TESIS
UNIVERSIDAD CIENTÍFICA DEL SUR

UNIVERSIDAD CIENTÍFICA DEL SUR

FACULTAD DE CIENCIAS EMPRESARIALES

CARRERA PROFESIONAL DE INGENIERÍA DE SISTEMAS DE INFORMACIÓN Y GESTIÓN

"Implementación de un SGSI bajo la norma ISO 27001 para la mejora de la seguridad de la información en la empresa Autosafe S.A.C."

Tesis para optar el Título Profesional de
Ingeniero de Sistemas de Información y Gestión

Presentado por:

Rolando Alberto Zamudio de la Cruz (0000-0002-4881-2150)

James Ayrton Ontiveros Ordinola (0000-0001-9552-6125)

Asesor:

Martin Isidro Velásquez Medina (0000-0003-0742-911X)

Lima - Perú

2026

Tesis publicada con autorización del autor
No olvide citar esta tesis

ACTA DE SUSTENTACIÓN DE TESIS

Lima, 24 de setiembre del 2026

Los integrantes del Jurado de tesis:

Presidente	**Carlos Enrique López Sovero**
Miembro 1	**Robert Roy Saavedra Jiménez**
Miembro 2	**Manuel Antonio Pereyra Acosta**

Se reúnen para evaluar la tesis titulada:
"Implementación de un SGSI bajo la norma ISO 27001 para la mejora de la seguridad de la información en la empresa Autosafe S.A.C."
con código de registro **PRE-107-2023-00007**.

Presentado por los bachilleres:
Rolando Alberto Zamudio de la Cruz
James Ayrton Ontiveros Ordinola

Para optar al título profesional de
Ingeniería de Sistemas de Información y Gestión

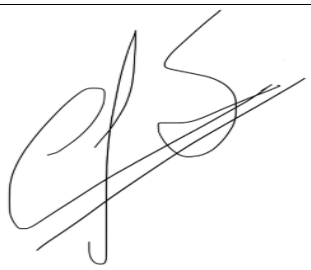
Asesorado por:
Martin Isidro Velasquez Medina

Luego de haber evaluado el informe final de tesis y evaluado el desempeño del estudiante de la Carrera de **Ingeniería de Sistemas de Información y Gestión** en la sustentación, concluyen de manera unánime (X) por mayoría simple ( ) calificar a:

Tesista:	**Rolando Alberto Zamudio de la Cruz**		
Nota (en letras):	**Trece**		
Aprobado (X)	Aprobado - Muy buena ( )	Aprobado - Sobresaliente ( )	Desaprobado ( )

Tesista:	**James Ayrton Ontiveros Ordinola**		
Nota (en letras):	**Trece**		
Aprobado (X)	Aprobado - Muy buena ( )	Aprobado - Sobresaliente ( )	Desaprobado ( )

Los miembros del jurado firman en señal de conformidad.

	
Carlos Enrique López Sovero	Martin Isidro Velasquez Medina
Presidente del Jurado	*Asesor*

	
Robert Roy Saavedra Jiménez	Manuel Antonio Pereyra Acosta
Miembro 1	*Miembro 2*

ANEXO: FORMATO DE DECLARACIÓN DE ORIGINALIDAD DE CONTENIDO DE INFORME FINAL DE TESIS O TRABAJO DE INVESTIGACIÓN

UNIVERSIDAD CIENTÍFICA DEL SUR

DECLARACIÓN DE ORIGINALIDAD DE CONTENIDO DEL INFORME FINAL DE TESIS / TRABAJO DE INVESTIGACIÓN (versión 2.0) [1]

Lima, 29 de Setiembre del 2026

Señor,
Percy Manuel Mayta Tristán
Vicerrector de Investigación
Universidad Científica del Sur
Presente. –

De nuestra consideración,

Los abajo firmantes –Rolando Alberto Zamudio de la Cruz y James Ayrton Ontiveros Ordinola egresado(s) del Programa académico de Ingeniería de Sistemas de Información y Gestión de la Universidad Científica del Sur, y el asesor/la asesora de tesis Martin Isidro Velásquez Medina declaramos que este informe final de tesis/trabajo de investigación titulado "Implementación de un SGSI bajo la norma ISO 27001 para la mejora de la seguridad de la información en la empresa", que presentamos para optar el título profesional/grado académico de Ingeniería de Sistemas de información y Gestión, es original.

En consecuencia, declaramos que el informe no contiene plagio ni total ni parcial; que, cuando se utilizó información de fuentes externas, se reconoció su autoría mediante la citación correspondiente; y que los resultados obtenidos son producto íntegro de nuestra investigación y no han sido falseados ni fabricados. Todo ello en cumplimiento del Código de ética en la Investigación, Reglamento de Disciplina de Pregrado y Posgrado, Reglamento de Propiedad Intelectual, Normas y procedimientos de los trabajos de investigación para la obtención de títulos profesionales y grados académicos [2], que afirmamos conocer en su totalidad.

Declaramos, además, que no se han utilizado herramientas de inteligencia artificial (IA), ni generativas ni de ningún otro tipo, en ninguna fase del desarrollo de la investigación ni en la redacción del informe final de tesis/trabajo de investigación. Todo el material contenido en este informe fue elaborado íntegramente por Rolando Alberto Zamudio de la Cruz y James Ayrton Ontiveros Ordinola sin asistencia de herramienta alguna de IA.

Declaramos, además, que no se han utilizado herramientas de inteligencia artificial (IA) generativa, de forma parcial ni total, en ninguna fase del desarrollo de la investigación ni en la redacción del informe final de tesis/trabajo de investigación. Sí declaro haber utilizado herramientas de IA no generativa para la corrección ortográfica y los formatos de referencia, conforme a la normativa de la Universidad [3]. Todo el material ha sido revisado por Rolando Alberto Zamudio de la Cruz y James Ayrton Ontiveros Ordinola, quien(es) asume(n) la responsabilidad de su contenido.

Por ello, en caso de identificarse alguna situación de plagio, falsificación o fabricación de resultados, uso indebido de IA generativa o uso no declarado de IA, nos sometemos al proceso de investigación que establezca la Universidad y aceptamos las sanciones que pudieran corresponder. También declaramos conocer las normativas institucionales que regulan las sanciones aplicables en estos casos, incluido el de la compra y venta de tesis.

Firmamos en conformidad con lo declarado,

[1] En conformidad con la Resolución del Consejo Directivo N° 084-2022-SUNEDU/CD
[2] Los documentos están en: https://repositorio.cientifica.edu.pe/handle/20.500.12805/3652
[3] GEA-GIE-POL-05 Política del uso de inteligencia artificial



Firma tesista
DNI: 48194180



Firma tesista
DNI: 10550273



Firma del asesor de tesis
DNI: 42940129

INFORME DE REVISIÓN DE ORIGINALIDAD

Título del documento evaluado. Implementación de un SGSI bajo la norma ISO 27001 para la mejora de la seguridad de la información en la empresa Autosafe S.A.C..

Autores. Rolando Alberto Zamudio de la Cruz; James Ayrton Ontiveros Ordinola.

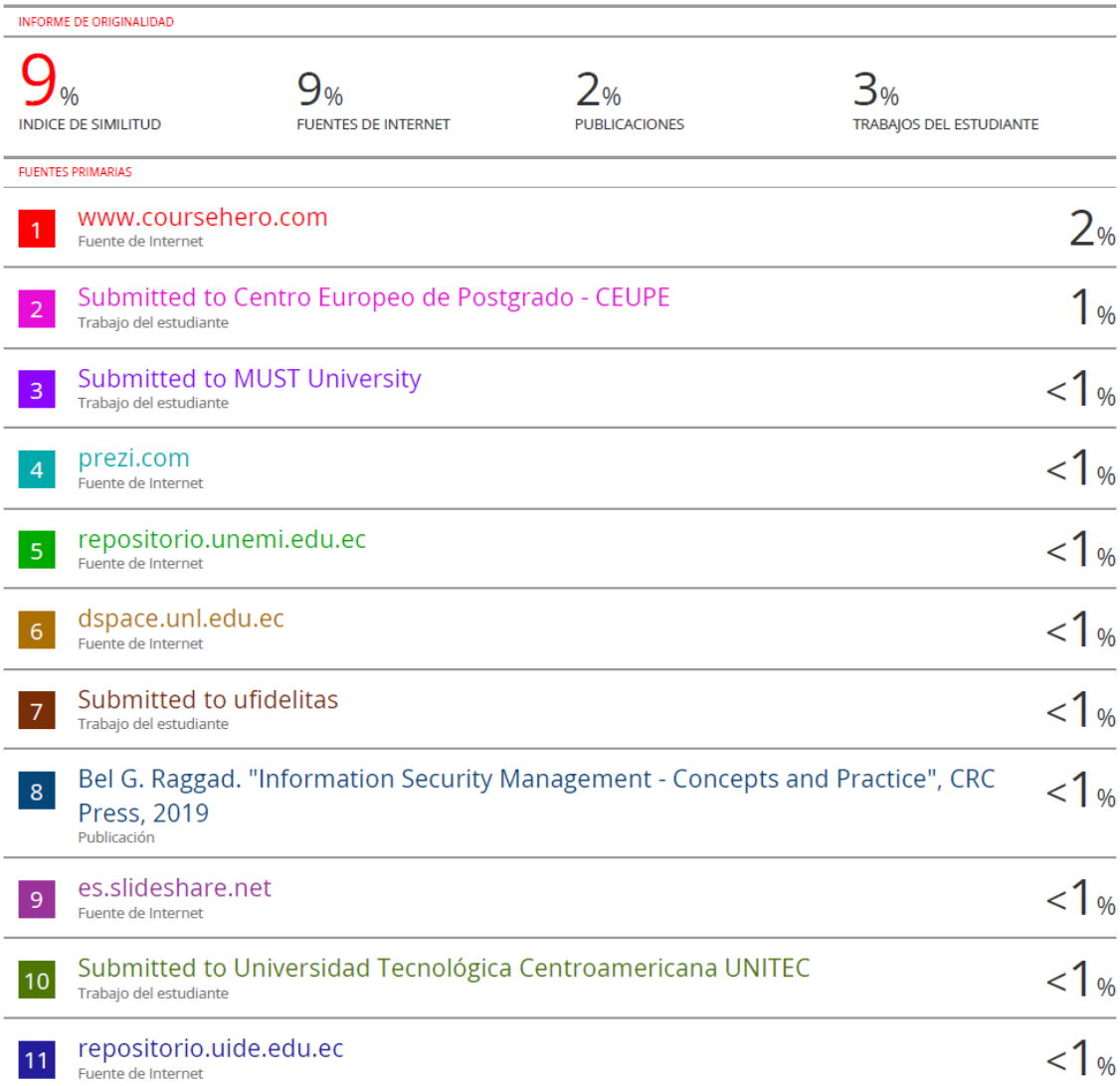
Mecanismo de revisión de originalidad. Evaluación con Turnitin (ID 3092818784).

Código de registro. PRE-107-2023-00007.

Resultado de la evaluación. 9%.

Revisado por. Jorge André Layza Diaz.

Comentarios sobre la revisión. Filtros usados: excluir fuentes de menos de 12 palabras.



INFORME DE ORIGINALIDAD

9%	9%	2%	3%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	www.coursehero.com Fuente de Internet	2%
2	Submitted to Centro Europeo de Postgrado - CEUPE Trabajo del estudiante	1%
3	Submitted to MUST University Trabajo del estudiante	<1%
4	prezi.com Fuente de Internet	<1%
5	repositorio.unemi.edu.ec Fuente de Internet	<1%
6	dspace.unl.edu.ec Fuente de Internet	<1%
7	Submitted to ufidelitas Trabajo del estudiante	<1%
8	Bel G. Raggad. "Information Security Management - Concepts and Practice", CRC Press, 2019 Publicación	<1%
9	es.slideshare.net Fuente de Internet	<1%
10	Submitted to Universidad Tecnológica Centroamericana UNITEC Trabajo del estudiante	<1%
11	repositorio.uide.edu.ec Fuente de Internet	<1%

Resumen

En el contexto actual de la transformación digital, las organizaciones enfrentan un incremento constante de amenazas a la seguridad de la información, lo que expone a riesgos elevados la confidencialidad, integridad y disponibilidad de los activos de información. Ante esta problemática, la presente investigación tuvo como objetivo implementar un Sistema de Gestión de la Seguridad de la Información (SGSI) basado en los controles de la norma ISO/IEC 27001 en la empresa AUTOSAFE S.A.C., con el propósito de fortalecer la seguridad informática y reducir los riesgos asociados a accesos no autorizados y pérdida de información.

Los tres pilares de la seguridad de la información se denominan CIA (por sus siglas en inglés): Confidencialidad (Confidentiality), Integridad (Integrity) y Disponibilidad (Availability). Estos tres principios son igualmente esenciales: proteger la confidencialidad garantiza que la información solo sea accesible a usuarios autorizados; garantizar la integridad asegura la exactitud y completitud de los datos; y asegurar la disponibilidad garantiza que los sistemas e información estén accesibles cuando se requieran. En el presente estudio, los tres pilares son evaluados de forma conjunta como dimensiones interdependientes del SGSI.

La investigación se desarrolló bajo un enfoque mixto (cuantitativo y cualitativo), utilizando la metodología de estudio de caso. Para la recolección y análisis de datos se aplicaron encuestas, auditorías de seguridad, pruebas de penetración (pentesting) y evaluaciones comparativas del estado de la seguridad antes y después de la implementación del SGSI.

Los resultados evidencian mejoras numéricas significativas en los principales indicadores evaluados. La efectividad en la identificación de activos se incrementó del 50 % al 90 %, mientras que la confidencialidad y la integridad de la información aumentaron del 45 % al 85 % y del 50 % al 90 %, respectivamente. Asimismo, la gestión de accesos y roles presentó una mejora promedio del 40 %, al migrar de un esquema de accesos genéricos a un modelo basado en usuarios únicos, roles y perfiles. En relación con la gestión de riesgos, la efectividad se elevó del 40 % al 80 %, y el nivel de conformidad con la norma ISO/IEC 27001 alcanzó el 95 % tras la implementación del SGSI.

Tesis publicada con autorización del autor
No olvide citar esta tesis

Se concluye que la implementación del SGSI bajo la norma ISO/IEC 27001 permitió elevar de manera significativa el nivel de seguridad de la información, mejorar la eficiencia operativa y fortalecer la confianza de clientes y socios estratégicos, demostrando la efectividad del modelo aplicado en la organización.

Palabras clave: Seguridad de la información, ISO 27001, Sistema de Gestión de Seguridad de la Información (SGSI), Gestión de riesgos, Transformación digital

Tesis publicada con autorización del autor
No olvide citar esta tesis

TESIS
UNIVERSIDAD CIENTÍFICA DEL SUR

Abstract

In the current context of digital transformation, organizations face a continuous increase in information security threats, which exposes the confidentiality, integrity, and availability of information assets to high levels of risk. In response to this challenge, this research aimed to implement an Information Security Management System (ISMS) based on the controls of the ISO/IEC 27001 standard in a GPS service company, with the purpose of strengthening information security and reducing the risks associated with unauthorized access and information loss.

The study was conducted using a mixed-methods approach (quantitative and qualitative) and followed a case study methodology. Data collection and analysis were carried out through surveys, security audits, penetration testing (pentesting), and comparative evaluations of the organization's security status before and after the implementation of the ISMS.

The results show significant numerical improvements in the main evaluated indicators. The effectiveness of asset identification increased from 50% to 90%, while information confidentiality and integrity improved from 45% to 85% and from 50% to 90%, respectively. In addition, access and role management showed an average improvement of 40%, transitioning from a generic access scheme to a model based on unique users, roles, and profiles. Regarding risk management, effectiveness increased from 40% to 80%, and the level of compliance with the ISO/IEC 27001 standard reached 95% after the ISMS implementation.

It is concluded that the implementation of the ISMS under the ISO/IEC 27001 standard significantly enhanced the organization's information security level, improved operational efficiency, and strengthened trust among clients and strategic partners, demonstrating the effectiveness of the implemented model.

Keywords: Information Security, Information Security Management System (ISMS), Risk Management, Digital Transformation

Tesis publicada con autorización del autor
No olvide citar esta tesis