UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO

FACULTAD DE INGENIERÍA CIVIL, DE SISTEMAS Y DE ARQUITECTURA

TESIS

Para Optar el Título Profesional de:

INGENIERO DE SISTEMAS

Propuesta de un SGSI basado en ISO 27001:2013, para mejorar la seguridad de la información de las áreas de informática y administración de la Municipalidad distrital de Salas, 2024.

Autor:

Bach. Rolando Ysaias Valiente Arce

Asesor:

MSc. Ing. Gavino Marcelo Loyaga Orbegoso

ORCID: https://orcid.org/0000-0002-5706-1192

LAMBAYEQUE, PERÚ

17 de julio de 2026

UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO

FACULTAD DE INGENIERÍA CIVIL, DE SISTEMAS Y DE ARQUITECTURA

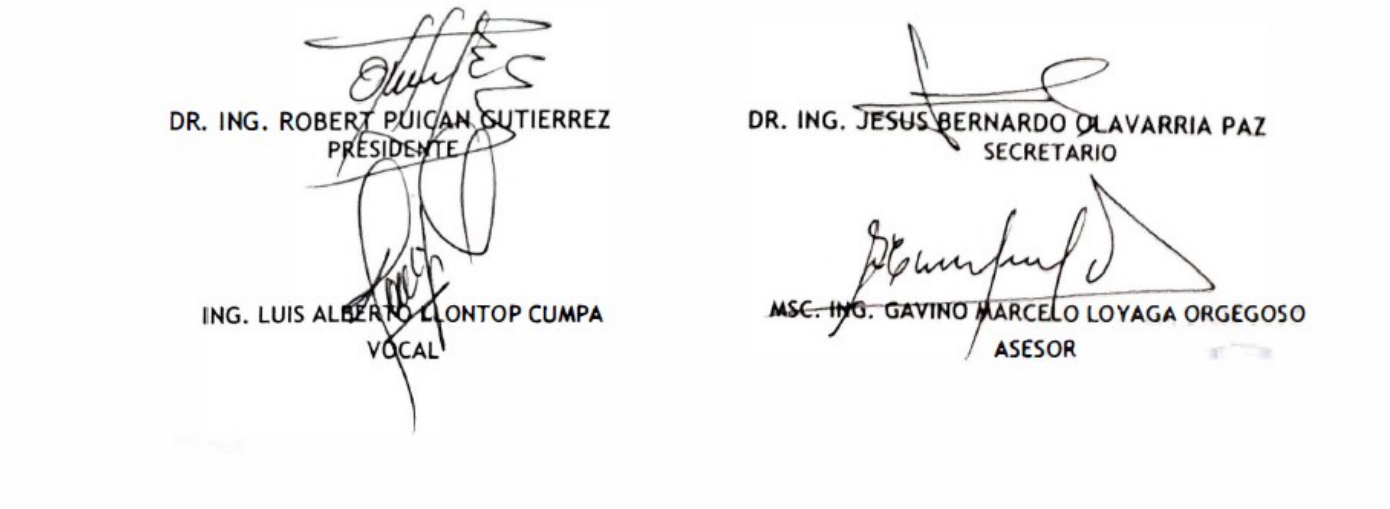
TESIS

Propuesta de un SGSI basado en ISO 27001:2013, para mejorar la seguridad de la información de las áreas de informática y administración de la Municipalidad distrital de Salas, 2024.

Para Optar el Título Profesional de:

INGENIERO DE SISTEMAS

Aprobada por los miembros del jurado:



UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO
FACULTAD DE INGENIERÍA CIVIL DE SISTEMAS Y DE ARQUITECTURA
UNIDAD DE INVESTIGACIÓN

ACTA DE SUSTENTACIÓN N°010-2026-UI-FICSA

Siendo las 10:30 am horas del día 17 de julio del 2026, se reunieron de manera presencial los miembros de jurado de la tesis titulada: **"PROPUESTA DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN, BASADO EN ISO 27001:2013, PARA MEJORAR LA SEGURIDAD DE LA INFORMACIÓN DE LAS ÁREAS DE INFORMÁTICA Y ADMINISTRACIÓN DE LA MUNICIPALIDAD DISTRITAL DE SALAS,2024"**, con código N° IS_V_2024_011, designado por Resolución Decanal Virtual N° 471-2024-UNPRG-FICSA con la finalidad de Evaluar y Calificar la sustentación de la tesis antes mencionada, conformado por los siguientes docentes:

DR. ING. ROBERT PUICAN GUTIERREZ	PRESIDENTE
DR. ING. JESUS BERNARDO OLAVARRIA PAZ	SECRETARIO
ING. LUIS ALBERTO LLONTOP CUMPA	VOCAL

Asesorado por MSC. ING. GAVINO MARCELO LOYAGA ORGEGOSO.

El acto de sustentación fue autorizado por OFICIO VIRTUAL N° 162-2026-UIFICSA, la tesis fue presentada y sustentada por el Bachiller: ROLANDO YSAIAS VALIENTE ARCE, tuvo una duración de ..60.....minutos. Después de la sustentación, y absueltas las preguntas y observaciones de los miembros del jurado; se procedió a la calificación respectiva:

	NUMERO	LETRAS	CALIFICATIVO
ROLANDO YSAIAS VALIENTE ARCE	.....17.....	.....DIECISIETE.....	.....BUENO.....

Por lo que queda APTO para obtener el Título Profesional de INGENIERO DE SISTEMAS de acuerdo con la Ley Universitaria 30220 y la normatividad vigente de la Facultad de Ingeniería Civil De Sistemas y de Arquitectura de la Universidad Nacional Pedro Ruiz Gallo.

Siendo las ...11:30AM Se dio por concluido el presente acto académico, dándose conformidad al presente acto, con la firma de los miembros del jurado.

DR. ING. ROBERT PUICAN GUTIERREZ
PRESIDENTE

DR. ING. JESUS BERNARDO OLAVARRIA PAZ
SECRETARIO

ING. LUIS ALBERTO LLONTOP CUMPA
VOCAL

MSC. ING. GAVINO MARCELO LOYAGA ORGEGOSO
ASESOR

JHFF/bcm

UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO
FACULTAD DE INGENIERÍA CIVIL, DE SISTEMAS Y DE ARQUITECTURA
UNIDAD DE INVESTIGACIÓN

"Año de la universalización de la salud".

CONSTANCIA DE VERIFICACIÓN DE ORIGINALIDAD DE TESIS

Según Res. N° 659-2020-R

Yo, Ing. Msc. Gavino Marcelo Loyaga Orbegoso**, asesor de tesis del bachiller**:

ROLANDO YSAIAS VALIENTE ARCE

TITULADA:

PROPUESTA DE UN SGSI BASADO EN ISO 27001:2013, PARA MEJORAR LA SEGURIDAD DE LA INFORMACIÓN DE LAS ÁREAS DE INFORMÁTICA Y ADMINISTRACIÓN DE LA MUNICIPALIDAD DISTRITAL DE SALAS, 2024

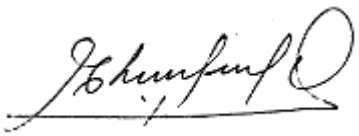
Luego de la revisión exhaustiva del documento constato que la misma tiene un índice de similitud de 23% verificable en el reporte de similitud del programa TURNITIN.

El suscrito analizó dicho reporte y concluyó que cada una de las coincidencias detectadas NO CONSTITUYEN PLAGIO. A mi leal saber y entender la tesis cumple con todas las normas para el uso de citas y referencias establecidas por la Universidad Nacional Pedro Ruiz Gallo.

Se expide la presente según lo dispuesto en la Resolución Nº 659-2020-R, de fecha 7 de julio de 2026 formativa para la obtención de Grados y Títulos de la UNPRG:

Lambayeque, 03 de agosto del 2026

ATENTAMENTE,



Ing. Msc. Gavino Marcelo Loyaga Orbegoso
DNI. 16483687

Se adjunta:
Recibo digital de Turnitin
Revisión de informe en Turnitin

Tesis

INFORME DE ORIGINALIDAD

23%	23%	%	%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	hdl.handle.net Fuente de Internet	3%
2	repositorio.unjfsc.edu.pe Fuente de Internet	1%
3	www.coursehero.com Fuente de Internet	1%
4	repositorio.utn.edu.ec Fuente de Internet	1%
5	repository.unipiloto.edu.co Fuente de Internet	1%
6	www.slideshare.net Fuente de Internet	1%
7	repository.unipiloto.edu.co:8080 Fuente de Internet	1%
8	repositorio.unbosque.edu.co Fuente de Internet	<1%
9	dspace.ucacue.edu.ec Fuente de Internet	<1%
10	repositorio.ucp.edu.pe Fuente de Internet	<1%
11	repositorio.unprg.edu.pe Fuente de Internet	<1%
12	repositorio.utp.edu.co Fuente de Internet	<1%
13	www.researchgate.net Fuente de Internet	<1%
14	care.org.pe Fuente de Internet	<1%
15	repositorio.unamba.edu.pe Fuente de Internet	<1%

MSC. ING. GAVINO MARCELO LOYAGA ORGEGOSO
ASESOR

DNI: 16483687

16	repositorio.ucsg.edu.ec Fuente de Internet	<1 %
17	dspace.unach.edu.ec Fuente de Internet	<1 %
18	repositorio.upt.edu.pe Fuente de Internet	<1 %
19	alicia.concytec.gob.pe Fuente de Internet	<1 %
20	www.ccn-cert.cni.es Fuente de Internet	<1 %
21	dspace.espoch.edu.ec Fuente de Internet	<1 %
22	rus.ucf.edu.cu Fuente de Internet	<1 %
23	core.ac.uk Fuente de Internet	<1 %
24	repositorio.uleam.edu.ec Fuente de Internet	<1 %
25	polux.unipiloto.edu.co:8080 Fuente de Internet	<1 %
26	ribuni.uni.edu.ni Fuente de Internet	<1 %
27	pe.isotools.org Fuente de Internet	<1 %
28	repositorio.ujcm.edu.pe Fuente de Internet	<1 %
29	repositorio.upeu.edu.pe Fuente de Internet	<1 %
30	repositorio.uta.edu.ec Fuente de Internet	<1 %
31	repository.uniminuto.edu Fuente de Internet	<1 %
32	estrategia.gobiernoenlinea.gov.co Fuente de Internet	<1 %

MSC. ING. GAVINO MARCELO LOYAGA ORGEGOSO
ASESOR

DNI: 16483687

33	repositorio.ucv.edu.pe Fuente de Internet	<1 %
34	repositorio.unsch.edu.pe Fuente de Internet	<1 %
35	repositorio.unitec.edu.co Fuente de Internet	<1 %
36	repositorio.uns.edu.pe Fuente de Internet	<1 %
37	ri.ujat.mx Fuente de Internet	<1 %
38	worldwidescience.org Fuente de Internet	<1 %
39	www.theibfr.com Fuente de Internet	<1 %
40	docs.google.com Fuente de Internet	<1 %
41	repositorio.uncp.edu.pe Fuente de Internet	<1 %
42	repository.unad.edu.co Fuente de Internet	<1 %
43	damianiso27002.blogspot.com Fuente de Internet	<1 %
44	repositorio.unheval.edu.pe Fuente de Internet	<1 %
45	repositorio.espe.edu.ec Fuente de Internet	<1 %
46	repositorio.uladech.edu.pe Fuente de Internet	<1 %
47	repositorio.unfv.edu.pe Fuente de Internet	<1 %
48	risti.xyz Fuente de Internet	<1 %
49	apirepositorio.unh.edu.pe Fuente de Internet	<1 %
	documents.mx	

DNI: 16483687

50	Fuente de Internet	<1 %
51	repository.ucc.edu.co Fuente de Internet	<1 %
52	dspace-uh-tmp.igniteonline.la Fuente de Internet	<1 %
53	repositorioacademico.upc.edu.pe Fuente de Internet	<1 %
54	pt.slideshare.net Fuente de Internet	<1 %
55	www.asisonline.org Fuente de Internet	<1 %
56	ecomchaco.com.ar Fuente de Internet	<1 %
57	repositorio.upci.edu.pe Fuente de Internet	<1 %
58	www11.urbe.edu Fuente de Internet	<1 %
59	boletines.prisadigital.com Fuente de Internet	<1 %
60	cdn.www.gob.pe Fuente de Internet	<1 %
61	ddd.uab.cat Fuente de Internet	<1 %
62	repositorio.uancv.edu.pe Fuente de Internet	<1 %
63	repositorio.ug.edu.ec Fuente de Internet	<1 %
64	repositorio.unap.edu.pe Fuente de Internet	<1 %
65	repositorio.unsm.edu.pe Fuente de Internet	<1 %
66	repository.unab.edu.co Fuente de Internet	<1 %
67	files.core.ac.uk Fuente de Internet	

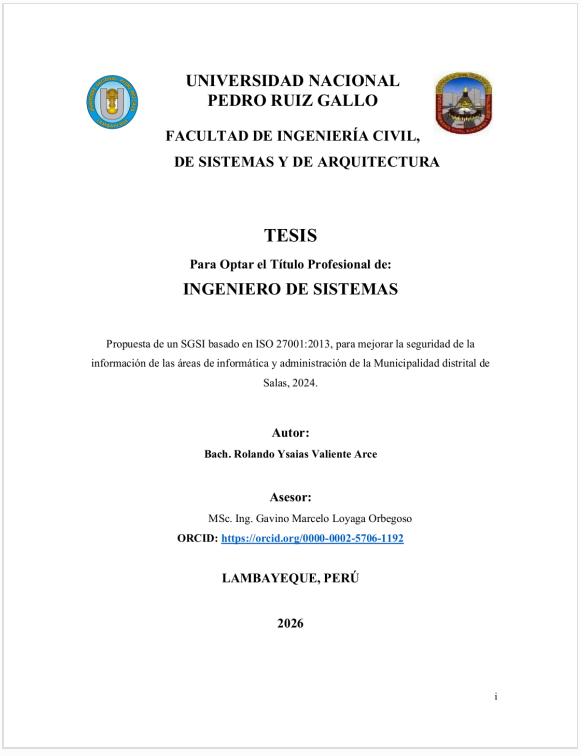
DNI: 16483687

Recibo digital

Este recibo confirma quesu trabajo ha sido recibido por Turnitin. A continuación podrá ver la información del recibo con respecto a su entrega.

La primera página de tus entregas se muestra abajo.

Autor de la entrega:	Rolando Valiente
Título del ejercicio:	Quick Submit
Título de la entrega:	Tesis
Nombre del archivo:	Informe_tesis_-_Rolando_-_SGSI_-_ISO27001_-_MDS.pdf
Tamaño del archivo:	2.97M
Total páginas:	70
Total de palabras:	15,469
Total de caracteres:	95,866
Fecha de entrega:	03-ago-2026 11:43a. m. (UTC-0500)
Identificador de la entrega:	3007678533



UNIVERSIDAD NACIONAL
PEDRO RUIZ GALLO

FACULTAD DE INGENIERÍA CIVIL,
DE SISTEMAS Y DE ARQUITECTURA

TESIS

Para Optar el Título Profesional de:

INGENIERO DE SISTEMAS

Propuesta de un SGSI basado en ISO 27001:2013, para mejorar la seguridad de la información de las áreas de informática y administración de la Municipalidad distrital de Salas, 2024.

Autor:

Bach. Rolando Ysaias Valiente Arce

Asesor:

MSc. Ing. Gavino Marcelo Loyaga Orbegoso

ORCID: https://orcid.org/0000-0002-5706-1192

LAMBAYEQUE, PERÚ

2026

i

MSC. ING. GAVINO MARCELO LOYAGA ORGEGOSO
ASESOR

DNI: 16483687

DEDICATORIA

A Dios, fuente de sabiduría y fortaleza en cada paso de este camino.

A mis padres, Wiston y Doris, pilares fundamentales de mi vida. Por su amor inquebrantable, sus sacrificios silenciosos y la fe que siempre depositaron en mí. Esta conquista es, ante todo, la suya.

A mi esposa, Paola, mi compañera y soporte incondicional. Por tu paciencia infinita, por ser mi refugio en los momentos de mayor presión y por creer en mí incluso cuando yo dudaba. Esta meta se logra contigo y para ti.

A mis hijos, Evelyn Gricelda, Azury Paola y Rolando Manuel, mis motores y razón de ser. Que este logro les enseñe que, con perseverancia y estudio, no hay sueño inalcanzable. Les dedico cada línea de este trabajo con la esperanza de inspirar su propio futuro.

A la memoria de mi hermanito Cristian, cuyo recuerdo puro y amoroso, aun partiendo a los cuatro años, sigue siendo una luz en nuestro corazón. Esta tesis también es para ti, que desde el cielo velas por la familia.

A mis hermanos, Wiston y María, por su apoyo constante y por ser cómplices en la travesía de la vida.

AGRADECIMIENTO

Mi más sincero y profundo agradecimiento a:

A la Universidad Nacional Pedro Ruiz Gallo, mi alma máter, por brindarme las herramientas académicas y los valores para mi formación profesional. En especial, a mi Asesor de Tesis, MSc. Ing. Gavino Marcelo Loyaga Orbegoso, por su guía experta, sus valiosas críticas constructivas y su disponibilidad durante todo el proceso de investigación. Su conocimiento y dedicación fueron fundamentales para dar forma y rigor a este trabajo.

A los docentes de la Escuela Profesional de Ingeniería de Sistemas, cuyo conocimiento, entrega y pasión por la enseñanza dejaron una huella imborrable en mi perfil profesional.

A mis compañeros de estudio y amigos, en especial al grupo con el que compartí tantas horas de proyectos y aprendizaje colaborativo. Su compañerismo hizo más llevadero el camino.

De manera muy especial, a mi familia (mencionada en la dedicatoria), por ser el sostén emocional que me permitió dedicar el tiempo y la energía necesarios para culminar este proyecto. Sin su red de amor y comprensión, este objetivo no habría sido posible.

Finalmente, a todas las personas que, de una u otra forma, contribuyeron con un grano de arena a la realización de este sueño. Mi eterna gratitud.

RESUMEN

En los ultimos cinco años, se ha evidenciado que muchos estudios coinciden que la información es uno de los activos más importantes de las entidades publicas y empresas privadas, de modo que las organizaciones deben resguardar dichas informaciones y los activos de información; por ello, através de una breve entrevista a los trabajadores de la municipalidad distrital de Salas, manifestaron que, en los ultimos años han tenido pérdida de información, si bien no fueron incidencias graves, se encuentran preocupados, puesto que en la municipalidad no cuentan con politicas y controles de seguridad necesaria para proteger a la información sensible; por ello, en la presente investigación se planteó el objetivo de proponer un modelo de SGSI basado en ISO 27001:2013, para garantizar la seguridad de la información del área de informática y administración de la Municipalidad Distrital de Salas; para lograrlo, se realizó un estudio con enfoque cuantitativo, con diseño no experimental, con alcance descriptivo, asimimo se empleó la metodología del ciclo de Deming para el modelado de SGSI y metodología Magerit, para la etapa de análisis de riesgos; en cuanto a los resultados, revelaron que, el 70% de los tipos de activos de información tienen un valor alto y tienen una criticidad alta; por otro lado, sólo los anexos A.5, A.13 y A.18 de ISO 27001:2013 tienen un porcentaje de implementación aceptable, por lo que la propuesta, contempla la implementación de controles necesario de manera progresiva en un año, asimismo efatiza la capacitación, puesto que el 60% de personal entrevistado desconocian los protocolos de reporte de incidencias de seguridad de la información. Finalmente se concluye que el modelo del SGSI está descrita siguiendo rigurosamente las pautas del ciclo de Deming y fue validada por 3 expertos, de manera que el modelo puede ser adaptada e implementada por otras municipalidades o entidades públicas.

Palabras clave: Seguridad de la información, SGSI para municipalidad de salas, Metodología Magerit, ISO27001/2013

ABSTRACT

In the last five years, many studies have shown that the Information is one of the most important assets of public entities and companies private, so organizations must safeguard such information and the information assets Therefore, through a brief interview with the workers of the The district municipality of Salas stated that, in recent years, they have experienced data loss. While these incidents were not serious, they are concerned because the municipality lacks the necessary security policies and controls to protect sensitive information. Therefore, this research aimed to propose an Information Security Management System (ISMS) model based on ISO 27001:2013 to guarantee the security of information in the IT and administration area of the Salas District Municipality. To achieve this, a quantitative study with a nonexperimental, descriptive design was conducted. The Deming cycle methodology was used for ISMS modeling, and the Magerit methodology was employed for the risk analysis stage. The results revealed that 70% of the information asset types have high value and high criticality. On the other hand, only Annexes A.5, A.13, and A.18 of ISO 27001:2013 have an acceptable implementation rate. Therefore, the proposal contemplates the progressive implementation of the necessary controls over one year. It also emphasizes training, since 60% of the personnel interviewed were unaware of the information security incident reporting protocols. Finally, it is concluded that the ISMS model is described following the Deming cycle guidelines and was validated by three experts, so the model can be adapted and implemented by other municipalities or public entities.

Keywords: Information security, ISMS for Salas municipality, Magerit methodology, ISO27001/2013

INDICE DE CONTENIDO

RESUMEN vii
ABSTRACT viii
INDICE DE CONTENIDO ix
INDICE DE TABLAS xii
ÍNDICE DE FIGURAS xiii
I. NTRODUCCIÓN 14
1.1. Planteamiento de la Investigación 14
1.1.1. Síntesis de la Situación Problemática 14
1.1.2. Formulación del problema de investigación 15
1.2. Objetivos 15
1.2.1. Objetivo general 15
1.2.2. Objetivos específicos 15
II. MARCO TEÓRICO 16
2.1. Antecedentes 16
2.2. Bases teóricas 21
2.2.1. Sistema de gestión de seguridad de la información 21
2.2.2. Seguridad de la información 22
2.2.3. ISO/IEC 27001:2013 23
2.2.4. Metodología MAGERIT 24
2.2.5. Ciclo de Deming 25
2.2.5.1. Planificar (Plan) 25
2.2.5.2. Hacer (Do) 26
2.2.5.3. Verificar (Check) 26
2.2.5.4. Actuar (Act) 26
2.3. Marco conceptual 27
2.3.1. Activo de información 27
2.3.2. Valor de activo de información 28
2.3.3. Impacto 28
2.3.4. Riesgo 29
2.3.5. Probabilidad 29
2.3.6. Amenazas 30
2.3.7. Degradación 30
III. DISEÑO METODOLÓGICO 31

3.1. Tipo de investigación 31
3.1.1. La investigación básica....31
3.2. Enfoque de la Investigación 31
3.2.1. Enfoque cuantitativo,....31
3.3. Diseño de Investigación 32
3.3.1. El diseño no experimental 32
3.4. Nivel de investigación 32
3.4.1. Descriptivo 32
3.5. Las variables de estudio: 33
3.6. Operacionalización de Variables 34
3.7. Población y muestra 35
3.7.1. Población....35
3.7.2. Muestra....35
3.7.3. Muestreo....35
3.8. Técnicas, instrumentos, equipos y materiales 35
3.9. Procedimientos....35
3.10. Método de análisis de datos....36
IV. RESULTADOS....37
4.1. Modelo de SGSI para MDS....37
4.1.1. Plan (Planificar)....37
4.1.1.1. Analizar los controles y políticas actuales 37
4.1.1.2. Alcance del SGSI 45
4.1.1.3. Stakeholders del SGSI 45
4.1.1.4. Análisis y gestión de riesgos (Magerit)....48
4.1.1.5. Tratamiento de riesgos....50
4.1.1.6. Selección de controles de seguridad 51
4.1.1.7. Políticas y procedimientos del SGSI-MDS....51
4.1.2. Do (Hacer o ejecutar) 53
4.1.2.1. Plan de formación y concienciación 53
4.1.3. Check (Verificar o Revisar)....56
4.1.3.1. Matriz para la medición de la eficiencia del SGSI 56
4.1.3.1. KPIs de interés de alta directiva....56
4.1.4. Act (Actuar o ajustar) 57
4.1.4.1. Matriz de ajustes del modelo de SGSI 57
4.2. Validar el modelo propuesto....57
V. Discusión de resultados 58
VI. CONCLUSIONES 60

VII. RECOMENDACIONES.....62
BIBLIOGRAFÍA 63
ANEXOS 66

INDICE DE TABLAS

Tabla 1 *Operacionalización de variables* 34
Tabla 2 *Identificación de los activos de información de MDS* 43
Tabla 3 *Análisis de controles actuales* 44
Tabla 4 *Roles y funciones del equipo SGSI* 46
Tabla 5 *Análisis y gestión de riesgos* 48
Tabla 6 *Calificativo de riesgo* 48
Tabla 7 *Calificativo de amenaza* 49
Tabla 8 *Calificativo de vulnerabilidad* 49
Tabla 9 *Calificativo de probabilidad de ocurrencia* 49
Tabla 10 *Calificativo de Consecuencia* 50
Tabla 11 *Tratamiento de riesgos* 50
Tabla 12 *Selección de controles de seguridad según la 27001:2013* 51
Tabla 13 *Matriz de capacitación* 53
Tabla 14 *Matriz para las actividades de implementación y operación* 54
Tabla 15 *Matriz para la medición de la eficiencia del SGSI* 56
Tabla 16 *KPIs de interés de alta directiva* 56
Tabla 17 *Matriz de ajustes del modelo de SGSI* 57

ÍNDICE DE FIGURAS

Figura 1 *Ciclo de Deming* 27
Figura 2 *Procedimiento de la ejecución de la investigación* 36
Figura 3 *Organigrama de municipalidad distrital de Salas* 39
Figura 4 *Organigrama que interviene el proceso de requerimiento y conformidad de pagos a terceros* 40
Figura 5 *Organigrama para el SGSI en la MDS* 47

I. NTRODUCCIÓN

1.1. Planteamiento de la Investigación

1.1.1. Síntesis de la Situación Problemática

En el ámbito internacional, la seguridad de la información , es un tema de mucha importancia para las organizaciones, puesto que se ha incrementado los riesgos y las vulnerabilidades de la información, dicho incremento es por el auge de las conexiones virtuales y el trabajo remoto; asimismo, se estima que las organizaciones pierden aproximadamente el 5% de sus ingresos de manera anual, por algún tipo de fraude o corrupción; por ello, la estimación total de pérdidas económicas a nivel mundial es de 4,7 trillones de dólares (Novasoft, 2023). Por otro lado, se manifiesta que hay un incremento de brechas de seguridad de la información debido a escasa habilidad en ciberseguridad, puesto que entre el año 2021 y el 2022, las organizaciones sufrieron el incremento de un 53% de 5 o más brechas de seguridad, por lo que se necesitarían 3.40 millones profesionales para cubrir dichos déficit de personal en ciberseguridad; asimismo, se manifiesta que el 68% de las organizaciones se enfrentan a riesgos cibernéticos adicionales, puesto que hay escasez de personal para cubrir los puestos de trabajo en las áreas de tecnologías de la información (DatacenterDynamics, 2023).

En el ámbito nacional, se manifiesta que, con el avance de la digitalización y el incremento de trabajo remoto, las organizaciones se encuentran a mayor riesgo de ser víctimas de robo de información, puesto que el 95% de los problemas de robo de información, es por descuidos del recurso humano, debido a esta realidad, BASC Perú, el 14 de febrero del 2023, concientizó a más de 450 empleados de las empresas certificadas a nivel nacional, mediante el seminario llamado “el valor de proteger la información, las personas y las organizaciones” (BASC, 2023).

A nivel local, las organizaciones y entidades públicas no son ajenos a esta realidad, puesto que en la Municipalidad Distrital de Salas, donde se entrevistó a 9 colaboradores del área de sistemas y administración, mediante la cual manifestaron que durante el año 2023, se presentaron incidencias de pérdidas de información, un aproximado de 20 informaciónes de tipo digital y en físico; si bien, dichas pérdidas de información no fueron tan catastróficos

para la Municipalidad, los empleados de dicha área se encuentran preocupados porque se pueden presentar más casos de robos de información que afecte al flujo de procesos de dicha área. Por todo lo antes mencionados, se propone una solución, mediante una propuesta de un Sistema de Gestión de Seguridad de la información (SGSI), el mismo que tendrá la finalidad de mitigar los riesgos de robo de información de la Municipalidad Distrital de Salas.

1.1.2. Formulación del problema de investigación

¿Un modelo de SGSI basado en ISO 27001:2013, podrá mejorar la seguridad de la información del área de informática y administración de la Municipalidad Distrital de Salas?

1.2. Objetivos

1.2.1. Objetivo general

Proponer un modelo de SGSI basado en ISO 27001:2013, para mejorar la seguridad de la información del área de informática y administración de la Municipalidad Distrital de Salas, 2024.

1.2.2. Objetivos específicos

- ✓ Analizar los controles y políticas actuales respecto a la seguridad de la información, para identificar los riesgos de pérdida de la información.
- ✓ Identificar los controles y políticas adecuados de seguridad de la información, para las áreas de informática y administración de la Municipalidad Distrital de Salas.
- ✓ Elaborar plan de acción, para la fase de implementación y operación del SGSI basado en ISO 27001:2013 propuesto.
- ✓ Validar el modelo propuesto de SGSI basado en ISO 27001:2013, para proteger la información de las áreas de informática y administración de la Municipalidad Distrital de Salas.

II. MARCO TEÓRICO

2.1. Antecedentes

Para determinar el uso de la inteligencia artificial a través del Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO 27001, se realizó una investigación no experimental, transversal, de enfoque mixto y de nivel descriptivo. Entre los resultados de dicha investigación, se identificaron los activos informáticos de la organización y se analizaron los riesgos, sugiriendo desarrollar un plan de prevención y seguimiento a los riesgos, analizar la implementación de IA y sus resultados. El estudio determinó que no es recomendable involucrar sistemas y herramientas tecnológicas en la rehabilitación social o inteligencia artificial en dispositivos electrónicos antes de establecer un SGSI-ISO/IEC27001 porque no garantiza su funcionamiento. rehabilitación social, como también IA en mecanismos electrónicos, ya que no se asegura su funcionamiento. (Donoso, et al, 2023).

Hernández et al. (2024), desarrollaron una investigación propositiva de un plan de implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma NTC-ISO/IEC 27001:2013; Dicha investigación se realizó en una institución de educación superior, con el propósito de fortalecer la seguridad de los activos de información y reducir las amenazas que vulneran la confidencialidad, integridad y disponibilidad de la información institucional. En cuanto a la metodología, la investigación fue abordada de manera aplicada, no experimental, de tipo descriptiva-propositiva; así como tambien se empleó el ciclo de mejora continua Plan-Do-Check-Act (PDCA). Obteniendo resultados que revelaron que la institución tiene fallas en la forma en que gestiona la seguridad de la información, principalmente por la ausencia de políticas formales, procedimientos documentados y controles de seguridad alineados a estándares internacionales. Concluyendo que, un SGSI basado en la norma ISO/IEC 27001:2013, es viable, adaptable y es una estrategia que permite reducir los riesgos asociados a la seguridad de la información, estandarizar procesos y fortalecer la cultura de seguridad dentro de la organización.

La investigación de Gala, Suwandaru y Anshar (2025), con el objetivo de analizar el nivel de implementación de la norma ISO/IEC 27001:2013 en PT. Bank Sulselbar, emplearon la

metodología, como tipo analítico-descriptivo, con diseño no experimental, asimismo, emplearon técnicas como entrevistas, revisión de documentos y listas de verificación fundamentadas en la norma ISO/IEC 27001:2013, para recopilar datos; de manera que se encontró los resultados que revelan que la organización había implementado parcialmente los controles de seguridad de la información, evidenciando mejoras en la gestión de accesos, protección de activos de información y definición de responsabilidades de seguridad. Sin embargo, se identificaron fallas en la gestión de riesgos, que no apoya a la sostenibilidad del SGSI en el tiempo; por otro lado, los autores consideran que se debe fortalecer la mejora continua del SGSI, formalizando procesos, capacitando continuamente al personal y analizando periódicamente los riesgos, puesto que, son beneficiosos para la gestión de seguridad de la información, fortaleciendo la protección de la información crítica y el control interno.

Por su parte, Fernández (2023), desarrolló una investigación con el objetivo de proponer la implementación de un SGSI basado en la norma ISO/IEC 27001:2013. Con el propósito de proteger los activos de información del área de tecnologías de la información de la Alcaldía Distrital de Las Zanjas. Para ello, realizó una investigación con enfoque aplicado, no experimental, de alcance descriptivo y propositivo, inicialmente realizó un análisis de riesgos que permitió identificar activos críticos, amenazas, vulnerabilidades y niveles de riesgo asociados con la gestión de la información en el área TI. Mediante la cual, los resultados revelaron que la organización tenía serias deficiencias como: ausencia de políticas formales, procedimientos documentados y controles de seguridad estandarizados; Asimismo, el investigador manifiesta que, un SGSI basado en la norma ISO/IEC 27001:2013, podría reducir los riesgos de pérdida, modificación o divulgación no autorizada de información. Además, la propuesta es viable y aplicable en las organizaciones del sector público, específicamente en el área de informática, en donde se concentran los activos de información críticos y los procesos tecnológicos para la gestión institucional.

A nivel nacional, para disminuir los riesgos de pérdida de información a un nivel aceptable, se planteó como objetivo diseñar un SGSI basado en la ISO/IEC 27001:2014 para la empresa ITS Business SAC. Para ello, se llevó a cabo una investigación de diseño no

experimental, descriptiva, donde la muestra estuvo conformada por seis trabajadores de la empresa ITS Business SAC. El diseño del SGSI se realizó en tres etapas: diagnóstico, preparación y planificación. A través de estas etapas se definió el alcance del SGSI, se usó la metodología MAGERIT V3 para el análisis de riesgos y definición de controles. Se determinó que la empresa ITS Business SAC logró la certificación ISO/IEC 27001 gracias al diseño del SGSI (Huamalí, 2021).

Para mejorar el porcentaje de incidencias de pérdida de información en Soltesi S.A.C, planteó como objetivo determinar la influencia de un SGSI en la empresa. Para ello, se realizó una investigación aplicada, de diseño experimental (preexperimental) y de alcance explicativo, utilizando como muestra 22 fichas de registro de incidencias. Se logró que la solución de incidencias sobre integridad informativa mejorara de 32 % a 75 %, y que con UGELs en la región Lambayeque este mejorara de 17 % a 81 %. Cabe mencionar que las auditorías se realizaron antes y 1 mes después de la implementación del SGSI. Finalmente, el estudio determinó que el SGSI mejoró la seguridad de la información en Soltesi S.A.C. (Poma, 2021).

La investigación de Ruiz Loo (2024) buscó analizar el Sistema de Gestión de Seguridad de la Información (SGSI) en el área de Seguridad, Gobierno y Servicio de Scotiabank Perú S.A., según la norma ISO/IEC 27001. El objetivo era verificar la efectividad y el cumplimiento de los controles de seguridad implementados.

La investigación fue descriptiva-evaluativa, no experimental en su metodología. Para la recopilación de datos se emplearon técnicas como entrevistas, revisión de documentos y listas de verificación basadas en los controles del Anexo A y los requisitos de la norma ISO/IEC 27001. También se realizó una revisión del estado de los procedimientos de gestión de seguridad de la información, lo que permitió identificar fortalezas y debilidades en la implementación del SGSI.

Los resultados indicaron que la subárea evaluada cumple en gran medida con los requisitos de la norma, sobre todo en lo que se refiere a la gestión de accesos, protección de activos informáticos y definición de roles y responsabilidades de seguridad. Pero se identificaron oportunidades de mejora en la gestión de riesgos, en la documentación de

procedimientos y en la mejora continua del SGSI. Esto podría comprometer la sostenibilidad del sistema en el futuro.

En conclusión, la investigación determinó que la evaluación del SGSI en base a la norma ISO/IEC 27001 permite conocer de manera objetiva el nivel de madurez del sistema y las principales áreas de mejora. El autor llega a la conclusión de que la aplicación de la norma de forma continua mejora la administración de la seguridad de la información y reduce los riesgos en caso de incidentes de seguridad. Indica que los resultados obtenidos pueden servir de guía a otras organizaciones, incluso públicas, que deseen auditar o mejorar su SGSI en sectores como las tecnologías de la información y los servicios tecnológicos.

León y Tufino (2025), desarrollaron una investigación en la Municipalidad Distrital de Santa María, buscando analizar la relación entre el Sistema de Gestión de Seguridad de la Información (SGSI) y la gestión del riesgo informático; realizando estudio con un enfoque cuantitativo, diseño no experimental y de alcance descriptivo-correlacional, teniendo como muestra de estudio al personal del área de informática y las unidades administrativas que manejan información. Mediante la cual, los resultados indicaron que la municipalidad aplica en un nivel medio el SGSI, fallando principalmente en la identificación y tratamiento de riesgos, capacitación del personal y definición de políticas de seguridad; a su vez, existe una dependencia entre el sistema de gestión de seguridad de la información y la gestión de riesgos. Finalmente concluyen que, para fortalecer la gestión de riesgos de información en entidades públicas como los municipios, se debe implementar un SGSI con el propósito de fortalecer la protección de los activos de información, reducir la probabilidad de incidentes de seguridad y fortalecer la toma de decisiones en la administración pública.

A nivel local y regional, desarrollar un modelo integral de seguridad de la información que apoye en fortalecer la seguridad de los activos de información financiera que se encuentran en las entidades públicas. El estudio se fundamentó en la problemática actual relacionada con la falta de un marco estructurado de seguridad de la información, exponiendo a las Unidades de Gestión Educativa Local a riesgos que atentan contra la confidencialidad, integridad y disponibilidad de la información financiera; en cuanto al enfoque metodológico, se utilizó el enfoque cuantitativo, con diseño no experimental de nivel descriptivo-propositivo. Para la recolección de datos, se emplearon técnicas como la revisión documental

y la aplicación de instrumentos dirigidos al personal responsable de la gestión de la información financiera, lo que permitió diagnosticar el estado actual de la seguridad de la información en las UGEL de la región Lambayeque; mediante la cual los resultados evidenciaron deficiencias en la gestión de riesgos, inexistencia de políticas de seguridad, limitada concienciación del personal y escasa implementación de controles técnicos y administrativos, puesto que, cumplían solo con el 32% de controles recomendados por la ISO/IEC 27001 y además el modelo propuesto, fue expuesta a la revisión de profesionales expertos, quienes manifestaron que el modelo propuesto tiene una confiabilidad del 72%; por tanto, aporta fundamentos teóricos y metodológicos sobre la implementación de modelos de seguridad de la información en instituciones públicas, además de evidenciar la necesidad de adoptar enfoques sistemáticos para la gestión del riesgo y la protección de la información sensible (Taboada, 2021).

Por su parte, Baca (2023), Para fortalecer la protección de los activos de información y mejorar la gestión de riesgos en los procesos tecnológicos y administrativos de una institución pública, desarrolló una investigación para diseñar un Sistema de Gestión de Seguridad de la Información (SGSI) para la Unidad de Gestión Educativa Local (UGEL) Chiclayo, basado en las normas ISO/IEC 27001:2013 e ISO/IEC 27002. Para ello, empleó una investigación aplicada, con un diseño no experimental y de alcance descriptivo-propositivo. Se utilizaron técnicas como el análisis documental, entrevistas al personal del área de informática y listas de verificación basadas en los controles definidos en la norma ISO/IEC 27001 para realizar un diagnóstico de la situación actual. Asimismo, se identificaron y clasificaron los activos de información y se valoraron las amenazas, vulnerabilidades y riesgos, lo que permitió determinar el nivel de cumplimiento de la entidad con el estándar.

Como hallazgos, el diagnóstico arrojó que la gestión de la seguridad de la información era altamente deficiente, ya que no contaba con políticas formales, procedimientos documentados ni controles estandarizados de seguridad. El estudio, de tipo cuantitativo, halló que gran parte de los controles evaluados presentaban un cumplimiento bajo o nulo. Esto elevaba el riesgo de los activos informáticos críticos de la UGEL Chiclayo. Con base en estos hallazgos se desarrolló un SGSI, el cual incluye políticas de seguridad, objetivos de control, procedimientos operativos y controles específicos del Anexo A de la norma ISO/IEC 27001. Su objetivo es reducir los riesgos identificados.

Finalmente, los resultados mostraron que desarrollar un SGSI basado en la norma ISO/IEC 27001 es una herramienta para mejorar la gestión de la seguridad de la información en las organizaciones públicas del sector educativo. El autor indica que la implementación del sistema propuesto reduciría los riesgos de pérdida, alteración o divulgación no autorizada de la información. Además, fortalecería la cultura de seguridad de la información en la institución y podría ser replicado en otras instituciones públicas con características similares.

2.2. Bases teóricas

2.2.1. Sistema de gestión de seguridad de la información

De acuerdo con la International Organization for Standardization y la International Electrotechnical Commission, el SGSI es el marco que permite a una organización establecer, implementar, operar, supervisar, revisar, mantener y mejorar continuamente la seguridad de la información, adoptando un enfoque basado en la gestión del riesgo. La norma ISO/IEC 27001:2013 define los requisitos que deben cumplirse para asegurar una protección adecuada de la información en función del contexto organizacional y de los riesgos identificados (ISO/IEC, 2013).

Desde la perspectiva de autores especializados en seguridad de la información, Whitman y Mattord (2018) señalan que el SGSI integra de manera coherente los componentes técnicos, organizacionales y humanos de la seguridad, permitiendo una gestión integral de los riesgos de información. Los autores enfatizan que un SGSI eficaz no se limita a la implementación de controles tecnológicos, sino que promueve una cultura organizacional orientada a la seguridad.

Por su parte, Stallings (2019) define el SGSI como un enfoque sistemático para la gestión de la seguridad de la información que busca reducir los riesgos a niveles aceptables mediante la aplicación continua de políticas, procedimientos y controles. El autor destaca que la adopción de un SGSI facilita la identificación temprana de vulnerabilidades y fortalece la capacidad de respuesta ante incidentes de seguridad.

Asimismo, Calder y Watkins (2010) sostienen que el SGSI es un elemento clave de la gobernanza de la seguridad de la información, ya que promueve la participación de la alta dirección, la asignación clara de responsabilidades y la mejora continua del sistema. Según los autores, la implementación de un SGSI basado en estándares internacionales contribuye

a fortalecer la confianza de las partes interesadas y a asegurar el cumplimiento normativo. Es un conjunto de normas, prácticas y prácticas utilizadas para administrar, controlar, resguardar y mejorar la seguridad de la información de una organización; El SGSI protege la información de la organización contra riesgos de seguridad como acceso no autorizado, robo, destrucción y modificación. Además, está baasada en estándares y marcos de referencia, como la norma ISO 27001, y es aplicada a la gestión de los procesos relacionados con la protección de la información, como la evaluación de riesgos, la implementación de controles de seguridad, la formación y concientización del personal y la mejora continua (Culot et al., 2021). Por otro lado, mediante la implementación de un sistema de gestión de seguridad de la información (SGSI) de acuerdo con la norma ISO 27001, se pueden establecer diagnósticos, gestión de riesgos, mecanismos adecuados y seguimiento de equipos. Los resultados muestran que el uso de dispositivos electrónicos, la vigilancia interactiva y la inteligencia artificial para el seguimiento de personas privadas de libertad pueden crear escenarios preventivos y proactivos para las decisiones de políticas públicas en el área de seguridad, así como un mecanismo para mejorar la gestión pública (Donoso et al., 2023).

2.2.2. Seguridad de la información

De acuerdo con la International Organization for Standardization y la International Electrotechnical Commission, la seguridad de la información se define como la preservación de la confidencialidad, integridad y disponibilidad de la información, incluyendo otras propiedades como la autenticidad, trazabilidad y no repudio. Esta definición resalta que la información debe ser protegida independientemente de su forma, ya sea física, digital o verbal (ISO/IEC, 2013). Desde la perspectiva de autores especializados, Whitman y Mattord (2018) señalan que la seguridad de la información comprende las medidas adoptadas para proteger los activos informacionales contra amenazas internas y externas, destacando que su gestión efectiva requiere un enfoque integral que incluya aspectos tecnológicos, organizacionales y humanos. Los autores enfatizan que la seguridad de la información no es un estado estático, sino un proceso continuo de gestión y mejora. Por su parte, Stallings (2019) define la seguridad de la información como la protección de los sistemas de información y los datos que estos procesan frente a riesgos que puedan comprometer su funcionamiento y confiabilidad. El autor subraya que una adecuada seguridad de la información es fundamental para garantizar la confianza de los usuarios y la continuidad del

negocio. Asimismo, Pfleeger y Pfleeger (2015) sostienen que la seguridad de la información implica la implementación de controles preventivos, detectivos y correctivos, orientados a minimizar el impacto de incidentes de seguridad. Según los autores, la seguridad de la información debe integrarse en los procesos organizacionales y alinearse con los objetivos estratégicos de la institución.

2.2.3. ISO/IEC 27001:2013

De acuerdo con la International Organization for Standardization y la International Electrotechnical Commission, la ISO/IEC 27001:2013 proporciona un marco estructurado que permite a las organizaciones identificar los riesgos que afectan a la información, evaluarlos y aplicar controles adecuados para reducirlos a niveles aceptables. La norma enfatiza que la seguridad de la información debe gestionarse como un proceso continuo, alineado con los objetivos estratégicos de la organización y adaptado a su contexto interno y externo (ISO/IEC, 2013). Desde la perspectiva de autores especializados en seguridad de la información; Whitman y Mattord (2018), señalan que la ISO/IEC 27001:2013 constituye uno de los estándares más reconocidos para la gestión de la seguridad de la información, debido a su enfoque integral y basado en riesgos. Los autores destacan que la norma no se limita a aspectos técnicos, sino que incorpora componentes organizacionales, legales y humanos, lo que facilita una protección más efectiva de los activos de información.

Por su parte, Stallings (2019) indica que la ISO/IEC 27001:2013 permite establecer políticas, procedimientos y controles de seguridad de manera coherente y sistemática, favoreciendo la mejora continua del SGSI. Según el autor, la adopción de esta norma contribuye a fortalecer la resiliencia organizacional frente a incidentes de seguridad y ciberamenazas. Asimismo, Calder y Watkins (2010) sostienen que la ISO/IEC 27001:2013 proporciona una base sólida para la gobernanza de la seguridad de la información, ya que promueve la responsabilidad de la alta dirección, la asignación adecuada de recursos y la integración de la seguridad en los procesos del negocio. Los autores resaltan que su aplicación es especialmente relevante en organizaciones que gestionan información sensible o crítica, como las entidades públicas.

2.2.4. Metodología MAGERIT

De acuerdo con su definición oficial, MAGERIT es una metodología que proporciona los principios, técnicas y herramientas necesarias para la gestión sistemática de los riesgos de los sistemas de información, con el objetivo de reducirlos a niveles aceptables mediante la implementación de salvaguardas adecuadas. La metodología se basa en la identificación de activos, amenazas y vulnerabilidades, así como en la evaluación de la probabilidad y el impacto de los riesgos asociados (Consejo Superior de Administración Electrónica [CSAE], 2012). MAGERIT establece un proceso ordenado que comprende etapas como la identificación y valoración de activos, el análisis de amenazas y vulnerabilidades, la estimación de riesgos, la evaluación del impacto y la definición de medidas de tratamiento del riesgo. Asimismo, incorpora conceptos clave como la degradación de los activos y la dependencia entre ellos, permitiendo un análisis integral de la seguridad de la información (CSAE, 2012). Desde el punto de vista de su alineación con estándares internacionales, la metodología MAGERIT es compatible con la norma ISO/IEC 27005, ya que ambas promueven un enfoque basado en la gestión del riesgo como eje central de la seguridad de la información. En este sentido, MAGERIT puede ser utilizada como una herramienta práctica para apoyar la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) conforme a la norma ISO/IEC 27001:2013 (ISO/IEC, 2018).

Por su parte, Gómez y Martínez (2017) señalan que MAGERIT es una metodología especialmente adecuada para el sector público, debido a su enfoque sistemático, su lenguaje claro y su capacidad para adaptarse a diferentes contextos organizacionales. Los autores destacan que MAGERIT facilita la toma de decisiones al proporcionar criterios objetivos para la priorización de riesgos y la selección de controles de seguridad. Asimismo, Whitman y Mattord (2018), desde una perspectiva general de la seguridad de la información, resaltan la importancia de metodologías formales de análisis de riesgos como MAGERIT, ya que permiten identificar de manera estructurada las amenazas y evaluar sus impactos, contribuyendo a una gestión eficaz de la seguridad y a la protección de los activos críticos de información.

2.2.5. Ciclo de Deming

En el contexto de la seguridad de la información, la norma ISO/IEC 27001:2013 adopta explícitamente el ciclo PDCA como fundamento para la gestión del SGSI. En la fase Plan, se establecen las políticas de seguridad, se identifican los activos de información y se realiza el análisis y tratamiento de riesgos. En la fase Do, se implementan y operan los controles de seguridad definidos. En la fase Check, se monitorea y evalúa el desempeño del SGSI mediante auditorías internas y revisiones. Finalmente, en la fase Act, se aplican acciones correctivas y de mejora para fortalecer continuamente la seguridad de la información (ISO/IEC, 2013). Desde la perspectiva de autores especializados en seguridad de la información, Whitman y Mattord (2018) señalan que el uso del ciclo PDCA permite mantener la seguridad como un proceso dinámico, en el que las políticas y controles se ajustan continuamente en función de los cambios en el entorno de amenazas. Los autores destacan que este enfoque es esencial para garantizar la eficacia a largo plazo de los sistemas de seguridad de la información. De manera similar, Stallings (2019) afirma que la aplicación del ciclo de Deming en la gestión de la seguridad de la información facilita la integración de la seguridad en los procesos organizacionales, asegurando que los controles no solo se implementen, sino que sean evaluados y mejorados de forma permanente.

2.2.5.1. Planificar (Plan)

La fase Planificar consiste en establecer los objetivos, políticas, procesos y procedimientos necesarios para lograr los resultados esperados. En el contexto de la seguridad de la información, esta etapa implica identificar los activos de información, analizar y evaluar los riesgos, definir los controles de seguridad y establecer un plan de tratamiento del riesgo acorde con los objetivos de la organización. De acuerdo con la ISO/IEC 27001:2013, la fase de planificación es fundamental para definir el alcance del SGSI y adoptar un enfoque basado en riesgos, permitiendo seleccionar controles adecuados para proteger la confidencialidad, integridad y disponibilidad de la información (ISO/IEC, 2013). Autores como Whitman y Mattord (2018) destacan que una planificación adecuada es clave para asegurar la coherencia entre los riesgos identificados y los controles implementados.

2.2.5.2. Hacer (Do)

La fase Hacer se refiere a la implementación y operación de los procesos planificados. En seguridad de la información, esta etapa implica ejecutar los controles definidos, capacitar al personal, asignar responsabilidades y poner en marcha los procedimientos de seguridad establecidos en el SGSI.

Según Calder y Watkins (2010), esta fase permite materializar las políticas de seguridad en acciones concretas, integrando los controles técnicos, organizativos y humanos. Los autores señalan que la correcta ejecución del SGSI depende en gran medida del compromiso del personal y del liderazgo de la alta dirección.

2.2.5.3. Verificar (Check)

La fase Verificar consiste en supervisar, medir y evaluar el desempeño de los procesos implementados, comparando los resultados obtenidos con los objetivos y políticas establecidos. En el ámbito de la seguridad de la información, esta etapa incluye auditorías internas, revisiones de cumplimiento, análisis de incidentes y medición de indicadores de desempeño del SGSI.

De acuerdo con Pfleeger y Pfleeger (2015), la verificación permite identificar desviaciones, debilidades y oportunidades de mejora en los controles de seguridad, contribuyendo a una gestión proactiva de los riesgos. La ISO/IEC 27001:2013 enfatiza la importancia de esta fase para asegurar la eficacia del SGSI y el cumplimiento de los requisitos normativos.

2.2.5.4. Actuar (Act)

La fase Actuar se orienta a la aplicación de acciones correctivas y preventivas basadas en los resultados de la fase de verificación. En seguridad de la información, esta etapa implica corregir las no conformidades detectadas, mejorar los controles existentes y actualizar las políticas y procedimientos del SGSI.

Según Stallings (2019), la fase de actuación es esencial para fortalecer la madurez de1 sistema de seguridad de la información, ya que permite adaptar el SGSI a los cambios del entorno tecnológico y a la evolución de las amenazas. Esta fase cierra el ciclo y da inicio a una nueva iteración de mejora continua.

Figura 1

Ciclo de Deming

Nota. tomada de (Cajahuamán, 2021).

2.3. Marco conceptual

2.3.1. Activo de información

Según la metodología MAGERIT, un activo de información se define como todo elemento que tiene valor para la organización y que es necesario para el logro de sus objetivos, incluyendo no solo la información en sí, sino también los recursos que la soportan, procesan o transmiten. MAGERIT clasifica los activos en distintas categorías, tales como información, servicios, aplicaciones, equipos, redes, instalaciones y personas, resaltando que la pérdida de confidencialidad, integridad o disponibilidad de estos activos puede generar impactos significativos en la organización (Consejo Superior de Administración Electrónica [CSAE], 2012).

Desde la perspectiva de la norma ISO/IEC 27001:2013, los activos de información comprenden la información y los elementos asociados a su tratamiento, tales como sistemas, procesos, recursos humanos y tecnológicos. La norma enfatiza que estos activos deben ser identificados, inventariados y protegidos de manera adecuada, de acuerdo con su nivel de criticidad y el riesgo al que se encuentran expuestos, con el fin de garantizar la confidencialidad, integridad y disponibilidad de la información (ISO/IEC, 2013).

Por su parte, Whitman y Mattord (2018) señalan que los activos de información incluyen datos, información y conocimiento, así como los componentes físicos y lógicos que permiten su almacenamiento, procesamiento y transmisión. Los autores destacan que la correcta identificación de los activos es un paso fundamental para una gestión efectiva de la seguridad de la información, ya que permite priorizar los esfuerzos de protección y asignar controles adecuados. Asimismo, Stallings (2019) define los activos de información como los recursos críticos que respaldan las operaciones de una organización y que, en caso de ser comprometidos, pueden afectar la continuidad del negocio y la confianza de los usuarios. Desde este enfoque, los activos no se limitan a los sistemas informáticos, sino que abarcan procesos, servicios y personas involucradas en el ciclo de vida de la información.

2.3.2. Valor de activo de información

Asimismo, MAGERIT señala que el valor de los activos debe evaluarse de manera cualitativa o cuantitativa, considerando dimensiones como el impacto legal, operativo, económico y reputacional. Esta valoración permite identificar los activos críticos y constituye la base para el análisis de riesgos y la selección de salvaguardas adecuadas (CSAE, 2012).

Desde la perspectiva de la norma ISO/IEC 27001:2013, el valor de los activos de información se relaciona directamente con el riesgo asociado a su uso, almacenamiento y procesamiento. La norma enfatiza que los activos deben ser protegidos de acuerdo con su nivel de importancia para la organización, considerando el impacto potencial sobre el negocio en caso de incidentes de seguridad, lo que implica valorar dichos activos para una adecuada gestión del riesgo de la información (ISO/IEC, 2013).

2.3.3. Impacto

MAGERIT enfatiza que la evaluación del impacto no se limita a una valoración económica, sino que debe considerar las consecuencias sobre la continuidad del servicio, el cumplimiento normativo y la confianza de los ciudadanos o usuarios. En el ámbito de las entidades públicas, un impacto elevado puede traducirse en la interrupción de servicios esenciales, sanciones legales o pérdida de credibilidad institucional (CSAE, 2012). Desde la perspectiva de la norma ISO/IEC 27005, el impacto es entendido como el resultado negativo de un incidente de seguridad de la información, expresado en términos de daño al negocio. La norma indica que el impacto debe ser evaluado para determinar la severidad del riesgo,

considerando efectos financieros, operativos y legales, así como el impacto en la imagen y reputación de la organización (ISO/IEC, 2018).

2.3.4. Riesgo

Según la metodología MAGERIT, el riesgo se define como la combinación de la probabilidad de ocurrencia de una amenaza y el impacto que dicha amenaza puede generar sobre un activo de información. MAGERIT establece que el riesgo surge cuando una amenaza aprovecha una vulnerabilidad y afecta las propiedades de confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de los activos. En este sentido, el nivel de riesgo se determina a partir de la valoración del impacto y la estimación de la probabilidad o frecuencia del evento adverso (Consejo Superior de Administración Electrónica [CSAE], 2012). Asimismo, MAGERIT enfatiza que el riesgo no debe analizarse únicamente desde una perspectiva técnica, sino también considerando las consecuencias operativas, legales, económicas y reputacionales para la organización. En el contexto de las entidades públicas, un riesgo elevado puede traducirse en la interrupción de servicios esenciales, incumplimiento normativo y pérdida de confianza ciudadana (CSAE, 2012). Desde el enfoque de la norma ISO/IEC 27005, el riesgo de la información se define como el efecto de la incertidumbre sobre los objetivos organizacionales, expresado como una combinación de las consecuencias de un incidente de seguridad de la información y la probabilidad de su ocurrencia. La norma resalta que la gestión del riesgo debe ser un proceso sistemático y continuo, alineado con los objetivos estratégicos de la organización (ISO/IEC, 2018).

2.3.5. Probabilidad

Asimismo, MAGERIT señala que la probabilidad no es un valor estático, sino que puede variar en función de factores como los cambios tecnológicos, el comportamiento humano, la aparición de nuevas amenazas y el nivel de madurez de los controles de seguridad implementados. Por ello, la metodología recomienda su revisión periódica como parte del proceso continuo de gestión de riesgos (CSAE, 2012). Desde la perspectiva de la norma ISO/IEC 27005, la probabilidad es entendida como la posibilidad de que ocurra un incidente de seguridad de la información, teniendo en cuenta la presencia de amenazas, vulnerabilidades y controles existentes. La norma destaca que la estimación de la probabilidad contribuye a una evaluación más precisa del riesgo y a la toma de decisiones informadas sobre el tratamiento del mismo (ISO/IEC, 2018).

2.3.6. Amenazas

De acuerdo con la metodología MAGERIT, una amenaza se define como cualquier causa potencial de un incidente no deseado que pueda provocar daño a un activo de información. MAGERIT señala que las amenazas pueden ser de origen natural, humano o tecnológico, y que su materialización puede afectar las propiedades de seguridad de los activos, tales como la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad. Asimismo, la metodología proporciona un catálogo de amenazas que facilita su identificación sistemática durante el análisis de riesgos (Consejo Superior de Administración Electrónica [CSAE], 2012). MAGERIT enfatiza que las amenazas, por sí solas, no generan riesgo, sino cuando se combinan con vulnerabilidades existentes en los activos. En este sentido, la correcta identificación de amenazas permite evaluar su probabilidad de ocurrencia y su impacto potencial, contribuyendo a una adecuada estimación del riesgo (CSAE, 2012). Desde la perspectiva de la norma ISO/IEC 27005, las amenazas son entendidas como las posibles causas de un incidente de seguridad de la información, que pueden resultar en daños a la organización. La norma resalta que las amenazas pueden ser intencionales o accidentales, internas o externas, y que su análisis debe considerar el contexto organizacional y el entorno tecnológico en el que opera la entidad (ISO/IEC, 2018).

2.3.7. Degradación

Según la metodología MAGERIT, la degradación se define como la pérdida o reducción del valor de un activo de información debido a la afectación de sus propiedades de seguridad, tales como la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad. MAGERIT señala que la degradación puede ser total o parcial y que su análisis es fundamental para determinar el impacto que un incidente de seguridad genera sobre los activos y los servicios que estos soportan (Consejo Superior de Administración Electrónica [CSAE], 2012). Asimismo, MAGERIT establece que la degradación de un activo no siempre implica su destrucción completa, sino que puede manifestarse como una pérdida temporal de disponibilidad, una alteración parcial de la información o una divulgación no autorizada. La magnitud de la degradación dependerá del tipo de amenaza, de la vulnerabilidad explotada y de la eficacia de las salvaguardas implementadas (CSAE, 2012).

Desde la perspectiva de la norma ISO/IEC 27005, la degradación puede entenderse como la reducción del desempeño o de las características de seguridad de un activo de información,

resultante de un incidente de seguridad. La norma asocia este concepto con la afectación de la confidencialidad, integridad o disponibilidad, lo cual influye directamente en la severidad del impacto y en la evaluación del riesgo (ISO/IEC, 2018).

III. DISEÑO METODOLÓGICO

3.1. Tipo de investigación

3.1.1. La investigación básica

Se basa en generar más conocimiento a partir de conocimientos ya existentes, sin embargo, los nuevos conocimientos generados no son verificados o contrastados mediante pruebas exhaustivas, por lo que principalmente son propuestas de solución a la problemática identificada (Hernández, et al., 2018); por tanto, la presente investigación es de tipo básica, porque el investigador pretende generar conocimiento adicional mientras busca solucionar las incidencias de pérdida de información en la municipalidad distrital de Salas, mediante la propuesta de un modelo de SGSI.

3.2. Enfoque de la Investigación

3.2.1. Enfoque cuantitativo,

Según Hernández et al. (2018), el enfoque cuantitativo utiliza la recolección de datos para probar hipótesis con base en la medición numérica y el análisis estadístico, permitiendo establecer patrones de comportamiento y verificar teorías existentes. Los autores indican que este enfoque sigue un proceso secuencial y estructurado, que inicia con la delimitación del problema, continúa con la formulación de hipótesis y culmina con el análisis e interpretación de los resultados. Asimismo, Bernal (2016) indica que la investigación cuantitativa se caracteriza por la precisión en la medición de las variables y por la utilización de métodos estadísticos para el análisis de los datos, lo que contribuye a la validez y confiabilidad de los resultados obtenidos. El autor destaca que este enfoque es especialmente útil cuando se requiere evaluar el nivel, grado o frecuencia de un fenómeno. Por tanto, la presente investigación, es de enfoque cuantitativo, se pretende medir en porcentajes a los indicadores de la seguridad de la información.

3.3. Diseño de Investigación

3.3.1. El diseño no experimental

Según Hernández et al. (2018), los estudios no experimentales son aquellos en los que no se manipulan las variables, sino que se observan situaciones ya existentes para analizarlas posteriormente. Los autores señalan que este diseño resulta apropiado cuando no es posible o no es ético modificar las variables de estudio, siendo ampliamente utilizado en investigaciones sociales. Por su parte, Tamayo y Tamayo (2014) indican que el diseño no experimental es fundamental cuando se busca realizar diagnósticos de una situación específica, ya que permite conocer el estado actual del fenómeno sin alterar su desarrollo natural. Este diseño es común en estudios descriptivos y correlacionales, donde el interés principal es analizar las características y relaciones entre variables. Por tanto, en la presente investigación tiene un diseño no experimental, porque se pretende describir la propuesta de modelo de sistema de gestión de seguridad de la información (SGSI) y la seguridad de la información.

3.4. Nivel de investigación

3.4.1. Descriptivo

Según Hernández et al. (2018), la investigación descriptiva busca especificar las propiedades, características y perfiles de personas, grupos, comunidades, procesos u objetos que sean sometidos a análisis. Los autores señalan que este nivel permite medir o recolectar información de manera independiente o conjunta sobre los conceptos o variables de interés, con el propósito de describirlos tal como se presentan en la realidad. Desde esta perspectiva, el nivel descriptivo no pretende comprobar hipótesis causales, sino caracterizar un fenómeno mediante la observación, medición y sistematización de datos. En este sentido, Bernal (2016) indica que la investigación descriptiva se orienta a detallar las situaciones y eventos tal como ocurren, permitiendo conocer la estructura, funcionamiento y comportamiento del fenómeno analizado. Por su parte, Tamayo y Tamayo (2014) sostienen que el nivel descriptivo permite registrar, analizar e interpretar la naturaleza actual y la composición de un fenómeno, siendo especialmente útil cuando el investigador requiere un diagnóstico de la situación existente. Por tanto, la presente investigación tuvo un nivel descriptivo, puesto que se describe la situación actual como se encuentra las medidas de seguridad de la información en las areas

administrativas e informáticas de la municipalidad distrital de Salas, asi como tambien la descripción de modelo propuesto de un SGSI basada en la ISO/IEC27001/2013.

3.5. Las variables de estudio:

- ✓ ***Variable Independiente:*** Modelo de Sistema de Gestión de Seguridad de la Información.
- ✓ ***Variable Dependiente:*** Seguridad de la información

3.6. Operacionalización de Variables

Tabla 1

Operacionalización de variables

Variable	Definición Conceptual	Definición operacional	Dimensión	Indicadores	Instrumento	Escala
Variable independiente Sistema de Gestión de Seguridad de la Información	Es un conjunto de normas, prácticas y prácticas utilizadas para administrar, controlar, resguardar y mejorar la seguridad de la información de una organización; El SGSI protege la información de la organización contra riesgos de seguridad como acceso no autorizado, robo, destrucción y modificación (Donoso et al., 2023).	El modelo SGSI buscará proporcionar el aseguramiento de la información, a través de los 5 tipos de controles basada en la ISO/IEC 27001	Dominios de la ISO 27001:2013	Políticas de S.I Organización de la S.I. Seguridad de los RR.HH. Gestión de activos Control de accesos Criptografía Seguridad física y ambiental Seguridad de las operaciones Seguridad de las comunicaciones Adquisición, desarrollo y mantenimiento de sistema Relaciones con proveedores. Gestión de incidentes de S.I. Aspectos de S.I. de la continuidad del negocio. Cumplimiento	Guía de Entrevista	**Ordinal**
Variable dependiente Seguridad de la información	Es la protección de los datos contra el acceso, el uso, la divulgación, la alteración, la destrucción o la pérdida no autorizados. Para lograr esto, se deben implementar las medidas y controles de seguridad adecuados para proteger la información (Sánchez et al., 2021).	Se pretende resguardar los pilares de la seguridad de la información, mediante la propuesta del modelo de SGSI.	Pilar de seguridad de la información	Integridad Confidencialidad Disponibilidad	Guía de Entrevista	**Ordinal**

3.7. Población y muestra

3.7.1. Población

Según (Ñaupas, et al., 2018), estos están conformados por un grupo determinado de elementos, individuos u objetos, que tienen uno o más características en común. Por tanto, la población de la presente investigación, son 9 personas, que laboran en el área de informatica y administración de la Municipalidad Distrital de Salas.

3.7.2. Muestra

Según (Ñaupas, et al., 2018), es una porción o el global de la población. Por tanto, al tener una población pequeña, se tomará la totalidad, es decir, 9 personas, que laboran en el área de informática y administración de la Municipalidad Distrital de Salas.

3.7.3. Muestreo

No se emplea ninguna técnica de muestreo, puesto que la muestra a estudiar es la totalidad de la población.

3.8. Técnicas, instrumentos, equipos y materiales

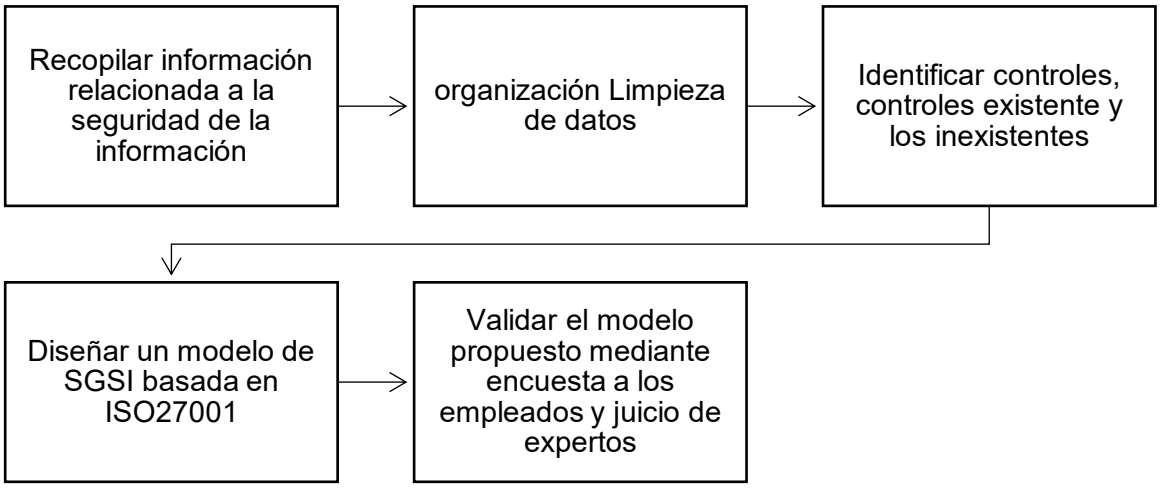
Según (Ñaupas, et al., 2018), las técnicas son las instrucciones que facilitan la recolección de los datos en el desarrollo de la investigación, estos pueden ser tangible y/o no tangible; estas técnicas pueden ser una encuesta (con su instrumento cuestionario), entrevista (formulación de preguntas estructuradas), fichajes (fichas), etc., por tanto, en la presente investigación, se empleará la técnica de entrevista.

3.9. Procedimientos

En la presente investigación, necesariamente se realizó entrevista al personal que labora en el área de informática y areas administrativas de la Municipalidad Distrital de Salas, con la finalidad de conocer la situación actual respecto a la seguridad de la información y los controles que estos tienen.

Figura 2

Procedimiento de la ejecución de la investigación



3.10. Método de análisis de datos

Según Hernández, et al., (2018), el análisis de datos, se toma en cuenta el diseño de la investigación, asi como el nivel o alcance del estudio, también se toma en cuenta a las técnicas de recolección y herramientas utilizadas, con la finalidad de llegar a una conclusión objetiva de la investigación.

IV. RESULTADOS

4.1. Modelo de SGSI para MDS

4.1.1. Plan (Planificar)

4.1.1.1. Analizar los controles y políticas actuales

4.1.1.1.1. Contexto de la organización.

La municipalidad distrital de Salas, es una de las entidades públicas del estado orientado a brindar servicios de administración de recursos públicos, sin fines de lucro en el distrito de Salas.

En su contexto social

La distribución social del distrito (rural, disperso) exige una estrategia fuerte de acercamiento al ciudadano y servicios descentralizados. Por otro lado, la gestión de personal parece tener tensiones considerables que podrían afectar la institucionalidad interna, a causa de que el alcalde y el gerente se negaron a la reposición de un trabajador.

En su contexto económico

Hay potencial para desarrollo productivo, pero la baja ejecución presupuestal y los costos operativos del entorno rural podrían frenar la efectividad de las inversiones, puesto que la ejecución del presupuesto, en algunos meses fueron menos de 35%.

En su contexto político

La Municipalidad de Salas tiene una estructura formal bien definida y mecanismos participativos, pero enfrenta desafíos importantes en cumplimiento normativo y rendición de cuentas, considerando casos judiciales y de baja ejecución presupuestal.

En su contexto de gestión de trámites y procesos internos

Existen bases formales sólidas (TUPA, mesa de partes, rendición de cuentas). Pero la ejecución de proyectos complejos está sujeta a debilidades de control interno, supervisión y responsabilidad institucional. Puesto que, un informe de la Contraloría revela problemas en proyectos de inversión (como saneamiento), lo que sugiere que algunos procesos internos de supervisión, recepción de obra, y control no están siendo ejecutados de manera óptima.

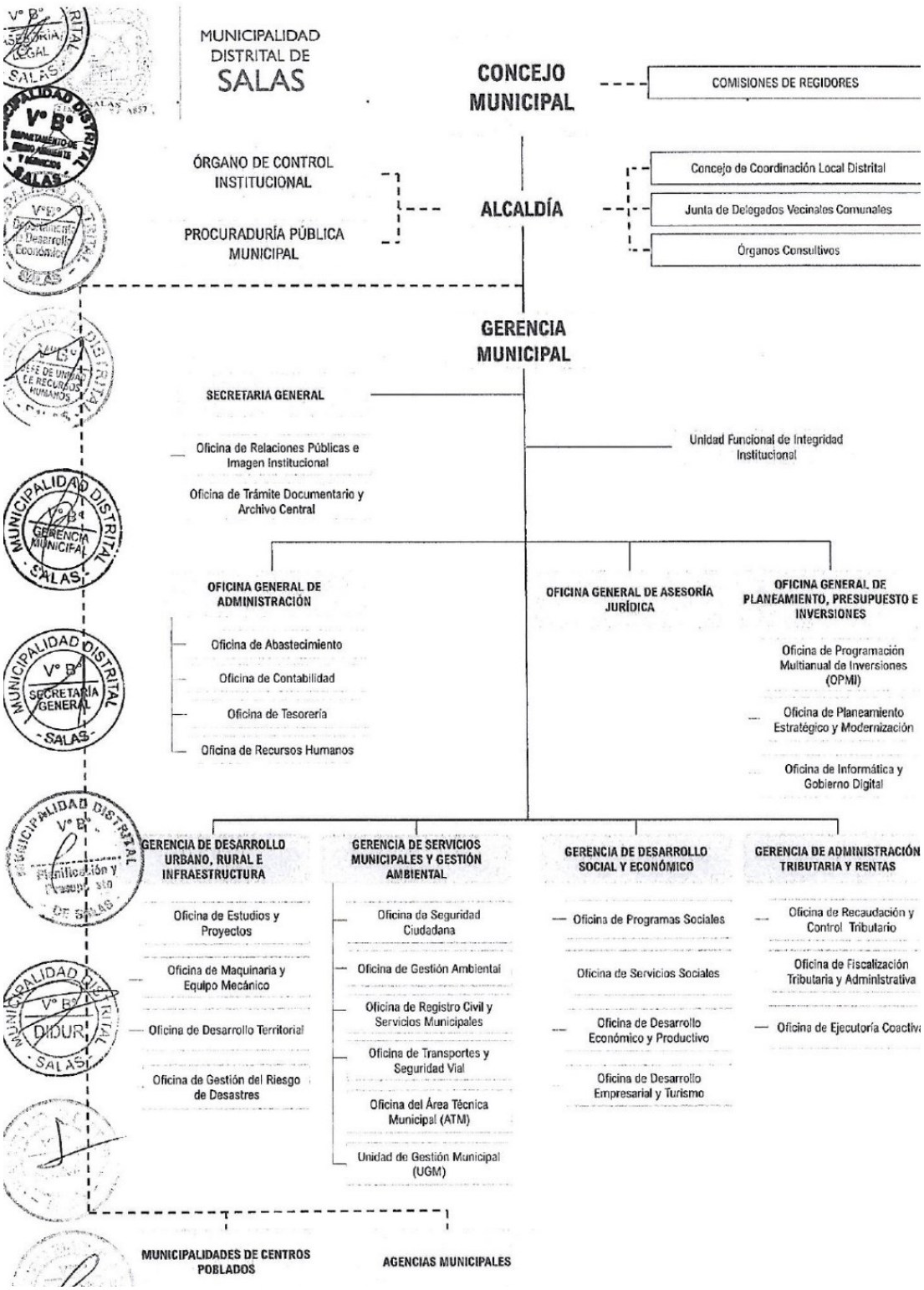
Diseño de proceso de administración e informática

En su contexto de estructura orgánica

La Municipalidad Distrital de Salas cuenta con una estructura organizativa formal y normativa**,** con órganos claramente definidos y mecanismos de participación ciudadana. Si se aprovechan oportunidades como la capacitación, la participación ciudadana y la cooperación técnica externa, la municipalidad puede mejorar significativamente su desempeño y fortalecer la confianza ciudadana. Para ello, administrativamente la municipalidad distrital de Salas está dividida, principalmente en cinco gererencias y 29 oficinas.

Figura 3

Organigrama de municipalidad distrital de Salas

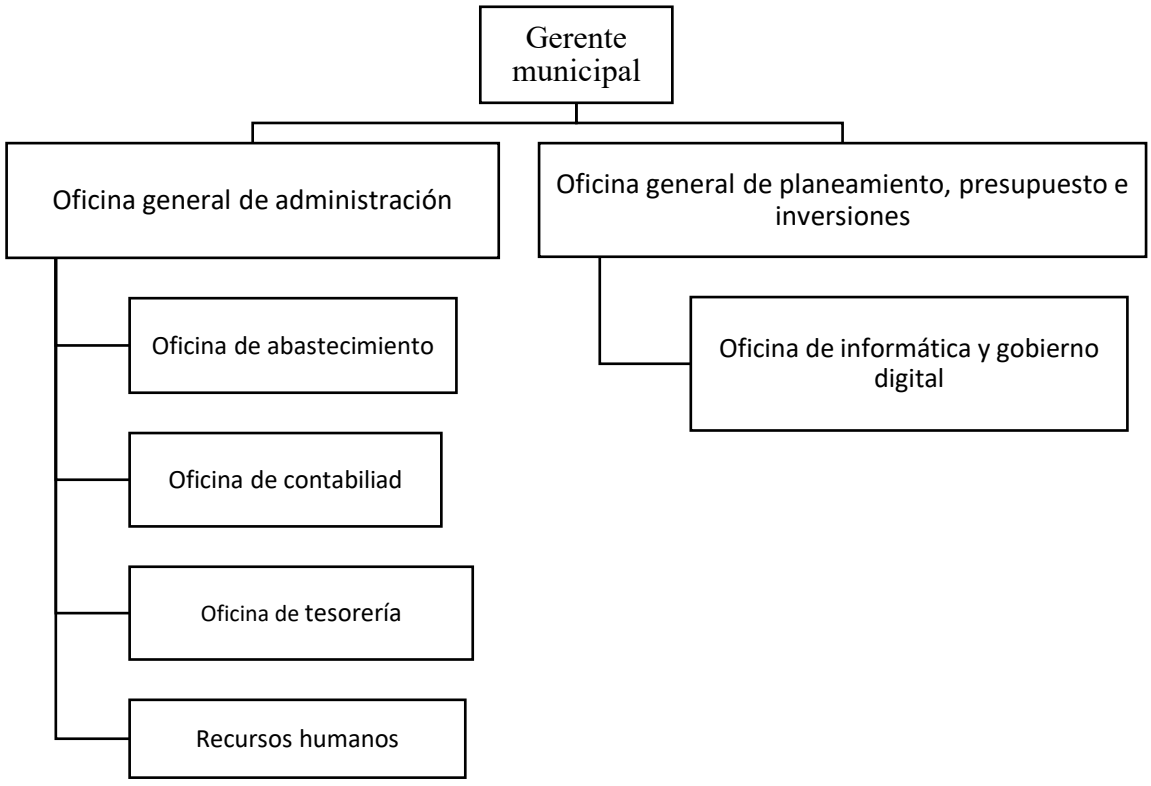


4.1.1.1.2. Análisis de procesos

En la municipalidad distrital de Salas existen diferentes procesos, para la presente investigación se analizó el proceso de requerimiento de personal como tercero (personal no permanente), y la conformidad de pago de los mismos; puesto que es unos de los procesos que mayor cantidad de información genera. En dichos procesos intervienen las areas de: gerente municipal, oficina general de administración, oficina de abastecimiento, oficina de contabilidad, oficina de tesorería, recursos humanos, oficina general de planeamiento, presupuesto e inversiones, y oficina de informática y gobierno digital.

Figura 4

Organigrama que interviene el proceso de requerimiento y conformidad de pagos a terceros



Análisis de proceso de requerimiento de personal como tercero

Cuando una unidad orgánica detecta que es necesario contratar un servicio especializado y profesional que el personal permanente de la entidad no puede brindar, comienza el procedimiento. El jefe del área que lo requiere hace la petición de servicio, que tiene que contener la justificación técnica, el perfil profesional necesario, el alcance del servicio, el tiempo para ejecutarlo y la cantidad a pagar. También debe incluir de dónde proviene el financiamiento.

La investigación revela que, en la práctica, los requisitos de personal como tercero no siempre están claramente definidos, con descripciones generales que pueden causar confusión entre un contrato laboral encubierto y una ubicación de servicios. Este escenario supone un riesgo a nivel administrativo y legal para la municipalidad.Posteriormente, el requerimiento es evaluado por la Oficina de Planeamiento y Presupuesto, la cual verifica la disponibilidad presupuestal y emite la certificación de crédito presupuestario. Este paso es fundamental, ya que la contratación de servicios sin certificación presupuesta1 previa contraviene la normativa del Sistema Nacional de Presupuesto y es susceptible de observaciones por los órganos de control.

La Oficina de Abastecimiento o la Oficina de Recursos Humanos examina la adecuación normativa del requerimiento, asegurándose de que el servicio no esté relacionado con tareas permanentes, que el perfil profesional coincida con lo pedido y que el tipo de contratación sea apropiado. No obstante, se han detectado debilidades vinculadas a la ausencia de criterios estandarizados para determinar cuándo es apropiado contratar a un tercero.

Cuando el requerimiento es aprobado, se avanza con la elección del profesional y la firma del contrato de locación de servicios. Este contrato define los productos que se entregarán, las responsabilidades, los plazos y las condiciones de pago. Sin embargo, en ciertas situaciones, los contratos no tienen indicadores claros de cumplimiento, lo que complica la evaluación subsiguiente del servicio proporcionado.

Análisis del proceso de conformidad de pagos por recibos por honorarios

El servicio proporcionado por el profesional contratado es lo que da comienzo al proceso de conformidad de pagos. Cuando se acaba el periodo o entregable especificado en el contrato, el tercero emite un recibo por honorarios que debe estar correctamente registrado en la Superintendencia Nacional de Aduanas y de Administración Tributaria (SUNAT).

Es el jefe inmediato o responsable del área de usuario quien tiene la responsabilidad de emitir la conformidad del servicio, confirmando que el profesional cumplió con los términos contractuales y que los productos o actividades fueron presentados satisfactoriamente. Este documento es el principal respaldo de la procedencia del pago.

El analisis de dicho proceso, evidencia que la conformidad de pagos es uno de los aspectos más críticos, puesto que, en numerosas ocasiones, se emite sin tener evidencia objetiva que avale si el servicio se ha cumplido o no. Esta evidencia puede ser informes técnicos, productos entregables o indicadores de desempeño. Esta práctica eleva la probabilidad de que ocurran observaciones por parte de los órganos de control y pagos indebidos.

Después de que se emite la conformidad, el expediente es enviado a la oficina de Contabilidad para que se registre el devengado en el Sistema Integrado de Administración Financiera (SIAF). Luego, pasa a la Oficina de Tesorería para programar y llevar a cabo el pago. En estos periodos se detectan demoras habituales que surgen por inconsistencias en la documentación, equivocaciones en los recibos de honorarios o fallas en la coordinación entre áreas.

4.1.1.1.3. Identificación de los activos de información

Tabla 2

Identificación de los activos de información de MDS

Cód. de activo	Activo de información	Cant.	Frecuencia de funcionamiento	Resguardo	Descripción	Valor del activo	Criticidad
A.I. - 01	Servidor Virtual (SIGA Y SIAF)	2	24/7	Alojado en los servidores del estado peruano	Acceso mediante la aplicación web del estado.	Alto	Alto
A.I. – 02	Computadora de escritorio (PC)	7	Día laborable	Ubicada en escritorio de madera	Marcas de equipos (LG y Dell)	Alto	Alto
A.I. – 03	Computadora personal (Laptop)	4	Día laborable	Ubicada en escritorio de madera	Marcas de equipos (Lenovo y Acer)	Alto	Alto
A.I. – 04	Impresora Básico	2	Día laborable	Ubica junto a la Pc	HP (impresión a blanco y negro)	bajo	Bajo
A.I. – 05	Impresoras multifuncional	3	Día laborable	Ubicado en mueble independiente y/o junto a laptop	Epson y Canon	Medio	Medio
A.I. – 06	Disco de almacenamiento externo (incluye Memoria USB).	6	Cuando se requiere	En cajones del escritorio de cada responsable de área.	Kingston y SanDisk	Medio/Alto	Medio/Alto
A.I. – 07	Archivador físico	66	Cuando se requiere	Oficina de cada área	Archivadores de palanca de marca Artesco	Alto	Alto
A.I. – 08	Router	1	Diario (no apagan el servicio)	Área de informática	Equipo del proveedor (Movistar)	Alto	Alto
A.I. – 09	Switch	2	Diario (no apagan el servicio)	Ubicada en el área de RR.HH y Logística	Equipos de 16 puertos LAN, de mara TP-link	Alto	Alto
A.I. – 10	Personal de las áreas de administrativas e informática	9	Diario	El personal no es controlado en el ingreso ni salida de su labor	Todos los responsables de área tienen estudios superior universitarios y los asistentes (superior técnico).	Alto	Alto

Nota. En la tabla se muestra los activos de información ubicadas en las áreas de administración (recursos humanos, contabilidad, tesorería y logística) e informática.

4.1.1.1.4. Análisis de controles actuales

Tabla 3

Análisis de controles actuales

Medidas de seguridad de la información actuales según la ISO 27001:2013			
Anexo	**Controles basados en dominios de ISO 27001:2013**	**% de cumplimiento**	**Observaciones**
Anexo A.5	Políticas de seguridad de la información	83%	
Anexo A.6	Organización de la seguridad de la información	23%	
Anexo A.7	Seguridad de los recursos humanos	45%	
Anexo A.8	Gestión de activos	23%	
Anexo A.9	Control de acceso	45%	
Anexo A.10	Criptografía	0%	No aplica
Anexo A.11	Seguridad física y ambiental	23%	
Anexo A.12	Seguridad de las operaciones	45%	
Anexo A.13	Seguridad de las comunicaciones	83%	
Anexo A.14	Adquisición, desarrollo y mantenimiento del sistema	0%	No aplica
Anexo A.15	Relaciones con los proveedores	23%	
Anexo A.16	Gestión de incidentes de seguridad de la información	23%	
Anexo A.17	Aspectos de seguridad de la información de la continuidad del negocio	0%	No aplica
Anexo A.18	Cumplimiento	92%	

Nota. Cabe mencionar que, el 60% del personal desconoce el protocolo de reporte de incidentes, lo que retrasa la respuesta ante la pérdida de alguna información o activo de información.

En la tabla anterior claramente se puede observar que por el momento no es necesario considerar la pronta implementación de controles de anexo A.14, puesto que los sistemas son tercerizados, de igual manera el anexo A.10 porque el área de informática solo se dedica a resolver las incidencias sólo en su primer nivel. Por otro lado, los controles de los anexos A.5, A.13 y A.18, tienen un gran porcentaje de implementación y cumplimiento.

4.1.1.2. Alcance del SGSI

El alcance de SGSI comprende, a los procesos, los activos de información, el personal y los sistemas asociados a las áreas de administración Oficina general de administración, Oficina de abastecimiento, Contabilidad, Tesorería, Recursos humanos, Oficina general de planeamiento, presupuesto e inversiones, y Oficina de informática y gobierno digital.

. Esto abarca desde la administración de documentos y las finanzas hasta los recursos humanos, la infraestructura tecnológica, el soporte técnico de sistemas. Aplica a todas las ubicaciones donde se procesa información bajo la custodia de dichas áreas, incluidos los servicios tecnológicos tercerizados.

4.1.1.3. Stakeholders del SGSI

Las partes interesadas del SGSI incluyen: alcalde, gerente de la municipalidad distrital de Salas, responsables del SGSI, usuarios internos (propietarios de procesos), auditores, Cada uno ejerce roles vitales como auditor, garante de cumplimiento, implementador de técnicas, líder, protector de la información, cumplidor de políticas.

4.1.1.3.1. Roles y funciones

Tabla 4

Roles y funciones del equipo SGSI

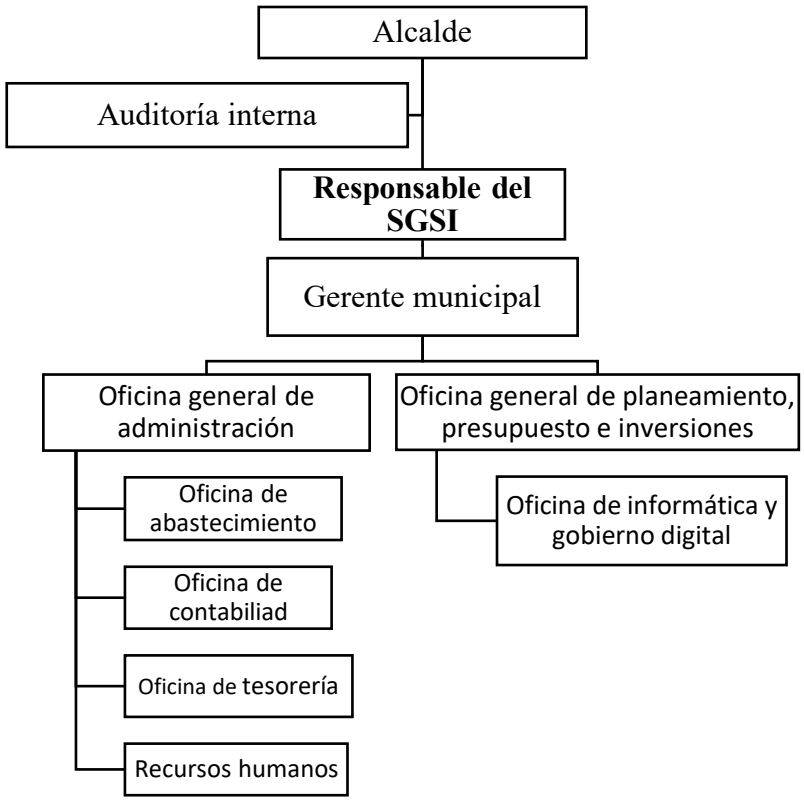
Item	Rol	Cantidad	Funciones
01	Alcalde	1	✓Aprobar la implementación de la propuesta del SGSI. ✓Proporcionar los recursos necesarios para la implementación y operación de los controles de seguridad de la información. ✓Revisar los reportes del desempeño del SGSI, durante la operación de la misma.
02	Auditor interno	3	✓Elaborar informes y recomendaciones, realizando auditorías de seguimiento o certificación y evaluando la conformidad con ISO 27001:2013.
03	Responsable del SGSI	1	✓Planificar auditorías internas y externas, mantener actualizado el inventario de documentos y activos del SGSI, identificar riesgos y coordinar su tratamiento, dirigir la implementación y mantenimiento del SGSI, definir controles de seguridad y asegurar su cumplimiento, elaborar informes de desempeño del SGSI.
04	Gerente	1	✓Asegurarse que los objetivos estratégicos y prioridades, para cumplir con los objetivos de la gestión municipal. ✓Asegurar que el SGSI se integre con los procesos acorde a las necesidades de la municipalidad. ✓Revisar el desempeño del SGSI y participar en la mejora continua del SGSI.
05	Usuarios internos (dueños del proceso)	6	✓Seguir las políticas de seguridad y los procedimientos establecidos, haciendo uso correcto de los sistemas, equipos y accesos, e informando incidentes o anomalías para proteger las credenciales e información a la que se tiene acceso.

Nota. Cabe aclarar que, los usuarios internos están conformado por los dueños de los procesos, estos son los jefes de cada una de las áreas implicadas (informática, administración, recursos humanos, logística, tesorería, y contabilidad).

4.1.1.3.2. Organigrama para operar el SGSI

Figura 5

Organigrama para el SGSI en la MDS



Nota. Se propone incorporar a responsable del SGSI y la creación del equipo de auditoría.

4.1.1.4. Análisis y gestión de riesgos (Magerit)

Tabla 5

Análisis y gestión de riesgos

Itm	Activo	Amenaza	Vulnerabilidad	Probabilidad	Riesgo	Consecuencia
A.I. - 01	Servidor Virtual (SIGA Y SIAF)	M	V	60%	A	M
A.I. – 02	Computadora de escritorio (PC)	M	V	40%	M	S
A.I. – 03	Computadora personal (Laptop)	M	V	60%	A	M
A.I. – 04	Impresora Básico	M	V	40%	M	S
A.I. – 05	Impresoras multifuncional	M	V	40%	M	S
A.I. – 06	Disco de almacenamiento externo (incluye Memoria USB).	B	PV	40%	A	I
A.I. – 07	Archivador físico	M	PV	40%	A	M
A.I. – 08	Router	M	V	60%	A	M
A.I. – 09	Switch	A	MV	40%	A	M
A.I. – 10	Personal de las áreas de administración e informática	A	MV	40%	A	M

Donde:

Tabla 6

Calificativo de riesgo

Calificativo	***Descripción***
Alto (A)	Es altamente probable que el riesgo se materialice.
Moderado (M)	Es posible que el riesgo se concrete
Bajo (B)	Es improbable que el riesgo se haga realidad.

Tabla 7

Calificativo de amenaza

Calificativo	***Descripción***
Alto (A)	Suceso que tiene la posibilidad de suceder de inmediato
Medio (M)	El evento tiene la posibilidad de suceder en un plazo medio.
Bajo (B)	El suceso puede suceder a largo plazo.

Tabla 8

Calificativo de vulnerabilidad

Categoría	**Descripción**
Extremadamente vulnerable (EV)	Demasiado vulnerable frente a la pérdida de cualquier dato.
Muy vulnerable (MV)	Muy delicado frente a cualquier pérdida de información.
Vulnerable (V)	Vulnerable frente a cualquier pérdida de datos.
Poco vulnerable (PV)	Baja vulnerabilidad frente a cualquier pérdida de datos.
Mínimamente vulnerable (mV)	Fragilidad mínima ante cualquier pérdida de datos.

Tabla 9

Calificativo de probabilidad de ocurrencia

Categoría	**Descripción**
Casi seguro (entre 81% - 100%) (CS)	La certeza de que haya pérdida de información es muy elevada.
Muy probable (entre 61% - 80%) (MP)	El nivel de certeza de que se pierda información es elevado.
Probable (entre 41% - 60%) (P)	Es mediano el nivel de seguridad de que se pierda información.
Poco Probable (entre 21% - 40%) (PP)	La certeza de que la información se pierda podría ser significativa.
Raro (entre 1% - 20%) (R)	Es muy poca la probabilidad de que se pierda información.

Tabla 10

Calificativo de Consecuencia

Categoría	Descripción
Mayor (M)	El proceso del área administrativa y el de informática se verán muy afectados.
Importante (I)	El proceso de las áreas administrativa e informática se verá significativamente impactado.
Significativo (S)	El proceso del área administrativa y la informática se verá perjudicado.
Regular (R)	El proceso de las áreas administrativas e informáticas se verá alterado, pero es factible tomar.
Menor (m)	Se asume que el proceso del área administrativa y de informática se verá afectado en menor medida.

4.1.1.5. Tratamiento de riesgos

Tabla 11

Tratamiento de riesgos

Itm	Activo	Riego	Tratamiento
A.I. - 01	Servidor Virtual (SIGA Y SIAF)	A	Mitigar
A.I. – 02	Computadora de escritorio (PC)	M	Asumir
A.I. – 03	Computadora personal (Laptop)	A	Asumir
A.I. – 04	Impresora Básico	M	Asumir
A.I. – 05	Impresoras multifuncional	M	Asumir
A.I. – 06	Disco de almacenamiento externo (incluye Memoria USB).	A	Asumir
A.I. – 07	Archivador físico	A	Asumir
A.I. – 08	Router	A	Transferir / Asumir
A.I. – 09	Switch	A	Asumir
A.I. – 10	Personal de las áreas de administración e informática	A	Asumir

4.1.1.6. Selección de controles de seguridad

Tabla 12

Selección de controles de seguridad según la 27001:2013

Implementación de controles según prioridad			
Anexo	**Controles basados en dominios de ISO 27001:2013**	**% de cumplimiento**	**Prioridad de implementación**
Anexo A.5	Políticas de seguridad de la información	83%	3er trimestre
Anexo A.6	Organización de la seguridad de la información	23%	1er trimestre
Anexo A.7	Seguridad de los recursos humanos	45%	2do trimestre
Anexo A.8	Gestión de activos	23%	1er trimestre
Anexo A.9	Control de acceso	45%	2do trimestre
Anexo A.10	Criptografía	0%	No aplica
Anexo A.11	Seguridad física y ambiental	23%	1er trimestre
Anexo A.12	Seguridad de las operaciones	45%	2do trimestre
Anexo A.13	Seguridad de las comunicaciones	83%	3er trimestre
Anexo A.14	Adquisición, desarrollo y mantenimiento del sistema	0%	No aplica
Anexo A.15	Relaciones con los proveedores	23%	1er trimestre
Anexo A.16	Gestión de incidentes de seguridad de la información	23%	1er trimestre
Anexo A.17	Aspectos de seguridad de la información de la continuidad del negocio	0%	1er trimestre
Anexo A.18	Cumplimiento	92%	3er trimestre

4.1.1.7. Políticas y procedimientos del SGSI-MDS

4.1.1.7.1. Políticas

Siguiendo las políticas se deberá cumplir lo siguiente:

- ✓ Fija el compromiso de la municipalidad de salvaguardar la información, cumplir con las leyes, manejar riesgos y optimizar de manera constante el SGSI.
- ✓ Determina niveles: Publica, uso interno y confidencial, así como las reglas para su manejo, almacenaje y desecho.
- ✓ Controla la creación, modificación y eliminación de usuarios; el empleo de privilegios; así como las revisiones periódicas de accesos.

- ✓ Regula el acceso a servidores, equipos esenciales, instalaciones y archivo central.
- ✓ Regula el empleo de correo electrónico, internet, redes, aparatos y software municipales.
- ✓ Establece la manera de reportar, registrar y abordar los incidentes de seguridad.
- ✓ Implementa estrategias para garantizar que los servicios vitales funcionen durante catástrofes.
- ✓ Requiere evaluaciones a proveedores críticos, acuerdos de confidencialidad y cláusulas de seguridad.
- ✓ Establece la metodología, los encargados y la periodicidad para examinar y gestionar riesgos.
- ✓ Regula el tratamiento seguro de datos ciudadanos conforme a la ley.

4.1.1.7.2. Procedimientos

- ✓ Reconocer activos, analizar los riesgos, establecer controles y actualizar el plan de tratamiento.
- ✓ Asignar permisos, auditar accesos y administrar altas/bajas de usuarios. Documentar lecciones aprendidas, registrar incidentes, analizarlos y solucionarlos.
- ✓ Hacer copias de seguridad, comprobar su integridad y probar las restauraciones.
- ✓ Desplegar el BCP/DRP en situaciones de emergencia y registrar los resultados de simulacros.
- ✓ Examinar, aceptar, poner a prueba e implementar modificaciones en los sistemas municipales
- ✓ Administrar el ciclo de vida de los activos, designar responsables, etiquetar y gestionar inventario.
- ✓ Vigilar el CCTV, controlar las visitas y registrar los accesos físicos. Regular el uso de la navegación, la protección antimalware y el correo institucional.
- ✓ Establecer criterios de seguridad, evaluar a los proveedores y monitorear su desempeño.

4.1.2. Do (Hacer o ejecutar)

4.1.2.1. Plan de formación y concienciación

Con el objetivo de fomentar una cultura organizacional orientada a la seguridad de la información en la municipalidad distrital de Salas, se propone ser el siguiente plan.

4.1.2.1.1. Matriz de capacitación

Tabla 13

Matriz de capacitación

Item	Fase	Orientado a:	Contenido	Estrategia	Duración	Modalidad
01	Sensibilización y cultura organizacional	Todo el personal	Conceptos básicos: *confidencialidad, integridad, disponibilidad.* Riesgos comunes: *phishing, ingeniería social, contraseñas, uso seguro de equipos.* Política de seguridad de la organización. Rol de cada colaborador en el SGSI.	Charlas, videos, ejercicios prácticos, evaluaciones cortas.	No menor de 6 horas	Presencial
02	Capacitación para el equipo responsable del SGSI	Equipo de Seguridad y Responsables de procesos	ISO/IEC 27001:2022 Gestión del riesgo (Magerit) Gobernanza y documentación	Talleres, laboratorios, ejercicios con casos reales, simulaciones de riesgos.	No menor de 40 horas	Presencial
03	Capacitación técnica especializada	Personal de informática	Gestión de accesos y cuentas privilegiadas Seguridad de redes y firewalls Backup y continuidad del negocio Gestión de vulnerabilidades manejo seguro de datos sensibles	Laboratorios prácticos, entornos simulados, talleres con herramientas.	No menor de 60 horas	Semi presencial
04	Capacitación para auditores internos	Equipo de auditoría interna o personal designado.	Interpretación de la norma ISO 27001 Principios de auditoría basados en ISO 19011 Técnicas de entrevistas y revisión documental Gestión de hallazgos y no conformidades Elaboración de informes de auditoría	Casos prácticos y simulación de auditoría real.	No menor de 30 horas	Presencial
05	Capacitación para la operación continua del SGSI	Propietarios de procesos, responsables de activos, personal de TI y seguridad.	Gestión de activos de información Registro y tratamiento de incidentes Seguimiento de controles Revisión de métricas e indicadores del SGSI Requisitos legales y regulatorios aplicables Mejora continua y revisión por la dirección	Talleres y reuniones periódicas de seguimiento.	No menor de 20 horas	Semi presencial

Nota. Los indicadores a evaluar durante el proceso de capacitación serán: Porcentaje de personal capacitado (según fase) y resultados de evaluaciones de conocimiento

4.1.2.1.2. Matriz para las actividades de implementación y operación

Tabla 14

Matriz para las actividades de implementación y operación

Item	Grupo de controles	Actividades de	Registros de operación
01	Controles Organizativos	Elaboración/actualización de políticas del SGSI. Designación formal de responsables de la información. Inclusión de cláusulas de seguridad en contratos con proveedores.	Políticas aprobadas Registros de capacitación Compromisos de confidencialidad firmados Evaluación de seguridad de proveedores Lista de roles y responsabilidades del SGSI
02	Controles de Gestión de Activos	Inventario completo de activos (información, software, hardware, personas, servicios). Clasificación de la información según sensibilidad. Etiquetado y procedimientos de manejo de la información.	Inventario de activos actualizado Registro de clasificación Registro de transferencias de activos Registro de eliminación o destrucción segura
03	Controles de Control de Accesos	Definir roles y niveles de acceso. Implementar procedimientos de alta, modificación y baja de usuarios. Revisiones periódicas de accesos. Endurecimiento de autenticación (MFA si aplica).	Solicitudes de alta/ modificación / baja de usuarios Registros de revisiones de accesos Logs de accesos al sistema Registro de incidentes de acceso
04	Seguridad Física y Ambiental	Control de acceso físico (tarjetas, biometría). CCTV, alarmas, sensores. Políticas de escritorio limpio y pantalla limpia.	Registro de acceso físico Registro de mantenimiento de CCTV Registro de fallas o incidentes físicos

Item	Grupo de controles	Actividades de	Registros de operación
05	Seguridad Operacional	Procedimientos de operación segura. Gestión de parches y actualizaciones. Backups periódicos y pruebas de restauración. Implementación de SIEM o sistema de logs centralizado.	Registro de cambios (RFC) Registro de parches aplicados Resultados de análisis de vulnerabilidades Registro de respaldos y restauraciones Logs de eventos y auditoría
06	Seguridad en las Comunicaciones	Segmentar redes según criticidad. Usar canales cifrados para transferencia de información. Políticas de envío seguro de correos y archivos.	Registro de monitoreo de red Registro de incidentes de comunicaciones Aprobaciones de intercambio de información sensible
07	Relación con Proveedores	Evaluación inicial de seguridad del proveedor. Monitoreo continuo de cumplimiento	Evaluaciones de proveedores Auditorías a proveedores SLA y evidencias de cumplimiento
08	Gestión de Incidentes	Definir proceso para reporte y tratamiento. Establecer niveles de severidad. Identificar causas raíz.	Registro de incidentes Registro de eventos Lecciones aprendidas Registros de acciones correctivas
09	Continuidad del Negocio	Realizar BIA. Crear BCP y DRP. Pruebas periódicas de continuidad.	Resultados del BIA Resultados de pruebas BCP/DRP Planes actualizados
10	Cumplimiento	Auditoría interna anual del SGSI. Gestión de no conformidades. Revisión por la dirección.	Informes de auditoría Registro de acciones correctiva. Minutas de revisión por la dirección

4.1.3. Check (Verificar o Revisar)

Durante la operación del SGSI propuesto para la municipalidad distrital de Salas, se tendrán en cuenta los siguientes indicadores al momento de revisar el funcionamiento del SGSI.

4.1.3.1. Matriz para la medición de la eficiencia del SGSI

Tabla 15

Matriz para la medición de la eficiencia del SGSI

Item	KPI	Descripción	Fórmula	Frecuencia	Meta
01	Cumplimiento de Controles del SGSI	Porcentaje de controles del SoA implementados	(Controles implementados / Controles aplicables) × 100	Mensual	≥ 90 %
02	Cierre de auditorías internas	Velocidad de cierre de no conformidades	(# NC cerradas / # NC totales) × 100	Trimestral	≥ 85 %
03	Participación en capacitaciones	Nivel de asistencia del personal	(Personas capacitadas / Total personas) × 100	Semestral	≥ 95 %
04	Incidentes reportados vs detectados	Madurez del proceso de reporte	(Incidentes reportados / Incidentes detectados por TI) × 100	Mensual	≥ 75%

Nota. El responsable del SGSI, es el responsable de administrar la presente matriz.

4.1.3.1. KPIs de interés de alta directiva

Tabla 16

KPIs de interés de alta directiva

Item	KPI	Indicador
01	Nivel de madurez del SGSI	Escala de lickert (1 - 5)
02	Riesgo residual total	Tendencia mensual
03	Nº de incidentes críticos	Debe ir a la baja
04	Disponibilidad de servicios clave	≥ 90 %
05	Cumplimiento de auditoría interna	≥ 85%

4.1.4. Act (Actuar o ajustar)

4.1.4.1. Matriz de ajustes del modelo de SGSI

Tabla 17

Matriz de ajustes del modelo de SGSI

Item	Directriz de mejora	Listado de actividades necesarias
01	Implementación de acciones correctivas	
02	Actualizar el análisis y evaluación de riesgos	
03	Ajustar políticas, controles y procedimientos	
04	Optimización de KPIs y mecanismos de medición	
05	Mejoras derivadas de la Revisión por la Dirección	
06	Actualizar documentación del SGSI	
07	Mejorar controles que fallaron o no fueron suficientes	
08	Actualizar formación y concientización	
09	Acción sobre proveedores y terceros	
10	Verificar eficacia de las mejoras implementadas	

4.2. Validar el modelo propuesto.

Mediante el juicio de 3 expertos, se validó el modelo del SGSI propuesto, con una calificación de correcto sin observaciones ni sugerencias de mejora.

V. Discusión de resultados

En relación con la identificación y valoración de los activos de información, los resultados muestran que el 70 % de los activos presentan un valor y criticidad altos, lo cual confirma que la información manejada por la municipalidad es sensible y estratégica. Este hallazgo coincide con lo reportado por Donoso et al. (2023), quienes destacan que la correcta identificación de activos y el análisis de riesgos constituyen la base para cualquier iniciativa tecnológica, incluyendo la inteligencia artificial, y que no es recomendable implementar soluciones avanzadas sin antes contar con un SGSI formalmente establecido. De manera similar, Fernández (2023) y Baca (2023) identificaron que las entidades públicas presentan activos críticos altamente expuestos debido a la ausencia de controles y políticas de seguridad estructuradas.

Respecto al nivel de implementación de los controles de la norma ISO/IEC 27001:2013, los resultados revelaron que únicamente los anexos A.5 (Políticas de seguridad de la información), A.13 (Seguridad en las comunicaciones) y A.18 (Cumplimiento) presentan un nivel de implementación aceptable, mientras que el resto de los controles muestran deficiencias significativas. Esta situación es consistente con los estudios de Hernández et al. (2024) y Gala et al. (2025), quienes concluyen que muchas organizaciones implementan de forma parcial la norma, priorizando ciertos controles operativos, pero descuidando aspectos clave como la gestión de riesgos, la documentación de procesos y la mejora continua, lo que compromete la sostenibilidad del SGSI en el tiempo.

Asimismo, los resultados de esta investigación evidencian debilidades en la gestión de riesgos de seguridad de la información, lo cual refuerza lo señalado por Ruiz Loo (2024), quien identificó que, incluso en organizaciones con un nivel aceptable de cumplimiento normativo, la falta de una gestión de riesgos sistemática y documentada puede afectar la madurez del SGSI. De igual forma, León y Tufino (2025) demostraron que existe una relación directa entre el nivel de implementación del SGSI y la eficacia en la gestión del riesgo informático, concluyendo que las entidades públicas que no fortalecen este componente incrementan su exposición a incidentes de seguridad.

En cuanto al factor humano, los resultados de la presente investigación indican que el 60 % del personal desconoce los protocolos de reporte de incidentes de seguridad de la

información, lo cual representa una vulnerabilidad significativa. Este hallazgo es congruente con lo señalado por Taboada (2021) y Baca (2023), quienes evidencian una limitada concienciación y capacitación del personal como una de las principales causas del bajo cumplimiento de los controles de seguridad en instituciones públicas. En este contexto, la propuesta del modelo de SGSI enfatiza la capacitación continua como un eje transversal, lo que coincide con las recomendaciones de Gala et al. (2025) sobre la necesidad de fortalecer la cultura de seguridad para garantizar la efectividad del sistema.

Por otro lado, la propuesta del modelo de SGSI, estructurada bajo el ciclo de mejora continua de Deming (Planificar, Hacer, Verificar y Actuar) y utilizando la metodología MAGERIT para el análisis de riesgos, se alinea con experiencias exitosas reportadas a nivel nacional, como la de Huamalí (2021), quien logró la certificación ISO/IEC 27001 tras la aplicación de un SGSI diseñado de forma sistemática. Aunque la presente investigación no tuvo como objetivo la certificación inmediata, los resultados sugieren que la implementación progresiva de los controles propuestos en un periodo de un año permitiría reducir significativamente los riesgos identificados.

Finalmente, la validación del modelo por expertos respalda su viabilidad, adaptabilidad y aplicabilidad, lo cual coincide con las conclusiones de Fernández (2023) y Poma (2021), quienes demostraron que un SGSI bien diseñado contribuye a reducir los riesgos de pérdida, alteración o divulgación no autorizada de la información, además de mejorar la cultura organizacional en seguridad de la información. En este sentido, el modelo propuesto no solo responde a las necesidades específicas de la Municipalidad Distrital de Salas, sino que también puede ser replicado en otras municipalidades y entidades públicas con características similares.

VI. CONCLUSIONES

Conclusión general: Se consiguió crear y proponer un modelo de Sistema de Gestión de Seguridad de la Información (SGSI) que se fundamenta en el estándar ISO/IEC 27001:2013, pero que fue modificado para ser apropiado a la situación organizativa, operativa y regulatoria del municipio distrital de Salas. Esto posibilitó definir un marco estructurado para salvaguardar los activos informáticos y administrativos. En líneas generales, la investigación revela que un SGSI fundamentado en la norma ISO 27001 es una herramienta estratégica; esta permite optimizar la seguridad de los datos, incrementar la transparencia a nivel institucional, disminuir los riesgos operativos y colaborar para que los servicios municipales se mantengan, a su vez la propuesta en mensión, fue validada por tres expertos.

CE01: El análisis del contexto organizacional mostró debilidades importantes en la administración de la seguridad de la información, particularmente en los ámbitos vinculados con el manejo de activos, organización y seguridad física, gestión de incidentes y continuidad del negocio. Esto justificó la necesidad de instaurar un SGSI formal y sistemático. En lo que respecta a la identificación y clasificación de los activos informáticos, se pudieron identificar aquellos que son críticos como el personal clave, sistemas SIAF y SIGA, archivos físicos e infraestructura de red; todos ellos tienen un alto nivel de criticidad y valor para que la municipalidad pueda mantener sus procesos institucionales.

CE02: La evaluación y manejo de los riesgos, llevados a cabo por la metodología MAGERIT, concluyó que la mayor parte de los activos esenciales contienen riesgos moderados y altos, sobre todo vinculados con vulnerabilidades humanas y organizacionales. Esto demostró la necesidad de establecer controles preventivos y correctivos conforme a la norma ISO 27001. Tomando en cuenta las restricciones operativas y presupuestarias del municipio, el tratamiento de riesgos se enfocó en estrategias de mitigación, transferencia y aceptación, estableciendo una perspectiva factible y realista para la implementación gradual de los controles de seguridad de la información. Un plan de implementación por etapas fue establecido al escoger y priorizar los controles del Anexo A de la ISO/IEC 27001, centrándose en los que tienen un impacto más grande en la seguridad de la información y un cumplimiento inferior. Esto asegura una mejora paulatina del nivel de madurez del SGSI. La definición de políticas y procedimientos del SGSI mejoró la gobernanza de la seguridad de

la información, al establecer directrices explícitas sobre cómo gestionar la información, controlar los accesos, lidiar con incidentes, mantener relaciones con proveedores y garantizar la continuidad del negocio. Esto ayudó a estandarizar prácticas seguras en el municipio.

CE03: Al abordar una de las principales debilidades detectadas, como la falta de conocimiento del personal sobre los procedimientos para reportar incidentes, el plan de formación y concienciación, de implementación y operación, sugerido ayuda a reforzar la cultura organizacional de seguridad de la información. La inclusión de indicadores clave de desempeño (KPI) posibilitó la creación de métodos para el seguimiento, la evaluación y la mejora constante del SGSI. Esto facilita que la alta dirección tomara decisiones y promovió la efectividad del sistema con el transcurso del tiempo.

CE04: La confirmación de la pertinencia, coherencia y aplicabilidad del SGSI sugerido fue posible gracias a la validación del modelo por medio de expertos, quienes lo calificaron como correcto y sin observaciones. Esto evidencia que el modelo es técnicamente sólido y factible para ser aplicado en la Municipalidad Distrital de Salas.

VII. RECOMENDACIONES

Se recomienda a futuros investigadores, extender el alcance de la investigación, incluyendo otras áreas operativas de la municipalidad o haciendo comparaciones entre distintas municipalidades, para estudiar el grado de madurez del SGSI en diversos contextos institucionales del sector público.

Se recomienda realizar, estudios experimentales o cuasi-experimentales que habiliten la evaluación del impacto real de la puesta en marcha del SGSI en indicadores como el fortalecimiento del cumplimiento normativo, la mejora de la disponibilidad de los sistemas y la disminución de incidentes relacionados con la seguridad.

Se recomienda hacer un análisis más profundo del factor humano, considerando el comportamiento de los usuarios, la conciencia y la cultura organizacional en lo que respecta a la seguridad de la información, pues el personal es uno de los factores de riesgo más significativos que se han detectado en este estudio.

BIBLIOGRAFÍA

Baca Flores, V. M. (2023). *Diseño de un sistema de gestión de la seguridad de la información para la Unidad de Gestión Educativa Local – Chiclayo*. *Ingeniería: Ciencia, Tecnología e Innovación, 3*(1).

BASC. (15 de 02 de 2023). *https://www.bascperu.org*. Obtenido de El 95% de los problemas de ciberseguridad es por descuidos humanos: https://www.bascperu.org/comunicaciones8.php?id=2440

Bustamante García, S., Valles Coral, M. Á., Cuellar Rodríguez, I. E., & Lévano Rodrígue, D. (2021). Policies based on ISO 27001: 2013 and its influence on information security management in municipalities of Peru. *ENFOQUE UTE, 12*(2). doi:https://doi.org/10.29019/enfoqueute.743

Cajahuamán Rojas, J. L. (2021). *Aplicación del Ciclo Deming para mejorar la Productividad del Proceso de la Flotación Bulk en la Empresa Alpamarca, Junín 2021.* Universidad César Vallejo. Facultad de ingeniería y arquitectura . Obtenido de https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/63193/Cajahuaman_RJL-SD.pdf?sequence=1&isAllowed=y

Culot, G., Nassimbeni, G., Podrecca, M., & Sartor, M. (2021). The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda. *TQM Journal, 33*(7), 30. doi:https://doi.org/10.1108/TQM-09-2020-0202

DatacenterDynamics. (27 de 03 de 2023). *https://www.datacenterdynamics.com/*. Recuperado el 12 de 02 de 2024, de Aumentan las brechas de seguridad por falta de habilidades en ciberseguridad: https://www.datacenterdynamics.com/es/noticias/aumentan-las-brechas-de-seguridad-por-falta-de-habilidades-en-ciberseguridad/

DataPeers. (15 de 03 de 2022). *https://datapeers.itpeers.com*. Recuperado el 14 de 05 de 2024, de Consecuencias desastrosas de la falta de seguridad de los datos: https://datapeers.itpeers.com/es/consequencias-desastrosas-da-falta-de-seguranca-dos-dados/

Donoso Vargas, D., Calahorrano Recalde, C., & Donoso Vargas, S. (04 de 2023). Aplicación del SGSI ISO 27001 en el sistema de rehabilitación social de Ecuador. *Revista Universidad y Sociedad, 15*(2), 11. Obtenido de http://scielo.sld.cu/pdf/rus/v15n2/2218-3620-rus-15-02-274.pdf

Encalada Maza, G. D. (2023). *Auditoria informática física y lógica mediante el uso de metodología MAGERIT en la Unidad Educativa "Alessandro Volta" periodo 2022.* Universidad Laica "Eloy Alfaro" de Manabi. Obtenido de https://repositorio.uleam.edu.ec/bitstream/123456789/4600/1/ULEAM-INFOR-0121.pdf

Hernández Sampieri, R. F. (2016). *Metodología de la investigación: las rutas: cuantitativa ,cualitativa y mixta* (6ta ed.). México: Mc Graw Hill Education.

Huamalí Alhuay, M. W. (2021). *Diseño de un sistema de gestión de seguridad de la información bajo el enfoque de la ISO/IEC 27001 para la empresa ITS business SAC- Lima.* Universidad Nacional José María Arguedas. Apurimac : Facultad de ingeniería . Obtenido de https://repositorio.unajma.edu.pe/handle/20.500.14168/826

Morales, F., Toapanta, S., & Toasa, R. M. (2020). Implementación de un Sistema de Gestión de Seguridad de la Información. *Revista Iberica de Sistemas e Tecnologias de Informacao*, 15. Obtenido de https://www.researchgate.net/profile/Renato-Mauricio-Toasa-G/publication/339956501_Implementacion_de_un_sistema_de_seguridad_perimetral_como_estrategia_de_seguridad_de_la_informacion/links/5e95ffa5a6fdcca78915c13f/Implementacion-de-un-sistema-de-seguridad

Novasoft. (24 de 01 de 2023). *https://www.novasoft.com.co*. Recuperado el 13 de 05 de 2024, de Seguridad de la información: un problema crítico para las empresas: https://www.novasoft.com.co/seguridad-de-la-informacion-un-problema-critico-para-las-empresas/

Ñaupas Paitán, H., Valdivia Dueñas, M. R., Palacios Vilela, J. J., & Romero Delgado, H. E. (2018). *Metodología de la investigación Cuantitativa - Cualitativa y Redacción de la Tesis.* Bogotá: Ediciones de la u.

Poma Ramos, A. (2021). *SGSI con ISO 27001 aplicado a la empresa SOLTESI S.A.C. del distrito de Jesús María 2021* . Universidad Cesar Vallejo. Lima: Facultad de ingeniería y arquitectura. Recuperado el 15 de 01 de 2024, de https://repositorio.ucv.edu.pe/handle/20.500.12692/117149

Sánchez-Sánchez, P. A., García González, J. R., Triana, A., & Perez Coronell, L. (2021). Medida de nivle de seguridad informática de las pequeñas y medianas empresas (PYMEs) en Colombia. Información Tecnológica. *Información tecnológica, 32*(5), 8. doi:http://dx.doi.org/10.4067/S0718-07642021000500121

Taboada Cornetero, L. R. (2021). *Modelo de seguridad de la información para contribuir en la mejora de la seguridad de los activos de información financiera de las Unidades de Gestión Educativa Local de Lambayeque.* Universidad Católica Santo Toribio de Mogrovejo. Chiclayo: EPG - USAT. Obtenido de https://tesis.usat.edu.pe/handle/20.500.12423/3451

Ruiz Loo, D. M. (2024). *Evaluación del sistema de gestión de seguridad de la información según la norma ISO/IEC 27001 en el sub área de seguridad, gobierno y servicio del Scotiabank Perú S.A., San Isidro 2023* [Tesis de licenciatura, Universidad Científica del Perú].

Sánchez-Sánchez, P. A., García González, J. R., Triana, A., & Perez Coronell, L. (2021). Medida de nivle de seguridad informática de las pequeñas y medianas empresas (PYMEs) en Colombia. Información Tecnológica. *Información tecnológica, 32*(5), 8. doi:http://dx.doi.org/10.4067/S0718-07642021000500121

Stallings, W. (2019). *Effective cybersecurity: A guide to using best practices and standards*. Addison-Wesley.

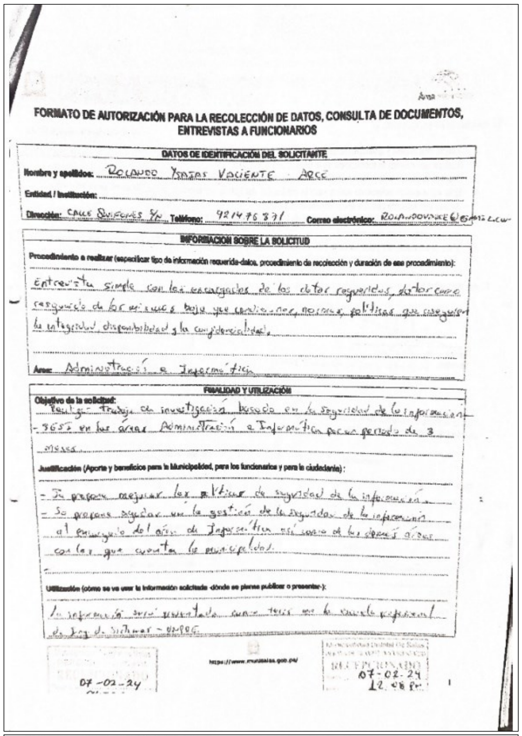
Tamayo y Tamayo, M. (2014). *El proceso de la investigación científica* (5.ª ed.). Limusa.

Taboada Cornetero, L. R. (2021). *Modelo de seguridad de la información para contribuir en la mejora de la seguridad de los activos de información financiera de las Unidades de Gestión Educativa Local de Lambayeque.* Universidad Católica Santo Toribio de Mogrovejo. Chiclayo: EPG - USAT. Obtenido de https://tesis.usat.edu.pe/handle/20.500.12423/3451

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

ANEXOS

Anexo 01: carta de aceptación para realizar la investigación en la MDS



FORMATO DE AUTORIZACIÓN PARA LA RECOLECCIÓN DE DATOS, CONSULTA DE DOCUMENTOS, ENTREVISTAS A FUNCIONARIOS

DATOS DE IDENTIFICACIÓN DEL SOLICITANTE

Nombre y apellidos: Rolando Ysaias Valiente Arce

Entidad / Institución:

Dirección: Calle Quiñones S/N Teléfono: 921476871 Correo electrónico: [illegible]

INFORMACION SOBRE LA SOLICITUD

Procedimiento a realizar (especificar tipo de información requerida-datos, procedimiento de recolección y duración de ese procedimiento):

Entrevista simple con los encargados de los datos requeridos, datos como resguardo de los mismos bajo qué condiciones, normas, políticas que aseguren la integridad, disponibilidad y la confidencialidad.

Área: Administración e Informática

FINALIDAD Y UTILIZACIÓN

Objetivo de la solicitud: Realizar trabajo de investigación basado en la seguridad de la información - ISO en las áreas Administración e Informática por un periodo de 3 meses.

Justificación (Aporte y beneficios para la Municipalidad, para los funcionarios y para la ciudadanía):

- Se propone mejorar las políticas de seguridad de la información.
- Se propone ayudar en la gestión de la seguridad de la información al encargado del área de Informática así como de las demás áreas con las que cuenta la municipalidad.

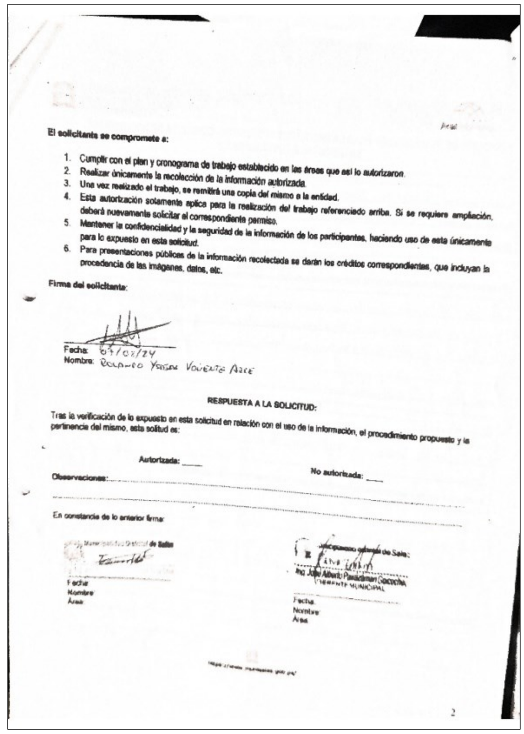
Utilización (cómo se va usar la información solicitada -dónde se piensa publicar o presentar-):

La información será presentada como tesis en la escuela profesional de Ing. de Sistemas - UNPRG.

https://www.munisalas.gob.pe/

RECEPCIONADO 07-02-24 12:48 pm

1



El solicitante se compromete a:

1. Cumplir con el plan y cronograma de trabajo establecido en las áreas que así lo autorizaron.
2. Realizar únicamente la recolección de la información autorizada.
3. Una vez realizado el trabajo, se remitirá una copia del mismo a la entidad.
4. Esta autorización solamente aplica para la realización del trabajo referenciado arriba. Si se requiere ampliación, deberá nuevamente solicitar el correspondiente permiso.
5. Mantener la confidencialidad y la seguridad de la información de los participantes, haciendo uso de esta únicamente para lo expuesto en esta solicitud.
6. Para presentaciones públicas de la información recolectada se darán los créditos correspondientes, que incluyan la procedencia de las imágenes, datos, etc.

Firma del solicitante:

Fecha: 07/02/24

Nombre: Rolando Ysaias Valiente Arce

RESPUESTA A LA SOLICITUD:

Tras la verificación de lo expuesto en esta solicitud en relación con el uso de la información, el procedimiento propuesto y la pertinencia del mismo, esta solitud es:

Autorizada: ____ No autorizada: ____

Observaciones:

En constancia de lo anterior firma:

Municipalidad Distrital de Salas

Fecha

Nombre

Área

Municipalidad Distrital de Salas

Ing. José Alberto Pasiadman Gacocha

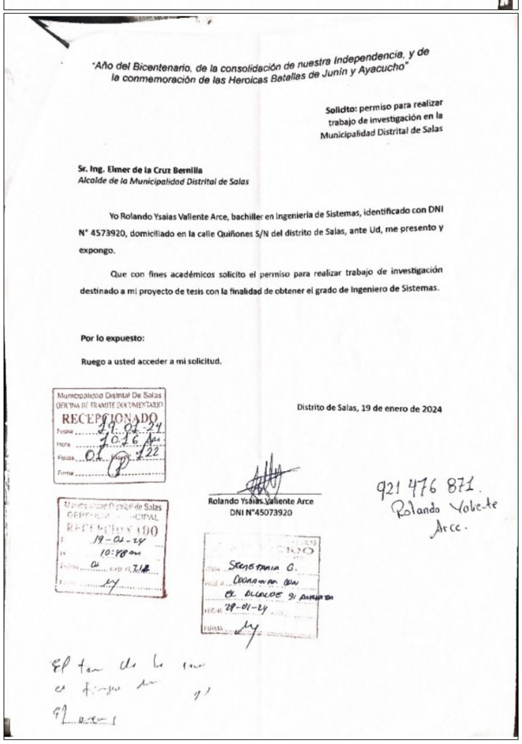
GERENTE MUNICIPAL

Fecha

Nombre

Área

2



"Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las Heroicas Batallas de Junín y Ayacucho"

Solicito: permiso para realizar trabajo de investigación en la Municipalidad Distrital de Salas

Sr. Ing. Elmer de la Cruz Bernilla
Alcalde de la Municipalidad Distrital de Salas

Yo Rolando Ysaias Valiente Arce, bachiller en Ingeniería de Sistemas, identificado con DNI N° 4573920, domiciliado en la calle Quiñones S/N del distrito de Salas, ante Ud, me presento y expongo.

Que con fines académicos solicito el permiso para realizar trabajo de investigación destinado a mi proyecto de tesis con la finalidad de obtener el grado de Ingeniero de Sistemas.

Por lo expuesto:

Ruego a usted acceder a mi solicitud.

Distrito de Salas, 19 de enero de 2024

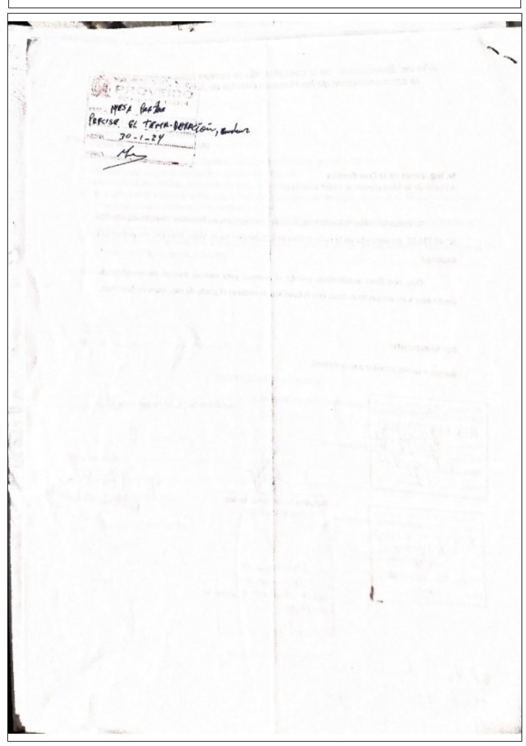
Municipalidad Distrital De Salas
OFICINA DE TRAMITE DOCUMENTARIO
RECEPCIONADO
Fecha 19-01-24
Hora 10:16 am
Folios 01 122

Rolando Ysaias Valiente Arce
DNI N°45073920

921 476 871.
Rolando Valiente Arce.

Municipalidad Distrital de Salas
RECEPCIONADO 19-01-24 10:48 am

Secretaria G. Coordinar con el alcalde 91 [illegible]
Fecha 29-01-24



Mesa Partes
Precise el tema-relación [illegible]
30-1-24

Anexo 02: Validación del modelo de SGSI por expertos

EVALUACIÓN DE PROPUESTA DE MODELO DE SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA MUNICIPALIDAD DISTRITAL DE SALAS

Apellidos y nombres de Experto: __Yanayaco Silva Gerson Dallan___DNI N°: _74868333___
Título y/o Grado de: _____Ingeniero de Sistemas_____
C.I.P. del experto: ____382634_____Fecha de revisión: ___26 de noviembre del 2025_____

TÍTULO DE TESIS: PROPUESTA DE UN SGSI BASADO EN ISO 27001:2013, PARA GARANTIZAR LA SEGURIDAD DE LA INFORMACIÓN DE LAS ÁREAS DE INFORMÁTICA Y ADMINISTRACIÓN DE LA MUNICIPALIDAD DISTRITAL DE SALAS, 2024

En la tabla de evaluación de experto, usted tiene la facultad de calificar el modelo de sistema de gestión de seguridad de la información, según su conocimiento y experiencia laboral.
Asimismo, se solicita alguna recomendación o sugerencia a tomar en cuenta.

TABLA DE EVALUACIÓN DE EXPERTOS

Maque con una "**X**", según corresponda.

ÍTEM	PREGUNTAS	Calificación				
		1	2	3	4	5
1	Se identifica de manera adecuada la situación actual de las medidas de seguridad de la información de las áreas de administración e informática, se describe adecuadamente el alcance del SGSI, gestión de riesgos, controles propuestas y plan de formación y concienciación.					X
2	Se describe adecuadamente los lineamientos para la etapa de implementación y operación del SGSI					X
3	Se describe adecuadamente los lineamientos para la verificación de la medición de los indicadores de la operación del SGSI					X
4	Se describe adecuadamente los lineamientos para realizar acciones de mejora en los controles y/o modelo de SGSI.					X

Donde:
1: Totalmente en desacuerdo
2: En desacuerdo
3: ni de acuerdo, ni en desacuerdo
4: de acuerdo
5: totalmente de acuerdo.

En conclusión, el modelo de sistema de gestión de seguridad de la información propuesto, es:
Válido y puede ser implementado (X)
Requiere ajustes antes de ser implementado ( )
No es válido ( )

Recomendaciones:

_____
_____

Lambayeque, 07 de noviembre del 2025

Nombre: Gerson Dallan Yanayaco Silva
DNI: 74868333
CIP: 382634

EVALUACIÓN DE PROPUESTA DE MODELO DE SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA MUNICIPALIDAD DISTRITAL DE SALAS

Apellidos y nombres de Experto: José Manuel Bruno Sarmiento. DNI N°: 41927454

Título y/o Grado de: Ingeniero de Sistemas / Maestro en Administración de Negocios

C.I.P. del experto: 171200 Fecha de revisión: 18/11/2025

TÍTULO DE TESIS: PROPUESTA DE UN SGSI BASADO EN ISO 27001:2013, PARA GARANTIZAR LA SEGURIDAD DE LA INFORMACIÓN DE LAS ÁREAS DE INFORMÁTICA Y ADMINISTRACIÓN DE LA MUNICIPALIDAD DISTRITAL DE SALAS, 2024

En la tabla de evaluación de experto, usted tiene la facultad de calificar el modelo de sistema de gestión de seguridad de la información, según su conocimiento y experiencia laboral.
Asimismo, se solicita alguna recomendación o sugerencia a tomar en cuenta.

TABLA DE EVALUACIÓN DE EXPERTOS

Maque con una "**X**", según corresponda.

ÍTEM	PREGUNTAS	Calificación				
		1	**2**	**3**	**4**	**5**
1	Se identifica de manera adecuada la situación actual de las medidas de seguridad de la información de las áreas de administración e informática, se describe adecuadamente el alcance del SGSI, gestión de riesgos, controles propuestas y plan de formación y concienciación.					X
2	Se describe adecuadamente los lineamientos para la etapa de implementación y operación del SGSI					X
3	Se describe adecuadamente los lineamientos para la verificación de la medición de los indicadores de la operación del SGSI					X
4	Se describe adecuadamente los lineamientos para realizar acciones de mejora en los controles y/o modelo de SGSI.				X	

Donde:
1: Totalmente en desacuerdo
2: En desacuerdo
3: ni de acuerdo, ni en desacuerdo
4: de acuerdo
5: totalmente de acuerdo.

En conclusión, el modelo de sistema de gestión de seguridad de la información propuesto, es:
Válido y puede ser implementado (X)
Requiere ajustes antes de ser implementado ( )
No es válido ( )

Recomendaciones: En general el modelo es válido y puede ser implementado.

Lambayeque, 18 de noviembre del 2025

Nombre: Bruno Sarmiento José Manuel
DNI: 41927454
CIP: 171200

EVALUACIÓN DE PROPUESTA DE MODELO DE SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA MUNICIPALIDAD DISTRITAL DE SALAS

Apellidos y nombres de Experto: Michael Kenneth Lizana Fernández. DNI N°: 47926538

Título y/o Grado de: Ingeniero de Sistemas / Maestro en Gestión Pública

C.I.P. del experto: 291363 Fecha de revisión: 18/11/2025

TÍTULO DE TESIS: PROPUESTA DE UN SGSI BASADO EN ISO 27001:2013, PARA GARANTIZAR LA SEGURIDAD DE LA INFORMACIÓN DE LAS ÁREAS DE INFORMÁTICA Y ADMINISTRACIÓN DE LA MUNICIPALIDAD DISTRITAL DE SALAS, 2024

En la tabla de evaluación de experto, usted tiene la facultad de calificar el modelo de sistema de gestión de seguridad de la información, según su conocimiento y experiencia laboral. Asimismo, se solicita alguna recomendación o sugerencia a tomar en cuenta.

TABLA DE EVALUACIÓN DE EXPERTOS

Maque con una "**X**", según corresponda.

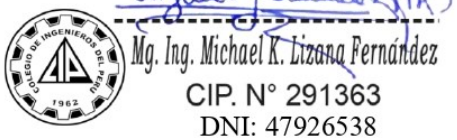
ÍTEM	PREGUNTAS	Calificación				
		1	2	3	4	5
1	Se identifica de manera adecuada la situación actual de las medidas de seguridad de la información de las áreas de administración e informática, se describe adecuadamente el alcance del SGSI, gestión de riesgos, controles propuestas y plan de formación y concienciación.					X
2	Se describe adecuadamente los lineamientos para la etapa de implementación y operación del SGSI					X
3	Se describe adecuadamente los lineamientos para la verificación de la medición de los indicadores de la operación del SGSI					X
4	Se describe adecuadamente los lineamientos para realizar acciones de mejora en los controles y/o modelo de SGSI.				X	

Donde:
1: Totalmente en desacuerdo
2: En desacuerdo
3: ni de acuerdo, ni en desacuerdo
4: de acuerdo
5: totalmente de acuerdo.

En conclusión, el modelo de sistema de gestión de seguridad de la información propuesto, es:
Válido y puede ser implementado (X)
Requiere ajustes antes de ser implementado ( )
No es válido ( )

Recomendaciones: En general el modelo es válido y puede ser implementado.

Lambayeque, 18 de noviembre del 2025



Mg. Ing. Michael K. Lizana Fernández
CIP. N° 291363
DNI: 47926538

Anexo 03: Tomas fotográficas de recolección de datos mediante entrevista y ficha de observación