

## INFORME DE ORIGINALIDAD

12%

INDICE DE SIMILITUD

11%

FUENTES DE INTERNET

2%

PUBLICACIONES

4%

TRABAJOS DEL  
ESTUDIANTE

## FUENTES PRIMARIAS

1	<a href="http://hdl.handle.net">hdl.handle.net</a> Fuente de Internet	1%
2	Submitted to Instituto Superior de Artes, Ciencias y Comunicación IACC Trabajo del estudiante	<1%
3	<a href="http://repositorio.ug.edu.ec">repositorio.ug.edu.ec</a> Fuente de Internet	<1%
4	<a href="http://www.coursehero.com">www.coursehero.com</a> Fuente de Internet	<1%
5	<a href="http://www.slideshare.net">www.slideshare.net</a> Fuente de Internet	<1%
6	<a href="http://openaccess.uoc.edu">openaccess.uoc.edu</a> Fuente de Internet	<1%
7	<a href="http://repositorio.untels.edu.pe">repositorio.untels.edu.pe</a> Fuente de Internet	<1%
8	<a href="http://repositorio.uncp.edu.pe">repositorio.uncp.edu.pe</a> Fuente de Internet	<1%
9	<a href="http://riunet.upv.es">riunet.upv.es</a> Fuente de Internet	<1%



**FORMULARIO DE AUTORIZACIÓN PARA LA  
PUBLICACIÓN DE TRABAJOS DE INVESTIGACIÓN EN  
EL REPOSITORIO INSTITUCIONAL DE LA UNTELS  
(Art. 45° de la ley N° 30220 – Ley)**

Autorización de la propiedad intelectual del autor para la publicación de tesis en el Repositorio Institucional de la Universidad Nacional Tecnológica de Lima Sur (<https://repositorio.untels.edu.pe>), de conformidad con el Decreto Legislativo N° 822, sobre la Ley de los Derechos de Autor, Ley N° 30035 del Repositorio Nacional Digital de Ciencia, Tecnología e Innovación de Acceso Abierto, Art. 10° del Rgto. Nacional de Trabajos de Investigación para optar grados académicos y títulos profesionales en las universidades – RENATI Res. N° 084-2022-SUNEDU/CD, publicado en El Peruano el 16 de agosto de 2022; y la RCO N° 061-2023-UNTELS del 01 marzo 2023.

**TIPO DE TRABAJO DE INVESTIGACIÓN**

- 1). TESIS ( )      2). TRABAJO DE SUFICIENCIA PROFESIONAL ( x )

**DATOS PERSONALES**

Apellidos y Nombres:	RUBEN VICTOR SANCHEZ MARIN
D.N.I.:	72875684
Otro Documento:	
Nacionalidad:	PERUANA
Teléfono:	933107914
e-mail:	2012200140@untels.edu.pe

**DATOS ACADÉMICOS**

**Pregrado**

Facultad:	FACULTAD DE INGENIERÍA Y GESTIÓN
Programa Académico:	TRABAJO DE SUFICIENCIA PROFESIONAL
Título Profesional otorgado:	INGENIERO ELECTRÓNICO Y TELECOMUNICACIONES

**Postgrado**

Universidad de Procedencia:	
País:	
Grado Académico otorgado:	

**Datos de trabajo de investigación**

Título:	"IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE INFORMACIÓN Y EVENTOS DE SEGURIDAD PARA LA DETECCIÓN DE AMENAZAS EN UNA ENTIDAD PÚBLICA DEL SECTOR SALUD"
Fecha de Sustentación:	14 DE DICIEMBRE DEL 2024
Calificación:	APROBADO POR UNANIMIDAD
Año de Publicación:	2025



### AUTORIZACIÓN DE PUBLICACIÓN EN VERSIÓN ELECTRÓNICA

A través de la presente, autorizo la publicación del texto completo de la tesis, en el Repositorio Institucional de la UNTELS especificando los siguientes términos:

Marcar con una X su elección.

- 1) Usted otorga una licencia especial para publicación de obras en el REPOSITORIO INSTITUCIONAL DE LA UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR.

Si autorizo \_\_\_\_\_ No autorizo  X

- 2) Usted autoriza para que la obra sea puesta a disposición del público conservando los derechos de autor y para ello se elige el siguiente tipo de acceso.

Derechos de autor		
TIPO DE ACCESO	ATRIBUCIONES DE ACCESO	ELECCIÓN
ACCESO ABIERTO 12.1(*)	<b>info:eu-repo/semantics/openAccess</b> (Para documentos en acceso abierto)	( )

- 3) Si usted dispone de una **PATENTE** puede elegir el tipo de **ACCESO RESTRINGIDO** como derecho de autor y en el marco de confiabilidad dispuesto por los numerales 5.2 y 6.7 de la directiva N° 004-2016-CONCYTEC DEGC que regula el Repositorio Nacional Digital de CONCYTEC (Se colgará únicamente datos del autor y el resumen del trabajo de investigación).

Derechos de autor		
TIPO DE ACCESO	ATRIBUCIONES DE ACCESO	ELECCIÓN
ACCESO RESTRINGIDO	<b>info:eu-repo/semantics/restrictedAccess</b> (Para documentos restringidos)	(x)
	<b>info:eu-repo/semantics/embargoedAccess</b> (Para documentos con períodos de embargo. Se debe especificar las fechas de embargo)	( )
	<b>info:eu-repo/semantics/closedAccess</b> (para documentos confidenciales)	( )

(\*) <http://renati.sunedu.gob.pe>



UNIVERSIDAD NACIONAL  
TECNOLÓGICA DE LIMA SUR

Rellene la siguiente información si su trabajo de investigación es de acceso restringido:

Atribuciones de acceso restringido:

info:eu-repo/semantics/restrictedAccess

Motivos de la elección del acceso restringido:

El motivo de la restricción se debe a que hay datos de la empresa confidenciales  
o datos que no deben ser públicos.

SANCHEZ MARIN RUBEN VICTOR

APELLIDOS Y NOMBRES

72875684

DNI

Firma y huella:



Lima, 28 de enero del 20 25

**UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR**

**FACULTAD DE INGENIERÍA Y GESTIÓN  
ESCUELA PROFESIONAL DE INGENIERÍA ELECTRÓNICA Y  
TELECOMUNICACIONES**



**“IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE INFORMACIÓN  
Y EVENTOS DE SEGURIDAD PARA LA DETECCIÓN DE AMENAZAS  
EN UNA ENTIDAD PÚBLICA DEL SECTOR SALUD”**

**TRABAJO DE SUFICIENCIA PROFESIONAL**

Para optar el Título Profesional de

**INGENIERO ELECTRÓNICO Y TELECOMUNICACIONES**

**PRESENTADO POR EL BACHILLER**

SANCHEZ MARIN, RUBEN VICTOR

ORCID: 0009-0006-4829-1662

**ASESOR**

CAMPOS AGUADO, FREDY

ORCID: 0000-0003-3419-925X

**Villa El Salvador**

**2024**



## ACTA DE SUSTENTACIÓN DE TRABAJO DE SUFICIENCIA PROFESIONAL PARA OBTENER EL TÍTULO PROFESIONAL DE INGENIERO ELECTRÓNICO Y TELECOMUNICACIONES

En Villa El Salvador, siendo las 12:00 horas del día 14 de diciembre del año 2024, reunidos en las instalaciones de la UNTELS, los miembros del Jurado Evaluador, integrado por:

PRESIDENTE: **Dr. Santiago Linder Rubiños Jimenez** ORCID N° 0000-0003-0095-6988 Colegiatura N°112655

SECRETARIO: **Mg. José Ambrosio Machuca Mines** ORCID N° 0000-0002-7069-7654 Colegiatura N°158894

VOCAL : **Mg. Pablo Andrés Villegas Chunga** ORCID N° 0009-0004-1623-7173 Colegiatura N°199274

Nombrados por Resolución de Decanato N° 232-2024, de fecha 12 de diciembre 2024, quienes dan inicio a la Sesión Pública de Sustentación del Trabajo de Suficiencia Profesional.

Acto seguido, el aspirante al Título Profesional de **Ingeniero Electrónico y Telecomunicaciones**

Don (ña): **RUBEN VICTOR SANCHEZ MARIN** identificado(a) con D.N.I. N° 72875684; procedió con la Sustentación del Trabajo de Suficiencia Profesional Titulado: **IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE INFORMACIÓN Y EVENTOS DE SEGURIDAD PARA LA DETECCIÓN DE AMENAZAS EN UNA ENTIDAD PÚBLICA DEL SECTOR SALUD**

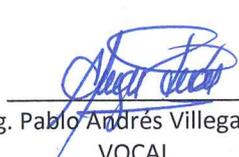
Autorizado mediante Resolución de Decanato N° 237-2024, de fecha 12 de diciembre de 2024, de conformidad con las disposiciones del Reglamento General para el Otorgamiento de Grado Académico y Título Profesional vigente, sustentó y absolvió las interrogantes que le formularon los señores miembros del Jurado Evaluador. Concluida la Sustentación se procedió a la evaluación y calificación correspondiente, de acuerdo al **Art. 57°** del Reglamento General para optar el Título Profesional.

CALIFICACIÓN		CONDICIÓN	EQUIVALENCIA
NÚMERO	LETRAS		
16	DIECISEIS	APROBADO POR UNANIMIDAD	BUENO

Siendo las 12:30 PM del día 14 de diciembre del 2024, se dio por concluido el acto de sustentación, firmando el jurado evaluador el Acta de Sustentación y con firma del sustentante en señal de conformidad.

  
Dr. Santiago Linder Rubiños Jimenez  
PRESIDENTE

  
Mg. José Ambrosio Machuca Mines  
SECRETARIO

  
Mg. Pablo Andrés Villegas Chunga  
VOCAL

  
RUBEN VICTOR SANCHEZ MARIN  
SUSTENTANTE

**Nota: Artículo 50°.** - Para el inicio y desarrollo de la sustentación se requiere la presencia física y permanente de los integrantes del jurado. De faltar algún miembro del jurado, la sustentación procederá con los dos integrantes presentes. En caso de ausencia del presidente del jurado, ésta será asumida por el jurado de mayor categoría y antigüedad. En caso de ausencia de dos (02) integrantes del jurado, se suspenderá el acto de sustentación, pudiendo reprogramarse dentro de los cinco (05) días hábiles siguientes, sin perjuicio de aplicar el artículo 62° del presente Reglamento.

## **DEDICATORIA**

Dedico este trabajo a mi madre Yolanda Marin por ayudarme y brindarme su apoyo en todo el periodo universitario a mi hermano Giampiere que con su apoyo incondicional supo guiarme en toda la etapa universitaria.

## **AGRADECIMIENTOS**

Agradezco a los docentes de mi casa de estudios UNTELS por las enseñanzas adquiridas a lo largo de mi formación universitaria.

.

## ÍNDICE

ÍNDICE .....	iv
ÍNDICE DE TABLAS .....	vi
ÍNDICE DE FIGURAS .....	vii
RESUMEN .....	ix
INTRODUCCIÓN .....	x
CAPÍTULO I ASPECTOS GENERALES .....	12
1.1. Contexto .....	12
1.2. Delimitación del Proyecto .....	13
1.2.1. Temporal.....	13
1.2.2. Espacial .....	13
1.3. Objetivos .....	13
1.3.1. Objetivo general.....	13
1.3.2. Objetivos específicos .....	13
CAPÍTULO II MARCO TEÓRICO.....	14
2.1. Antecedentes.....	14
2.1.1. Antecedentes Nacionales .....	14
2.1.2 Antecedentes Internacionales.....	17
2.2. Bases teóricas .....	18
2.2.1. Centro de Operaciones de Seguridad (SOC) .....	18
2.2.2. Gestión de información y eventos de seguridad .....	22
2.2.3. Plataformas de monitoreo.....	26
2.2.4. Tecnología de gestión de eventos e información de seguridad –SIEM 28	
2.2.5. Estándares y normas de seguridad .....	31
2.2.6. Principios básicos de la seguridad informática .....	35
2.3. Definición de términos básicos .....	36
CAPÍTULO III DESARROLLO DEL TRABAJO PROFESIONAL .....	38
3.1. Determinación y análisis del problema .....	38
3.2. Modelo de solución propuesto:.....	41
3.3. Resultados.....	55
CONCLUSIONES.....	64
RECOMENDACIONES .....	65

REFERENCIAS BIBLIOGRÁFICAS .....	66
ANEXOS .....	71

## ÍNDICE DE TABLAS

<b>Tabla 1</b> <i>Característica recomendadas según el hardware</i> .....	45
<b>Tabla 2</b> <i>Cumplimiento de pruebas realizadas</i> .....	54
<b>Tabla 3</b> <i>Eventos del syslog monitoreados por el SIEM en 2024</i> .....	60

## ÍNDICE DE FIGURAS

<b>Figura 1</b> Esquema de funcionamiento de un SOC .....	22
<b>Figura 2</b> Comparación entre un IDS e IPS .....	30
<b>Figura 3</b> Estructura General del estándar ISO / IEC 27032.....	32
<b>Figura 4</b> Comparativa entre el NIS CSF y las buenas prácticas COBIT 5.....	33
<b>Figura 5</b> Estructura del marco NIST v 1.1. ....	34
<b>Figura 6</b> Denuncias de ciberseguridad ante la PNP .....	39
<b>Figura 7</b> Etapas de implementación de proyecto.....	41
<b>Figura 8</b> Dispositivos de seguridad utilizando protocolo SNMP.....	42
<b>Figura 9</b> Monitoreo mediante plataforma Opmanger .....	43
<b>Figura 10</b> Configuración en el portal de monitoreo Opmanger .....	43
<b>Figura 11</b> Transferencia de transmisión y recepción en la interface ethernet1-1- WAN.....	44
<b>Figura 12</b> Descarga del software LOG360 .....	45
<b>Figura 13.</b> Descarga del software LOG360 .....	46
<b>Figura 14</b> Perfil de servidor Syslog.....	47
<b>Figura 15</b> Interfaz de Configuración de Perfiles de Reenvío de Logs.....	47
<b>Figura 16</b> Reglas de política de seguridad .....	48
<b>Figura 17</b> Topología de sincronización del equipo firewall al servidor SIEM .....	48
<b>Figura 18</b> Licencia del SIEM Log360.....	49
<b>Figura 19</b> Descripción de accesos y roles al SIEM Log360.....	49
<b>Figura 20</b> Configuración de correos para el envío de notificaciones y alertas.....	50
<b>Figura 21</b> Configuración de notificaciones del SIEM Log360 .....	51
<b>Figura 22</b> Alertas registradas del SIEM Log360 .....	51
<b>Figura 23</b> Configuración de parámetros en el SIEM Log360 .....	52
<b>Figura 24</b> Configuración de Perfil de Alerta en Log360 para Notificaciones de Ataques.....	53
<b>Figura 25</b> Comprobación de conectividad mediante comando ping .....	56
<b>Figura 26</b> Monitorización del tiempo de actividad y carga del sistema .....	56
<b>Figura 27</b> Promedio de uso del CPU durante noviembre del 2024.....	57
<b>Figura 28</b> Promedio de uso del RAM durante noviembre del 2024 .....	58
<b>Figura 29</b> Uso de disco en la unidad D.....	59
<b>Figura 30</b> Detalles de la licencia de ManageEngine EventLog Analyzer .....	59

<b>Figura 31</b> Registro de tráfico Syslog en el firewall.....	60
<b>Figura 32</b> Tablero de monitoreo Log360 .....	61
<b>Figura 33</b> Alertas reportadas en la entidad de salud .....	62
<b>Figura 34</b> Alertas generada por Palo Alto.....	63

## RESUMEN

En la actualidad las instituciones del estado han incrementado la previsión ante cualquier incidente de ciberseguridad debido al incremento de los ataques en tal sentido existe el Decreto Supremo N° 132-2018-PCM - Estrategia Nacional de Ciberseguridad publicado por la PCM (Presidencia de consejo de ministros) que establece los criterios de seguridad digital en el ámbito nacional (PCM 2018). Esta investigación se enfoca en la puesta en marcha de un SIEM (Security information and event management) en la empresa Smart Global SAC para monitorear la infraestructura de tecnología información de una entidad pública del Perú en rubro de salud.

La empresa realizaba la monitorización de los equipos de infraestructura de sus clientes con una plataforma en base a los protocolos SNMP (Simple Network Management Protocol) y Netflow, los cuales presentaban limitaciones para describir los eventos ocurridos en la infraestructura TI de la entidad por ello que se decidió implementar un SIEM para mejorar la monitorización en tiempo real y prever las respuestas ante cualquier incidente de ciberseguridad seguridad de la infraestructura. Para ello proyecto consistió en el levantamiento de información de infraestructura del cliente, preparación e implementación del sistema, activación de las reglas perimetrales y validaciones del sistema.

Los resultados de la implementación muestran que se mejoró en 60% la seguridad de la infraestructura de la entidad ya que observaban eventos en tiempo real para su posterior mitigación.