Seguridad de Información Proceso de Gestión de Desarrollo de Software 2024
5	Gestión del Vicerrectorado 2024	1. Proceso de comunicación servidor computadora 2. Proceso de almacenamiento y visualización	7	7	4	18	18	Administración de Riesgos de Seguridad de Información Proceso de Gestión del Vicerrectorado 2024

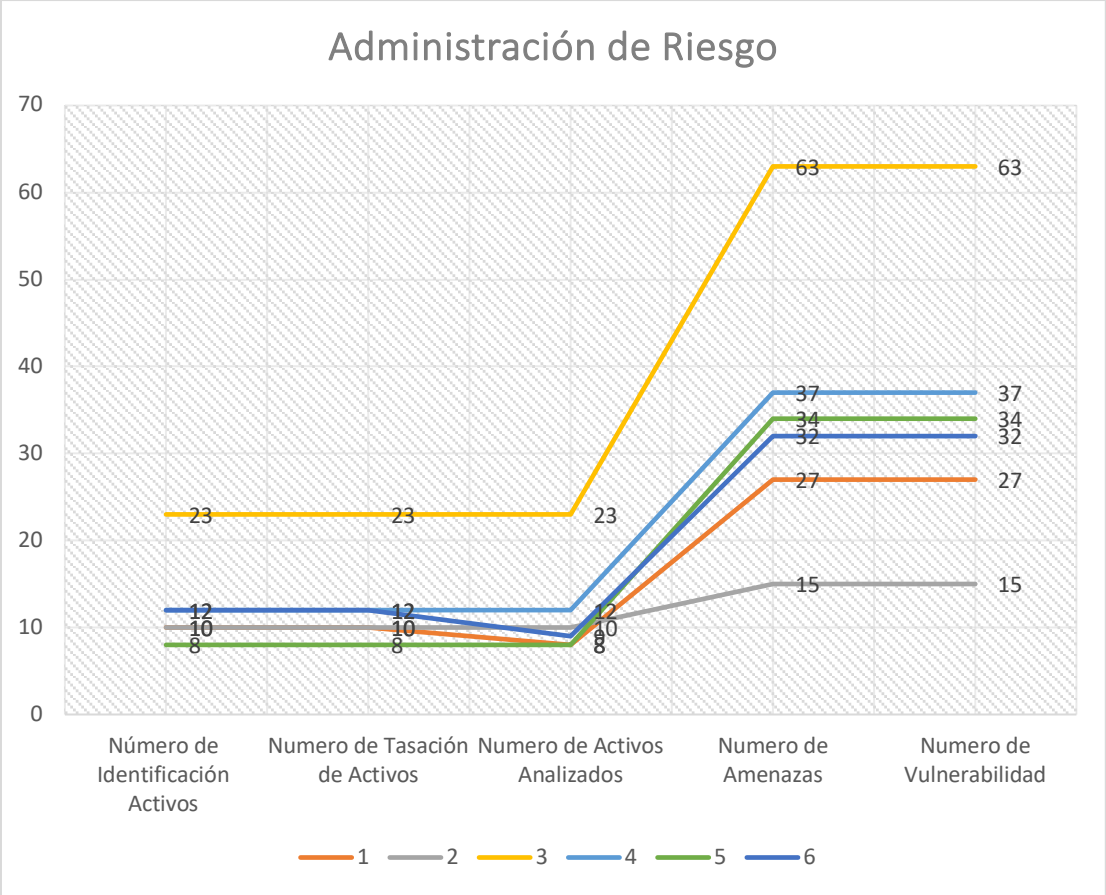
ECT | Revista Cientifica Emprendimiento Científico Tecnologico

ISSN: 2810 – 8493
https://revista.ectperu.org.pe/index.php/ect/index

6	Gestión de Tramite Documentario	Desarrollo de Software	12	12	9	33	33	Administración de Riesgos de Seguridad de Información Proceso de Gestión de Tramite Documentario
		TOTAL	70	70	60	178	178	

Fuente: Elaboración Propia

Gráfico N°1. Resumen de Administración de Riesgos del SGSI



Fuente: Elaboración Propia

Interpretación general de los resultados (sin duplicar conclusiones)

La evidencia estadística y la experiencia aplicada en entidades reales permiten observar que:

ISSN: 2810 – 8493
https://revista.ectperu.org.pe/index.php/ect/index

- La intervención formativa fortaleció la comprensión de la Seguridad de la Información.
- Los participantes lograron transferir ese conocimiento a entornos reales, aplicando adecuadamente identificación, tasación y análisis de riesgos.
- Las mejoras en las tres dimensiones evaluadas fueron consistentes, amplias y estadísticamente significativas.
- La práctica en organizaciones reales complementó el aprendizaje teórico y permitió obtener información auténtica sobre activos, amenazas y vulnerabilidades.

DISCUSIÓN

Los resultados obtenidos muestran que la intervención formativa en Seguridad de la Información logró un impacto significativo en la comprensión de los principios fundamentales del modelo CID y en el proceso de Administración de Riesgos. La mejora estadísticamente significativa entre el Pretest y el Postest ($d = 2.3162$; $p < 0.001$) evidencia un cambio sustancial en el nivel de dominio conceptual de los estudiantes, lo cual es consistente con lo reportado por Al-Dosari y Fetais (2023), quienes señalan que los programas formativos estructurados generan incrementos significativos en la capacidad para identificar riesgos y aplicar controles adecuados dentro de un SGSI.

Del mismo modo, la dimensión de integridad fue la que presentó el mayor incremento ($\Delta = 2.437$), lo que coincide con los hallazgos de Fajri y Harwahyu (2024), quienes destacan que esta dimensión es la más sensible a procesos de capacitación cuando se aborda desde un enfoque práctico basado en incidentes y en la evaluación de procesos críticos. De manera paralela, el conjunto de actividades desarrolladas en entidades reales —en las que se identificaron 70 activos, se tasaron los 70, se analizaron 60 activos críticos y se identificaron 178 amenazas y 178 vulnerabilidades confirma que la experiencia aplicada potencia la comprensión del análisis de riesgos, tal como lo desarrollan Jutif Andita y Aditya (2024) en sus estudios sobre aprendizaje situado en auditoría de seguridad.

Asimismo, los resultados del presente trabajo son coherentes con Guevara-Vega et al. (2023), quienes sostienen que la identificación exhaustiva de amenazas y vulnerabilidades es un componente decisivo para comprender la exposición real de una organización frente a incidentes. La correspondencia entre los datos recogidos en campo

ISSN: 2810 – 8493
https://revista.ectperu.org.pe/index.php/ect/index

y el aumento conceptual detectado mediante el cuestionario sugiere que los estudiantes lograron transferir su aprendizaje teórico a escenarios organizacionales auténticos, fortaleciendo la relación entre la comprensión conceptual y la capacidad analítica.

El fortalecimiento simultáneo de las tres dimensiones del modelo CIA también guarda relación con lo planteado por Nurbojatmiko et al. (2024), quienes señalan que el desarrollo de competencias en SGSI se incrementa cuando los participantes adquieren una visión integral de la interacción entre activos, amenazas y vulnerabilidades. Este enfoque se ve reflejado en la madurez lograda por los estudiantes, quienes, además de mejorar sus resultados estadísticos, lograron ejecutar adecuadamente procesos formales de análisis y evaluación de riesgos según los lineamientos de la NTP-ISO/IEC 17799 y la NTP ISO/IEC 27001:2014.

Por su parte, los aportes de Santos-Olmo et al. (2023) permiten afirmar que los marcos integrados de análisis resultan más efectivos cuando los usuarios comprenden claramente las relaciones entre los elementos del ecosistema de seguridad. Esto se evidencia en este estudio a través de la coherencia entre los resultados cuantitativos y la evidencia práctica recopilada en las organizaciones participantes. Complementariamente, lo propuesto por Hidayatullah et al. (2024) sobre la utilidad de ISO 27005 como referencia metodológica respalda la estructura de trabajo aplicada por los estudiantes durante la identificación, tasación y análisis de cada activo.

Los resultados también se alinean con Ulya et al. (2025), quienes afirman que el empleo de marcos estandarizados permite desarrollar análisis más objetivos y sistemáticos, especialmente cuando los equipos de trabajo participan en experiencias reales. De manera similar, el Systems Editorial Team (2025) sostiene que la integración de aprendizaje práctico con metodologías de análisis de riesgos favorece la consolidación de criterios técnicos y la adopción progresiva de buenas prácticas. La experiencia desarrollada en este estudio respalda estas afirmaciones, evidenciando que la intervención pedagógica permitió una apropiación efectiva de los estándares de seguridad.

En conjunto, los hallazgos demuestran que la combinación de formación teórica, trabajo práctico en entidades reales y aplicación de marcos normativos reconocidos constituye una estrategia altamente efectiva para fortalecer la comprensión y aplicación de la Administración de Riesgos. La evidencia cuantitativa y cualitativa coincide plenamente

ISSN: 2810 – 8493
https://revista.ectperu.org.pe/index.php/ect/index

con la producción científica reciente y reafirma que la intervención diseñada generó mejoras reales, medibles y coherentes con el comportamiento esperado en un proceso de formación profesional en Seguridad de la Información.

CONCLUSIONES

1. La intervención formativa en Seguridad de la Información produjo un efecto significativo en la comprensión del proceso de Administración de Riesgos; La diferencia promedio obtenida ($\bar{D} = 2.31520$) y la significancia estadística ($p < 0.001$) confirman que los estudiantes mejoraron de manera sustancial su capacidad para relacionar los principios de confidencialidad, integridad y disponibilidad con la gestión del riesgo, con un nivel de confianza del 95 %.
2. La formación fortaleció la comprensión de la identificación y tasación de activos según estándares internacionales; El trabajo aplicado en seis entidades permitió identificar 70 activos y realizar su tasación conforme a la NTP-ISO/IEC 17799, demostrando que los participantes desarrollaron competencias para ejecutar la primera fase del proceso de análisis de riesgos de manera estructurada y rigurosa.
3. Los estudiantes demostraron capacidad para realizar una evaluación de riesgos completa en entornos reales; Se analizaron 60 activos críticos, identificándose 178 amenazas y 178 vulnerabilidades según la metodología de la NTP-ISO/IEC 27001:2014. Estos resultados evidencian que la intervención no solo mejoró el conocimiento conceptual, sino que también fortaleció la capacidad operativa para aplicar un enfoque de riesgos dentro de un SGSI.

AGREDECIMIENTO

El equipo de investigación agradece a la Universidad Nacional de Ucayali (UNU) y a la Escuela Académico Profesional de Ingeniería de Sistemas por el apoyo institucional y financiero brindado durante la ejecución de esta investigación formativa.

Se extiende un agradecimiento profundo a los estudiantes de X Ciclo del Curso de Auditoria y Seguridad Informática que, con dedicación y esfuerzo, colaboraron en la sistematización de la evidencia, siendo su aporte un pilar fundamental para el desarrollo de esta investigación formativa.

ISSN: 2810 – 8493
https://revista.ectperu.org.pe/index.php/ect/index

Finalmente, se agradece también a las empresas participantes, que facilitaron el acceso a la información de sus procesos y activos de trabajo para el análisis técnico CID.

REFERENCIAS BIBLIOGRAFICAS

1. Al-Dosari, K., & Fetais, N. (2023). *Risk-management framework and information-security systems for small and medium enterprises (SMEs): A meta-analysis approach.* **Electronics, 12**(17), 3629. https://doi.org/10.3390/electronics12173629

2. Cruz Lucas, G. I., Figueroa Rodríguez, E. L., Cruz Lucas, N. I., & Abad Parrales, W. M. (2023). *Vulnerabilidad de datos en los sistemas información basado en la norma ISO 27001.* **Journal TechInnovation, 2**(2), 54–59. https://doi.org/10.47230/Journal.TechInnovation.v2.n2.2023.54-59

3. Fajri, K. S. A., & Harwahyu, R. (2024). *Information security management system assessment model by integrating ISO 27002 and ISO 27004.* **MALCOM: Indonesian Journal of Machine Learning and Computer Science, 4**(2), 498–506. https://doi.org/10.57152/malcom.v4i2.1245

4. Guevara-Vega, E. M. D., Delgado-Deza, J. R., & Mendoza-de-los-Santos, A. C. (2023). *Vulnerabilities and threats in information assets: A systematic review.* **Revista Científica de Sistemas e Informática, 3**(1), e461. https://doi.org/10.51252/rcsi.v3i1.461

5. Hidayatullah, D. E. R., Kunthi, R., & Harwahyu, R. (2024). *Design and analysis of information security risk management based on ISO 27005: Case study on Audit Management System (AMS) XYZ Internal Audit Department.* **International Journal of Electrical, Computer, and Biomedical Engineering, 2**(3), 395–413. https://doi.org/10.62146/ijecbe.v2i3.81

6. Jutif Andita, R., & Aditya, F. (2024). *Systematic literature review on information security risk management in public service organizations.* **JUTIF: Jurnal Teknik Informatika, 5**(1). https://doi.org/10.52436/1.jutif.2024.5.1.1223

7. Nurbojatmiko, N., Aini, Q., Wasiqi, N. C., Alfajri, M. F., Ulinnuha, Z., Purwati, Y. K., Ayu, I. K., & Yasmin, N. A. (2024). *Risk assessment maturity level of academic information system using ISO 27001 System Security Engineering–Capability Maturity Model.* **Journal of Applied Engineering and Technological Science, 5**(2), 941–954. https://doi.org/10.37385/jaets.v5i2.2971

ISSN: 2810 – 8493
https://revista.ectperu.org.pe/index.php/ect/index

8. Santos-Olmo, A., Sánchez, L. E., & Rosado, D. G. (2023). *Towards an integrated risk analysis security framework according to a systematic analysis of existing proposals.* **Frontiers of Computer Science, 18**, 183808. https://doi.org/10.1007/s11704-023-1582-6

9. Systems Editorial Team. (2025). *Recent trends in information and cyber security maturity assessment: A systematic literature review.* **Systems, 13**(1), 52. https://doi.org/10.3390/systems13010052

10. Ulya, A., Karima, A., Sukiman, T. S. A., Zulfia, A., & Rahmawati, R. (2025). *Information security risk analysis using ISO 31000:2018 and ISO 27001:2022.* **Brilliance: Research of Artificial Intelligence, 5**(2), 843–853. https://doi.org/10.47709/brilliance.v5i2.6564