UNIVERSIDAD NACIONAL AMAZÓNICA DE MADRE DE DIOS

FACULTAD DE INGENIERÍA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

TESIS

“Propuesta de implementación de un SGSI para la mejora de la seguridad de la información en la Notaría García Medina basado en la norma ISO/IEC 27001, Puerto Maldonado 2025”

PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS E INFORMÁTICA

AUTOR:

Bach. CARRILLO VENANCINO, Pablo Francisco

ASESOR:

Dr. GALLEGOS RAMOS, Nestor Antonio

PUERTO MALDONADO, 2025

UNIVERSIDAD NACIONAL AMAZÓNICA DE MADRE DE DIOS

FACULTAD DE INGENIERÍA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

TESIS

“Propuesta de implementación de un SGSI para la mejora de la seguridad de la información en la Notaría García Medina basado en la norma ISO/IEC 27001, Puerto Maldonado 2025”

PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS E INFORMÁTICA

AUTOR:

Bach. CARRILLO VENANCINO, Pablo Francisco

ASESOR:

Dr. GALLEGOS RAMOS, Nestor Antonio

PUERTO MALDONADO, 2025

RST-RI_Propuesta de implementación de un SGSI para la mejora de la seguridad de la información en la Notaría García Medina basado en la norma ISO/IEC 27001, Puerto Maldonado 2025

INFORME DE ORIGINALIDAD

8%	12%	8%	6%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	hdl.handle.net Fuente de Internet	2%
2	Submitted to Universidad Latina de Costa Rica Trabajo del estudiante	1%
3	repositorio.upci.edu.pe Fuente de Internet	1%
4	repositorio.unesum.edu.ec Fuente de Internet	1%
5	repositorio.unitec.edu Fuente de Internet	1%
6	Batista Pitti, Genarino. "Validacion de un Cuestionario que Mide los Enfoques de Aprendizaje y las Percepciones del Contexto de Aprendizaje en Estudiantes Chilenos Universitarios de Primer Ano.", Pontificia Universidad Catolica de Chile (Chile), 2020 Publicación	1%
7	repositorio.unicesar.edu.co Fuente de Internet	1%
8	Maraví Soto, Mayra Katheryne. "El desempeño docente y su influencia en el rendimiento académico de los estudiantes del 5to grado de educación secundaria de la I.E.P. “San Agustín”, del distrito de Ayacucho, año 2018", Universidad Católica los Ángeles de Chimbote (Peru) Publicación	1%
9	repositorio.utelesup.edu.pe Fuente de Internet	1%

Excluir citas	Activo	Excluir coincidencias	< 1%
Excluir bibliografía	Activo		

DEDICATORIA

A mis hijos, porque cada logro conseguido es para y por ellos, son mi sostén, mi fortaleza y mi valentía de seguir luchando por un futuro mejor.

Carrillo Venancino, Pablo Francisco.

AGRADECIMIENTOS

Agradecer en primer lugar a Dios, por la vida y la sabiduría para afrontar cada reto. A mi familia, por el apoyo que me brindan en cada paso y decisión. A mi esposa por ser la persona que me apoyó a seguir mis metas. A mis docentes de la carrera de ingeniería sistemas e informática de la UNAMAD que hicieron de mí una mejor persona y mejor profesional.

Carrillo Venancino, Pablo Francisco.

RESUMEN

La presente investigación tiene como objetivo determinar la influencia de la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), basado en la norma ISO/IEC 27001, en la mejora de la seguridad de la información en la organización. El estudio fue de tipo aplicada, con enfoque cuantitativo y diseño preexperimental de un solo grupo con medición pretest y postest (O_1–X–O_2). La muestra está conformada por 35 colaboradores, en la que se aplicó un cuestionario con escala Likert, validado mediante el coeficiente Alfa de Cronbach, obteniéndose valores superiores a 0.95, lo que evidencia alta confiabilidad. Dado que los datos no presentaron distribución normal (Shapiro- Wilk, $p < 0.05$), se utilizaron las pruebas no paramétricas de Wilcoxon y Rho de Spearman para el análisis estadístico. Los resultados mostraron que la implementación del SGSI tiene una correlación positiva muy fuerte y estadísticamente significativa con la seguridad de la información ($\rho = 0.947$; $p = 0.000$; $N = 35$). Estos resultados demuestran mejoras significativas en todas las dimensiones de la seguridad de la información tras la implementación del SGSI. Por tanto, se concluyó que la implementación del SGSI basado en la norma ISO/IEC 27001 influye de manera positiva, significativa y directa en la seguridad de la información en la Notaría García Medina, fortaleciendo la protección de los activos de información y reduciendo riesgos organizacionales.

Palabras clave: SGSI, ISO/IEC 27001, seguridad de la información, confidencialidad, integridad, disponibilidad.

ABSTRACT

This research aims to determine the influence of the implementation of an Information Security Management System (ISMS), based on the ISO/IEC 27001 standard, on improving information security within the organization. The study was applied in nature, with a quantitative approach and a pre-experimental design consisting of a single group with pretest and posttest measurements (O_1–X–O_2). The sample consisted of 35 collaborators, to whom a Likert-scale questionnaire was administered, validated using Cronbach's Alpha coefficient, obtaining values above 0.95, which indicates high reliability.

Since the data did not present a normal distribution (Shapiro–Wilk, $p < 0.05$), non-parametric tests such as Wilcoxon and Spearman's Rho were used for statistical analysis. The results showed that the implementation of the ISMS has a very strong and statistically significant positive correlation with information security ($\rho = 0.947$; $p = 0.000$; $N = 35$). These findings demonstrate significant improvements across all dimensions of information security following the implementation of the ISMS.

Therefore, it was concluded that the implementation of an ISMS based on the ISO/IEC 27001 standard has a positive, significant, and direct influence on information security at Notaría García Medina, strengthening the protection of information assets and reducing organizational risks.

Keywords: ISMS, ISO/IEC 27001, information security, confidentiality, integrity, availability.

PRESENTACIÓN

Este trabajo de tesis, desarrollado conforme a lo estipulado en el Reglamento General de Grados y Títulos de la UNAMAD para obtener el título en Ingeniería de Sistemas e Informática, plantea la implementación de un Sistema de Gestión de la Seguridad de la Información (SGSI) en la Notaría García Medina de Puerto Maldonado, tomando como referencia la norma ISO/IEC 27001.

Partiendo de un diagnóstico de la situación actual, se detectaron las vulnerabilidades, amenazas y debilidades presentes en los sistemas de la notaría. La iniciativa tiene como finalidad definir políticas, controles y procedimientos que se ajusten a los estándares de la norma, con el propósito de robustecer la confidencialidad, integridad y disponibilidad de la información. Adicionalmente, la propuesta pretende fomentar el cumplimiento normativo y la mejora continua en la gestión de la seguridad informática dentro del ámbito notarial digital.

La estructura de la tesis se compone de cuatro capítulos: el primero aborda la descripción y formulación del problema, los objetivos, variables, hipótesis, justificación y consideraciones éticas. El segundo capítulo presenta el marco teórico, incluyendo los antecedentes nacionales e internacionales y los fundamentos conceptuales que sirven de base para la investigación. El tercer capítulo detalla la metodología empleada, y el cuarto expone los resultados alcanzados. El documento finaliza con las conclusiones, sugerencias, bibliografía y anexos, entre los que se encuentran la matriz de consistencia, el instrumento de investigación y los documentos de autorización.

INTRODUCCIÓN

La transformación digital de las últimas décadas ha impactado profundamente al sector notarial, impulsando una transición hacia la reducción del uso de papel y la ampliación del acceso a los servicios notariales, estos, al custodiar y gestionar datos sensibles y documentación jurídica con validez probatoria, se han convertido en blancos potenciales para amenazas cibernéticas. Estas incluyen, entre otras, ciberataques sofisticados, accesos no autorizados y alteraciones malintencionadas de la información, lo cual vulnera directamente los principios fundamentales de la seguridad de la información: la confidencialidad, la integración y la disponibilidad de los datos.

A nivel internacional, se ha reconocido la importancia de establecer marcos normativos que aseguren la protección de la información. En este contexto, la norma ISO/IEC 27001 ofrece un conjunto de requisitos, controles y buenas prácticas destinados a identificar vulnerabilidades, mitigar amenazas y salvaguardar los activos digitales de las organizaciones.

Diversas investigaciones internacionales han demostrado que su implementación fortalece la gobernanza, incrementa la resiliencia organizacional y mejora la capacidad de respuesta ante incidentes de seguridad [1].

En el contexto nacional, la ley de Protección de Datos Personales (Ley N.º 29733) establece que tanto el titular como el encargado del banco de datos deben implementar medidas técnicas, organizativas y legales que aseguren la protección y seguridad de la información contenida en dichos sistemas. [2]. Esta normativa refuerza la necesidad de implementar mecanismos formales que permitan prevenir filtraciones, accesos indebidos y pérdida de información, especialmente en sectores donde se gestionan datos altamente sensibles como en las notarías.

En función de lo expuesto, se identificó como problemática principal la ausencia de un Sistema de Gestión de Seguridad de la Información (SGSI) en la Notaría García Medina, ubicada en la ciudad de Puerto Maldonado. La falta de controles estructurados, políticas de seguridad de la información y la ausencia de

cumplimiento de normas internacionales deja expuesta a la institución a riesgos que podrían afectar tanto su operatividad como la confianza de los usuarios.

Esta investigación es relevante para la región de Madre de Dios y el campo de la Ingeniería de Sistemas e Informática, debido a la limitada adopción de estándares de seguridad en el manejo de información sensible, además, la creciente preocupación por la protección de los datos personales exige que las instituciones que gestionan información sensible actúen con responsabilidad y transparencia. Las notarías, al ser intermediarias de fe pública, deben estar a la vanguardia en términos de ciberseguridad y cumplimiento normativo.

Se consideró como objetivo general proponer la implementación de un SGSI, en base a la norma ISO/IEC 27001, para fortalecer la seguridad en los sistemas notariales utilizados en la Notaría García Medina. Específicamente, se buscó diagnosticar el estado actual de la notaría en materia de seguridad y resguardo de la información, identificar vulnerabilidades y amenazas, y plantear medidas alineadas con los controles establecidos por dicha norma internacional.

El trabajo de investigación se estructura en cuatro capítulos. El Capítulo I presenta el planteamiento del problema, los objetivos, las hipótesis, la identificación de las variables y la justificación del estudio. El Capítulo II desarrolla el marco teórico, donde se abordan los fundamentos conceptuales de la seguridad de la información, el Sistema de Gestión de Seguridad de la Información y la norma ISO/IEC 27001, así como los antecedentes relacionados con investigaciones similares. El Capítulo III describe la metodología de la investigación, detallando el enfoque, diseño, población, técnicas e instrumentos de recolección de datos, así como los procedimientos utilizados para el análisis estadístico. Finalmente, el Capítulo IV expone los resultados obtenidos, su análisis e interpretación, las conclusiones derivadas del estudio y las recomendaciones orientadas a fortalecer la gestión de la seguridad de la información en la Notaría García Medina.

ÍNDICE

PRESENTACIÓN 7
INTRODUCCIÓN 8
1. CAPITULO I: PROBLEMA DE INVESTIGACIÓN 15
1.1. Descripción del problema 15
1.2. Formulación del problema 17
1.2.1. Problema general 17
1.2.2. Problemas específicos 17
1.3. Objetivos 17
1.3.1. Objetivo general 17
1.3.2. Objetivo especifico 17
1.4. Variables 18
1.5. Operacionalización de Variables 18
1.6. Hipótesis 19
1.6.1. Hipótesis General 19
1.6.2. Hipótesis Especificas 19
1.7. Justificación 19
1.8. Consideraciones éticas 21
2. CAPITULO II: MARCO TEORICO 22
2.1. Antecedentes de estudio 22
2.1.1. Internacionales 22
2.1.2. Nacionales 27
2.2. Marco Teórico 31
2.2.1. Las notarías en el Perú 31
2.2.2. El notario 32
2.2.3. Digitalización de las notarías en el Perú 33
2.2.4. Aspectos generales sobre las notarías en Madre de Dios 33
2.2.5. SISNOT 35
2.2.6. Norma ISO 27001 37
2.2.7. Análisis de riesgos 42
2.3. Definición de Términos 43
3. CAPITULO III: METODOLOGIA DE INVESTIGACIÓN 46
3.1. Tipo de Estudio 46
3.2. Diseño del Estudio 46
3.3. Población y Muestra 48

3.4. Métodos y Técnicas 48
3.5. Tratamiento de los Datos 52
4. CAPÍTULO IV: RESULTADOS DEL TRABAJO DE INVESTIGACIÓN 54
4.1. Estudio del contexto actual de la notaría 54
4.2. Fases de implementación del SGSI 59
4.3. Procesamiento, análisis e interpretación de resultados 121
CONCLUSIONES 137
SUGERENCIAS 138
REFERENCIAS BIBLIOGRAFICAS 139
ANEXOS 144
Anexo 1: Carta de compromiso de asesor 144
Anexo 2: Matriz de Operacionalización de Variables 145
Anexo 3: Matriz de Consistencia 147
Anexo 4: Instrumento 148
Anexo 5: Solicitud de autorización para realización de estudio 151
Anexo 6: Solicitud de validación de instrumento 152
Anexo 7: Ficha de Validación 155
Anexo 8: Consentimiento informado 161
Anexo 9: Acta de proyecto 162
Anexo 10: Política general de seguridad de la información 163
Anexo 11: Políticas complementarias 166
Anexo 12: Acta de cierre de proyecto 185

INDICE DE TABLAS

Tabla 1: Operacionalización de variables 18
Tabla 2: Cláusulas Clave de ISO/IEC 27001 y Preguntas Fundamentales para su Implementación 40
Tabla 3: Muestra considerada para el estudio de confiabilidad pretest 49
Tabla 4: Análisis de cada pregunta del cuestionario pretest 50
Tabla 5: Alfa de Cronbach para cuestionario pretest 50
Tabla 6: Muestra considerada para el estudio de confiabilidad postest 51
Tabla 7: Análisis de cada pregunta del cuestionario postest 51
Tabla 8: Alfa de Cronbach para cuestionario postest 52
Tabla 9: Análisis de conocimientos sobre seguridad de la información en la notaría 54
Tabla 10: Análisis de conocimientos sobre el nivel de importancia que se le da a la seguridad de la información en la notaría 55
Tabla 11: Análisis de frecuencia con la que el personal recibe capacitaciones sobre seguridad de la información en la notaría 56
Tabla 12: Análisis de nivel de conocimiento de los empleados sobre los riesgos a los que está expuesta la información en la notaría 57
Tabla 13: Análisis de nivel de conocimiento de los empleados sobre los riesgos a los que está expuesta la información en la notaría 58
Tabla 14: Misión, visión y objetivos de la Notaria García Medina de Puerto Maldonado 59
Tabla 15: Identificación de amenazas 65
Tabla 16: Identificación de vulnerabilidades 66
Tabla 17: Criterios para la tasa de ocurrencia del riesgo 68
Tabla 18: Criterios para la determinación de impacto 68
Tabla 19: Matriz de calor de probabilidad - impacto 69
Tabla 20: Tratamiento de riesgo 70
Tabla 21: Inventario general de activos identificados 72
Tabla 22: Valores designados a dimensiones de activos 75
Tabla 23: Determinación del valor de los activos 76
Tabla 24: Análisis de riesgos de los activos (Amenazas y vulnerabilidades) 78
Tabla 25: Tabla de evaluación de riesgos 84

Tabla 26: Mecanismos de control detectados..... 93
Tabla 27: Aspectos de la declaración de aplicabilidad.....103
Tabla 28: Escala de aceptación de la variable independiente.....121
Tabla 29: Prueba de normalidad para la dimensión Confidencialidad pre y post implementación del SGSI 122
Tabla 30: Prueba de Wilcoxon para la dimensión confidencialidad pre y post implementación del SGSI 123
Tabla 31: Prueba de normalidad para la dimensión Integridad pre y post implementación del SGSI 124
Tabla 32: Prueba de Wilcoxon para la dimensión integridad pre y post implementación del SGSI 125
Tabla 33: Prueba de normalidad para la dimensión Disponibilidad pre y post implementación del SGSI 126
Tabla 34: Prueba de Wilcoxon para la dimensión disponibilidad pre y post implementación del SGSI 127
Tabla 35: Prueba de normalidad para la VD pre y post implementación del SGSI 128
Tabla 36: Prueba de Wilcoxon para la VD pre y post implementación del SGSI 129
Tabla 37: Prueba de normalidad para la VD de independiente.....130
Tabla 38: Resultado de test de Spearman para validar la hipótesis general . 131
Tabla 39: Resultado del test de Spearman para validación de la hipótesis especifica N°1.....133
Tabla 40: Resultado del test de Spearman para validación de la hipótesis especifica N°2.....134
Tabla 41: Resultado del test de Spearman para validación de la hipótesis especifica N°3.....135

INDICE DE IMÁGENES

Figura 1: Organigrama notaría García Medina 33
Figura 2: Diagrama de procesos de los servicios prestados por la notaría 35
Figura 3: Última versión de SISNOT 36
Figura 4: Módulos de SISNOT 37
Figura 5: Modelo PDCA ISO 27001 39
Figura 6: Cláusulas del ISO/IEC 27001 39
Figura 7: Método de evaluación y tratamiento del riesgo 42
Figura 8: Resultados de cuestionario (pregunta 01) 55
Figura 9: Resultados de cuestionario (pregunta 02) 56
Figura 10: Resultados de cuestionario (pregunta 03) 57
Figura 11: Resultados de cuestionario (pregunta 04) 58
Figura 12: Resultados de cuestionario (pregunta 05) 59
Figura 13: Diagrama de flujo del funcionamiento general de la notaría 61
Figura 14: Diagrama de flujo del procesamiento de datos notariales 62
Figura 15: Diagrama del flujo del proceso de cobranza en la notaría 63
Figura 16: Diagrama de flujo del proceso de conservación documental 64
Figura 17: Resultados obtenidos para la variable independiente 121
Figura 18: Resultados obtenidos para la dimensión confidencialidad pre y post implementación del SGSI 124
Figura 19: Resultados obtenidos para la dimensión confidencialidad pre y post implementación del SGSI 126
Figura 20: Resultados obtenidos para la dimensión disponibilidad pre y post implementación del SGSI 128
Figura 21: Resultados obtenidos para la dimensión identificación de riesgos pre y post test 130

1. CAPITULO I: PROBLEMA DE INVESTIGACIÓN

1.1. Descripción del problema

En la actualidad, la protección de la información se ha convertido en una prioridad estratégica para instituciones públicas y privadas, debido al creciente número de ciberataques, filtraciones de datos, accesos no autorizados y gestión de la información sin políticas de seguridad. Según el Informe de Ciberseguridad 2024 publicado por la OEA [3] el 70% de las entidades públicas en América Latina no cuentan con una política integral de seguridad de la información, lo que las hace altamente vulnerables a incidentes.

Para las empresas, la información generada, almacenada y procesada es un activo esencial, su adecuada gestión y protección son fundamentales, ya que cualquier vulnerabilidad puede derivar en consecuencias legales, financieras y reputacionales. Según Lugo Marín, et al. [4] las empresas pueden incurrir en procesos legales, problemas financieros y otros si no toman las medidas necesarias para salvaguardar dichos elementos considerados como activos, ya que a la vez esta información puede ser de índole confidencial de usuarios externos a la empresa.

Rodriguez Baca et al. [5] dice que toda información debe ser protegida pero también debe estar disponible para ser accedida oportunamente. Considerando el enfoque de la seguridad de la información es necesario considerar tres elementos fundamentales como son: la confidencialidad, integridad y disponibilidad.

En el contexto nacional post-pandemia, la protección de la información sensible se ha posicionado como prioridad para las instituciones y compañías. De acuerdo con datos de la plataforma Threat Intelligence Insider Latin America de Fortinet [6] el Perú experimentó más de 613 millones de ataques cibernéticos durante el primer semestre de 2020.

Esta situación exige que las organizaciones adopten normas y políticas de protección de la información.

En el ámbito regional, la notaría García Medina no cuenta con la aplicación formal de un SGSI lo que evidencia una gestión empírica y no sistematizada de la seguridad de la información. Esta situación implica que los procesos vinculados al tratamiento, almacenamiento y transmisión de información sensible se desarrollen sin lineamientos estandarizados, incrementando la exposición a riesgos como accesos no autorizados, pérdida de datos, alteración de la información y vulnerabilidades tecnológicas. Considerando que la notaría administra información de carácter legal y confidencial, cuya integridad y disponibilidad resultan críticas para la fe pública y la confianza de los usuarios.

El estándar ISO/IEC 27001 establece directrices para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), proporcionando un marco estructurado para la identificación, evaluación y mitigación de riesgos en sistemas digitales [7].

Sin embargo, pese a su importancia, muchas organizaciones han adoptado soluciones tecnológicas sin considerar dicho enfoque, lo que las expone a distintas amenazas que comprometerían la seguridad de la información manejada.

Para solucionar ese dilema se propone la implementación de un SGSI bajo el marco del ISO 27001, el cual garantiza la confidencialidad, integridad y disponibilidad de la información de cualquier organización, además proporciona un marco normativo para detectar riesgos, desarrollar controles y mejorar de manera continua los procesos relacionados con la seguridad. Según Panaqué Dominguez et al. [8], su enfoque por procesos y su adaptabilidad a distintos contextos lo convierten en una herramienta clave para proteger información crítica y optimizar operaciones, fortaleciendo así la confianza en entornos digitales.

1.2. Formulación del problema

1.2.1. Problema general

- ¿En qué medida la propuesta de implementación de un SGSI en el marco ISO/IEC 27001 contribuye con la mejora de la seguridad de la información en la notaría García Medina en el año 2025?

1.2.2. Problemas específicos

- ¿En qué medida la propuesta de implementación de un SGSI en el marco ISO/IEC 27001 contribuye a mejorar la confidencialidad de la información en la notaría García Medina?
- ¿En qué medida la propuesta de implementación de un SGSI en el marco ISO/IEC 27001 contribuye a fortalecer la integridad de la información en la notaría García Medina?
- ¿En qué medida la propuesta de implementación de un SGSI en el marco ISO/IEC 27001 contribuye a mejorar la disponibilidad de la información en la notaría García Medina?

1.3. Objetivos

1.3.1. Objetivo general

- Evaluar en qué medida la propuesta de implementación de un SGSI en el marco de la norma ISO/IEC 27001 contribuye a mejorar la seguridad de la información en la notaría García Medina en el año 2025.

1.3.2. Objetivo especifico

- Evaluar en qué medida la propuesta de implementación de un SGSI en el marco de la norma ISO/IEC 27001 contribuye a mejorar la confidencialidad de la información en la notaría García Medina.
- Evaluar en qué medida la propuesta de implementación de un SGSI en el marco de la norma ISO/IEC 27001 contribuye a fortalecer la integridad de la información en la notaría García Medina.
- Evaluar en qué medida la propuesta de implementación de un SGSI en el marco de la norma ISO/IEC 27001 contribuye a mejorar la disponibilidad de la información en la notaría García Medina.

1.4. Variables

Variable Independiente: Propuesta de implementación de un SGSI basado en la norma ISO/IEC 27001

Variable Dependiente: Mejora de la seguridad de la información en la Notaría García Medina

1.5. Operacionalización de Variables

Tabla 1: Operacionalización de variables

Variables	Definición Conceptual	Dimensiones	Indicadores
Independiente: Implementación de un SGSI basado en la norma ISO/IEC 27001	Adopción de un conjunto de requisitos, controles y buenas prácticas internacionales para establecer, implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI) [9].	Política de seguridad de la información	Existencia de políticas documentadas y actualizadas
		Gestión de riesgos	Procesos de identificación, análisis y tratamiento de riesgos
		Mejora continua	Registro de auditorías internas/ acciones correctivas
		Capacitación y concientización	Programas de formación en seguridad de la información
Dependiente: Mejora de la seguridad de la información en la Notaría García Medina	Conjunto de medidas técnicas, organizativas y normativas implementadas para proteger los procesos y documentos notariales digitales contra amenazas que puedan comprometer su confidencialidad, integridad y disponibilidad. Esto incluye la protección frente a alteraciones indebidas, pérdidas de información y fallos en la continuidad operativa del servicio notarial digital [10].	Confidencialidad	Existencia de mecanismos para prevenir accesos no autorizados
		Integridad	Existencia de mecanismos de validación/ registros de modificaciones
		Disponibilidad	Accesibilidad y funcionamiento continuo del sistema

Fuente: Elaboración propia

1.6. Hipótesis

1.6.1. Hipótesis General

Hipótesis nula:

- **H0:** La propuesta de implementación de un SGSI en el marco de la norma ISO/IEC 27001, no contribuirá a mejorar la seguridad de la información en la notaría García Medina en el año 2025

Hipótesis alternativa:

- **H1:** La propuesta de implementación de un SGSI en el marco de la norma ISO/IEC 27001, contribuirá a mejorar la seguridad de la información en la notaría García Medina en el año 2025

1.6.2. Hipótesis Especificas

- **He1:** La propuesta de implementación de un SGSI en el marco de la norma ISO/IEC 27001 contribuirá a mejorar la confidencialidad de la información en la notaría García Medina en el año 2025.
- **He2:** La propuesta de implementación de un SGSI en el marco de la norma ISO/IEC 27001 contribuirá a fortalecer la integridad de la información en los sistemas notariales en el año 2025.
- **He3:** La propuesta de implementación de un SGSI en el marco de la norma ISO/IEC 27001 contribuirá a mejorar la disponibilidad de la información en los sistemas notariales en el año 2025.

1.7. Justificación

La presente tesis es pertinente, actual y necesaria, ya que responde a una problemática crítica en el ámbito notarial: la falta de una administración sistemática y estandarizada de la seguridad de la información. En este sentido, la propuesta de implementación de la norma ISO/IEC 27001 constituye una solución integral, al establecer un SGSI que permite identificar, evaluar y mitigar los riesgos inherentes al tratamiento de datos en entornos digitales.

Desde el punto de vista práctico, la norma ISO/IEC 27001 ofrece un enfoque organizado que garantiza la integridad, confidencialidad y disponibilidad de la información, según Toynsé de la Rosa [11] estos tres principios son fundamentales para los servicios notariales, ya que trabajan con datos sensibles y de alto valor legal, además un SGSI bien establecido admite a las organizaciones minimizar vulnerabilidades, evitar pérdidas económicas y proteger su reputación institucional.

En el ámbito teórico, esta investigación contribuye a enriquecer el conocimiento existente en la gestión de vulnerabilidades y riesgos de la información en instituciones notariales, un campo aún poco explorado en contextos latinoamericanos. Según Bustamante García et al. [12] los marcos internacionales como ISO 27001 permiten el desarrollo de una teoría aplicada de seguridad adaptada a sectores críticos, como por ejemplo las notarías.

Desde el punto de vista metodológico, el trabajo propone una propuesta de implementación sistemática, basada en las etapas del ciclo PHVA (Planificar, Hacer, Verificar, Actuar), lo que garantiza un enfoque replicable y sustentado. Como señala Moyano Hernández et al. [13] los marcos metodológicos basados en normas internacionales permiten una mejor medición de resultados y efectividad en la mitigación de riesgos.

El impacto social de esta investigación es también significativo. En Perú, muchas notarías aún no adoptan estándares de seguridad internacionales, lo que genera brechas de confianza en los ciudadanos respecto al manejo de sus datos personales. De acuerdo a la ley número 29733, los titulares de bancos de información personal deben garantizar su seguridad [2]. Promover una cultura de seguridad informática en este sector ayuda a proteger derechos como la privacidad y la integridad documental.

En cuanto al aspecto económico, la correcta aplicación de la norma ISO/IEC 27001 puede traducirse en reducción de costos por incidentes de seguridad, mejora en la gestión de procesos, y cumplimiento normativo, evitando sanciones. Esto es respaldado por la Organización Internacional

de Normalización (ISO), que destaca que los SGSI bien implementados mejoran la eficiencia organizacional y reducen costos asociados a brechas de seguridad [14].

En el plano tecnológico, esta investigación impulsa la modernización digital del sistema notarial, adecuándolo a las exigencias del siglo XXI. La transformación digital debe ir acompañada de prácticas de ciberseguridad sólidas, y como indica Chica Campuzano [15] la tecnología sin gestión de seguridad aumenta la exposición a ataques que comprometen la operatividad y confianza institucional.

1.8. Consideraciones éticas

La presente investigación cumple con los principios éticos fundamentales para garantizar la integridad del proceso investigativo y el respeto a los derechos de las personas y entidades involucradas, la investigación asegura el anonimato y la confidencialidad de los participantes. Toda la información recolectada mediante encuestas, entrevistas u otros instrumentos será utilizada exclusivamente con fines académicos, y los datos personales serán tratados de manera reservada.

La investigación se conducirá dentro de un marco de honestidad académica, evitando cualquier clase de plagio, manipulación de datos o prácticas que puedan comprometer la veracidad de los resultados. También se respetarán los derechos de autor de las fuentes consultadas, citándolas adecuadamente según normas ISO de acuerdo al reglamento general de grados y títulos de la UNAMAD.

2. CAPITULO II: MARCO TEORICO

2.1. Antecedentes de estudio

2.1.1. Internacionales

- La tesis de Alava Cuadra et al. [16] titulado **“DISEÑO DE UN SGSI BASADO EN EL ESTANDAR ISO 27001 PARA LA EMPRESA INVIMEDIC S.A.”**

  El objetivo general de esta tesis fue elaborar e implementar un Sistema de Gestión de la Seguridad de la Información basado en la norma ISO 27001 para la empresa INVIMEDIC S.A., con el fin de mitigar las vulnerabilidades en el diseño de seguridad de sus sistemas informáticos. La investigación aplicó un enfoque teórico-práctico basado en la norma ISO 27001, guiando el ciclo completo de creación, puesta en marcha, operación y mejora continua de un Sistema de Gestión de Seguridad de la Información (SGSI) personalizado para la organización. Se realizó un análisis exhaustivo de los fallos en el diseño de seguridad existente, seguido de la aplicación de controles y políticas alineados con el estándar internacional.

  Como resultado se pudo evidenciar que esta implementación permitió una gestión más eficiente y segura de los procesos empresariales, reduciendo las vulnerabilidades y fortaleciendo la protección de la información frente a amenazas externas.

  Conclusión: La investigación demostró que la adopción de un SGSI basado en ISO 27001 mejora la postura de seguridad de la organización, garantiza el cumplimiento de estándares internacionales y facilitó la gestión segura de los procesos críticos

del negocio, reduciendo la exposición a amenazas y garantizando la protección de los datos.

La investigación desarrollada guarda una relación directa con el presente estudio, ya que ambos se centran en la implementación de un Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001 como estrategia para mitigar vulnerabilidades y fortalecer la protección de los sistemas informáticos. Asimismo, coincide en la aplicación de controles y políticas alineadas con el estándar internacional.

- La tesis de Pulgarín García [17] titulada **"DISEÑO DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN BAJO LOS LINEAMIENTOS DEL ESTANDAR ISO/IEC 27001 PARA LA NOTARÍA ÚNICA DE LA CIUDAD DE DOSQUEBRADAS (RISARALDA)"**.

  El objetivo de este trabajo aplicado fue diseñar un Sistema de Gestión de Seguridad de la Información basado en la norma ISO 27001 para la Notaría Única de Dosquebradas, con el fin de identificar, categorizar y evaluar la criticidad de sus activos de información, permitiendo así una gestión más eficiente de los riesgos asociados. Se logró mapear los activos de información según su nivel de criticidad y establecer controles específicos para mitigar riesgos. La aplicación de estas normas permitió fortalecer los procesos internos en aspectos de seguridad, optimizar el seguimiento de vulnerabilidades por parte del área de TI y alinear los procesos organizacionales con estándares internacionales de ciberseguridad.

  Conclusión: El diseño del SGSI basado en ISO 27001 permitió a la Notaría Única de Dosquebradas identificar y priorizar controles de seguridad de manera eficiente, mejorando la protección de la información importante. La adopción de estos controles, vinculados a la categorización de activos, no solo facilitó el monitoreo continuo por parte del equipo de TI, sino que reforzó también la concientización colectiva en materia de seguridad, asegurando una

gestión que cumple con los estándares internacionales y eleva los niveles de seguridad.

El estudio presenta una alta similitud temática y contextual con la presente investigación, ya que ambos se desarrollan en el ámbito notarial y se fundamentan en el diseño de un SGSI basado en la norma ISO/IEC 27001. Este antecedente refuerza la importancia de la investigación actual, al demostrar que la aplicación de un SGSI en notarías contribuye significativamente a mejorar la seguridad de la información y el cumplimiento de estándares internacionales.

- La tesis de Cortés Malagón et al. [18] titulada "**DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) PARA LOS PROCESOS CRITICOS DE SUMMUM PROJECT BASADO EN LA NORMA NTC-ISO-IEC-27001**".

  El objetivo de este trabajo de investigación fue diseñar un SGSI para los procesos críticos de Summum Project, fundamentado en la norma NTC-ISO/IEC 27001, con el fin de resguardar sus activos estratégicos y reforzar su competitividad en el sector de gestión de proyectos petroleros. El estudio se desarrolló bajo un enfoque descriptivo, analizando la información recolectada sin alterar el entorno organizacional. Este tipo de investigación, también conocido como observacional o correlacional, permitió diagnosticar la situación actual de la seguridad de la información, identificando riesgos y necesidades sin intervenir en sus operaciones.

  El diseño del SGSI se centró en los procesos críticos del negocio, complementándose con un programa de concientización en seguridad de la información, el cual se desplegó inicialmente entre los líderes de cada área, con posibilidad de extenderse a todos los trabajadores, se generaron materiales de apoyo (guías, actividades periódicas y recursos didácticos) para promover buenas prácticas y reducir riesgos de ciberataques.

  Conclusión: La implementación del SGSI es fundamental para proteger los activos y establecer un entorno seguro. La concientización continua del personal mediante un plan estructurado y materiales educativos es clave para mitigar

amenazas y fomentar una cultura organizacional de seguridad. Este proyecto no solo fortalece la confiabilidad operativa, sino que también mejora la competitividad de la empresa en el sector petrolero, al comprometerse usando estándares internacionales de gestión de vulnerabilidades y riesgos.

La investigación se relaciona con el presente estudio desde un enfoque metodológico y conceptual, ya que ambos parten del diagnóstico de la situación actual de la seguridad de la información para diseñar un SGSI basado en la norma ISO/IEC 27001. Además, coincide en la importancia de la concientización del personal como elemento clave para la reducción de riesgos.

- La tesis de Gómez Sánchez et al. [19] "**IMPLEMENTACION SGSI EN LA UNIDAD DE RENTAS BASADO ENLA ISO 27001**".

  Este trabajo tuvo como objetivo principal desarrollar el marco base para implementar un SGSI en la Unidad de Rentas de la Gobernación de Caldas. Este documento base, alineado con la norma ISO/IEC 27001:2022, servirá para guiar el análisis organizacional y definir los controles de seguridad necesarios.

  La metodología incluyó un análisis de riesgos según ISO 31000, mediante entrevistas a 15 funcionarios (de 80 totales) para evaluar su conciencia sobre seguridad informática, junto con la revisión de procesos técnicos y portales web institucionales.

  Los resultados obtenidos son el desarrollo de un documento guía con políticas de seguridad adaptadas, medidas para proteger datos sensibles y un diagnóstico del nivel de sensibilización del personal. **Conclusión:** la implementación del SGSI es estratégica para proteger información crítica, mitigar riesgos como ciberataques o pérdida de datos, y fortalecer la confianza institucional, requiriendo asignación de recursos y capacitación continua. El documento sirve como hoja de ruta replicable para otras dependencias de la Gobernación, estableciendo bases para una cultura organizacional proactiva en ciberseguridad.

  El estudio guarda relación con la presente investigación al proponer la implementación de un SGSI basado en la norma ISO/IEC

27001:2022 en una entidad pública, con énfasis en el análisis de riesgos y la sensibilización del personal. Es similar en cuanto al uso de diagnósticos organizacionales y evaluación del nivel de concientización en seguridad de la información, lo que coincide con el enfoque aplicado en la Notaría García Medina. Los hallazgos del antecedente respaldan la relevancia de contar con un documento base y políticas formales para fortalecer la gestión de la seguridad de la información.

- La tesis de Busto Perez de Mendiguren [20] titulada **“PLAN DE IMPLEMENTACION DEL SGSI BASADO EN LA ISO/IEC 27001 DE LA EMPRESA TRADUX”.**

  El objetivo principal de esta tesis fue la creación e implantación integral de un SGSI para TRADUX, aplicando metodologías de análisis de riesgos y alineado con el marco de la norma ISO/IEC 27001. La investigación combinó un enfoque teórico, que permitió recopilar y analizar información diversa, con un carácter exploratorio, descriptivo y explicativo para evaluar el estado actual de la seguridad de la información en la empresa. Tras la elaboración e implementación de las propuestas del SGSI, se realizó un análisis exhaustivo que demostró una evolución significativa en los controles de seguridad, evidenciada en el gráfico radar, donde se observa un crecimiento notable en los distintos dominios, gracias a la ejecución de los proyectos y la adopción de un enfoque de mejora continua.

  Conclusión: Con un compromiso sólido hacia la excelencia y el cumplimiento de la norma ISO/IEC 27001:2022, TRADUX ha fortalecido sustancialmente sus controles de seguridad. La implementación de las iniciativas propuestas permitirá alcanzar un nivel de madurez superior, optimizando así su postura de seguridad y garantizando una gestión robusta y proactiva de los riesgos.

  La tesis se relaciona con la presente investigación al abordar la implementación integral de un SGSI basado en la norma ISO/IEC 27001, incorporando el enfoque de mejora continua y evaluación del nivel de madurez de los controles de seguridad. Ambos estudios

coinciden en demostrar que la aplicación sistemática del SGSI genera mejoras significativas en la postura de seguridad organizacional.

2.1.2. Nacionales

- La tesis de Esquicha Flores [21] titulada **“ISO 27001: SEGURIDAD DE LA INFORMACIÓN Y SU IMPACTO EN EL PRINCIPIO DE NEGOCIO EN MARCHA PARA EMPRESAS QUE PRESTAN SERVICIOS TECNOLÓGICOS EN SAN ISIDRO, 2021”**.

  El objetivo de esta tesis fue evaluar el impacto de la implementación de la norma ISO 27001 en empresas de servicios tecnológicos en el distrito de San Isidro durante el 2021, considerando la creciente digitalización de procesos y la importancia de proteger los activos de información con un enfoque teórico-analítico, incluyendo las Normas Internacionales de Información Financiera (NIIF), para validar la relación entre seguridad de la información y continuidad operativa e integración de teoría, análisis de casos y estándares para evaluar cómo la ISO 27001 asegura el principio contable de negocio en marcha.

  Los resultados obtenidos son la protección de activos críticos: La ISO 27001 demostró ser un marco eficaz para salvaguardar la información, mitigando riesgos que podrían afectar la continuidad del negocio. Se identificó que algunas empresas presentaban dificultades en la integración de controles de seguridad con sus procesos contables, revelando la necesidad de mayor capacitación interdisciplinaria.

  Conclusión: La ISO 27001 no solo mejora la seguridad informática, sino que también respalda el principio de negocio en marcha al reducir amenazas que podrían interrumpir operaciones. Su adopción en empresas tecnológicas de San Isidro evidenció mayor ventaja competitiva al garantizar la confiabilidad de datos financieros y operativos.

  La investigación guarda una relación teórica con el presente estudio, al analizar la implementación de la norma ISO/IEC 27001

como un factor clave para garantizar la continuidad operativa y la protección de los activos de información, además, sus conclusiones refuerzan la importancia de la seguridad de la información como elemento estratégico, lo cual sustenta la presente investigación al demostrar que la adopción de ISO 27001 contribuye a reducir riesgos que podrían afectar el funcionamiento de las organizaciones.

- La tesis de García Cruz [22] titulado **"PROPUESTA DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO 27001 PARA LA OFICINA DE TECNOLOGÍAS DE INFORMACIÓN DEL GOBIERNO REGIONAL DE PIURA".**

  El objetivo principal de esta investigación fue la implementación de un SGSI basado en la norma ISO/IEC 27001 para la Oficina de Tecnologías de la Información del Gobierno Regional de Piura, con el fin de reducir significativamente los riesgos asociados a la pérdida de información.

  Esta propuesta se centra en el diseño de un SGSI que asegure la integridad, confidencialidad y disponibilidad de los activos informáticos de la oficina, cumpliendo con los estándares internacionales de la norma ISO/IEC 27001.

  Conclusión: La implementación del sistema propuesto permitió mejorar significativamente los procesos de seguridad y comunicación de la información dentro de la Oficina de Tecnologías de la Información del Gobierno Regional Piura, contribuyendo así a fortalecer su gestión y reducir los riesgos asociados a la pérdida o vulnerabilidad de la información.

  El estudio presenta una relación directa con la presente investigación, ya que ambos proponen la aplicación de un SGSI basado en la norma ISO/IEC 27001 en entidades públicas, con el objetivo de proteger la confidencialidad, integridad y disponibilidad de la información. La similitud se evidencia en el enfoque orientado a la reducción de riesgos y al fortalecimiento de los procesos de seguridad de la información.

- El artículo de investigación de Rodríguez Baca et al. [5] titulado **“APLICACIÓN DE ISO 27001 Y SU INFLUENCIA EN LA SEGURIDAD DE LA INFORMACIÓN DE UNA EMPRESA PRIVADA PERUANA”**

  El objetivo de esta investigación fue examinar la incidencia de la implementación de la norma ISO/IEC 27001 en la seguridad informática de una empresa privada limeña. A través de observación directa y entrevistas estructuradas, se evaluó su impacto en los principios de integridad, confidencialidad y disponibilidad de la información.

  Como resultado se logró generar un impacto positivo y cuantificable, demostrando una influencia significativa en los tres pilares de la seguridad de la información: confidencialidad, integridad y disponibilidad.

  Conclusión: La ISO/IEC 27001 es un marco efectivo para elevar los estándares de seguridad de la información en empresas limeñas, al fortalecer la triada CIA (Confidencialidad, Integridad, Disponibilidad), además de generar una cultura organizacional proactiva frente a ciberataques o posibles amenazas de seguridad. El artículo se relaciona estrechamente con la presente investigación al analizar la influencia de la norma ISO/IEC 27001 en los pilares de la seguridad de la información, específicamente la confidencialidad, integridad y disponibilidad. Esta coincidencia conceptual fortalece la variable dependiente del presente estudio, al evidenciar que la aplicación del estándar ISO/IEC 27001 genera impactos positivos y medibles en la seguridad de la información.
- La tesis de López Aguirre [23] titulada **“IMPLEMENTACIÓN DEL SGSI, BASADO EN LA ISO/IEC 27001 PARA DAR TRATAMIENTO AL RIESGO EN UNA EMPRESA CONSTRUCTORA”.**

  El objetivo de esta tesis fue el desarrollo e implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO/IEC 27001 para una empresa del sector

construcción, proteger los activos informáticos de la organización frente a amenazas tanto internas como externas, asegurando la confidencialidad, integridad y disponibilidad de su información.

La implementación se estructuró en cuatro fases, alineadas con el ciclo de mejora continua PHVA (Planificar-Hacer-Verificar-Actuar). Como resultados tangibles, se logró una reducción significativa de incidentes de seguridad, generando ahorros en costos operativos, disminución de gastos por multas o pérdidas financieras, y un fortalecimiento de la postura de seguridad que incrementa su competitividad en procesos de licitación.

Conclusión: La implementación del SGSI permitió a la empresa gestionar amenazas de manera proactiva y optimizar procesos. El proyecto demostró ser económicamente.

La tesis de López Aguirre guarda relación con la presente investigación al desarrollar e implementar un SGSI basado en la norma ISO/IEC 27001 para el tratamiento del riesgo, utilizando el ciclo PHVA como eje metodológico. Ambos estudios coinciden en demostrar que la gestión sistemática de la seguridad de la información permite reducir incidentes, optimizar procesos y fortalecer la competitividad organizacional.

- La tesis de Herrera Velásquez [24] titulada **"SISTEMA DE GESTIÓN PARA LA SEGURIDAD DE LA INFORMACIÓN Y LA CONFIDENCIALIDAD DE LA INFORMACIÓN, HOSPITAL II-1 MOYOBAMBA, 2024"**.

  El objetivo de esta tesis fue determinar la relación entre el sistema de gestión de seguridad de la información y la confidencialidad de los datos en el Hospital II-1 de Moyobamba durante el año 2024, como metodología se realizó una investigación aplicada con enfoque cuantitativo, utilizando el método deductivo y un diseño no experimental transversal. La muestra incluyó a 16 trabajadores del hospital, a quienes se les aplicó un cuestionario para evaluar la eficiencia del sistema de seguridad y el nivel de confidencialidad de la información.

Dentro de los resultados se tuvo que los controles de seguridad mostraron efectividad en las dimensiones tecnológicas y de procesos/políticas, pero no en la dimensión cultural-organizacional, lo que revela una debilidad en esta área.

Conclusión: El estudio confirmó que un sistema de gestión de seguridad de la información bien implementado contribuye significativamente a mejorar la confidencialidad de los datos en el hospital. Sin embargo, se identificó la necesidad de fortalecer los aspectos culturales y organizacionales para garantizar una protección integral de la información sensible.

La investigación se relaciona con el presente estudio desde un enfoque metodológico y conceptual, al analizar la relación entre un sistema de gestión de seguridad de la información y la confidencialidad de los datos, utilizando un enfoque cuantitativo y un diseño no experimental. Este antecedente refuerza la importancia de evaluar la seguridad de la información mediante instrumentos estructurados y evidencia que la correcta implementación de un sistema de gestión contribuye a mejorar la protección de datos sensibles, aspecto central también en la presente investigación aplicada a la Notaría García Medina.

2.2. Marco Teórico

2.2.1. Las notarías en el Perú

Desde un enfoque jurídico-administrativo, la función notarial en el Perú se estructura como un servicio público de fe pública. Su labor se articula en torno a tres ejes fundamentales: la formalización y autenticación de actos jurídicos mediante instrumentos públicos dotados de presunción de legalidad y fuerza probatoria; la custodia protocolaria y reproducción fehaciente de dichos documentos, garantizando su integridad, autenticidad y disponibilidad perpetua para las partes intervinientes; y el ejercicio de un control de legalidad previo, que incluye la verificación del cumplimiento de las cargas tributarias y registrales asociadas a los actos autorizados,

actuando así como colaborador administrativo en la recaudación fiscal y en la correcta inscripción de los derechos.

Según el Poder Ejecutivo [25] La notaría es el despacho profesional donde el notario ejerce sus funciones de forma autónoma e imparcial, autorizando actos y hechos jurídicos, conservando los documentos, y garantizando la legalidad y autenticidad de los mismos.

Características principales:

- El Estado le confiere al notario el poder de dar fe pública.
- El notario no representa a ninguna de las partes, sino que vela por la legalidad del acto.
- A través del control de legalidad, registro y conservación de los documentos.
- Actúa como facilitador para los ciudadanos en trámites legales sin necesidad de acudir a un juez.

2.2.2. El notario

Según Vettori Gonzales [26] el notario es el profesional del derecho que en forma privada está autorizado como tercero imparcial para “dar fe”, es decir, valor de verdad a los actos y contratos que ante él se celebren.

De acuerdo con Gutiérrez Cabas [27] es un funcionario público autorizado para dar fe de los contratos, testamentos y otros actos extrajudiciales, conforme a leyes, es un funcionario investido por el estado, a fin de dar Fe Pública extrajudicial, en el orden civil.

El notario es el profesional del derecho que está autorizado para dar fe de los actos y contratos que ante él se celebran. Para ello formaliza la voluntad de los otorgantes, redactando los instrumentos a los que confiere autenticidad, conserva los originales y expide los traslados correspondientes [28].

2.2.3. Digitalización de las notarías en el Perú

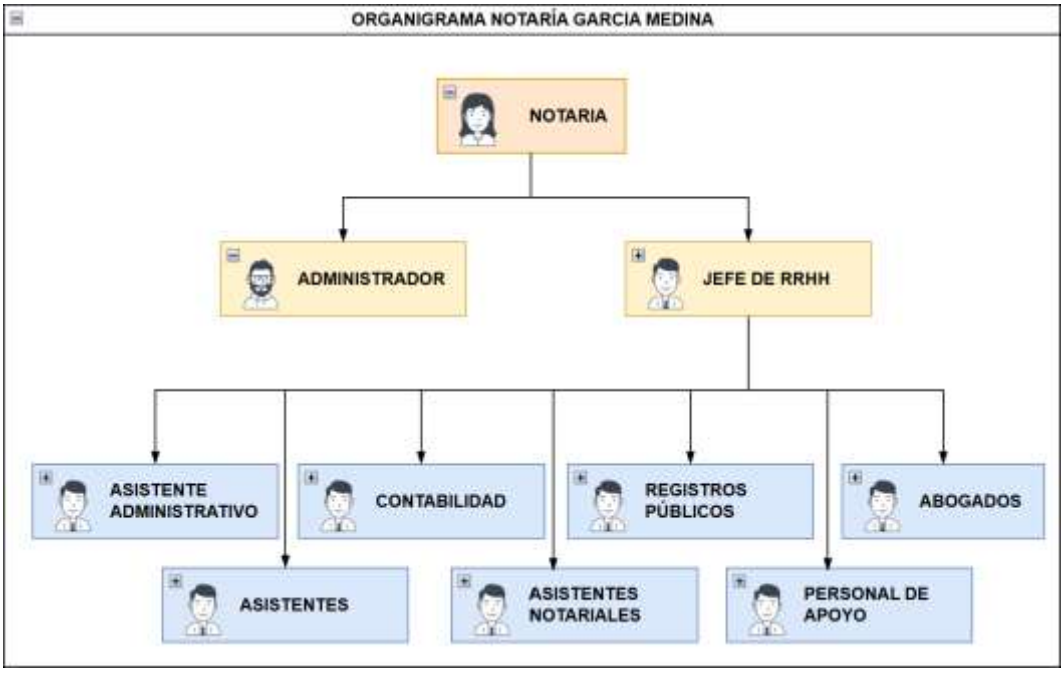
La integración de tecnologías de la información se ha vuelto indispensable en todos los ámbitos de la sociedad moderna. Las notarías, como instituciones fundamentales en la gestión legal, deben adaptarse activamente a este proceso de transformación digital para garantizar eficiencia, seguridad y accesibilidad en sus servicios. Enrique Quintero [29] dice que las políticas enfocadas en la Gestión de la Seguridad de la Información comprenden un conjunto de normas, reglas, procedimientos y buenas prácticas que establecen la forma en que se administran, protegen y comparten todos los activos y recursos de la organización, incluida la propia información.

2.2.4. Aspectos generales sobre las notarías en Madre de Dios

En la presente tesis, se trabajó con información brindada por la notaría “García Medina”, ubicado en el jirón Puno N°745 de la ciudad de Puerto Maldonado, la misma que viene desempeñando labores desde hace 11 años.

Organigrama de la notaría:

Figura 1: Organigrama notaría García Medina



Fuente: Elaboración propia

Según la página web de la notaría Garcia Medina [30] las actividades principales o servicios notariales brindados son:

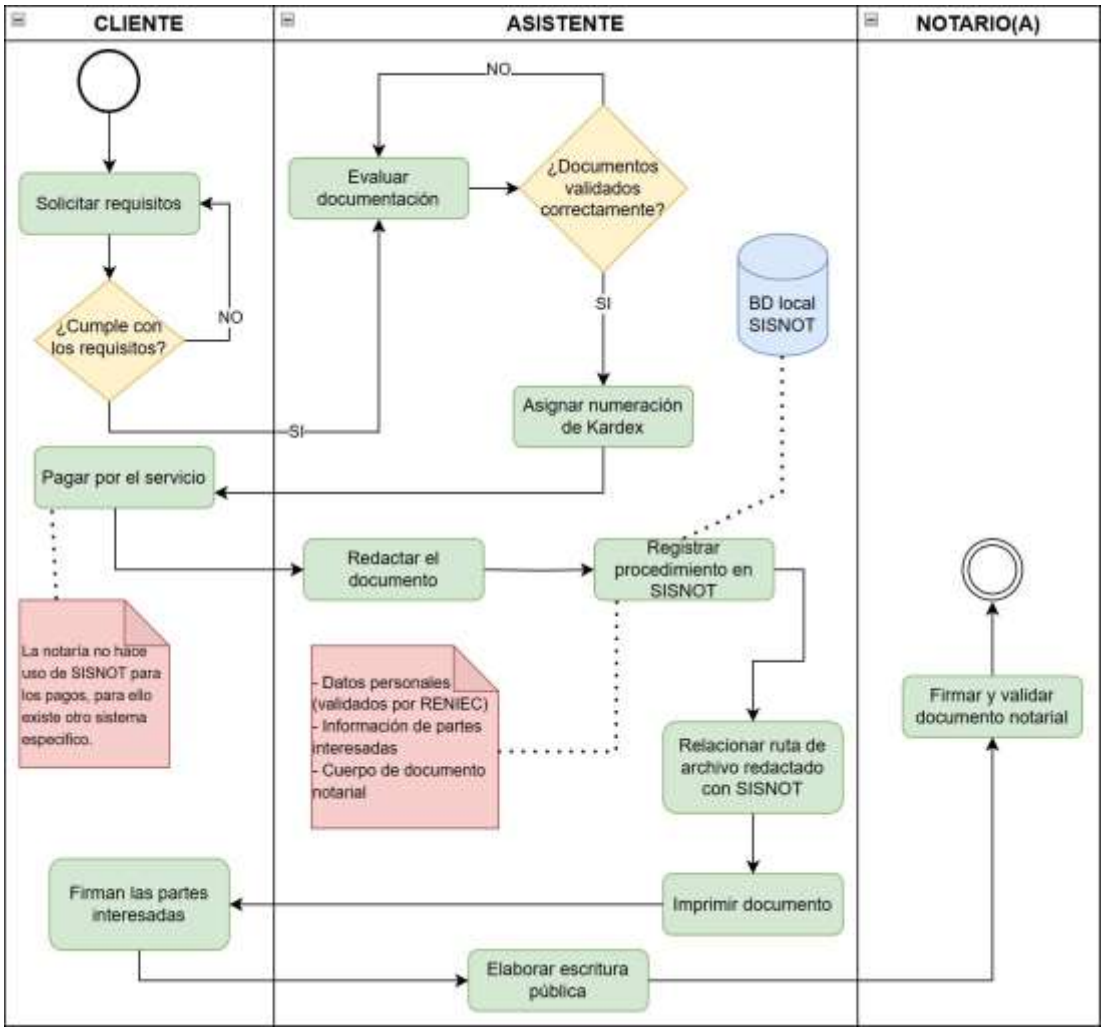
- Autorización para viajes de menores.
- Testamentos por escritura pública.
- Compraventas, donaciones, transferencias, cesión, adjudicación de bienes inmuebles.
- Matrimonio notarial.
- Constitución de empresa.
- Transferencias vehiculares.
- Sucesión intestada.
- Separación convencional y divorcio.
- Adopción.
- Unión de hecho.
- Certificación de firmas.
- Prescripción adquisitiva de dominio.
- Copias certificadas.
- Legalización de producciones.
- Cartas notariales.
- Protestos.

Las actividades o servicios mencionados requieren el cumplimiento obligatorio de ciertos procesos y requisitos. Para agilizar estas gestiones, se utiliza el sistema notarial SISNOT, una plataforma digital que brinda soporte a las notarías a nivel nacional, optimizando los trámites y garantizando mayor rapidez y eficiencia en su ejecución.

La notaría García Medina utiliza el SISNOT principalmente para el registro y validación de los datos del elaborador de documentos notariales y de las partes interesadas (clientes mayores de edad). Sin embargo, no emplea este sistema para el área de pagos, ya que cuenta con un sistema propio para gestionar transacciones financieras. Toda la información registrada por los usuarios del SISNOT se almacena en los servidores locales de la notaría, donde

se resguarda datos de alta importancia. En términos generales, el funcionamiento de la notaría sigue el siguiente proceso:

Figura 2: Diagrama de procesos de los servicios prestados por la notaría



Fuente: Elaboración propia

2.2.5. SISNOT

SISNOT (Sistema Notarial) es un sistema que sirve para gestionar, automatizar y hacer más eficiente la administración de registros, notificaciones y procedimientos legales o administrativos en entidades públicas o privadas como notarías, facilitando la digitalización, seguridad y control de la información [31].

Figura 3: Última versión de SISNOT

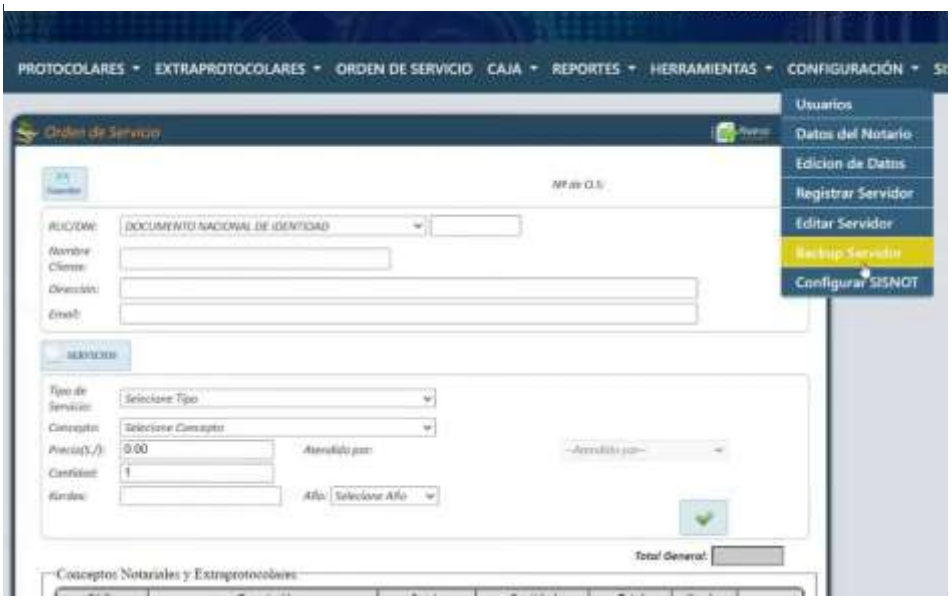


Fuente: SINOT V3.0

La última versión de este sistema es el 3.0, Las principales mejoras incluyen:

- Nueva funcionalidad para conectarse con RENIEC y otros registros públicos.
- Implementación de la firma digital avanzada para firmar documentos electrónicamente.
- Mejoras en la interfaz gráfica para facilitar el uso.
- Nuevas opciones en reportes, etiquetas, y generación automática de anexos.
- La encriptación del código fuente para mayor seguridad y protección de la propiedad intelectual.
- La integración con el sistema de facturación electrónica.
- La actualización automática y respaldo de datos.
- Mejoras en los procesos protocolarios, incluyendo la digitalización de actas, testigos, y registros.
- Nuevas funciones en la gestión de órdenes de servicio, seguimiento y control de estados.

Figura 4: Módulos de SISNOT



Fuente: SISNOT V3.0

Los aspectos importantes del SISNOT son:

1. **Digitalización de procesos:** Facilita la gestión digital de registros y notificaciones, reduciendo el uso de papel.
2. **Seguridad de la información:** Incluye funciones como firma digital y encriptación para proteger los datos.
3. **Automatización:** Mejora la eficiencia mediante funciones automatizadas en procesos administrativos.
4. **Cumplimiento normativo:** Permite ajustarse a normativas legales y estándares de seguridad, como ISO 27001.
5. **Integración con otros sistemas:** Conexión con plataformas externas como RENIEC y facturación electrónica.

2.2.6. Norma ISO 27001

Esta norma constituye un estándar internacional que proporciona a las organizaciones un marco sistemático para establecer, implementar, mantener y mejorar de manera continua un Sistema de Gestión de la Seguridad de la Información (SGSI). Su propósito fundamental es salvaguardar la confidencialidad, integridad y disponibilidad de los datos corporativos críticos. Esto se materializa mediante la implementación de controles y procesos diseñados

para prevenir accesos no autorizados, garantizar la exactitud y preservación de la información, y asegurar su accesibilidad para las partes autorizadas en el momento requerido.

El estándar ISO 27001 menciona los requerimientos necesarios para implementar adecuadamente un SGSI. Publicada por primera vez en 2005, otorga las directrices para crear, aplicar, mantener y mejorar de forma continua este sistema dentro del entorno organizacional [32].

Describe los requisitos esenciales para mantener, implementar y mejorar de manera continua un sistema que garantice la integridad, confidencialidad y disponibilidad de los datos y de los sistemas de información [33].

Seguir esta norma demuestra que una empresa se toma en serio la protección de su información y que toma medidas para mantenerla segura, lo que genera confianza tanto internamente como con clientes y socios.

Como se puede observar en la imagen N°5, el estándar ISO 27001 se fundamenta en el ciclo Planificar-Hacer-Verificar-Actuar (PDCA), también denominado ciclo de Deming.

- **Planificar:** Determinar los objetivos, los recursos requeridos, los requerimientos de los clientes y partes interesadas, así como las políticas organizativas, identificando además los riesgos y oportunidades.
- **Hacer:** Ejecutar las acciones y planes establecidos.
- **Verificar:** Hacer seguimiento y evaluar los procedimientos para determinar su desempeño en relación con las políticas, objetivos, requisitos y actividades planificadas, y comunicar los resultados obtenidos.
- **Actuar:** Implementar acciones correctivas y de mejora continua para optimizar el rendimiento cuando sea necesario.

Figura 5: *Modelo PDCA ISO 27001*



Fuente: Tomado de "Guía de implementación de sistemas de Gestión de seguridad de la información" [33]

La norma ISO 27001 consta de 10 secciones conocidas como cláusulas.

Los requerimientos de la norma ISO 27001 que deben cumplirse se especifican en las cláusulas 4.0 a 10.0. La organización debe cumplir con todos los requisitos de las cláusulas 4.0 - 10.0. No pueden declarar una o más cláusulas como no aplicables a ellos. No pueden declarar que una o más cláusulas no les son aplicables [34].

Figura 6: *Cláusulas del ISO/IEC 27001*



Fuente: Organización Internacional de Normalización (2013). ISO/IEC 27001

Tabla 2: Cláusulas Clave de ISO/IEC 27001 y Preguntas Fundamentales para su Implementación

	Descripción General	Preguntas Clave
4. Contexto de la organización	Comprender la organización y su contexto, incluyendo las partes interesadas, sus necesidades y expectativas, y determinar el alcance del Sistema de Gestión de Seguridad de la Información (SGSI).	• ¿Cuáles son los factores internos y externos relevantes para la seguridad de la información de la organización? • ¿Quiénes son las partes interesadas y cuáles son sus requisitos de seguridad de la información? • ¿Cuál es el alcance del SGSI y por qué se ha definido de esa manera? • ¿Cómo interactúa el SGSI con otros sistemas de gestión?
5. Liderazgo	La alta dirección debe demostrar liderazgo y compromiso con el SGSI, estableciendo la política de seguridad de la información, asignando roles y responsabilidades, y asegurando la integración del SGSI en los procesos de la organización.	• ¿Cómo demuestra la alta dirección su liderazgo y compromiso con la seguridad de la información? • ¿Se ha establecido una política de seguridad de la información que sea adecuada para el propósito de la organización? • ¿Se han definido y comunicado los roles, responsabilidades y autoridades en materia de seguridad de la información? • ¿Se proporcionan los recursos necesarios para el SGSI?
6. Planificación	Establecer los objetivos de seguridad de la información y planificar cómo alcanzarlos, incluyendo la identificación y tratamiento de los riesgos y oportunidades relacionados con la seguridad de la información.	• ¿Cuáles son los objetivos de seguridad de la información de la organización? • ¿Cómo se miden estos objetivos? • ¿Cómo se identifican, analizan y evalúan los riesgos de seguridad de la información? • ¿Qué opciones de tratamiento de riesgos se han seleccionado y cómo se implementarán? ¿Cómo se planifican las acciones para abordar los riesgos y oportunidades?
7. Apoyo	Proporcionar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del SGSI, incluyendo personas	• ¿Qué recursos se necesitan para el SGSI (humanos, infraestructura, financieros, etc.)? ¿Se asegura la competencia del personal que realiza trabajos que afectan la seguridad de la información?

	competentes, infraestructura, ambiente de trabajo, recursos de seguimiento y medición, y conocimiento organizacional.	• ¿Se mantiene la información documentada requerida por el SGSI y la norma? • ¿Cómo se gestiona el conocimiento organizacional relevante para la seguridad de la información?
8. Operación	Implementar y controlar los procesos necesarios para cumplir con los requisitos de seguridad de la información y los objetivos establecidos, incluyendo la evaluación y tratamiento de riesgos, la gestión de cambios y la planificación y control de los procesos externalizados.	• ¿Cómo se implementan y controlan los procesos para cumplir con los objetivos de seguridad de la información? • ¿Cómo se implementan las evaluaciones y los planes de tratamiento de riesgos? • ¿Cómo se gestionan los cambios que pueden afectar la seguridad de la información? • ¿Cómo se asegura la seguridad de la información en los procesos externalizados?
9. Evaluación del desempeño	Monitorear, medir, analizar y evaluar el desempeño del SGSI, incluyendo la realización de auditorías internas y la revisión por la dirección.	• ¿Cómo se monitorea y mide el desempeño del SGSI? ¿Cómo se analizan y evalúan los resultados del monitoreo y la medición? • ¿Se realizan auditorías internas a intervalos planificados? • ¿Cómo se lleva a cabo la revisión por la dirección y qué se incluye en ella? • ¿Cómo se utilizan los resultados de la evaluación del desempeño para la mejora continua?
10. Mejora	Implementar acciones para mejorar continuamente la idoneidad, adecuación y eficacia del SGSI, incluyendo la corrección y prevención de no conformidades.	• ¿Cómo se gestionan y corrigen las no conformidades? • ¿Se toman acciones correctivas para eliminar las causas de las no conformidades? • ¿Cómo se evalúa la necesidad de acciones preventivas para evitar futuras no conformidades? • ¿Cómo se busca la mejora continua del SGSI?

Fuente: Elaboración propia

2.2.7. Análisis de riesgos

El análisis de riesgos es el proceso mediante el cual se identifican los activos críticos de un sistema y las amenazas que pueden comprometer su disponibilidad, confidencialidad e integridad, es esencial cuantificar y evaluar el nivel de riesgo, con el fin de determinar su grado de aceptabilidad y, en función de ello, establecer medidas de intervención que permitan reducir su impacto o probabilidad de ocurrencia.

La imagen N°7 representa un esquema del método de evaluación y tratamiento del riesgo utilizado en la gestión de la seguridad de la información, alineado con enfoques como el ISO/IEC 27001. El diagrama muestra un proceso secuencial e interrelacionado, donde cada etapa alimenta a la siguiente para una adecuada toma de decisiones.

Figura 7: *Método de evaluación y tratamiento del riesgo*



Fuente: Tomado de “Análisis y evaluación de riesgos aplicados a la seguridad de la información”[35]

2.3. Definición de Términos

- **SGSI**: Un Sistema de Gestión de la Seguridad de la Información (SGSI) es el conjunto de políticas, procedimientos, procesos y controles establecidos en una organización con el propósito de salvaguardar la información frente a amenazas que puedan comprometer su confidencialidad, integridad y disponibilidad [8].
- **Contexto externo**: Se refiere a las condiciones externas que rodean a la organización y que pueden influir en el logro de sus objetivos. Estas condiciones incluyen factores sociales, culturales, políticos, legales, regulatorios, financieros, tecnológicos, económicos y ambientales, así como el nivel de competencia existente en los ámbitos internacional, nacional, regional o local. [36].
- **Contexto interno**: Se refiere a las condiciones internas de la organización que influyen en el cumplimiento de sus objetivos. Abarca todos los elementos que pueden impactar la forma en que se gestionan los riesgos, incluyendo la estructura organizativa, la gobernanza, los roles y responsabilidades, así como las políticas, objetivos y estrategias definidas. Además, considera las capacidades internas en cuanto a recursos, conocimientos, personal, tecnología, procesos y tiempo disponible [36].
- **Control**: Son mecanismos implementados para gestionar los riesgos, que pueden incluir políticas, procedimientos, normas, prácticas o estructuras organizacionales. Estos controles pueden tener naturaleza técnica, administrativa, legal o de gestión [37].
- **Gestión de riesgos**: Son las medidas estructuradas que se implementan para gestionar y controlar los riesgos dentro de una organización. Estas permiten reconocer, analizar, atender y supervisar los riesgos que podrían afectar la confidencialidad, integridad y disponibilidad de la información. Su propósito principal es salvaguardar los activos informáticos ante posibles amenazas internas o externas que comprometan su seguridad, mediante la identificación de los activos críticos, las amenazas y vulnerabilidades, así como la evaluación de los impactos y la probabilidad de que ocurran [38].

- **Ciberataque**: Es una operación maliciosa diseñada para debilitar la confianza en los modelos de seguridad y control de una organización o nación, exponiendo sus puntos ciegos, vulnerabilidades o fallos de implementación [39].
- **Amenaza**: Es la posibilidad de que ocurra un ataque que pueda causar perjuicio a la organización, es cualquier factor o situación que pueda afectar negativamente el correcto funcionamiento de un sistema informático, capaz de causar daños, ya sean físicos o lógicos, a los activos informáticos y a los sistemas de información [40].
- **Gobierno de seguridad de la información**: Es el conjunto de políticas, estructuras, responsabilidades y procedimientos definidos por una organización para orientar, supervisar y evaluar la gestión de la seguridad de la información. Su objetivo principal es asegurar que la seguridad esté alineada con las metas estratégicas del negocio, garantizando una adecuada gestión de los riesgos y un uso eficiente de los recursos disponibles [41].
- **Ley de Protección de Datos:** Es el marco legal que protege el derecho fundamental a la privacidad y a la protección de los datos personales, estableciendo las obligaciones que deben cumplir las organizaciones públicas y privadas en el tratamiento, almacenamiento y uso de dicha información. [2].
- **Riesgo:** Es la probabilidad de que se produzca un evento adverso que comprometa el cumplimiento de los objetivos del negocio y genere consecuencias negativas sobre los activos de información, poniendo en riesgo su confidencialidad, integridad o disponibilidad. [42].
- **Tratamiento del riesgo:** Es el proceso de elegir e implementar acciones para modificar o controlar un riesgo, es la etapa del proceso de gestión de riesgos en la que se deciden e implementan las acciones necesarias para modificar o controlar un riesgo identificado, con el fin de reducir su probabilidad de ocurrencia, su impacto o ambos [35].
- **Mejora continua:** La mejora continua constituye un principio esencial dentro de un Sistema de Gestión de Seguridad de la Información (SGSI) y hace referencia al proceso permanente de revisión, análisis y

optimización de las políticas, controles, procesos y procedimientos de seguridad, con el propósito de mantener y fortalecer la eficacia del sistema ante los riesgos actuales y futuros [43].

- **Activos de información:** Son todos aquellos recursos que poseen valor para una organización y que necesitan ser protegidos adecuadamente, ya que su pérdida, alteración o acceso no autorizado puede afectar el cumplimiento de los objetivos del negocio [44].
- **Confidencialidad**: Conforme a la norma ISO 27001, constituye uno de los tres pilares esenciales de la seguridad de la información junto con la integridad y la disponibilidad y se refiere a asegurar que la información solo sea accesible por personas, entidades o procesos debidamente autorizados, evitando su divulgación no autorizada [45].

- **Integridad**: Es la cualidad que protege la exactitud y totalidad de los activos, se encarga de asegurar que cualquier modificación en la información solo se realice con el permiso adecuado [46].
- **Disponibilidad**: Es la característica que asegura que un recurso esté accesible y utilizable cuando se necesite [8].

3. CAPITULO III: METODOLOGIA DE INVESTIGACIÓN

3.1. Tipo de Estudio

La presente investigación es de tipo aplicada, dado que busca utilizar conocimientos teóricos existentes, especialmente los provistos por el estándar ISO/IEC 27001 mediante la propuesta de implementación de un SGSI en el contexto de los sistemas notariales y la seguridad de la información de la notaría.

Según Castro Maldonado et al. [47] la investigación aplicada recurre a los conocimientos ya alcanzados en la investigación básica para encaminarlos al cumplimiento de objetivos específicos; por tanto, este tipo de investigación considera todo el conocimiento existente en un área concreta, que será aplicado en el intento de solucionar problemas específicos.

Cabe mencionar que el enfoque de la presente investigación es mixto, ya que combina tanto métodos cuantitativos como cualitativos para lograr una comprensión más integral del fenómeno estudiado. Se emplearán encuestas estructuradas para obtener datos medibles (cuantitativos), y también se considerarán entrevistas abiertas o análisis documental para comprender la profundidad del contexto (cualitativos).

3.2. Diseño del Estudio

La presente investigación tiene un diseño preexperimental, con un solo grupo de estudio al que se le aplicó una medición antes (pretest) y después (postest) de la propuesta de implementación del Sistema de Gestión de Seguridad de la Información (SGSI). Este diseño permitió evaluar los cambios generados por la intervención sin la utilización de un grupo de control, lo cual resulta adecuado debido a las características organizacionales de la notaría y al enfoque aplicado de la investigación.

El esquema es el siguiente:

$$G \rightarrow O_1 \rightarrow X \rightarrow O_2$$

Donde:

- **G** = Grupo único (35 trabajadores de la notaría)
- **O_1** = Medición pretest
- **X** = propuesta de implementación del SGSI
- **O_2** = Medición postest

Hernández Sampieri [48] menciona que el diseño preexperimental se caracteriza por utilizar un solo grupo al que se le evalúa antes de recibir el tratamiento experimental (prueba previa), luego se le expone al estímulo o intervención, y finalmente se le mide nuevamente después de la aplicación (prueba posterior).

La principal ventaja de este diseño es que proporciona un punto de referencia inicial, lo que permite observar el nivel del grupo en las variables dependientes antes del tratamiento y realizar un seguimiento de sus cambios tras la intervención.

El diseño preexperimental de un solo grupo con medición pretest y postest (O_1–X–O_2) se emplea en la presente investigación debido a las características del contexto organizacional y a la naturaleza aplicada del estudio. Este diseño resulta pertinente en la Notaría García Medina, donde la intervención se aplica a la totalidad del personal involucrado en la gestión de la información. Asimismo, el diseño preexperimental permite comparar el nivel de seguridad de la información antes y después de la aplicación de la propuesta del Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001, facilitando la identificación de los cambios observados tras la intervención. En este sentido, el diseño seleccionado es coherente con los objetivos del estudio, ya que posibilita evaluar la efectividad de la propuesta en un entorno real, manteniendo la validez operativa de los resultados.

3.3. Población y Muestra

Como población se tuvo a un conjunto de 40 personas que trabajan en la notaría García Medina de Puerto Maldonado- Madre de Dios, las cuales participan dentro del flujo de la información gestionada por la notaría.

La fórmula de determinación de muestra fue la siguiente:

$$n = \frac{Z^2 * p * q * N}{E^2 * (N - 1) + Z^2 * p * q}$$

$$n = \frac{1.96^2 * 0.5 * 0.5 * 40}{0.05^2 * (50 - 1) + 1.96^2 * 0.5 * 0.5}$$

$$n = \frac{38.416}{1.0829} \cong 35.48$$

$$n = 35$$

Donde:

- **n:** Tamaño de la muestra= 35 personas.
- **N:** Tamaño total de la población = 40 personas.
- **Z:** Nivel de confianza de 95% ≅ 1.96.
- **E:** Margen de error aceptable = 0.05
- **p:** Probabilidad de que ocurra el evento ≅ 0.5
- **q:** Probabilidad de que no ocurra el evento ≅ 0.5

3.4. Métodos y Técnicas

Método:

Se hace uso del método cuantitativo, ya que según Pelekais [49] es una excelente herramienta, proporciona información objetiva estadísticamente confiable, que para la mayoría puede ser relativamente fácil entender, por ejemplo: un gráfico de pastel o un histograma.

Técnicas:

- **La entrevista:** Es una técnica de recopilación de información mediante una conversación profesional; los resultados a lograr en la misión dependen en gran medida del nivel de comunicación entre el investigador y los participantes en la misma [50].

- **La observación:** La observación es esencial para dar cuenta de un fenómeno. Es una técnica muy empleada tanto en la investigación cualitativa como en la cuantitativa [51].
  Puede ser clasificada en varios tipos:

Instrumentos de investigación:

Para la investigación se usó el cuestionario, según Medina et al. [52] es una herramienta valiosa en la recopilación de información y se utiliza ampliamente en diversos campos, incluyendo la investigación, la evaluación, la educación y la evaluación del desempeño.

Confiabilidad del instrumento:

1. **Cuestionario pretest:**
   El cuestionario pretest fue dirigido a una muestra de 35 personas, donde se evalúa los resultados para la variable dependiente, como se muestra en la tabla.

Tabla 3: Muestra considerada para el estudio de confiabilidad pretest

Resumen de procesamiento de casos

		N	%
Casos	Válido	35	100,0
	Excluido[a]	0	,0
	Total	35	100,0

a. La eliminación por lista se basa en todas las variables del procedimiento.

Los resultados de la tabla Nº 4 evidencian que todas las preguntas del cuestionario pretest presentan una correlación total de elementos corregida alta, con valores comprendidos entre 0,779 y 0,880, superando ampliamente el umbral mínimo recomendado (0,30). Esto indica que cada ítem mantiene una relación sólida con el constructo global que se pretende medir, demostrando coherencia interna entre las preguntas del instrumento.

Tabla 4: Análisis de cada pregunta del cuestionario pretest

Estadísticas de total de elemento

	Media de escala si el elemento se ha suprimido	Varianza de escala si el elemento se ha suprimido	Correlación total de elementos corregida	Alfa de Cronbach si el elemento se ha suprimido
P1	15,34	42,997	,835	,984
P2	15,37	42,299	,870	,983
P3	15,60	40,365	,977	,978
P4	15,57	41,546	,925	,980
P5	15,51	41,139	,942	,979
P6	15,60	40,835	,935	,980
P7	15,63	40,652	,964	,978
P8	15,57	40,782	,961	,978

Fuente: Elaboración propia

Asimismo, la tabla Nº 5 muestra un Alfa de Cronbach de 0,957 para un total de 8 ítems, lo que indica una confiabilidad excelente del instrumento. Este valor supera ampliamente el umbral mínimo aceptable (0,70), evidenciando una alta consistencia interna entre las preguntas, es decir, los ítems miden de manera homogénea el mismo constructo. En consecuencia, el cuestionario resulta estadísticamente confiable para la medición de la variable evaluada.

Tabla 5: Alfa de Cronbach para cuestionario pretest

Estadísticas de fiabilidad

Alfa de Cronbach	N de elementos
,983	8

Fuente: Elaboración propia

2. Cuestionario postest:

El cuestionario postest fue dirigido a una muestra de 35 personas, donde se evalúa los resultados para la variable dependiente e independiente, como se muestra en la tabla.

Tabla 6: Muestra considerada para el estudio de confiabilidad postest

Resumen de procesamiento de casos

		N	%
Casos	Válido	35	100,0
	Excluido[a]	0	,0
	Total	35	100,0

a. La eliminación por lista se basa en todas las variables del procedimiento.

Los resultados de la tabla de Nº 7 evidencian que todos los ítems del cuestionario presentan una correlación total de elementos corregida alta, con valores que oscilan aproximadamente entre 0,740 y 0,964, superando ampliamente el valor mínimo recomendado (0,30). Esto demuestra que cada pregunta mantiene una relación fuerte y consistente con el total de la escala, contribuyendo adecuadamente a la medición del constructo evaluado.

Tabla 7: Análisis de cada pregunta del cuestionario postest

Estadísticas de total de elemento

	Media de escala si el elemento se ha suprimido	Varianza de escala si el elemento se ha suprimido	Correlación total de elementos corregida	Alfa de Cronbach si el elemento se ha suprimido
P1	62,74	97,785	,845	,980
P2	62,74	97,255	,883	,980
P3	62,69	98,987	,890	,980
P4	62,77	98,182	,832	,980
P5	62,74	99,550	,817	,981
P6	62,69	99,634	,782	,981
P7	62,71	98,504	,828	,980
P8	62,77	99,476	,740	,982
P9	62,77	97,652	,924	,979
P10	62,69	97,575	,883	,980
P11	62,83	96,146	,964	,979
P12	62,83	95,087	,941	,979
P13	62,83	96,146	,964	,979
P14	62,74	98,138	,820	,981
P15	62,83	95,793	,894	,980
P16	62,77	97,770	,862	,980

Fuente: Elaboración propia

La tabla Nº 8 muestra un Alfa de Cronbach de 0,981 correspondiente a un total de 16 ítems, lo cual indica una confiabilidad excelente del instrumento. Este valor supera ampliamente el umbral mínimo aceptable de 0,70, evidenciando una alta consistencia interna entre las preguntas del cuestionario. En consecuencia, los ítems presentan un elevado grado de homogeneidad y coherencia en la medición del constructo evaluado, por lo que el instrumento resulta estadísticamente confiable y adecuado para su aplicación.

Tabla 8: Alfa de Cronbach para cuestionario postest

Estadísticas de fiabilidad

Alfa de Cronbach	N de elementos
,981	16

Fuente: Elaboración propia

3.5. Tratamiento de los Datos

Para el tratamiento y procesamiento de los datos recopilados utilizamos la estadística descriptiva e inferencial.

En el caso de nuestra variable independiente (Propuesta de implementación de un SGSI basado en la norma ISO/IEC 27001) estaremos ocupando la estadística descriptiva, ya que medimos el nivel de satisfacción del usuario con respecto a la implementación del SGSI en la notaría, mediante una escala que va del 1 al 5 el cual representa los niveles de medición desde muy malo a muy bueno.

Para nuestra variable dependiente (Mejora de la seguridad de la información en la Notaría García Medina) utilizamos la medición ordinal la cual es cuantitativa y nos permite ordenar en función de mayor o menor valor de un atributo.

Procedimiento de aplicación del pretest y postest

El procedimiento de recolección de datos se desarrolló en dos momentos claramente diferenciados: pretest y postest. En una primera etapa, se aplicó el pretest al personal de la Notaría García Medina el 05 de julio del

año 2025, con la finalidad de diagnosticar el nivel inicial de seguridad de la información. Para ello, se utilizó un cuestionario estructurado con escala tipo Likert, cuya aplicación tuvo una duración aproximada de 20 a 25 minutos por participante. La aplicación se realizó de manera presencial, en el ambiente laboral de la notaría y durante el horario de trabajo, garantizando la comprensión adecuada de los ítems y la participación voluntaria de los encuestados.

Posteriormente, se ejecutó la intervención, consistente en la aplicación de la propuesta del Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001, la cual incluyó actividades de sensibilización del personal, revisión y formulación de políticas de seguridad, identificación de activos de información y establecimiento de controles orientados a la protección de la información. Una vez culminada esta etapa, se aplicó el postest el 18 de setiembre del mismo año, empleando el mismo instrumento de medición utilizado en el pretest.

El intervalo de tiempo entre el pretest y el postest fue de aproximadamente dos meses y medio, periodo considerado suficiente para que las acciones implementadas generaran efectos observables en el nivel de seguridad de la información. Las condiciones de aplicación del postest fueron equivalentes a las del pretest, manteniendo el mismo entorno físico, las mismas instrucciones, la misma escala de medición y la misma modalidad de aplicación, con la finalidad de minimizar sesgos y asegurar la comparabilidad de los resultados. Este procedimiento permitió obtener mediciones consistentes antes y después de la intervención, fortaleciendo la validez operativa del diseño preexperimental adoptado en la investigación.

4. CAPÍTULO IV: RESULTADOS DEL TRABAJO DE INVESTIGACIÓN

4.1. Estudio del contexto actual de la notaría

Se hizo una evaluación sobre el contexto actual de la organización, donde se realizó una serie de preguntas al personal que labora en la notaría García Medina, para conocer su percepción sobre la seguridad de la información, obteniéndose los siguientes resultados:

Para la pregunta 01:

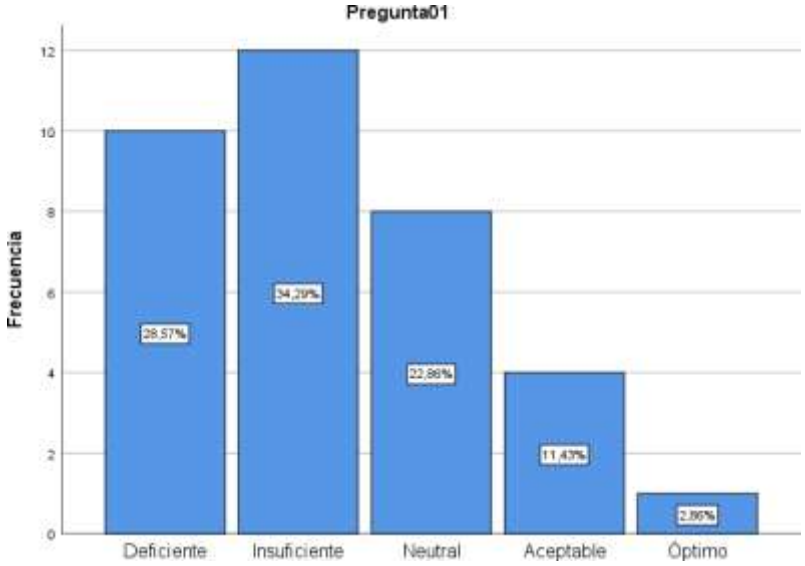
La tabla Nº 9 muestra que la mayoría del personal presenta bajo nivel de conocimiento en seguridad de la información, ya que el 62,9 % se concentra en los niveles deficiente e insuficiente. Un 22,9 % se ubica en un nivel neutral, mientras que solo el 14,3 % alcanza niveles aceptable u óptimo. En conjunto, los resultados evidencian la necesidad de fortalecer la capacitación y concientización del personal en materia de seguridad de la información.

Tabla 9: Análisis de conocimientos sobre seguridad de la información en la notaría

Pregunta01: Mi nivel de conocimiento sobre seguridad de la información es:				
		Frecuencia	Porcentaje válido	Porcentaje acumulado
Válido	Deficiente	10	28,6	28,6
	Insuficiente	12	34,3	62,9
	Neutral	8	22,9	85,7
	Aceptable	4	11,4	97,1
	Óptimo	1	2,9	100,0
	Total	35	100,0	

Fuente: Elaboración propia

Figura 8: Resultados de cuestionario (pregunta 01)



Fuente: Elaboración propia

Para la pregunta 02:

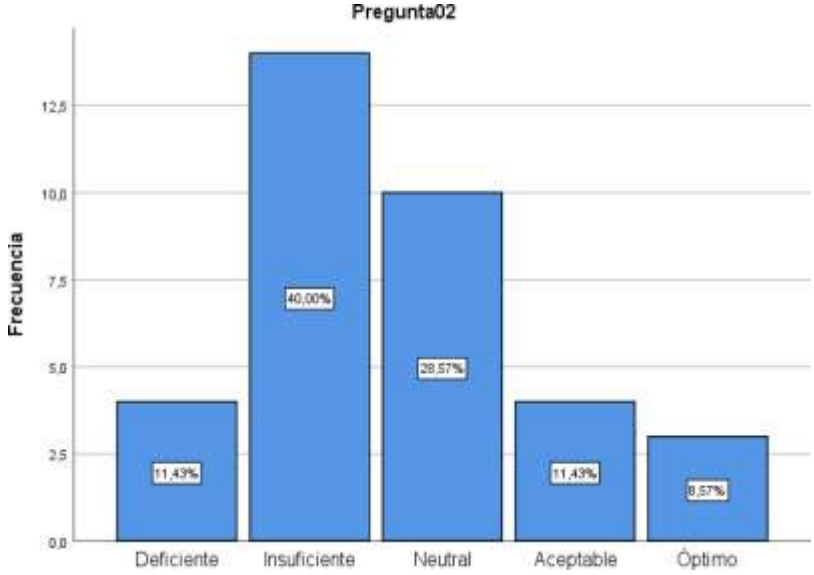
Los resultados de la segunda pregunta evidencian una desconexión preocupante entre la percepción del personal y la cultura organizacional en seguridad de la información. Según la tabla Nº 10 más de la mitad (51.4%) considera que la notaría le da poca o ninguna importancia al tema, un 28.6% se mantiene neutral y apenas un 20% percibe un compromiso real. Esta falta de confianza se traduce en desmotivación, descuidos y una cultura donde cumplir con la seguridad parece solo un requisito formal. Por ello, es urgente implementar un SGSI que, más allá de las políticas, demuestre con acciones y recursos que la seguridad es una prioridad y que la organización respalda a su equipo en este desafío.

Tabla 10: Análisis de conocimientos sobre el nivel de importancia que se le da a la seguridad de la información en la notaría

Pregunta02: Considero que el nivel de importancia que se le da a la seguridad de la información en mi organización es:				
		Frecuencia	Porcentaje válido	Porcentaje acumulado
Válido	Deficiente	4	11,4	11,4
	Insuficiente	14	40,0	51,4
	Neutral	10	28,6	80,0
	Aceptable	4	11,4	91,4
	Óptimo	3	8,6	100,0
	Total	35	100,0	

Fuente: Elaboración propia

Figura 9: Resultados de cuestionario (pregunta 02)



Fuente: Elaboración propia

Para la pregunta 03:

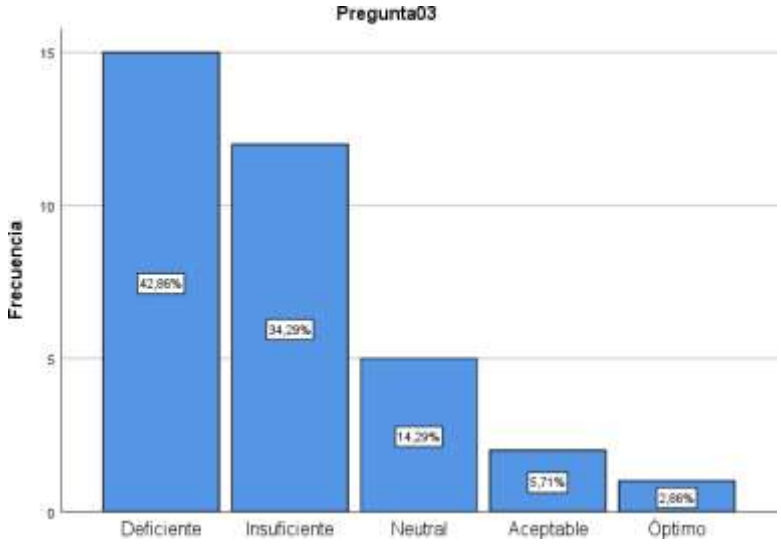
Los resultados de la tercera pregunta muestran una carencia crítica en la formación del personal: el 77.1% considera que sus capacitaciones en seguridad de la información son deficientes o insuficientes. Esto refleja no solo la falta de inversión en competencias esenciales para proteger los activos digitales, sino también el mensaje implícito de que la seguridad no es una prioridad real. Incluso el 14.3% que se mantiene neutral percibe las capacitaciones como esporádicas o superficiales. La ausencia casi total de evaluaciones positivas confirma la urgencia de establecer un programa de formación estructurado y constante, que fortalezca la cultura organizacional y reduzca los riesgos humanos y técnicos.

Tabla 11: Análisis de frecuencia con la que el personal recibe capacitaciones sobre seguridad de la información en la notaría

Pregunta03: La frecuencia con la que recibo capacitaciones sobre seguridad de la información es:				
		Frecuencia	Porcentaje válido	Porcentaje acumulado
Válido	Deficiente	15	42,9	42,9
	Insuficiente	12	34,3	77,1
	Neutral	5	14,3	91,4
	Aceptable	2	5,7	97,1
	Óptimo	1	2,9	100,0
	Total	35	100,0	

Fuente: Elaboración propia

Figura 10: Resultados de cuestionario (pregunta 03)



Fuente: Elaboración propia

Para la pregunta 04:

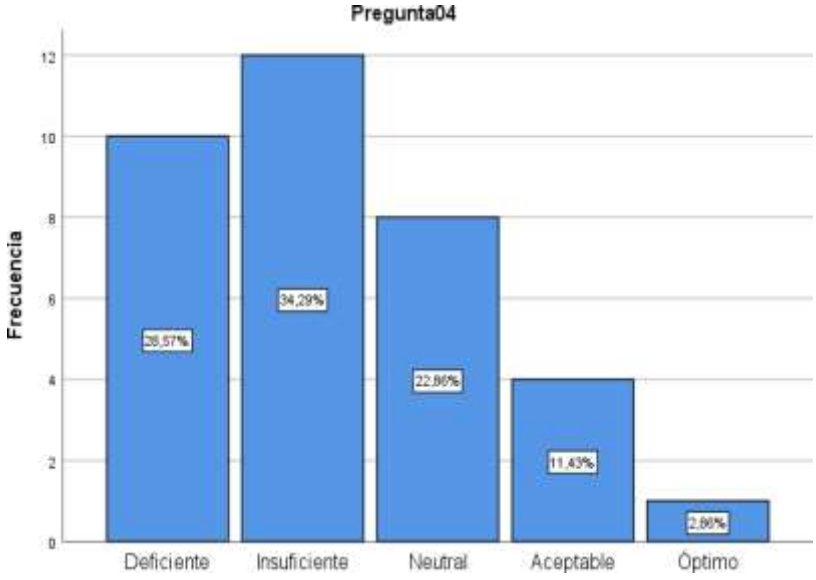
Los resultados de la cuarta pregunta reflejan una preocupante falta de conciencia frente a los riesgos informáticos: el 62.9% del personal admite tener un conocimiento deficiente o insuficiente, mientras que un 22.9% permanece en neutralidad, lo que evidencia falta de confianza incluso para reconocer amenazas. Solo 5 personas muestran un nivel adecuado u óptimo, confirmando que la gestión de riesgos se percibe más como una tarea externa que como una responsabilidad individual. Esta brecha de conciencia deja al equipo vulnerable y refuerza la urgencia de implementar un SGSI que, además de identificar y evaluar riesgos, los comunique de manera clara y constante para transformar la pasividad en prevención.

Tabla 12: Análisis de nivel de conocimiento de los empleados sobre los riesgos a los que está expuesta la información en la notaría

Pregunta04: Mi nivel de conocimiento sobre los riesgos a los que está expuesta la información que manejo es:				
		Frecuencia	Porcentaje válido	Porcentaje acumulado
Válido	Deficiente	10	28,6	28,6
	Insuficiente	12	34,3	62,9
	Neutral	8	22,9	85,7
	Aceptable	4	11,4	97,1
	Óptimo	1	2,9	100,0
	Total	35	100,0	100,0

Fuente: Elaboración propia

Figura 11: Resultados de cuestionario (pregunta 04)



Fuente: Elaboración propia

Para la pregunta 05:

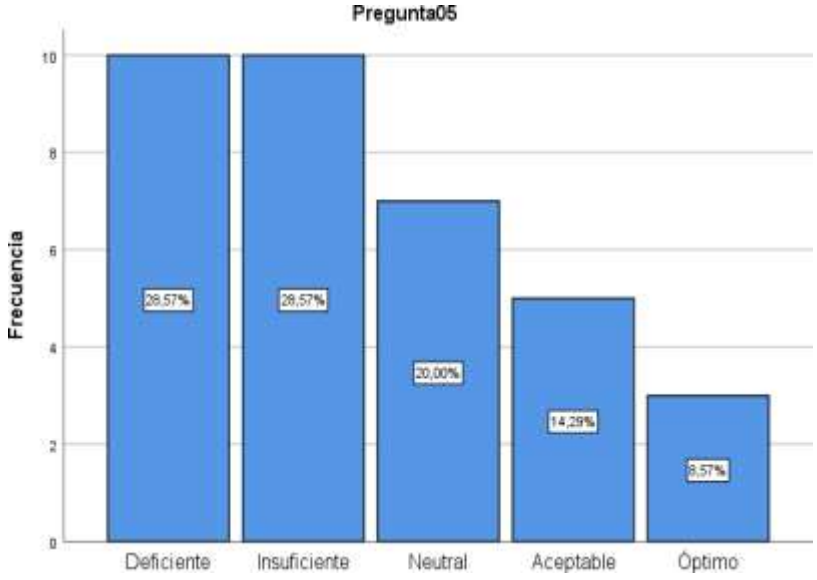
Los resultados de la quinta pregunta muestran una seria fragmentación en la gobernanza de la seguridad informática. El 57.1% del personal percibe poca o nula claridad sobre quién es el responsable de esta área. Este vacío genera descoordinación ante incidentes y transmite la idea de que la seguridad no tiene un responsable dentro de la organización. Un 20% se mantiene en neutralidad, reforzando la ambigüedad, y solo 8 personas identifican un referente claro. Esta falta de gobernanza no solo dificulta la aplicación de políticas consistentes, sino que debilita la cultura de seguridad. De allí la urgencia de plantear la implementación un SGSI que asigne roles definidos y otorgue a un responsable la autoridad para liderar este compromiso.

Tabla 13: Análisis de nivel de conocimiento de los empleados sobre los riesgos a los que está expuesta la información en la notaría

Pregunta05: La claridad y comunicación sobre quién es el responsable de la seguridad de la información en mi organización es:				
		Frecuencia	Porcentaje válido	Porcentaje acumulado
Válido	Deficiente	10	28,6	28,6
	Insuficiente	10	28,6	57,1
	Neutral	7	20,0	77,1
	Aceptable	5	14,3	91,4
	Óptimo	3	8,6	100,0
	Total	35	100,0	

Fuente: Elaboración propia

Figura 12: Resultados de cuestionario (pregunta 05)



Fuente: Elaboración propia

4.2. Fases de implementación del SGSI

- **Fase 1: Definir objetivos del negocio:**

  Es esencial que notarios, administradores, personal técnico y usuarios reconozcan y establezcan prioridades en los objetivos que respalden la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) conforme al estándar ISO/IEC 27001. Dichos objetivos deben estar alineados con la misión y visión de la institución.

Tabla 14: Misión, visión y objetivos de la Notaria García Medina de Puerto Maldonado

Pilares de la notaría Garcia Medina de Puerto Maldonado	
Misión	Según la página web de la notaría García Medina [30], “Brindar seguridad jurídica de confianza, oportuna, con soluciones integrales, innovadoras, de calidad, actualizadas, personalizadas, con una comunicación permanente, con responsabilidad social y profesionalismo”.
Visión	Según su página web [30] “Ofrecer a nuestros usuarios plena satisfacción en el servicio prestado”.
Objetivos	• Proteger la información notarial frente a accesos no autorizados. • Preservar la integridad de la información legal. • Asegurar la disponibilidad continua del sistema notarial. • Cumplir con normativas vigentes. • Generar confianza en los usuarios.

Fuente: Elaboración propia

- **Fase 2: Obtener el apoyo de la alta dirección:**

  La alta dirección debe asumir un rol activo, proporcionando respaldo estratégico y recursos suficientes para ejecutar el proyecto, incluyendo personal capacitado y tecnologías adecuadas. Este compromiso se refleja en la aprobación de políticas de seguridad y el fomento de una cultura organizacional enfocada en la protección de la información.

  Como señala Lopes et al. [53], una cultura organizacional robusta en seguridad de la información es fundamental para mitigar los riesgos asociados al factor humano, ampliamente reconocido como el eslabón más débil en la protección de los activos digitales.

  En este contexto, se desarrolló un acta de constitución de proyecto dirigida a la notaría, en la cual se detallaron los objetivos y el alcance del mismo. Este documento fue presentado a la alta dirección de la Notaría García Medina para su revisión y aprobación, y se encuentra incluido en el anexo 9 como Acta de Constitución del Proyecto.

  Como paso siguiente, se redactó una política integral de seguridad de la información que define el marco de acción en la notaría. Esta estipula las funciones, obligaciones y las consecuencias por incumplimientos, materializando el compromiso de la dirección con la salvaguarda de la información y el cuidado de los activos institucionales. (Anexo 10: Política General de la Seguridad de la Información).

- **Fase 3: Determinar alcance**

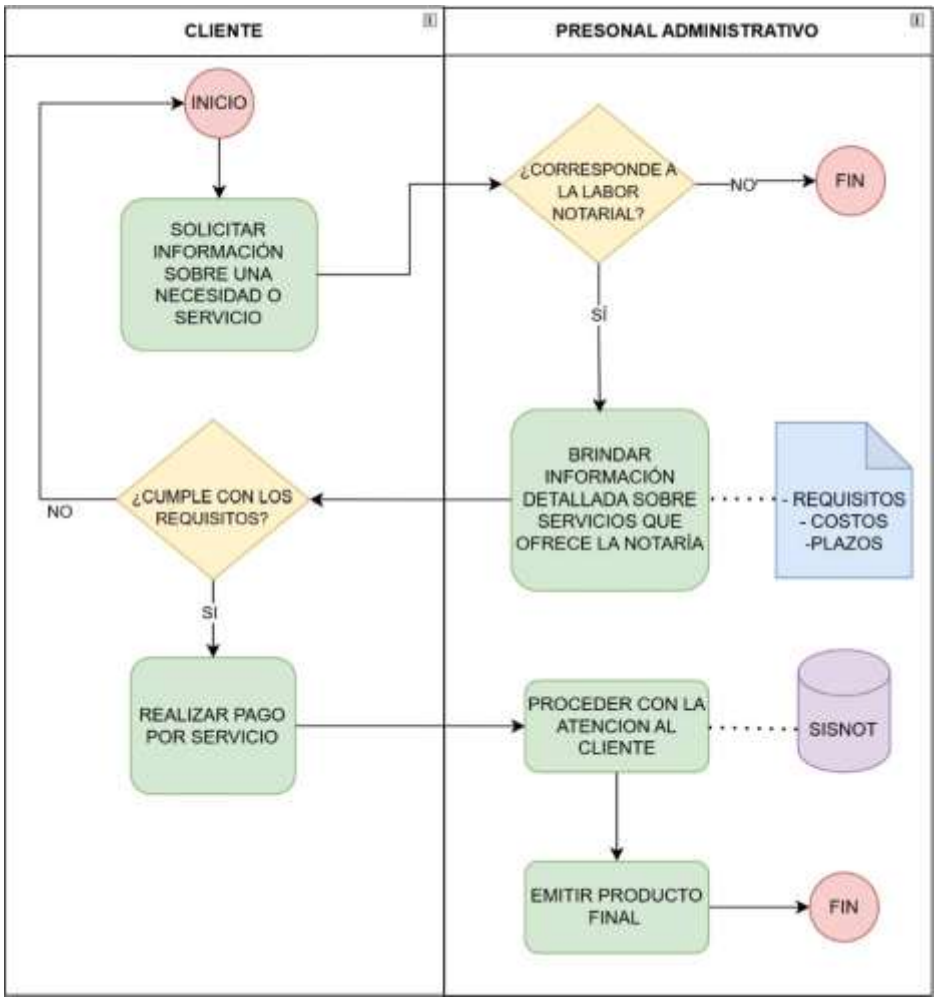
  La delimitación del alcance del SGSI para la Notaría García Medina se estableció con base en una evaluación de sus objetivos estratégicos y los procesos operativos críticos que requiere la institución.

  Para establecer dicho alcance, se identificaron los procesos centrales vinculados al tratamiento de la información sensible, jurídica y administrativa que forma parte del servicio notarial. Los procesos incluidos en el alcance del SGSI son los siguientes:

  - **Atención al cliente:** Proceso mediante el cual la notaría inicia el contacto con los usuarios que requieren servicios notariales. El

protocolo se establece según el tipo de trámite solicitado (escrituras públicas, legalizaciones, poderes, etc.). De ser aceptada la solicitud, el cliente presenta la documentación correspondiente y se coordina la atención.

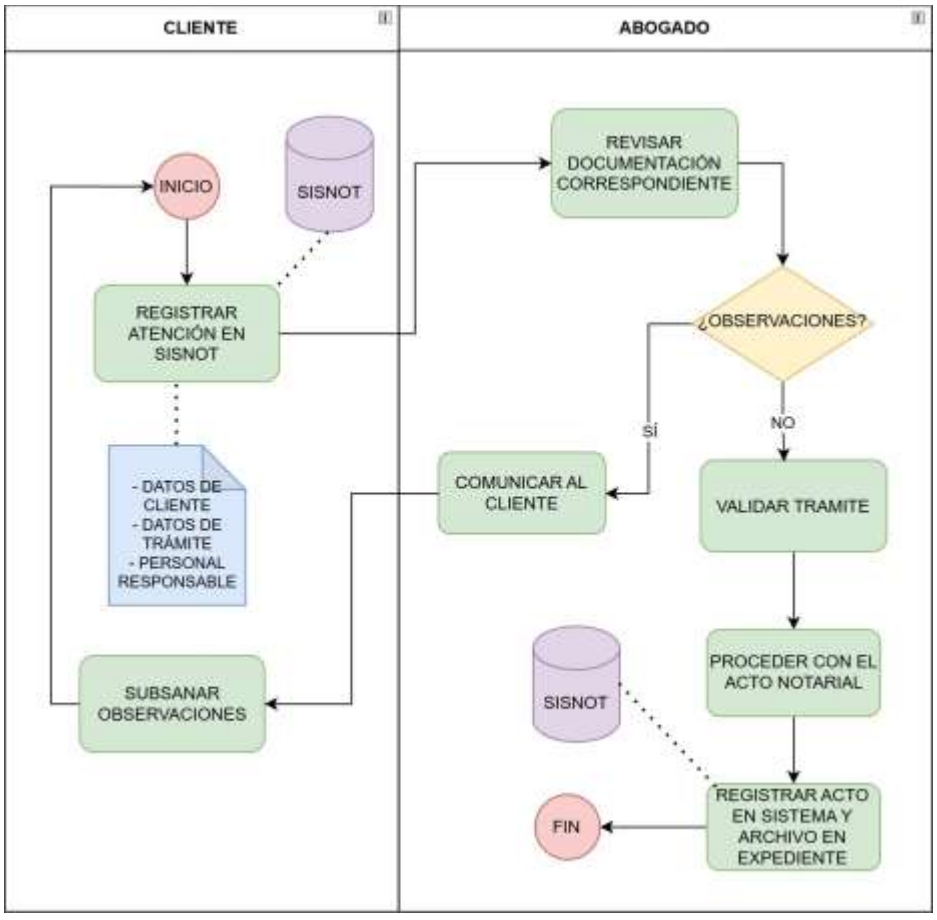
Figura 13: Diagrama de flujo del funcionamiento general de la notaría



Fuente: Elaboración propia

- **Procesamiento de datos:** Procedimiento donde el personal autorizado registra la información del cliente y del trámite en el sistema notarial. Posteriormente, el notario o el abogado responsable revisa y valida los documentos y la información registrada. En caso de observaciones, se comunica al cliente para subsanarlas antes de la formalización del acto notarial. Una vez validados los datos, se genera el parte notarial o la escritura pública, que queda registrada en el sistema y en los archivos físicos de la notaría.

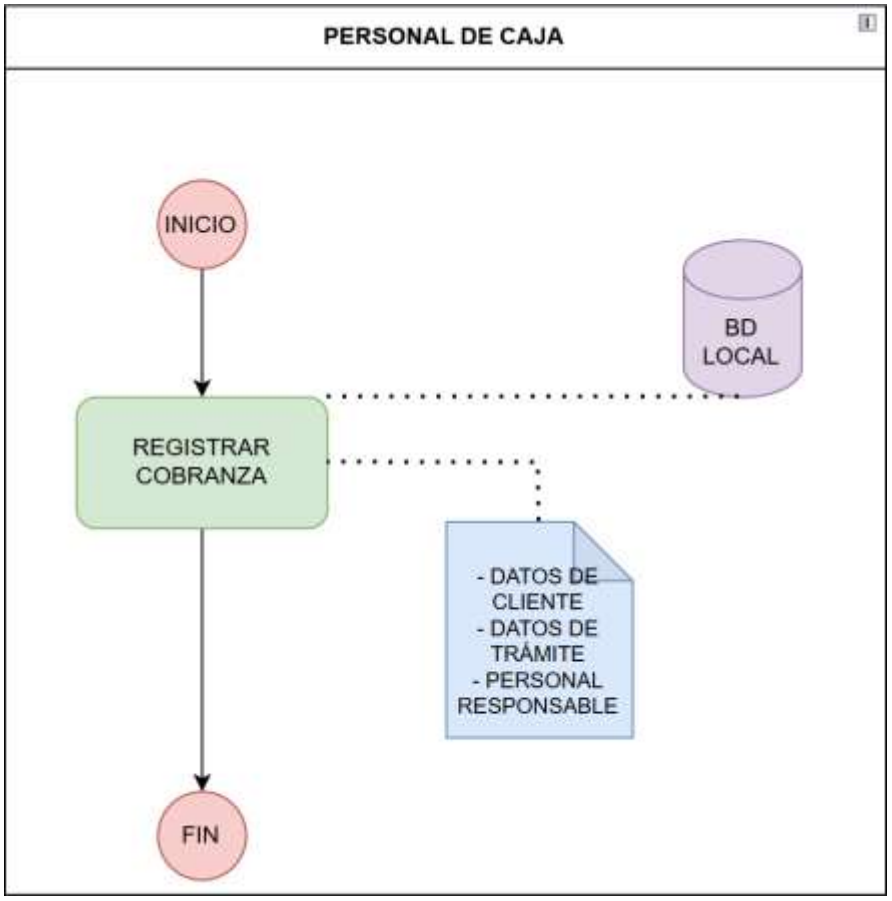
Figura 14: Diagrama de flujo del procesamiento de datos notariales



Fuente: Elaboración propia

- **Cobranza:** Proceso en el cual se verifican los pagos realizados por los clientes en las cuentas bancarias o en efectivo en la caja de la notaría.

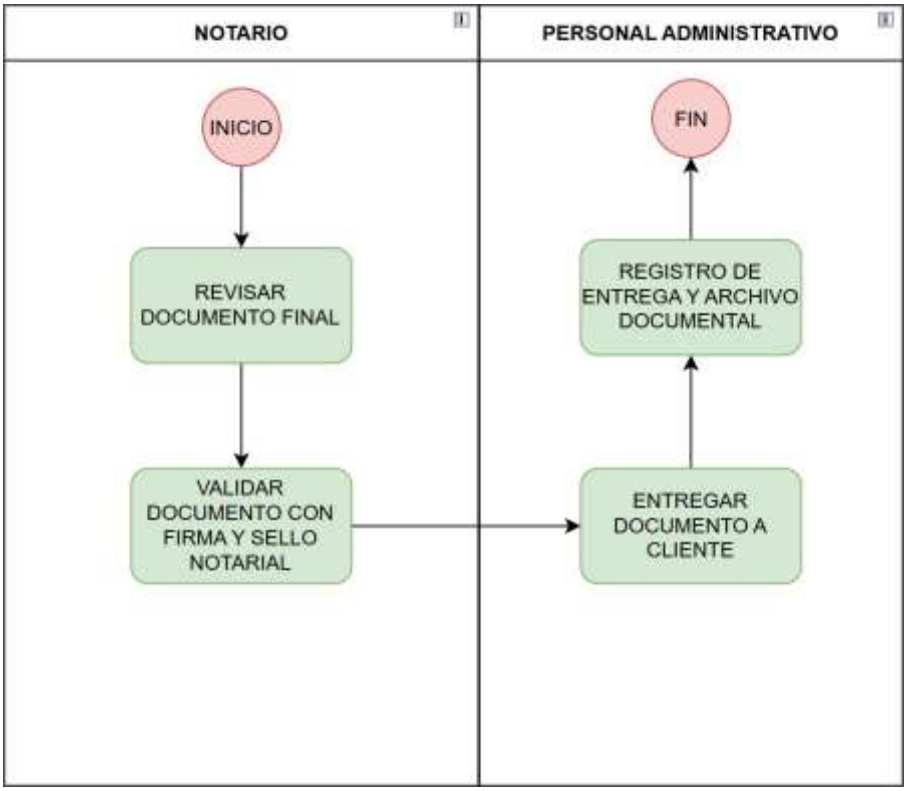
Figura 15: Diagrama del flujo del proceso de cobranza en la notaría



Fuente: Elaboración propia

- **Conservación documental:** Proceso mediante el cual la notaría asegura el archivo y custodia de las escrituras públicas, partes notariales y demás documentos. Este proceso garantiza la trazabilidad, seguridad jurídica y disponibilidad de los documentos a futuro, cumpliendo con la normativa vigente y las obligaciones de archivo establecidas por la ley.

Figura 16: Diagrama de flujo del proceso de conservación documental



Fuente: Elaboración propia

- **Fase 4: Determinar el análisis de riesgos**

  Durante esta fase, se utilizó un inventario de amenazas y vulnerabilidades vinculadas a cada activo de información relevante. Mediante el cruce de estos elementos, se logró identificar los riesgos potenciales asociados a cada activo. Una vez identificados, los riesgos fueron valorados según su nivel de criticidad, destinándose un plan de tratamiento específico para la mitigación o control de aquellos catalogados como altos o críticos.

  El origen de las amenazas puede ser Intencionado (I), Casual (C) o Ambiental (A).

Tabla 15: Identificación de amenazas

Tipo	Amenaza	Origen
Daño físico	Daño por fuego	C-I-A
	Daño por agua	C-I-A
	Contaminación	C-I-A
	Polvo, corrosión	C-I-A
Eventos naturales	Fenómenos climáticos	A
	Fenómenos sísmicos	A-I-C
	Inundaciones, Incendios	A
Fallo de servicios esenciales	Falla en el aire acondicionado	C-I
	Falla en energía eléctrica	C-I-A
	Falla de conexión a internet	C-I-A
Compromiso a la información	Espionaje	I
	Robo de documentos	I
	Robo de equipos	I
	Recuperación de información de equipos desechados	I
	Manipulación de hardware	I
	Manipulación de software	C-I
Fallas técnicas	Falla de equipos	C
	Saturación de los sistemas de información	C-I
	Malfuncionamiento de software	C
	Falta de mantenimiento de software	C-I
	Falta de mantenimiento de hardware	C-I
Acciones no autorizadas	Uso no autorizado de equipos	I
	Copia fraudulenta de información	I
	Uso de software sin licencia	C-I
	Datos inconsistentes	I
Compromiso de funciones	Abuso de funciones	C-I
	Falsificación de funciones	I
	Negación de accesos	I
	No disponibilidad de personal	C-I-A

Fuente: elaboración propia

Tabla 16: Identificación de vulnerabilidades

Tipo	Vulnerabilidad
Hardware	Mantenimiento inadecuado o deficiente
	Ausencia de un plan de renovación periódica
	Sensibilidad a acumulación de polvo, humedad o residuos
	Control de modificaciones ineficaz o inexistente
	Exposición a variaciones o picos de voltaje
	Sensibilidad a fluctuaciones de temperatura
	Almacenamiento inapropiado o sin medidas de protección
Software	Ausencia de una fase de pruebas de software
	Presencia de fallos o errores en el código
	Sesiones de usuario que no se cierran correctamente
	Reutilización de dispositivos de almacenamiento sin un borrado seguro
	Carecer de funcionalidades de registro para auditoría
	Asignación incorrecta o deficiente de permisos de acceso
	Diseño de interfaz de usuario poco intuitiva o complicada
	Documentación del sistema incompleta o inexistente
	Ausencia de un sistema de verificación de identidad
	Gestión deficiente de claves de acceso (contraseñas)
	No realización de copias de seguridad de la información
Red	Canales de comunicación sin cifrado o protección
	Infraestructura de cableado en mal estado o deficiente
	Diseño de la red con configuraciones inseguras
Personal	Escasez de dotación de personal
	Procedimientos de selección y contratación inapropiados
	Manejo inadecuado de los recursos tecnológicos (software y hardware)
	Concienciación y formación insuficiente en seguridad de la información

	Falta de supervisión de las actividades realizadas con la información
Sitio	Control deficiente de los accesos físicos a las instalaciones
	Localización en una zona de riesgo ante fenómenos naturales
	Suministro eléctrico con interrupciones o variaciones frecuentes
	Medidas de seguridad física insuficientes en la estructura del edificio, puertas y ventanas
Organización	Carencia de una metodología para identificar y valorar riesgos
	No realización de revisiones o auditorías de forma regular
	Ausencia de una política formal para el tratamiento de la información
	Falta de un régimen sancionador ante incumplimientos de seguridad
	Ausencia de normativas para mantener puestos de trabajo y pantallas libres de información sensible
	Falta de un protocolo para informar sobre fallos de seguridad detectados

Fuente: Elaboración propia

A continuación, se procede a determinar el riesgo y su posible consecuencia; con base en esta última se establece el nivel de criticidad del riesgo. Los factores utilizados para determinar dicha criticidad son la probabilidad y el impacto.

En cuanto a la probabilidad, esta se refiere a la frecuencia o tasa de ocurrencia del riesgo, es decir, la posibilidad de que el evento identificado llegue a materializarse. A partir de esta valoración, se complementa el análisis con la estimación del impacto para definir con mayor precisión la prioridad de atención de cada riesgo.

Tabla 17: Criterios para la tasa de ocurrencia del riesgo

Nivel de probabilidad	Descripción	Frecuencia estimada
Raro	Ocurre en circunstancias atípicas.	Aproximadamente 1 cada 5 años.
Improbable	Es poco probable que ocurra, pero puede presentarse ocasionalmente.	Alrededor de 3 veces cada 5 años.
Posible	Podría suceder en algún momento durante las operaciones normales.	Cerca de 1 vez al año.
Probable	Es factible que ocurra con relativa frecuencia.	Entre 2 y 3 veces al año.
Muy posible	Alta probabilidad de ocurrencia o repetición constante.	5 o más al año.

Fuente: Elaboración propia

Con el propósito de valorar las repercusiones que tendría para la notaría la materialización de un riesgo, se establecieron una serie de criterios de evaluación. Estos permiten cuantificar la magnitud del perjuicio en dimensiones críticas como la confidencialidad, integridad y disponibilidad de los datos, además de su efecto sobre la operatividad, la imagen institucional y el cumplimiento de obligaciones legales.

Tabla 18: Criterios para la determinación de impacto

Impacto	Descripción
Bajo	El impacto de este evento es insignificante para la organización, sin consecuencias financieras, operacionales, reputacionales o legales. El efecto es únicamente interno, perceptible para los colaboradores, pero no para los clientes.
Moderado	Este riesgo ha sido clasificado como aceptable. En caso de materializarse, sus consecuencias operativas y financieras serían mínimas, sin afectar la reputación institucional ni acarrear sanciones legales. No obstante, existe la posibilidad de que genere observaciones por parte de los organismos reguladores.

Relevante	Impacto directo y de nivel medio. Un incidente de esta naturaleza podría resultar en sanciones por faltas leves, gastos operativos controlados para su mitigación, y un perjuicio medio a la imagen institucional.
Alto	El impacto para la organización es severo, clasificándose el riesgo como inaceptable. Esto conllevaría una investigación regulatoria, sanciones por infracciones graves, la obligatoria intervención de la alta dirección, incrementos operativos significativos y pérdidas financieras sustanciales.
Crítico	Un incidente de seguridad crítico, como una filtración masiva de datos, resultaría en daño reputacional catastrófico y pérdidas financieras cuantiosas. Las consecuencias incluirían intervención regulatoria con multas severas, fuga masiva de clientes y requeriría la gestión directa de la alta dirección.

Fuente: Tomado de Aguirre Mollehuanca [54] “Diseño de un SGSI para servicios postales del Perú”

Para clasificar qué tan crítico es un riesgo, consideramos tanto la chance de que ocurra como el daño que causaría. La tabla muestra los niveles de criticidad que obtuvimos al combinar estos dos factores.

Tabla 19: Matriz de calor de probabilidad - impacto

IMPACTO	Crítico	Medio	Alto	Alto	Crítico	Crítico
	Alto	Bajo	Medio	Alto	Alto	Crítico
	Relevante	Bajo	Medio	Medio	Alto	Alto
	Moderado	Bajo	Bajo	Medio	Medio	Medio
	Bajo	Bajo	Bajo	Bajo	Bajo	Medio
		Raro	Improbable	Posible	Probable	Muy posible
	PROBABILIDAD					

Fuente: Elaboración propia

El apetito al riesgo representa el nivel de exposición que una organización está dispuesta a asumir en el desarrollo de sus

actividades y la prestación de servicios. Dado que la notaría actualmente no ha definido formalmente este umbral, se propone como criterio que los riesgos clasificados como "Bajo" y "Medio" puedan ser aceptados, mientras que aquellos categorizados como "Alto" o "Crítico" deben ser sometidos a medidas de control y mitigación inmediata para reducir su nivel de criticidad hasta un rango aceptable.

Posterior a la identificación y clasificación de los riesgos según su nivel de criticidad, se debe proceder con su tratamiento, el cual puede incluir las siguientes estrategias: aceptación, reducción, evitación o transferencia del riesgo.

Tabla 20: Tratamiento de riesgo

Estrategia de Tratamiento	Descripción
Reducir el riesgo	Implementar controles para disminuir la probabilidad o el impacto del riesgo, hasta que el riesgo residual se encuentre dentro de un nivel aceptable.
Retener el riesgo	Aceptar conscientemente el riesgo sin aplicar medidas adicionales, basándose en que su nivel se considera tolerable según los criterios de la organización.
Evitar el riesgo	Eliminar por completo la actividad o condición que genera el riesgo, previniendo así cualquier posibilidad de materialización.
Transferir el riesgo	Compartir la responsabilidad financiera o operativa del riesgo con un tercero, mediante mecanismos como seguros o acuerdos contractuales.

Fuente: Elaboración propia

- **Fase 5: Preparar un inventario de los activos de la información:**
  En esta fase se identifican y valoran los activos de información de los procesos críticos del negocio, siguiendo la metodología establecida en la norma ISO/IEC 27001. Este paso es fundamental para determinar los activos esenciales que garantizan la operatividad de los procesos.

Para la clasificación de los activos de información identificados, se considerarán dos categorías principales:

- Activos Primarios: Aquellos que constituyen el valor central para la organización, como los procesos, actividades y la información misma que estos generan o gestionan.
- Activos de Soporte: Los elementos que permiten la existencia, procesamiento y almacenamiento de los activos primarios, incluyendo hardware, software, infraestructura de redes, personal clave y las instalaciones físicas (sitio).

Los activos son catalogados considerando los siguientes elementos:

- ID del Activo: Un identificador único que facilite su rastreo y referencia.
- Nombre del Activo: Denominación con la que se reconoce el activo.
- Descripción: Breve explicación de la naturaleza y propósito del activo.
- Proceso: Proceso funcional al cual pertenece el activo dentro de la organización.
- Subproceso: Actividad específica en la que el activo participa o se utiliza.
- Clasificación de Activo: Determinación de si el activo es primario (información, software, hardware) o secundario (soporte).
- Subclasificación del Activo: Clasificación más específica, como hardware, software, sitio, personal, etc.
- Propietario del Activo: Persona o área responsable de su gestión y protección.
- Ubicación: Dirección física o ubicación lógica del activo dentro de la infraestructura tecnológica o documental.

Esta información permite generar una visión integral del entorno informacional de la notaría y establecer medidas de protección alineadas con los riesgos identificados, contribuyendo a fortalecer la confidencialidad, integridad y disponibilidad de los datos procesados en dichos sistemas.

Tabla 21: Inventario general de activos identificados

ID Activo	Nombre	Descripción	Clasificación
R1	Notario	Titular de la notaría. Responsable legal de autenticar actos y hechos jurídicos, conferir fe pública a los documentos y garantizar su legalidad, validez y conservación. Es la máxima autoridad y tiene la responsabilidad última sobre la seguridad de la información.	Primario
R2	Administrador	Supervisa la gestión operativa, financiera y administrativa de la notaría. Actúa como enlace entre el notario y el personal, y es clave en la implementación y supervisión de las políticas del SGSI.	Primario
R3	Jefe de RRHH	Gestiona el ciclo laboral del personal (reclutamiento, contrataciones, capacitación). Es fundamental para aplicar controles de seguridad relacionados con el factor humano (acuerdos de confidencialidad, concienciación).	Primario
R4	Abogados	Asesoran legalmente a los clientes y redactan instrumentos notariales. Crean y gestionan activos de información altamente confidenciales (testamentos, poderes, contratos, etc.).	Primario
R5	Contabilidad	Gestiona la información financiera, presupuestaria y tributaria de la notaría. Maneja datos críticos que requieren controles de integridad y confidencialidad estrictos.	Primario
R6	Asistentes administrativos	Apoya las labores administrativas generales (gestión documental, atención al cliente, comunicación). Maneja información sensible y debe seguir procedimientos de seguridad para su manejo.	Soporte
R7	Asistentes notariales	Apoyan directamente al notario en la fe pública (redacción de minutas, preparación de documentos, protocolización). Tienen acceso directo a la información más sensible del proceso notarial.	Soporte

ID Activo	Nombre	Descripción	Clasificación
R8	Personal de apoyo	Incluye roles como recepcionistas, mensajeros y personal de limpieza. Aunque su acceso a la información es limitado, son clave para controles de seguridad física y de acceso.	Soporte
I1	Registros públicos	Maneja datos críticos que requieren controles de integridad y confidencialidad estrictos.	Primario
I2	Boleta/factura	Información física y/o digital que documenta transacciones financieras. Contiene datos sensibles del cliente y de la notaría. Debe protegerse su integridad y confidencialidad.	Primario
I4	Archivo	Conjunto de documentos físicos (protocolos notariales, escrituras públicas, actas, etc.) que constituyen el patrimonio documental legal de la notaría. Requiere medidas de seguridad física y controles de acceso estrictos.	Primario
I5	Documento final	Información resultante de un acto notarial. Tiene valor legal y debe ser íntegro, auténtico y accesible.	Primario
S1	SISNOT	Sistema Informático Notarial. Software esencial que gestiona los actos notariales, el protocolo y la emisión de documentos con valor legal. Es el activo más crítico, ya que alberga toda la información operativa. Requiere altos niveles de disponibilidad, integridad y confidencialidad.	Primario
S2	MS Office	Suite ofimática. Software utilizado para crear, editar y gestionar documentos de apoyo, hojas de cálculo y comunicaciones internas. Su configuración segura es clave para proteger la información.	Soporte
S3	Base de datos	Conjunto de datos estructurados que almacena toda la información del SISNOT (actos, partes involucradas, documentos). Es el activo de	Primario

ID Activo	Nombre	Descripción	Clasificación
		información digital más valioso. Su confidencialidad, integridad y disponibilidad son primordiales.	
H1	Computadora de escritorio	Hardware utilizado por el personal para acceder al SISNOT, gestionar correos y documentos. Punto de acceso principal a la información y potencial vector de amenazas si no está asegurado.	Soporte
H2	Lector biométrico	Hardware de seguridad utilizado para autenticar y controlar el acceso físico o lógico a áreas restringidas o sistemas. Protege activos críticos mediante la verificación de identidad.	Soporte
H3	Fotocopiadora/ impresora	Hardware multifuncional. Maneja documentos sensibles de manera constante. Muchos modelos almacenan datos en disco duro, por lo que deben considerarse en la política de seguridad.	Soporte
H4	Servidor de aplicaciones	Hardware donde se aloja y ejecuta el SISNOT y posiblemente otros sistemas. Activo crítico que centraliza el procesamiento y almacenamiento de datos. Requiere protección física y lógica.	Primario
H5	Conexión a Internet	Servicio de conectividad. Herramienta esencial para consultas a registros, comunicaciones e investigación. También representa un canal de riesgo que debe ser gestionado con firewalls, filtros y políticas de uso.	Primario
E1	Sitio	El sitio se refiere a la infraestructura física donde opera la Notaría García Medina, incluyendo sus instalaciones, áreas de trabajo y espacios de almacenamiento. Es un activo crítico que alberga recursos tecnológicos, documentación legal y personal.	Primario

Una vez identificados los activos asociados a cada proceso, se procederá a su valoración. Esta evaluación se realizará en función de las tres dimensiones de seguridad de la información definidas por la norma ISO/IEC 27001: **confidencialidad, integridad y disponibilidad**.

Cada una de estas dimensiones será calificada utilizando una escala del 1 al 4 (donde 1 es el impacto más bajo y 4 el más alto), de acuerdo con los criterios detallados en la tabla adjunta.

Tabla 22: Valores designados a dimensiones de activos

Nivel	Confidencialidad	Disponibilidad	Integridad
1 (Bajo)	Información pública. Su divulgación no representa ningún riesgo.	Interrupciones tolerables hasta por una semana.	Alteraciones no afectan las operaciones.
2 (Medio)	Uso interno. Una filtración tendría un impacto menor.	Interrupciones no deben exceder 24 horas.	Alteraciones causan impactos operativos leves.
3 (Alto)	Acceso restringido. Una filtración causaría daños significativos.	La interrupción máxima tolerable es de una hora.	Alteraciones provocan daños operativos moderados.
4 (Crítico)	Información estrictamente confidencial. Su filtración sería catastrófica.	Requiere disponibilidad continua e inmediata. Cero tolerancias a interrupciones.	Cualquier alteración genera un impacto crítico en el negocio.

Fuente: Elaboración propia

Una vez establecido el nivel de criticidad en cada dimensión (Confidencialidad, Disponibilidad e Integridad) para los activos de información, se calculará el promedio aritmético de estos valores para determinar su valoración global.

De acuerdo con el apetito de riesgo definido para la Notaría García Medina, se ha establecido un umbral crítico: aquellos activos con un promedio ≥ 3.0 serán clasificados como críticos y, por lo tanto,

priorizados para un análisis de riesgos exhaustivo, la implementación de tratamientos específicos y la propuesta de controles robustos, ya que representan los elementos esenciales que el SGSI busca proteger para garantizar la continuidad del servicio notarial y la confidencialidad de la información legal.

Tabla 23: Determinación del valor de los activos

ID	Nombre	Criterios de valorización			Valor final
		Confidencialidad	Disponibilidad	Integridad	
R1	Notario	0	2	0	1
R2	Administrador	0	3	0	1
R3	Jefe de RRHH	0	2	0	1
R4	Abogados	0	4	0	1
R5	Contabilidad	0	3	0	1
R6	Asistentes administrativos	0	3	0	1
R7	Asistentes notariales	0	3	0	1
R8	Personal de apoyo	0	3	0	1
I1	Registros públicos	4	4	4	4
I2	Boleta/factura	2	2	3	2
I4	Archivo	4	2	2	3
I5	Documento final	4	4	4	4
S1	SISNOT	4	4	4	4
S2	MS Office	1	1	2	1
S3	Base de datos	3	3	3	3

ID	Nombre	Criterios de valorización			Valor final
		Confidencialidad	Disponibilidad	Integridad	
H1	Computadora de escritorio	1	4	3	3
H2	Lector biométrico	1	1	1	1
H3	Fotocopiadora/ impresora	1	2	2	1
H4	Servidor de aplicaciones	4	3	4	3
H5	Conexión a Internet	1	4	2	2
E1	Sitio	3	4	4	4

Fuente: Elaboración propia

- **Fase 6: Gestionar los riesgos y crear un plan de tratamiento de riesgos**

  En esta etapa, se establece e implementa la estrategia de tratamiento para los riesgos previamente identificados y evaluados. Esta fase se concreta mediante la formulación de políticas de seguridad específicas, que contemplan la selección e implementación de controles organizativos y técnicos, el diseño de programas de capacitación y concientización dirigidos al personal, así como la definición de procedimientos operativos orientados a mitigar, transferir, evitar o aceptar los riesgos, en concordancia con el apetito de riesgo definido por la organización.

  La gestión de riesgos se desarrollará aplicando la metodología definida en la Fase 4 del proyecto. Tal como se estableció, el proceso comienza con la identificación y valoración de los activos de información críticos de la notaría. Una vez completado este paso esencial, se continuará con la identificación sistemática de las amenazas y vulnerabilidades

asociadas a cada activo, con el propósito de realizar una evaluación integral y precisa de los riesgos que podrían afectar a la institución.

Tabla 24: Análisis de riesgos de los activos (Amenazas y vulnerabilidades)

ID	Nombre	Vulnerabilidad	Amenaza
R1	Notario	Uso incorrecto de Software y Hardware	Uso de software sin licencia
		Cultura de seguridad insuficiente	Negación de accesos
R2	Administrador	Ausencia de personal	No disponibilidad de personal
		Uso incorrecto de Software y Hardware	Uso de software sin licencia
		Cultura de seguridad insuficiente	Negación de accesos
		Falta de mecanismo de monitoreo de acciones sobre manejo de información	
R3	Jefe de RRHH	Uso incorrecto de Software y Hardware	Uso de software sin licencia
		Cultura de seguridad insuficiente	Negación de accesos
		Falta de mecanismo de monitoreo de acciones sobre manejo de información	No disponibilidad de personal
R4	Abogados	Ausencia de personal	No disponibilidad de personal
		Proceso inadecuado de contratación	
		Uso incorrecto de Software y Hardware	Uso de software sin licencia
		Cultura de seguridad insuficiente	Negación de accesos
		Falta de mecanismo de monitoreo de acciones sobre manejo de información	Datos inconsistentes
R5	Contabilidad	Ausencia de personal	No disponibilidad de personal
		Proceso inadecuado de contratación	
		Uso incorrecto de Software y Hardware	Uso de software sin licencia
		Cultura de seguridad insuficiente	Negación de accesos

ID	Nombre	Vulnerabilidad	Amenaza
		Falta de mecanismo de monitoreo de acciones sobre manejo de información	Data inconsistente
R6	Asistentes administrativos	Ausencia de personal	No disponibilidad de personal
		Proceso inadecuado de contratación	
		Uso incorrecto de Software y Hardware	Uso de software sin licencia
		Cultura de seguridad insuficiente	Negación de accesos
		Falta de mecanismo de monitoreo de acciones sobre manejo de información	Espionaje, Robo de documentos, Robo de equipos
R7	Asistentes notariales	Ausencia de personal	No disponibilidad de personal
		Proceso inadecuado de contratación	Espionaje, Robo de documentos, Robo de equipos
		Uso incorrecto de Software y Hardware	Recuperación de información de equipos desechados
		Cultura de seguridad insuficiente	Manipulación de software
		Falta de mecanismo de monitoreo de acciones sobre manejo de información	
R8	Personal de apoyo	Ausencia de personal	No disponibilidad de personal
		Proceso inadecuado de contratación	
		Uso incorrecto de Software y Hardware	Uso de software sin licencia
		Cultura de seguridad insuficiente	Negación de accesos
		Falta de mecanismo de monitoreo de acciones sobre manejo de información	Data inconsistente, Espionaje, Robo de documentos,

ID	Nombre	Vulnerabilidad	Amenaza
			Robo de equipos
I1	Registros públicos	Falta de mecanismo de monitoreo de acciones sobre manejo de información	Fenómenos climáticos, Daño por agua, Contaminación
I2	Boleta/factura	Falta de mecanismo de monitoreo de acciones sobre manejo de información	Daño por agua, Contaminación, Data inconsistente, Malfuncionamiento de software
I4	Archivo	Falta de mecanismo de monitoreo de acciones sobre manejo de información	Robo de documentos
I5	Documento final	Falta de mecanismo de monitoreo de acciones sobre manejo de información	Contaminación, Polvo/corrosión, Daño por agua
S1	SISNOT	Prueba de software no existente	Malfuncionamiento de software
		Defectos del software	
		Falta de finalización de sesiones de usuarios	
		Interfaz de usuario compleja	
		Falta de mecanismo de autentificación	Copia fraudulenta de información
		Pobre gestión de contraseñas	
		Agentes externos	Falla en energía eléctrica
			Falla de conexión a internet
			Falta de mantenimiento de software
			Saturación de los sistemas de información
			Manipulación de software

ID	Nombre	Vulnerabilidad	Amenaza
S2	MS Office	Interfaz de usuario compleja	Recuperación de información de equipos desechados, Robo de documentos, Uso de software sin licencia, Data inconsistente
		Falta de documentación	
		Falta de respaldos	
S3	Base de datos	Falta de respaldos	Fenómenos sísmicos, Inundaciones /Incendios
		Falta de protección física del edificio ante incidentes naturales	
		Red energética inestable	Uso no autorizado de equipos
		Falta de procedimiento para reporte de debilidades en la seguridad	
		Falta de mecanismo de autentificación	Recuperación de información de equipos desechados
			Manipulación de hardware
H1	Computadora de escritorio	Mantenimiento insuficiente	Falta de mantenimiento de hardware
		Susceptibilidad al polvo, humedad y suciedad	
		Susceptible de cambio de voltaje	
		Susceptible al cambio de temperatura	Falla en el aire acondicionado
		Almacenamiento desprotegido	Uso no autorizado de equipos, Copia fraudulenta de información, Espionaje
H2		Falta de reemplazo periódico	

ID	Nombre	Vulnerabilidad	Amenaza
	Lector biométrico	Susceptibilidad al polvo, humedad y suciedad	Falla en energía eléctrica
			Robo de equipos
H3	Fotocopiadora/ impresora	Susceptible de cambio de voltaje	Falta de mantenimiento de hardware
		Susceptible al cambio de temperatura	
		Mantenimiento insuficiente	Malfuncionamiento de software
			Uso no autorizado de equipos
H4	Servidor de aplicaciones	Almacenamiento desprotegido	Copia fraudulenta de información
		Susceptible de cambio de voltaje	
		Susceptible al cambio de temperatura	Falla en el aire acondicionado
		Falta de documentación	Inundaciones /Incendios
		Falta de respaldos	
		Falta de protección física del edificio ante incidentes naturales	
		Líneas de comunicación no protegidas	Manipulación de software
		Falta de procedimientos de identificación y evaluación de riesgos	
		Falta de auditorías periódicas	
		Falta de política de manejo de información	Saturación de los sistemas de información
			Manipulación de hardware
			Falla en energía eléctrica

ID	Nombre	Vulnerabilidad	Amenaza
			Falla de conexión a internet
H5	Conexión a Internet	Líneas de comunicación no protegidas	Falla de conexión a internet
		Pobre cableado	Falla en energía eléctrica

Fuente: Elaboración propia

Una vez concluido el análisis de amenazas y vulnerabilidades, se procede a la elaboración del mapa de riesgos. A cada riesgo identificado se le asigna un valor de probabilidad de ocurrencia y un nivel de impacto, ambos cuantificados mediante escalas previamente definidas. El resultado de esta evaluación permite determinar la criticidad del riesgo al cruzar dichas variables, lo que facilita la priorización objetiva de los riesgos que pueden afectar los procesos de negocio más críticos de la notaría.

Para el tratamiento de los riesgos clasificados como altos o críticos, se definió que la estrategia más adecuada consiste en la implementación de controles de seguridad y la formulación de políticas específicas. Estas acciones están orientadas a que la organización mitigue de manera efectiva las amenazas que puedan comprometer sus activos de información, garantizando así la confidencialidad, integridad y disponibilidad de los datos esenciales para el correcto funcionamiento de la notaría.

Tabla 25: Tabla de evaluación de riesgos

ID Riesgo	ID Activo	Nombre	Riesgo	Consecuencias	Prob.	Impacto	Criticidad	Tratamiento
R01	R1	Notario	Utilización inadecuada de herramientas tecnológicas que violan los protocolos de seguridad establecidos.	Data inconsistente, malfuncionamiento de sistemas, vulnerabilidades explotables.	Probable	Alto	Medio	Reducir
R02			Falta de concienciación y formación en prácticas de seguridad entre el personal.	Uso de software sin licencia, accesos no autorizados, brechas de seguridad.	Probable	Alto	Medio	Reducir
R03	R2	Administrador	Falta de recursos humanos suficientes para mantener operaciones continuas y seguras.	Interrupción de servicios críticos, sobrecarga del personal existente.	Poco probable	Relevante	Alto	Reducir
R04			Manipulación inapropiada de sistemas que compromete la integridad de los datos.	Data inconsistente, errores en el sistema, pérdida de información.	Probable	Relevante	Alto	Reducir
R05			Desconocimiento de políticas de seguridad que lleva a prácticas de riesgo.	Vulnerabilidades de seguridad, accesos no controlados, fugas de información.	Probable	Crítico	Alto	Reducir
R06			Carecer de sistemas que vigilen y registren las actividades sobre la información.	Accesos no autorizados, detección tardía de incidentes, imposibilidad de auditoría.	Probable	Crítico	Alto	Reducir
R07	R3	Jefe de RRHH	Empleo erróneo de aplicaciones y equipos que conduce a fallos operativos.	Data inconsistente, inconsistencia en la información, procesos interrumpidos.	Probable	Relevante	Alto	Reducir

ID Riesgo	ID Activo	Nombre	Riesgo	Consecuencias	Prob.	Impacto	Criticidad	Tratamiento
R08			Ambiente donde no se priorizan las medidas de protección de datos.	Uso de software sin licencia, negligencia en el manejo de información sensible.	Probable	Crítico	Alto	Reducir
R09			Insuficiencia de controles para supervisar el tratamiento de información confidencial.	Accesos no autorizados a datos de personal, fugas de información.	Poco probable	Crítico	Alto	Reducir
R10	R4	Abogados	Escasez de abogados que afecta la continuidad operativa y la atención de casos.	Retrasos en procesos legales, acumulación de trabajo, errores por fatiga.	Poco probable	Alto	Alto	Reducir
R11			Falta de rigor en la selección de personal que puede introducir riesgos internos.	Contratación de personal no confiable, infiltración, malas prácticas.	Probable	Crítico	Alto	Reducir
R12			Manejo inapropiado de herramientas tecnológicas en el ámbito legal.	Data inconsistente en casos legales, pérdida de documentación crítica.	Probable	Relevante	Alto	Reducir
R13			Falta de adherencia a protocolos de confidencialidad y seguridad de información legal.	Fuga de información privilegiada, accesos no autorizados a expedientes.	Probable	Crítico	Alto	Reducir
R14			Carecer de supervisión sobre el manejo de información legal confidencial.	Accesos indebidos a datos sensibles, manipulación de evidencias o documentos.	Poco probable	Crítico	Alto	Reducir
R15	R5	Contabilidad	Falta de contadores que compromete la integridad financiera y el cierre de procesos.	Errores en estados financieros, incumplimiento de plazos legales.	Poco Probable	Alto	Alto	Reducir

ID Riesgo	ID Activo	Nombre	Riesgo	Consecuencias	Prob.	Impacto	Criticidad	Tratamiento
R16			Selección inapropiada de personal para manejar información financiera sensible.	Contratación de personal con intenciones fraudulentas, desvío de fondos.	Probable	Crítico	Alto	Reducir
R17			Manejo erróneo de software contable y equipos que almacenan data financiera.	Data financiera corrupta, errores en reportes, irregularidades contables.	Probable	Relevante	Alto	Reducir
R18			Ambiente donde no se protege adecuadamente la información financiera confidencial.	Fuga de información financiera, accesos no autorizados a cuentas.	Probable	Crítico	Alto	Reducir
R19	R6	Asistentes administrativos	Insuficiencia de personal para gestionar tareas administrativas críticas.	Acumulación de trabajo, retrasos en procesos operativos.	Poco probable	Alto	Alto	Reducir
R20			Falta de verificaciones rigurosas en la selección de personal administrativo.	Contratación de personal no idóneo o malintencionado, riesgo interno.	Probable	Crítico	Alto	Reducir
R21			Manejo inadecuado de herramientas ofimáticas y equipos.	Data inconsistente, pérdida de información administrativa, ineficiencia operativa.	Probable	Relevante	Alto	Reducir
R22			Desconocimiento de normas básicas de seguridad de la información.	Uso de software sin licencia, manejo indebido de datos sensibles, brechas de seguridad.	Probable	Relevante	Medio	Reducir
R23			Carecer de supervisión sobre el tratamiento de información administrativa.	Accesos no autorizados, fugas de información, espionaje, robo de documentos.	Poco probable	Crítico	Alto	Reducir

ID Riesgo	ID Activo	Nombre	Riesgo	Consecuencias	Prob.	Impacto	Criticidad	Tratamiento
R24	R7	Asistentes notariales	Falta de personal para apoyar procesos notariales esenciales.	Retrasos en servicios notariales, insatisfacción de clientes, pérdida de legitimidad.	Poco probable	Alto	Alto	Reducir
R25			Contratación sin filtros de seguridad de personal con acceso a información notarial crítica.	Infiltración, robo de información legal, sabotaje interno.	Probable	Crítico	Alto	Reducir
R26			Utilización incorrecta de sistemas notariales y equipos de almacenamiento.	Data inconsistente en actas notariales, invalidación de documentos, errores jurídicos.	Probable	Relevante	Alto	Reducir
R27			Ambiente que no prioriza la protección de datos sensibles del ámbito notarial.	Manipulación de software/hardware, accesos no autorizados a documentos legales.	Probable	Crítico	Alto	Reducir
R28			Falta de control sobre las acciones realizadas en sistemas que manejan información notarial.	Espionaje, robo de documentos, recuperación de información de equipos desechados.	Poco probable	Crítico	Alto	Reducir
R29	R8	Personal de apoyo	Escasez de personal de apoyo afecta la mantención y operación segura de la infraestructura.	Tareas de mantenimiento postergadas, entorno operativo inseguro.	Poco probable	Alto	Medio	Reducir
R30			Contratación sin verificación de personal con acceso físico a instalaciones críticas.	Robo de equipos, sabotaje físico, acceso no autorizado a áreas restringidas.	Probable	Crítico	Alto	Reducir
R31			Manejo inapropiado de herramientas y sistemas por parte del personal de apoyo.	Daño a equipos, configuración incorrecta de sistemas, data inconsistente.	Probable	Relevante	Alto	Reducir

ID Riesgo	ID Activo	Nombre	Riesgo	Consecuencias	Prob.	Impacto	Criticidad	Tratamiento
R32			Personal de apoyo no está entrenado en protocolos de seguridad.	Uso de software sin licencia, negligencia que conduce a accesos no autorizados o data inconsistente.	Probable	Crítico	Alto	Reducir
R33			No se supervisan las actividades del personal de apoyo con acceso a información e infraestructura.	Robo de documentos, robo de equipos, espionaje, manipulación de hardware/software.	Poco probable	Crítico	Alto	Reducir
R34	I1	Registros públicos	No hay control sobre el acceso y manipulación de registros públicos físicos.	Daño por agua, contaminación, pérdida irreversible de documentos legales.	Probable	Relevante	Bajo	Retener
R35	I2	Boleta/factura	Carecer de sistemas para auditar la generación y manejo de boletas/facturas.	Data inconsistente, malfuncionamiento de software, errores fiscales y contables.	Probable	Alto	Alto	Reducir
R36	I4	Archivo	No existe vigilancia adecuada sobre el archivo físico de documentos.	Daño por agua, contaminación, polvo, corrosión, inundaciones, incendios, robo de documentos.	Probable	Crítico	Alto	Reducir
R37	I5	Documento final	Falta de control sobre la custodia y preservación de documentos finales.	Contaminación, polvo, corrosión, daño por agua, deterioro de documentos importantes.	Probable	Relevante	Bajo	Retener
R38	S1	SISNOT	El software se implementa sin un protocolo de pruebas adecuado.	Malfuncionamiento de software, data inconsistente, fallas críticas en el sistema.	Poco probable	Alto	Alto	Reducir

ID Riesgo	ID Activo	Nombre	Riesgo	Consecuencias	Prob.	Impacto	Criticidad	Tratamiento
R39			El software contiene errores de programación no detectados.	Data inconsistente, pérdida de información.	Probable	Alto	Alto	Reducir
R40			Las sesiones de los usuarios no se cierran automáticamente tras un periodo de inactividad.	Acceso no autorizado a información confidencial si una estación queda desatendida.	Probable	Crítico	Alto	Reducir
R41			La dificultad para usar el sistema lleva a errores humanos.	Data inconsistente, ingresos incorrectos, demora en los procesos, frustración del usuario.	Probable	Relevante	Alto	Reducir
R42			No existe un sistema robusto para verificar la identidad de los usuarios.	Accesos no autorizados, suplantación de identidad, robo de información.	Probable	Crítico	Alto	Reducir
R43			Las contraseñas son débiles, se comparten o no se cambian regularmente.	Accesos no autorizados, saturación del sistema, manipulación de software.	Probable	Crítico	Alto	Reducir
R44	S2	MS Office	La complejidad de las suites ofimáticas lleva a su uso incorrecto.	Errores en documentos, data inconsistente, pérdida de formatos y información.	Probable	Relevante	Alto	Reducir
R45			No hay manuales o guías para el uso correcto del software.	Uso ineficiente, errores frecuentes, data inconsistente, dependencia de usuarios clave.	Probable	Relevante	Alto	Reducir
R46			No se realizan copias de seguridad de los documentos creados.	Pérdida permanente de información crítica ante fallos de hardware o software.	Poco probable	Crítico	Alto	Reducir
R47	S3	Base de datos	No existen copias de seguridad de la base de datos.	Pérdida completa e irreversible de toda la	Poco probable	Crítico	Medio	Retener

ID Riesgo	ID Activo	Nombre	Riesgo	Consecuencias	Prob.	Impacto	Criticidad	Tratamiento
				información empresarial ante un desastre.				
R48			El centro de datos no está protegido contra amenazas naturales.	Destrucción física de servidores por fenómenos sísmicos, inundaciones o incendios.	Improbable	Crítico	Medio	Retener
R49			La alimentación eléctrica del servidor es susceptible a cortes y fluctuaciones.	Caídas del servicio, corrupción de datos por apagones repentinos.	Poco probable	Alto	Alto	Reducir
R50			No hay un canal para que los usuarios reporten fallos o vulnerabilidades.	Vulnerabilidades no parcheadas, explotación continuada de fallos de seguridad.	Probable	Relevante	Alto	Reducir
R51			Control de acceso débil o inexistente a la base de datos.	Acceso no autorizado a toda la información, robo masivo de datos.	Probable	Crítico	Alto	Reducir
R52	H1	Computadora de escritorio	Las computadoras no reciben mantenimiento preventivo regular.	Fallas de hardware, pérdida de información.	Probable	Relevante	Alto	Reducir
R53			Los equipos están en entornos que aceleran su deterioro.	Cortocircuitos, sobrecalentamiento, fallas prematuras de componentes.	Probable	Relevante	Alto	Reducir
R54			Los equipos no están protegidos contra variaciones de energía.	Daño de componentes vitales, pérdida de información.	Poco probable	Relevante	Medio	Reducir
R55			Los equipos operan fuera de su rango térmico ideal.	Sobrecalentamiento, bloqueos del sistema, reducción de la vida útil del hardware.	Poco probable	Relevante	Medio	Reducir

ID Riesgo	ID Activo	Nombre	Riesgo	Consecuencias	Prob.	Impacto	Criticidad	Tratamiento
R56			Los equipos no están asegurados físicamente contra robo o acceso no autorizado.	Robo de equipos, acceso físico a información confidencial, copia fraudulenta de datos.	Poco probable	Crítico	Alto	Reducir
R57	H2	Lector biométrico	Los lectores no se renuevan según su vida útil, perdiendo precisión.	Fallas en el control de accesos, falsos rechazos o falsas aceptaciones.	Probable	Relevante	Alto	Reducir
R58			Los sensores se ensucian fácilmente en el entorno operativo.	Lecturas erróneas, incapacidad para identificar usuarios, indisponibilidad del control de acceso.	Probable	Relevante	Alto	Reducir
R59	H3	Fotocopiadora/impresora	Los equipos no tienen protección eléctrica.	Daño de circuitos internos, incendios, necesidad de reparaciones costosas.	Poco probable	Relevante	Medio	Reducir
R60			Los equipos están en entornos con mala climatización.	Sobrecalentamiento, atascos de papel, mala calidad de impresión.	Poco probable	Relevante	Medio	Reducir
R61			No hay un contrato de mantenimiento preventivo para los equipos.	Averías frecuentes, tiempos muertos, alto costo de reparaciones correctivas.	Probable	Relevante	Alto	Reducir
R62	H4	Servidor de aplicaciones	El servidor no está en un rack cerrado con llave o en una sala de acceso controlado.	Robo físico del servidor, manipulación hardware, extracción de discos duros.	Raro	Crítico	Medio	Retener
R63			El servidor no está conectado a un UPS o regulador de voltaje adecuado.	Apagados abruptos, corrupción del sistema operativo o de datos, daño hardware.	Poco probable	Alto	Alto	Reducir

ID Riesgo	ID Activo	Nombre	Riesgo	Consecuencias	Prob.	Impacto	Criticidad	Tratamiento
R64			La sala de servidores tiene un sistema de enfriamiento inadecuado.	Sobrecalentamiento, reinicios automáticos, falla catastrófica de componentes.	Poco probable	Alto	Alto	Reducir
R65			No existe documentación técnica de la configuración del servidor.	Dificultad para resolver problemas, dependencia de personal específico, errores en configuraciones.	Probable	Relevante	Alto	Reducir
R66			No se realizan backups completos del servidor.	Pérdida total de servicios y datos ante una falla del disco duro u otro componente.	Improbable	Crítico	Medio	Retener
R67			La sala de servidores es vulnerable a desastres naturales.	Destrucción completa del centro de datos por inundaciones, incendios o sismos.	Improbable	Crítico	Medio	Retener
R68			El cableado de red no está protegido o es susceptible a interceptación.	Intercepción de datos, espionaje, manipulación de información en tránsito.	Poco probable	Crítico	Alto	Reducir
R69			No se realizan análisis formales de riesgos de seguridad.	Vulnerabilidades desconocidas, falta de preparación ante incidentes, seguridad reactiva en lugar de proactiva.	Probable	Relevante	Alto	Reducir
R71			No hay directrices claras sobre cómo clasificar, manejar y destruir la información.	Manejo inconsistente de datos, fuga de información sensible, incumplimiento de normativas.	Probable	Crítico	Alto	Reducir
R72	H5	Conexión a Internet	La conexión a internet no está cifrada o se usan protocolos inseguros.	Intercepción de comunicaciones, robo de credenciales, accesos no autorizados desde el exterior.	Probable	Crítico	Alto	Reducir

ID Riesgo	ID Activo	Nombre	Riesgo	Consecuencias	Prob.	Impacto	Criticidad	Tratamiento
R73			La infraestructura de red interna (cableado) es de baja calidad o está mal instalada.	Fallas intermitentes de conexión, baja velocidad, pérdida de paquetes, interrupción de servicios.	Probable	Alto	Alto	Reducir

Fuente: Elaboración propia

Tabla 26: Mecanismos de control detectados

ID Riesgo	Riesgo	Criticidad	Cláusula	Controles ISO/IEC
R1	Acceso de usuarios no autorizados debido a que no se finalizó la sesión en el aplicativo.	Alto	A.9 Control de acceso A.11 Seguridad física y ambiental	A.9.4.3 - Los sistemas de gestión de contraseñas deben ser interactivos y garantizar la creación de contraseñas seguras y de alta calidad. A.11.2.9 - Debe implementarse una política de escritorio limpio, junto con una política de pantalla limpia para las áreas donde se realiza el procesamiento de la información.
R2	Utilización inadecuada de herramientas tecnológicas que violan los protocolos de seguridad establecidos.	Medio	A.8 Seguridad en los recursos humanos A.12 Seguridad de las operaciones	A.8.2.2 - Todos los empleados de la organización deben recibir formación y actualizaciones periódicas en políticas y procedimientos de seguridad.
R3	Falta de concienciación y formación en prácticas de seguridad entre el personal.	Medio	A.8 Seguridad en los recursos humanos A.7 Seguridad física y ambiental	A.8.2.2 - Todos los empleados de la organización deben recibir formación y actualizaciones periódicas en políticas y procedimientos de seguridad. A.7.3.1 - Se deben definir e implementar normas para el uso de equipos de procesamiento de información en áreas públicas.
R4	Falta de recursos humanos suficientes para mantener	Alto	A.6 Organización de la seguridad de la información	A.6.1.1 - Se debe definir una estructura de gestión que permita iniciar y controlar la implementación de la seguridad de la información dentro de la organización.

ID Riesgo	Riesgo	Criticidad	Cláusula	Controles ISO/IEC
	operaciones continuas y seguras.		A.7 Seguridad física y ambiental	
R5	Manipulación inapropiada de sistemas que compromete la integridad de los datos.	Alto	A.12 Seguridad de las operaciones A.14 Seguridad en el desarrollo y mantenimiento de sistemas	A.12.4.1 - Se deben establecer procedimientos para el control de malware, incluyendo la verificación de software y datos.
R6	Desconocimiento de políticas de seguridad que lleva a prácticas de riesgo.	Alto	A.8 Seguridad en los recursos humanos	A.8.2.2 - Todos los empleados de la organización deben recibir formación y actualizaciones periódicas en políticas y procedimientos de seguridad.
R7	Carecer de sistemas que vigilen y registren las actividades sobre la información.	Medio	A.12 Seguridad de las operaciones	A.12.4.1 - Se deben establecer procedimientos para el registro de eventos y la monitorización de sistemas.
R8	Empleo erróneo de aplicaciones y equipos que conduce a fallos operativos.	Alto		A.12.1.1 - Los procedimientos operativos deben ser documentados y puestos a disposición de todos los usuarios que lo necesitan.
R9	Ambiente donde no se priorizan las medidas de protección de datos.	Alto	A.8 Seguridad en los recursos humanos	A.8.2.2 - Todos los empleados y contratistas de la organización deben recibir formación y actualizaciones periódicas en políticas y procedimientos de seguridad, relevantes para su función.
R10	Insuficiencia de controles para supervisar el tratamiento de información confidencial.	Alto	A.12 Seguridad de las operaciones	A.12.4.1 - Se deben establecer procedimientos para el registro de eventos y la monitorización de sistemas.
R11	Escasez de abogados que afecta la continuidad operativa y la atención de casos.	Alto	A.6 Organización de la seguridad de la información	A.6.1.1 - Se debe definir una estructura de gestión que permita iniciar y controlar la implementación de la seguridad de la información.
R12	Falta de rigor en la selección de personal que puede introducir riesgos internos.	Alto	A.8 Seguridad en los recursos humanos	A.8.1.1 - Se deben definir roles y responsabilidades de seguridad para todo el personal.

ID Riesgo	Riesgo	Criticidad	Cláusula	Controles ISO/IEC
R13	Manejo inapropiado de herramientas tecnológicas en el ámbito legal.	Alto	A.12 Seguridad de las operaciones	A.12.1.1 - Los procedimientos operativos deben ser documentados y puestos a disposición de todos los usuarios que lo necesitan.
R14	Falta de adherencia a protocolos de confidencialidad y seguridad de información legal.	Alto		A.8.2.2 - Todos los empleados de la organización deben recibir formación y actualizaciones periódicas en políticas y procedimientos de seguridad, relevantes para su función.
R15	Carecer de supervisión sobre el manejo de información legal confidencial.	Alto		A.12.4.1 - Se deben establecer procedimientos para el registro de eventos y la monitorización de sistemas.
R16	Falta de contadores que compromete la integridad financiera y el cierre de procesos.	Alto	A.6 Organización de la seguridad de la información	A.6.1.1 - Se debe definir una estructura de gestión que permita iniciar y controlar la implementación de la seguridad de la información dentro de la organización.
R17	Selección inapropiada de personal para manejar información financiera sensible.	Alto	A.8 Seguridad en los recursos humanos	A.8.1.1 - Se deben definir roles y responsabilidades de seguridad para todo el personal.
R17	Manejo erróneo de software contable y equipos que almacenan data financiera.	Alto	A.12 Seguridad de las operaciones	A.12.1.1 - Los procedimientos operativos deben ser documentados y puestos a disposición de todos los usuarios que lo necesitan.
R18	Ambiente donde no se protege adecuadamente la información financiera confidencial.	Alto	A.8 Seguridad en los recursos humanos	A.8.2.2 - Todos los empleados y contratistas de la organización deben recibir formación y actualizaciones periódicas en políticas y procedimientos de seguridad.
R19	Insuficiencia de personal para gestionar tareas administrativas críticas.	Alto	A.6 Organización de la seguridad de la información	A.6.1.1 - Se debe definir una estructura de gestión que permita iniciar y controlar la implementación de la seguridad de la información.
R20	Falta de verificaciones rigurosas en la selección de personal administrativo.	Alto	A.8 Seguridad en los recursos humanos	A.8.1.1 - Se deben definir roles y responsabilidades de seguridad para todo el personal.

ID Riesgo	Riesgo	Criticidad	Cláusula	Controles ISO/IEC
R21	Manejo inadecuado de herramientas ofimáticas y equipos.	Alto	A.12 Seguridad de las operaciones	A.12.1.1 - Los procedimientos operativos deben estar debidamente documentados y ser accesibles para todos los usuarios que los requieran.
R22	Desconocimiento de normas básicas de seguridad de la información.	Alto		A.8.2.2 - Todos los empleados y contratistas de la organización deben recibir formación y actualizaciones periódicas en políticas y procedimientos de seguridad.
R23	Carecer de supervisión sobre el tratamiento de información administrativa.	Alto		A.12.4.1 - Se deben establecer procedimientos para el registro de eventos y la monitorización de sistemas.
R24	Falta de personal para apoyar procesos notariales esenciales.	Alto	A.6 Organización de la seguridad de la información	A.6.1.1 - Se debe definir una estructura de gestión que permita iniciar y controlar la implementación de la seguridad de la información.
R25	Contratación sin filtros de seguridad de personal con acceso a información notarial crítica.	Alto	A.8 Seguridad en los recursos humanos A.12 Seguridad de las operaciones	A.8.1.1 - Se deben asignar roles y responsabilidades correspondientes de seguridad para todo el personal.
R26	Utilización incorrecta de sistemas notariales y equipos de almacenamiento.	Alto		A.12.1.1 - Los procedimientos operativos deben ser documentados y puestos a disposición de todos los usuarios que lo necesitan.
R27	Ambiente que no prioriza la protección de datos sensibles del ámbito notarial.	Alto		A.8.2.2 - Todos los empleados y contratistas de la organización deben recibir formación y actualizaciones periódicas en políticas y procedimientos de seguridad, relevantes para su función.
R28	Falta de control sobre las acciones realizadas en sistemas que manejan información notarial.	Alto		A.12.4.1 - Se deben establecer procedimientos para el registro de eventos y la monitorización de sistemas.
R29	Escasez de personal de apoyo afecta la mantención y operación segura de la infraestructura.	Alto	A.6 Organización de la seguridad de la información	A.6.1.1 - Se debe definir una estructura de gestión que permita iniciar y controlar la implementación de la seguridad de la información.

ID Riesgo	Riesgo	Criticidad	Cláusula	Controles ISO/IEC
R30	Contratación sin verificación de personal con acceso físico a instalaciones críticas.	Alto	A.8 Seguridad en los recursos humanos	A.8.1.1 - Se deben definir los roles y responsabilidades de seguridad para todo el personal.
R31	Manejo inapropiado de herramientas y sistemas por parte del personal de apoyo.	Alto	A.12 Seguridad de las operaciones	A.12.1.1 - Los procedimientos operativos deben estar formalmente documentados y disponibles para todos los usuarios que los necesiten.
R32	Personal de apoyo no está entrenado en protocolos de seguridad.	Alto	A.8 Seguridad en los recursos humanos	A.8.2.2 - Todos los empleados y contratistas de la organización deben recibir formación y actualizaciones periódicas en políticas y procedimientos de seguridad, relevantes para su función.
R33	No se supervisan las actividades del personal de apoyo con acceso a información e infraestructura.	Alto	A.12 Seguridad de las operaciones A.11 Seguridad física y ambiental	A.12.4.1 - Se deben establecer procedimientos para el registro de eventos y la monitorización de sistemas.
R34	No hay control sobre el acceso y manipulación de registros públicos físicos.	Medio		A.11.1.1 - Se deben establecer perímetros de seguridad con el propósito de proteger las áreas que albergan información y servicios de procesamiento de datos.
R35	Carecer de sistemas para auditar la generación y manejo de boletas/facturas.	Alto		A.12.4.1 - Se deben establecer procedimientos para el registro de eventos y la monitorización de sistemas.
R36	No existe vigilancia adecuada sobre el archivo físico de documentos.	Alto		A.11.1.1 - Se deben definir perímetros de seguridad para proteger áreas que contienen información y servicios de procesamiento de la información.
R37	Falta de control sobre la custodia y preservación de documentos finales.	Bajo		
R38	El software se implementa sin un protocolo de pruebas adecuado.	Alto	A.14 Seguridad en el desarrollo y	A.14.2.1 - Se deben establecer reglas para el desarrollo de software y sistemas.

ID Riesgo	Riesgo	Criticidad	Cláusula	Controles ISO/IEC
R39	El software contiene errores de programación no detectados.	Alto	mantenimiento de sistemas	
R40	Las sesiones de los usuarios no se cierran automáticamente tras un periodo de inactividad.	Alto	A.9 Control de acceso	A.9.4.3 - Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar contraseñas de calidad.
R41	La dificultad para usar el sistema lleva a errores humanos.	Alto	A.12 Seguridad de las operaciones	A.12.1.1 - Los procedimientos operativos deben ser documentados y puestos a disposición de todos los usuarios que lo necesitan.
R42	No existe un sistema robusto para verificar la identidad de los usuarios.	Alto	A.9 Control de acceso	A.9.4.3 - Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar contraseñas de calidad.
R43	Las contraseñas son débiles, se comparten o no se cambian regularmente.	Alto		
R44	La complejidad de las suites ofimáticas lleva a su uso incorrecto.	Alto	A.12 Seguridad de las operaciones	A.12.1.1 - Los procedimientos operativos deben ser documentados y puestos a disposición de todos los usuarios que lo necesitan.
R45	No hay manuales o guías para el uso correcto del software.	Alto		
R46	No se realizan copias de seguridad de los documentos creados.	Alto		A.12.3.1 - Copias de respaldo de la información del software y de las imágenes del sistema deben ser tomadas y probadas regularmente en concordancia con una política de respaldo acordada.
R47	No existen copias de seguridad de la base de datos.	Medio		
R48	El centro de datos no está protegido contra amenazas naturales.	Medio	A.11 Seguridad física y ambiental	A.11.1.4 - Se deben proteger contra amenazas físicas y naturales las instalaciones de procesamiento de información.

ID Riesgo	Riesgo	Criticidad	Cláusula	Controles ISO/IEC
R49	La alimentación eléctrica del servidor es susceptible a cortes y fluctuaciones.	Alto		
R50	No hay un canal para que los usuarios reporten fallos o vulnerabilidades.	Alto	A.16 Gestión de incidentes de seguridad de la información	A.16.1.1 - Se deben establecer responsabilidades y procedimientos para la gestión de incidentes de seguridad de la información.
R51	Control de acceso débil o inexistente a la base de datos.	Alto	A.9 Control de acceso	A.9.1.1 - Se debe definir una política de control de acceso.
R52	Las computadoras no reciben mantenimiento preventivo regular.	Alto	A.11 Seguridad física y ambiental	A.11.2.4 - Se debe proteger el equipo contra cortes de energía y otras anomalías eléctricas utilizando UPS y reguladores de voltaje.
R53	Los equipos están en entornos que aceleran su deterioro.	Alto		
R54	Los equipos no están protegidos contra variaciones de energía.	Medio		
R55	Los equipos operan fuera de su rango térmico ideal.	Medio		
R56	Los equipos no están asegurados físicamente contra robo o acceso no autorizado.	Alto		A.11.1.1 - Deben delimitarse fronteras de protección para resguardar las áreas que albergan información y sistemas de procesamiento.
R57	Los sensores se ensucian fácilmente en el entorno operativo.	Alto		A.11.2.4 - Se debe proteger el equipo contra cortes de energía y otras anomalías eléctricas utilizando UPS y reguladores de voltaje.
R58	Los equipos no tienen protección eléctrica.	Alto		
R59	Los equipos están en entornos con mala climatización.	Medio		
R60	No hay un contrato de mantenimiento preventivo para los equipos.	Medio		

ID Riesgo	Riesgo	Criticidad	Cláusula	Controles ISO/IEC
R61	El servidor no está en un rack cerrado con llave o en una sala de acceso controlado.	Alto	A.11 Seguridad física y ambiental	A.11.2.4 - Se debe proteger el equipo contra cortes de energía y otras anomalías eléctricas utilizando UPS y reguladores de voltaje.
R62	El servidor no está conectado a un UPS o regulador de voltaje adecuado.	Medio		A.11.1.1 - Es necesario establecer perímetros de seguridad que resguarden las zonas con información y servicios de procesamiento de datos.
R63	La sala de servidores tiene un sistema de enfriamiento inadecuado.	Alto		A.11.2.4 - Se debe proteger el equipo contra cortes de energía y otras anomalías eléctricas utilizando UPS y reguladores de voltaje.
R64	No existe documentación técnica del servidor.	Alto		
R65	No se realizan backups completos del servidor.	Alto	A.12 Seguridad de las operaciones	A.12.1.1 - Es necesario documentar los procedimientos operativos y garantizar su acceso a los usuarios involucrados.
R66	La sala de servidores es vulnerable a desastres naturales.	Medio		A.12.3.1 - Es necesario generar y validar regularmente las copias de respaldo, de acuerdo con una política de respaldo definida.
R67	El cableado de red no está protegido o es susceptible a interceptación.	Medio	A.11 Seguridad física y ambiental	A.11.1.4 - Se deben proteger contra amenazas físicas y naturales las instalaciones de procesamiento de información.
R68	No se realizan análisis formales de riesgos de seguridad.	Alto	A.13 Seguridad de las comunicaciones	A.13.2.1 - Se deben establecer políticas, procedimientos y controles para la gestión de redes.
R69	No se realizan revisiones programadas de seguridad y configuración.	Alto	A.5 Políticas de seguridad de la información	A.5.1.1 - Se deben definir políticas para la seguridad de la información.
R70	No hay directrices claras sobre cómo clasificar, manejar y destruir la información.	Alto	A.12 Seguridad de las operaciones	A.12.1.1 - Es necesario documentar y facilitar el acceso a los procedimientos operativos a todos los usuarios involucrados.

ID Riesgo	Riesgo	Criticidad	Cláusula	Controles ISO/IEC
R71	La conexión a internet no está cifrada.	Alto	A.8 Seguridad en los recursos humanos	A.8.2.2 - Todos los empleados y contratistas de la organización deben recibir formación y actualizaciones periódicas en políticas y procedimientos de seguridad.
R72	La infraestructura de red interna (cableado) es de baja calidad o está mal instalada.	Alto Alto	A.13 Seguridad de las comunicaciones	A.13.1.1 - Se deben establecer políticas y procedimientos de seguridad para redes.

Fuente: Elaboración propia

- **Fase 7: Desarrollar normativas y procesos para el control de riesgos**

  Tras completar el análisis de los riesgos y la identificación de controles necesarios, se procede al diseño de la Declaración de Aplicabilidad. Este documento fundamental, exigido por la norma ISO/IEC 27001. Para cada control, se evalúa su aplicabilidad a la Notaría García Medina con base en criterios preestablecidos, como el nivel de riesgo, los requisitos legales y las necesidades específicas del negocio. En los casos en que un control no sea aplicable, se debe registrar una justificación formal que fundamente dicha exclusión, garantizando así que ninguna medida de seguridad relevante haya sido omitida sin una evaluación rigurosa.

Tabla 27: Aspectos de la declaración de aplicabilidad

5. Políticas de seguridad de la información											
5.1. Marco Directivo para la seguridad de la información											
Sección	Objetivo	Descripción	Aplicabilidad		Justificación de exclusión	Criterio de inclusión					Implementación en la notaría
			Sí	No		RL	OC	RN	BP	RA	
5.1.1.	Directrices de protección de datos	Se requiere formalizar en un documento las políticas de seguridad de la información ya existentes, para su difusión y conocimiento obligatorio por parte de todo el personal vinculado al SGSI.	X		-				X		Se hizo el documento de Política de Seguridad de la Información.
5.1.2	Análisis de directrices de seguridad informática	Se debe establecer un procedimiento para la revisión y actualización anual de las políticas de seguridad de la información, garantizando su pertinencia y efectividad permanentes.	X		-				X		Se realizó el documento de Política de Seguridad de la Información.

6. Políticas de seguridad de la información											
6.1. Organización interna											
Sección	Objetivo	Descripción	Aplicabilidad		Justificación de exclusión	Criterio de inclusión					Implementación en la notaría
			Sí	No		RL	OC	RN	BP	RA	
6.1.1.	Roles y compromisos en protección de datos	Se debe asignar de manera explícita los roles y obligaciones en ciberseguridad a cada miembro del SGSI, garantizando el cumplimiento normativo.	x		-				x		Se ha establecido y aplicado la Política de Seguridad de la Información, la cual especifica de manera clara las funciones y obligaciones del personal en la salvaguarda de los recursos tecnológicos.
6.1.2	Separación de deberes	Se debe segmentar las áreas críticas mediante la segregación de funciones, con el fin de asignar responsabilidades diferenciadas.			-				x	x	La notaría ha establecido sus procesos aplicando criterios de segregación de tareas.
6.1.3	Comunicación con organismos reguladores	Las políticas deben establecer un protocolo de comunicación continua y formal con los organismos reguladores de seguridad de la información.		X	La organización carece de canales establecidos de comunicación con autoridades reguladoras vinculadas a sus procesos de negocio						-

6. Políticas de seguridad de la información											
6.1. Organización interna											
Sección	Objetivo	Descripción	Aplicabilidad		Justificación de exclusión	Criterio de inclusión					Implementación en la notaría
			Sí	No		RL	OC	RN	BP	RA	
6.1.4.	Vinculación con colectivos especializados	El responsable de la seguridad debe gestionar la participación activa en foros y comunidades especializadas para mantener actualizados los conocimientos en ciberseguridad		X	Las actividades de seguridad informática deben ser ejecutadas por especialistas, no por el personal operacional.						-
6.1.5.	Seguridad informática en la administración de proyectos	La seguridad de la información se debe considerar en cualquier proyecto.		X	No representa un riesgo crítico.						-

7. Seguridad de los recursos humanos											
7.1. Antes de asumir el empleo											
Sección	Objetivo	Descripción	Aplicabilidad		Justificación de exclusión	Criterio de inclusión					Implementación en la notaría
			Sí	No		RL	OC	RN	BP	RA	
7.1.1.	Selección	Se debe implementar un proceso exhaustivo de verificación de antecedentes para todo el personal.		X	La antigüedad y estabilidad del equipo actual mitiga riesgos críticos.				X		-

7.1.2	Términos y condiciones del empleo	Se debe establecer un documento formal de acuerdos de confidencialidad y uso adecuado de recursos tecnológicos, de obligatoria firma por empleados, contratistas y terceros.	X		-	X	X				Mediante el Acuerdo de Confidencialidad, se declara que los procesos internos de la notaría son información reservada, cuya revelación acarrea sanciones penales.
7. Seguridad de los recursos humanos											
7.2. Durante la ejecución del empleo											
Sección	Objetivo	Descripción	Aplicabilidad		Justificación de exclusión	Criterio de inclusión					Implementación en la notaría
			Sí	No		RL	OC	RN	BP	RA	
7.2.2.	Estrategia integral de formación en ciberseguridad	Todos los empleados deben recibir formación en temas de ciberseguridad.	X						X		Los trabajadores de la notaría reciben capacitación continua para concienciarse sobre la importancia de proteger los datos y sistemas críticos.
7.2.3.	Proceso sancionador	Implementar sanciones para quienes violen las políticas de seguridad establecidas.	X						X		Fue desarrollado el marco normativo de seguridad, el cual determina las consecuencias y medidas disciplinarias aplicables en casos de violación.

8. Gestión de activos											
8.1. Responsabilidad por los activos											
Sección	Objetivo		Aplicabilidad		Justificación de exclusión	Criterio de inclusión					Implementación en la notaría
			Sí	No		RL	OC	RN	BP	RA	
8.1.1.	Catálogo de recursos	Disponer de un registro completo de sus activos.	X		-				X	X	La identificación y clasificación de activos vinculados a procesos organizativos dio como producto el Inventario de Activos de Información.
8.1.2.	Titularidad de recursos	Identificar y documentar al custodio actual de cada activo.	X		-				X	X	El inventario contiene registros actualizados que especifican al responsable asignado para cada activo de información.
8.1.3.	Uso adecuado de los recursos	Incluir un compromiso formal de los empleados sobre el uso correcto de los recursos de la organización.	X								Se elaboró una política de Gestión de Activos, la cual define los lineamientos para el uso adecuado de los recursos informativos por parte del personal.

8.1.4.	Restitución de recursos asignados	Establecer un procedimiento formal para que los empleados devuelvan los activos al reubicarse o desvincularse.	X								Se elaboró la política de Gestión de Accesos, la cual incluye disposiciones específicas sobre el procedimiento de devolución de activos tras la terminación del vínculo laboral del personal.

8. Gestión de activos											
8.2. Clasificación de la información											
Sección	Objetivo	Descripción	Aplicabilidad		Justificación de exclusión	Criterio de inclusión					Implementación en la notaría
			Sí	No		RL	OC	RN	BP	RA	
8.2.1.	Clasificación de la información	definir un método para categorizar la información con base en su valor y sensibilidad.		X	No representa un riesgo crítico.						-
8.2.2	Categorización de activos de información	Toda información debe clasificarse según su valor e importancia para la organización.		X	No representa un riesgo crítico.						-
8.2.3	Administración de activos	Se deben establecer procedimientos que garanticen el manejo adecuado de los activos de la organización.		X	Ya se consideró una política de gestión de activos						-

9. Control de accesos											
9.1. Requisitos del negocio para control de acceso											
Sección	Objetivo	Descripción	Aplicabilidad		Justificación de exclusión	Criterio de inclusión					Implementación en la notaría
			Sí	No		RL	OC	RN	BP	RA	
9.1.1.	Política de control de acceso	Se deben establecer políticas de acceso a la información basadas en privilegios definidos según las funciones de cada usuario.	X		-						Se hizo la Política de Gestión de Accesos.
9.1.2	Política sobre el uso de los servicios de red	Se debe definir el acceso a la red de acuerdo con las funciones y responsabilidades asignadas a cada usuario.	X		-						Se realizó la política de uso aceptable de los servicios de red y comunicaciones
9.2. Gestión de accesos de usuarios											
9.2.1.	Registro y cancelación del registro de usuarios	Contar con un registro vigente; así mismo, se debe proceder con la baja inmediata de aquellos que ya no formen parte de la notaría o ya no usen el sistema.	X		-	X	X	X	X	X	La revocación de accesos a sistemas debe realizarse inmediatamente después de la baja laboral del personal.
9.2.2.	Suministro de acceso de usuarios	Establecer un protocolo que faculte a los administradores del sistema para conceder o denegar el acceso a los usuarios.	X		-				X		Se debe implementar control de acceso con usuario y contraseña en todos los ordenadores.

9.2.3.	Control de accesos con permisos elevados	Es necesario definir permisos exclusivos de acceso con base en las responsabilidades funcionales de cada colaborador dentro de la organización.	X		-				X		Los accesos del sistema deben ser revisados cíclicamente.
9.2.4.	Control de datos secretos de verificación de identidad	Esta información debe estar limitada exclusivamente al personal con privilegios especiales.	X		-				X		Los privilegios para gestionar accesos en sistemas están limitados estrictamente a personal designado.
9.2.5.	Verificación de privilegios de acceso asignados	Se debe realizar una supervisión periódica de los privilegios concedidos a los usuarios, con el objetivo de verificar que estos sean apropiados.	X		-				X	X	Se realizan auditorías regulares de los permisos concedidos en el sistema.
9.2.6.	Administración de cambios en derechos de acceso	Al trasladarse o retirarse un usuario, se deben revocar o modificar sus privilegios de acceso a la información.	X		-	X			X		Al personal que deja la organización se le deben revocar los accesos a los sistemas de información de manera oportuna.

9.3. Responsabilidades de los usuarios											
9.3.1.	Uso de la información de autenticación secreta	Se deben crear perfiles de acceso para la información considerada crítica o de alta importancia para la empresa.	X						X	X	La administración de accesos debe ser realizada únicamente por empleados específicamente autorizados.
9.4. Control de acceso a sistemas y aplicaciones											
9.4.1.	Gestión de permisos de información	Solo el personal con autorización expresa puede acceder a la información, de acuerdo con las políticas establecidas.	X		-				X	X	Los activos físicos considerados críticos para la operación están resguardados en un área de acceso controlado, restringido para el público general.
9.4.2.	Procedimiento de ingreso seguro	Deben establecerse mecanismos de control de accesos que restrinjan el ingreso a datos sensibles.	X		-	X	X	X			Es obligatorio identificarse con usuario y contraseña para utilizar cualquier ordenador
9.4.3.	Gestión y control de contraseñas	Establecer políticas de administración de contraseñas que contemplen renovación periódica, bloqueo automático por intentos erróneos y parámetros técnicos para generación de claves fuertes.	X		-				X	X	Las políticas organizacionales de contraseñas han sido configuradas en todos los sistemas de información.

9.4.4.	Uso de programas utilitarios privilegiados	Se debe limitar el empleo de programas utilitarios debido a su potencial para comprometer la integridad de las contraseñas, ya que ciertas herramientas pueden exponerlas, generando brechas de seguridad.		X	No representa un riesgo crítico.						-
9.4.5.	Control de permisos para consultar y modificar código fuente	Se deben establecer políticas de acceso al código fuente, el cual debe estar restringido únicamente al personal autorizado.		X	No representa un riesgo crítico.						-

10. Criptografía											
10.1. Controles criptográficos											
Sección	Objetivo	Descripción	Aplicabilidad		Justificación de exclusión	Criterio de inclusión					Implementación en la notaría
			Sí	No		RL	OC	RN	BP	RA	
10.1.1.	Política sobre controles criptográficos	Aplicar cifrado para proteger la confidencialidad, integridad y disponibilidad de la información.		X	Los mecanismos de cifrado deben configurarse fuera del alcance de una política determinada.						-
10.1.2	Gestión de llaves	Es fundamental implementar medidas criptográficas que aseguren la protección de la información.	X		-	X			X		Las tablas a nivel de base de datos se encuentran cifradas.

11. Seguridad física y del entorno											
11.1. Áreas seguras											
Sección	Objetivo	Descripción	Aplicabilidad		Justificación de exclusión	Criterio de inclusión					Implementación en la notaría
			Sí	No		RL	OC	RN	BP	RA	
11.1.1.	Perímetros de seguridad	Debe definirse un perímetro de seguridad que restrinja el acceso físico a las ubicaciones donde se almacenan o procesan los activos de la organización.	X		-	X	X	X	X	X	Los recursos físicos esenciales deben situarse en entornos seguros, inaccesibles para personas no autorizadas
11.1.2.	Mecanismos de control de acceso físico	El acceso a ubicaciones críticas como centros de datos y áreas con información, debe restringirse con cerraduras.	X		-	X	X	X	X	X	Solo el personal autorizado puede ingresar al centro de datos
11.1.3.	Seguridad de las instalaciones	Se debe restringir el acceso a áreas delimitadas exclusivamente para personal autorizado, mediante señalización.	X		-	X	X	X			Todas las áreas restringidas de la notaría están correctamente identificadas con señales
11.1.4.	Seguridad frente a amenazas del entorno y factores ambientales	Instalar detectores de humo y humedad, distribuir extintores y controlar la climatización en cuartos técnicos como medidas de protección física	X		-				X	X	Como protección frente a riesgos internos, la notaría dispone de extintores, sistemas de alarma y luminarias

11.2. Equipos											
11.2.1.	Localización y resguardo de los equipos.	Los equipos deben situarse en ubicaciones seguras y controladas, con el propósito de protegerlos contra robos, accesos no autorizados y otras amenazas físicas.	X		-	X	X	X			El acceso al centro de datos está restringido únicamente a personal autorizado.
11.2.2.	Suministro de energía	Es esencial contar con un suministro eléctrico adecuado y un sistema de respaldo	X		-			X	X		Contar con planes de continuidad para mantener las operaciones en cualquier escenario.
11.2.3.	Cableado	Proteger el cableado eléctrico y de datos contra daños físicos e interceptación.	X		-						En la notaría las áreas cableadas reciben mantenimiento continuo y un personal designado.
11.2.4.	Mantenimiento de equipos	Implementar programas de mantenimiento preventivo y correctivo en intervalos regulares definidos.	X		-				X		Planificar revisiones técnicas anuales para todos los equipos y sistemas
11.2.8.	Equipo de usuarios desatendidos	Configurar bloqueos automáticos en equipos inactivos para proteger la información confidencial.	X		-	X	X	X			Los sistemas tienen bloqueo automático para prevenir acceso no autorizado
11.2.9.	Política de escritorio limpio y pantalla limpia	Definir procedimientos de escritorio limpio, asegurando la ausencia de papeles y medios de almacenamiento.	X		-	X	X	X	X	X	Mantener los escritorios libres de documentos confidenciales.

12.Seguridad de las operaciones											
12.1. Procedimientos operacionales y responsabilidades											
12.1.1.	Procedimientos de operación documentados	Los procedimientos y manuales de operación deben estar documentados y ser accesibles para todos.	X		-				X	X	La documentación de procesos de la empresa está disponible en una carpeta compartida para toda la organización.

12.2. Protección contra códigos maliciosos											
Sección	Objetivo	Descripción	Aplicabilidad		Justificación de exclusión	Criterio de inclusión					Implementación en la notaría
			Sí	No		RL	OC	RN	BP	RA	
12.2.1.	Controles contra códigos maliciosos	Es esencial mantener actualizado el software antimalware de los equipos informáticos	X		-				X		Se realizarán auditorías periódicas para verificar que todos los activos de software cuenten con antivirus actualizadas.
12.3. Copias de respaldo											
12.3.1.	Respaldo de la información	Se deben generar respaldos de la información y verificar mediante pruebas su conformidad con las políticas correspondientes.	X		-				X	X	Los activos de software requieren una copia de respaldo mensual que, tras ser revisada, debe almacenarse fuera del centro de operaciones.

13. Seguridad de las comunicaciones											
13.1. Gestión de la seguridad de las redes											
Sección	Objetivo	Descripción	Aplicabilidad		Justificación de exclusión	Criterio de inclusión					Implementación en la notaría
			Sí	No		RL	OC	RN	BP	RA	
13.1.1.	Control de redes	Es imperativo desplegar software especializado, como firewalls, sistemas de detección de intrusiones y mecanismos de autenticación robustos, para controlar y supervisar el acceso a la red corporativa.	X		-				X	X	El acceso al software está protegido por un directorio activo que requiere autenticación.

16.Gestion de incidentes de seguridad de la información											
16.1. Gestión de incidentes y mejoras en la seguridad de la información											
16.1.1.	Responsabilidades y procedimientos	Establecer protocolos de respuesta inmediata para abordar incidentes.	X		-				X		Se elaboró e implementó la Política de Gestión de Incidentes.

Sección	Objetivo	Descripción	Aplicabilidad		Justificación de exclusión	Criterio de inclusión					Implementación en la notaría
			Sí	No		RL	OC	RN	BP	RA	
16.1.2.	Reporte de eventos de seguridad	Se debe reportar todos los eventos relacionados con incidentes de seguridad de la información.	X		-				X		Los incidentes será registrada en el documento lógico

Sección	Objetivo	Descripción	Aplicabilidad		Justificación de exclusión	Criterio de inclusión					Implementación en la notaría
			Sí	No		RL	OC	RN	BP	RA	
16.1.3.	Reporte de debilidades de seguridad	Informar sobre eventos generados, con el fin de identificar recurrencias y debilidades.	X		-				X		"Incidentes de Seguridad de la Información".
16.1.5.	Respuesta a incidentes	Determinar los pasos a seguir para dar solución al incidente.	X		-						Política de Gestión de Incidentes.
16.1.7.	Recolección de evidencia	Definir un procedimiento para documentar los incidentes de tal forma que exista una evidencia	X		-				X		Se ha definido un documento Excel, en una carpeta compartida, en la cual se registrarán los incidentes que se suscitarán en la organización.

17. Aspectos de seguridad de la información de la gestión de continuidad de negocio											
17.1. Continuidad de seguridad de la información											
Sección	Objetivo	Descripción	Aplicabilidad		Justificación de exclusión	Criterio de inclusión					Implementación en la notaría
			Sí	No		RL	OC	RN	BP	RA	
17.1.1.	Planificación de la continuidad de la información	Establecer políticas de continuidad que aseguren la operatividad de procesos críticos.	X		-				X		Política de Gestión de Incidentes.

17.1.2.	Continuidad de la información	protocolos que garanticen la disponibilidad del negocio frente a eventos imprevistos.	X		-				X		Política de Gestión de Incidentes, la cual integra procesos para garantizar la continuidad operacional de la notaría ante eventos disruptivos.
18. Cumplimiento											
18.1. Cumplimiento de requisitos legales y contractuales											
Sección	Objetivo	Descripción	Aplicabilidad		Justificación de exclusión	Criterio de inclusión					Implementación en la notaría
			Sí	No		RL	OC	RN	BP	RA	
18.1.1.	Identificación de la legislación aplicable y de los requisitos contractuales	Definir el marco legal con el cual se debe regir la seguridad de la información.	X		-				X		Se diseñó la Política de Seguridad de la Información.
18.1.3.	Protección de registros	Establecer un protocolo que garantice la protección de los registros contra riesgos de robo, modificación no autorizada o divulgación indebida.	X		-	X	X	X			Se hizo controles preventivos que aseguran la seguridad de los registros.
18.1.4.	Privacidad y protección de datos personales	Cumplir con las políticas de la protección de datos personales	X		-	X	X	X	X	X	

18.2. Revisiones de seguridad de la información											
18.2.3.	Revisión del cumplimiento técnico	Se deben revisar que todo el personal conoce y cumple con las políticas de seguridad de la información	X		-	X	X	X	X	X	Se hizo evaluaciones anuales al SGSI.

Fuente: Elaboración propia.

El análisis recogido en la tabla anterior permitió identificar un conjunto de políticas específicas, necesarias para abordar aspectos concretos de la seguridad, cuya elaboración e implementación posterior se estableció como un objetivo clave. Es importante destacar que todas estas políticas particulares se alinean y derivan su autoridad de un marco superior: la Política General de Seguridad de la Información. Dicha política general actúa como el pilar fundamental que las respalda, garantizando coherencia, estableciendo los principios rectores y asegurando que, en su conjunto, formen un sistema de seguridad unificado y robusto.

Esta fase del proyecto consistió en evaluar el Sistema de Gestión de Seguridad de la Información (SGSI) implementado, con el objetivo de verificar el correcto diseño, implementación y operatividad de los controles seleccionados.

Todo el proceso de implementación y verificación se realizó en coordinación con la gerencia de la Notaría García Medina. Como culminación del proyecto, se suscribió un Acta de Cierre (Ver Anexo 12), la cual formaliza la finalización exitosa de la implementación del SGSI propuesto, detallando los entregables, el alcance cumplido y los acuerdos mutuos.

4.3. Procesamiento, análisis e interpretación de resultados

Para la variable independiente: Evaluación estadística de los resultados obtenidos mediante el instrumento de investigación

Para procesar los datos obtenidos relacionados a la variable independiente tomaremos una escala del 1 al 5 donde valoramos el nivel de implementación con respecto al sistema de gestión de seguridad de la información (SGSI) el cual se detalla de la siguiente manera:

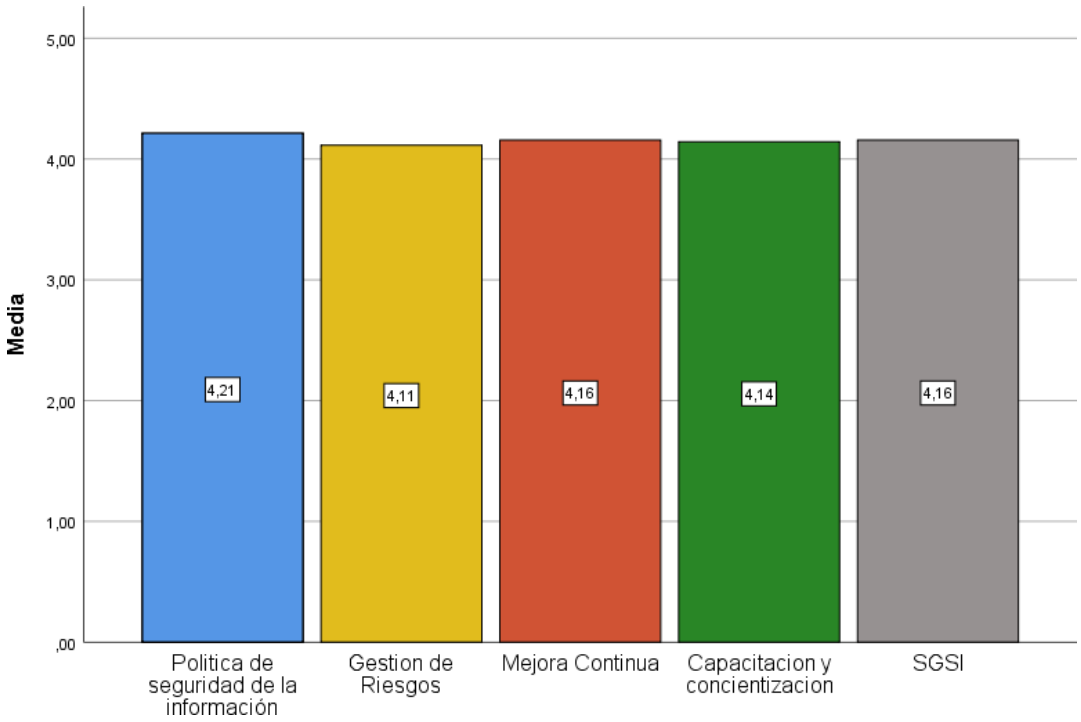
Tabla 28: Escala de aceptación de la variable independiente

1.00 – 1.80 → Deficiente
1.81 – 2.60 → Insuficiente
2.61 – 3.40 → Aceptable
3.41 – 4.20 → Bueno
4.21 – 5.00 → Óptimo

Fuente: Elaboración propia

Análisis estadístico:

Figura 17: Resultados obtenidos para la variable independiente



Fuente: Elaboración propia

La evaluación de la variable independiente mostró que el SGSI presenta un nivel de implementación bueno con un promedio general de 4.16 (escala 1–5). La dimensión de política de seguridad de la información alcanzo una aceptación de nivel óptimo, con un promedio de 4.21, las dimensiones: gestión de riesgos, mejora continua y concientización obtuvieron el valor promedio que esta entre la escala de aceptación de bueno, lo que sugiere la necesidad de fortalecer los mecanismos de revisión y actualización del sistema. En conjunto, estos resultados confirman que la organización cuenta con un SGSI consolidado, capaz de generar mejoras sostenibles en la seguridad de la información.

Para la variable dependiente: Comparación de resultados obtenidos mediante instrumento de investigación (pre vs post)

Para la primera dimensión de la variable dependiente: Confidencialidad

Prueba de normalidad:

Tabla 29: Prueba de normalidad para la dimensión Confidencialidad pre y post implementación del SGSI

Pruebas de normalidad						
	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
ConfidencialidadPreTest	,239	35	,000	,899	35	,004
ConfidencialidadPostTest	,244	35	,000	,825	35	,000
a. Corrección de significación de Lilliefors						

Fuente: Elaboración propia con SPSS

Planteamiento de la hipótesis:

- **Hipótesis nula (H_0):** No hay diferencia significativa en la dimensión confidencialidad entre Pre y Post test.
- **Hipótesis alternativa (H_1):** Sí hay diferencia significativa en la dimensión confidencialidad entre Pre y Post.

Interpretación de la tabla de normalidad:

Dado que el tamaño de nuestra muestra es de 35 personas, se trabajará con la prueba de Shapiro-Wilk, el cual es recomendado para muestras menores a 50. El valor importante es la significancia (Sig.)

- **Dimensión Confidencialidad Pre:**
  Shapiro-Wilk: p = 0.004 (< 0.05) → No sigue una distribución normal.
- **Dimensión Confidencialidad Post:**
  Shapiro-Wilk: p = 0.000 (< 0.05) → No sigue una distribución normal.

En conclusión, los datos no cumplen normalidad en ninguno de los dos casos por lo que se procederá a utilizar la prueba de Wilcoxon para determinar la correlación entre la dimensión confidencialidad pre y post.

Prueba de Wilcoxon:

Tabla 30: Prueba de Wilcoxon para la dimensión confidencialidad pre y post implementación del SGSI

Estadísticos de prueba[a]	
	ConfidencialidadPostTest - ConfidencialidadPreTest
Z	-4,848[b]
Sig. asintótica(bilateral)	,000
a. Prueba de rangos con signo de Wilcoxon	
b. Se basa en rangos negativos.	

Fuente: Elaboración propia con SPSS

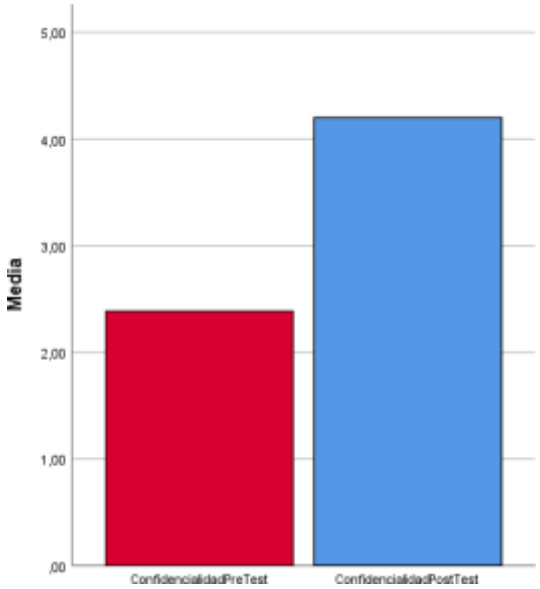
Interpretación del resultado:

- Estadístico Z = -4.865
  (El signo negativo es irrelevante, solo indica la dirección del cambio).
- Sig. asintótica (bilateral) = 0.000
  (SPSS lo redondea a tres decimales, lo correcto es p < 0.001).

Como p < 0.05, se rechaza la hipótesis nula (H_0).

La prueba de rangos con signo de Wilcoxon mostró diferencias significativas en la dimensión Confidencialidad entre el pretest y el postest (Z = -4.865, p < 0.001). Estos resultados indican que la propuesta de implementación del SGSI en el marco de la norma ISO/IEC 27001 produjo una mejora estadísticamente significativa en la confidencialidad de la información en la notaría García Medina.

Figura 18: Resultados obtenidos para la dimensión confidencialidad pre y post implementación del SGSI



Fuente: Elaboración propia con SPSS

Para la segunda dimensión de la variable dependiente: Integridad

Prueba de normalidad:

Tabla 31: Prueba de normalidad para la dimensión Integridad pre y post implementación del SGSI

Pruebas de normalidad						
	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
IntegridadPreTest	,251	35	,000	,883	35	,001
IntegridadPostTest	,259	35	,000	,849	35	,000
a. Corrección de significación de Lilliefors						

Fuente: Elaboración propia con SPSS

Planteamiento de la hipótesis:

- **Hipótesis nula (H_0):** No hay diferencia significativa en la dimensión integridad entre Pre y Post test.
- **Hipótesis alternativa (H_1):** Sí hay diferencia significativa en la dimensión integridad entre Pre y Post.

Interpretación de la tabla de normalidad:

Dado que el tamaño de nuestra muestra es de 35 personas, se trabajará con la prueba de Shapiro-Wilk, el cual es recomendado para muestras menores a 50. El valor importante es la significancia (Sig.)

- **Dimensión Integridad Pre:**
  Shapiro-Wilk: p = 0.001 (< 0.05) → No sigue una distribución normal.
- **Dimensión Integridad Post:**
  Shapiro-Wilk: p = 0.000 (< 0.05) → No sigue una distribución normal.

En conclusión, los datos no cumplen normalidad en ninguno de los dos casos por lo que se procederá a utilizar la prueba de Wilcoxon para determinar la correlación entre la dimensión confidencialidad pre y post.

Prueba de Wilcoxon:

Tabla 32: Prueba de Wilcoxon para la dimensión integridad pre y post implementación del SGSI

Estadísticos de prueba[a]	
	IntegridadPostTest - IntegridadPreTest
Z	-4,973[b]
Sig. asintótica(bilateral)	,000
a. Prueba de rangos con signo de Wilcoxon	
b. Se basa en rangos negativos.	

Fuente: Elaboración propia con SPSS

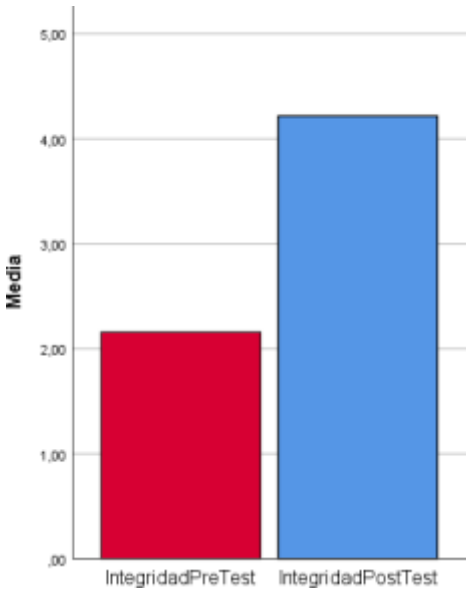
Interpretación del resultado:

- Estadístico Z = -4.973
  (El signo negativo es irrelevante, solo indica la dirección del cambio).
- Sig. asintótica (bilateral) = 0.000
  (SPSS lo redondea a tres decimales, lo correcto es p < 0.001).

Como p < 0.05, se rechaza la hipótesis nula (H_0).

La prueba de rangos con signo de Wilcoxon mostró diferencias significativas en la dimensión Integridad entre el pretest y el postest (Z = -4.973, p < 0.001). Estos resultados evidencian que la propuesta de implementación del SGSI en el marco de la norma ISO/IEC 27001 produjo una mejora significativa de la integridad de la información en los sistemas notariales.

Figura 19: Resultados obtenidos para la dimensión confidencialidad pre y post implementación del SGSI



Fuente: Elaboración propia con SPSS

Para la tercera dimensión de la variable dependiente: Disponibilidad

Prueba de normalidad:

Tabla 33: Prueba de normalidad para la dimensión Disponibilidad pre y post implementación del SGSI

Pruebas de normalidad						
	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
DisponibilidadPreTest	,234	35	,000	,891	35	,002
DisponibilidadPostTest	,303	35	,000	,798	35	,000
a. Corrección de significación de Lilliefors						

Fuente: Elaboración propia con SPSS

Planteamiento de la hipótesis:

- **Hipótesis nula (H_0):** No hay diferencia significativa en la dimensión disponibilidad entre Pre y Post test.
- **Hipótesis alternativa (H_1):** Sí hay diferencia significativa en la dimensión disponibilidad entre Pre y Post.

Interpretación de la tabla de normalidad:

Dado que el tamaño de nuestra muestra es de 35 personas, se trabajará con la prueba de Shapiro-Wilk, el cual es recomendado para muestras menores a 50. El valor importante es la significancia (Sig.)

- **Dimensión Disponibilidad Pre:**
  Shapiro-Wilk: p = 0.002 (< 0.05) → No sigue una distribución normal.
- **Dimensión Disponibilidad Post:**
  Shapiro-Wilk: p = 0.000 (< 0.05) → No sigue una distribución normal.

En conclusión, los datos no cumplen normalidad en ninguno de los dos casos por lo que se procederá a utilizar la prueba de Wilcoxon para determinar la correlación entre la dimensión confidencialidad pre y post.

Prueba de Wilcoxon:

Tabla 34: Prueba de Wilcoxon para la dimensión disponibilidad pre y post implementación del SGSI

Estadísticos de prueba[a]	
	DisponibilidadPostTest - DisponibilidadPreTest
Z	-4,952[b]
Sig. asintótica(bilateral)	,000
a. Prueba de rangos con signo de Wilcoxon	
b. Se basa en rangos negativos.	

Fuente: Elaboración propia con SPSS

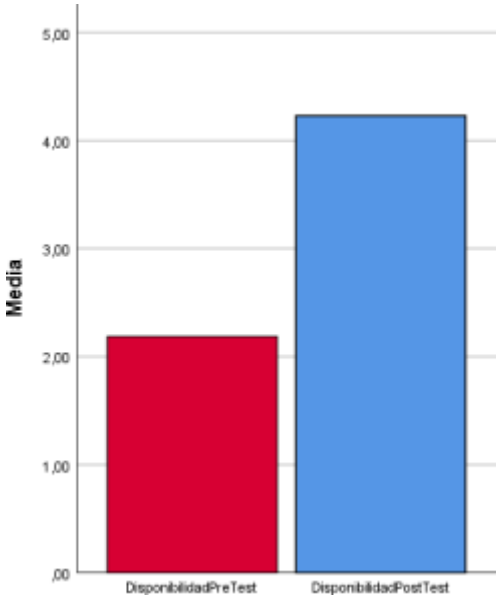
Interpretación del resultado:

- Estadístico Z = -4.952
  (El signo negativo es irrelevante, solo indica la dirección del cambio).
- Sig. asintótica (bilateral) = 0.000
  (SPSS lo redondea a tres decimales, lo correcto es p < 0.001).

Como p < 0.05, se rechaza la hipótesis nula (H_0).

La prueba de rangos con signo de Wilcoxon evidenció diferencias significativas en la dimensión Disponibilidad entre el pretest y el postest (Z = -4.952, p < 0.001). Estos resultados indican que la propuesta de implementación del SGSI en el marco de la norma ISO/IEC 27001 produjo una mejora de manera significativa la disponibilidad de la información en los sistemas notariales.

Figura 20: Resultados obtenidos para la dimensión disponibilidad pre y post implementación del SGSI



Fuente: Elaboración propia con SPSS

Para la variable dependiente: La seguridad de la información en la Notaría García Medina, mediremos los promedios generales de las dimensiones de ambos resultados (pre y post).

Prueba de normalidad:

Tabla 35: Prueba de normalidad para la VD pre y post implementación del SGSI

Pruebas de normalidad						
	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
PromGeneralPreTest	,222	35	,000	,894	35	,003
PromGeneralPostTest	,259	35	,000	,845	35	,000
a. Corrección de significación de Lilliefors						

Fuente: Elaboración propia con SPSS

Planteamiento de la hipótesis:

- **Hipótesis nula (H_0):** No hay diferencias significativas en la seguridad de la información antes y después de la implementación del SGSI.
- **Hipótesis alternativa (H_1):** Sí hay diferencias significativas en la seguridad de la información antes y después de la implementación del SGSI.

Interpretación de la tabla de normalidad:

Dado que el tamaño de nuestra muestra es de 35 personas, se trabajará con la prueba de Shapiro-Wilk, el cual es recomendado para muestras menores a 50. El valor importante es la significancia (Sig.)

- **Dimensión Identificación de riesgos Pre:**
  Shapiro-Wilk: p = 0.003 (< 0.05) → No sigue una distribución normal.
- **Dimensión Identificación de riesgos Post:**
  Shapiro-Wilk: p = 0.000 (< 0.05) → No sigue una distribución normal.

En conclusión, los datos no cumplen normalidad en ninguno de los dos casos por lo que se procederá a utilizar la prueba de Wilcoxon para determinar la correlación entre la dimensión confidencialidad pre y post.

Prueba de Wilcoxon:

Tabla 36: Prueba de Wilcoxon para la VD pre y post implementación del SGSI

Estadísticos de prueba[a]	
	PromGeneralPostTest - PromGeneralPreTest
Z	-4,967[b]
Sig. asintótica(bilateral)	,000
a. Prueba de rangos con signo de Wilcoxon	
b. Se basa en rangos negativos.	

Fuente: Elaboración propia con SPSS

Interpretación del resultado:

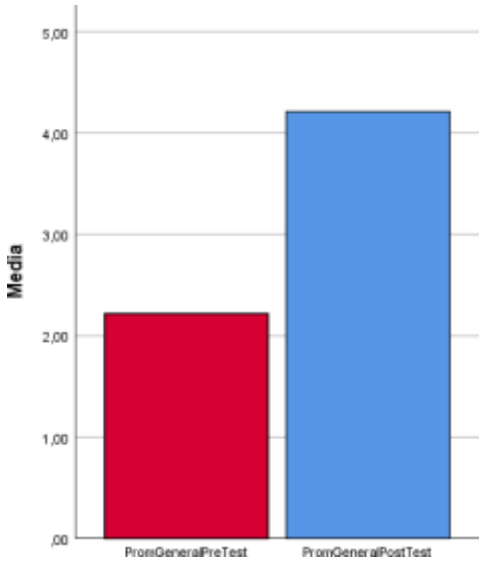
- Estadístico Z = -4.967
  (El signo negativo es irrelevante, solo indica la dirección del cambio).
- Sig. asintótica (bilateral) = 0.000
  (SPSS lo redondea a tres decimales, lo correcto es p < 0.001).

Como p < 0.05, se rechaza la hipótesis nula (H_0).

La prueba de rangos con signo de Wilcoxon evidenció diferencias significativas en el promedio general de la seguridad de la información entre el pretest y el postest (Z = -4.967, p < 0.001). Este resultado confirma la hipótesis general, demostrando que la implementación del SGSI en el marco de la norma ISO/IEC

27001 contribuyó de manera significativa a mejorar la seguridad de la información en la notaría García Medina.

Figura 21: Resultados obtenidos para la dimensión identificación de riesgos pre y post test



Fuente: Elaboración propia con SPSS

Para la variable independiente: Implementación de un SGSI basado en la norma ISO/IEC 27001

PRUEBA DE HIPOTESIS GENERAL

Formulación de hipótesis:

- **Hipótesis nula (H_0):** La propuesta de implementación de un SGSI en el marco de la norma ISO/IEC 27001 no contribuirá a mejorar la seguridad de la información en la notaría García Medina en el año 2025.
- **Hipótesis alternativa (H_1):** La propuesta de implementación de un SGSI en el marco de la norma ISO/IEC 27001 contribuirá a mejorar la seguridad de la información en la notaría García Medina en el año 2025.

Tabla 37: Prueba de normalidad para la VD de independiente

Pruebas de normalidad						
	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
Variable Dependiente	,259	35	,000	,845	35	,000
Variable Independiente	,243	35	,000	,847	35	,000
a. Corrección de significación de Lilliefors						

Fuente: Elaboración propia

Interpretación de la tabla de normalidad:

Dado que el tamaño de nuestra muestra es de 35 personas, se trabajará con la prueba de Shapiro-Wilk, el cual es recomendado para muestras menores a 50. El valor importante es la significancia (Sig.)

- **Variable Dependiente: Seguridad de la información**
  Shapiro-Wilk: p = 0.000 (< 0.05) → No sigue una distribución normal.
- **Variable Independiente: Sistema de gestión de la información**
  Shapiro-Wilk: p = 0.000 (< 0.05) → No sigue una distribución normal.

En conclusión, los datos no cumplen normalidad en ninguno de los dos casos por lo que se procederá a utilizar la prueba de Spearman para determinar la correlación entre la variable dependiente e independiente.

Prueba estadística:

- ρ (rho de Spearman) = fuerza y dirección de la relación, Si:
  - 0.00–0.19 = muy débil
  - 0.20–0.39 = débil
  - 0.40–0.59 = moderada
  - 0.60–0.79 = fuerte
  - 0.80–1.0 = muy fuerte
- Sig. (p valor) = significancia estadística.
- Si p < 0.05, la relación es significativa.

Tabla 38: Resultado de test de Spearman para validar la hipótesis general

Correlaciones				
			Variable Dependiente	Variable Independiente
Rho de Spearman	Variable Dependiente	Coeficiente de correlación	1,000	,947**
		Sig. (bilateral)	.	,000
		N	35	35
	Variable Independiente	Coeficiente de correlación	,947**	1,000
		Sig. (bilateral)	,000	.
		N	35	35
**. La correlación es significativa en el nivel 0,01 (bilateral).				

Fuente: Elaboración propia con SPSS

Resultados:

- ρ (rho de Spearman) = 0.947
- p valor = 0.000 (p < 0.001)
- N = 35

El análisis de Spearman evidenció una correlación positiva muy fuerte entre la implementación del SGSI (VI) y el nivel global de seguridad de la información (VD) (ρ = 0.947, p < 0.001). Este resultado confirma la hipótesis general de la investigación, demostrando que la implementación de un SGSI basado en la norma ISO/IEC 27001 tiene un impacto directo y significativo en la mejora de la seguridad de la información en la notaría García Medina.

PRUEBA DE HIPÓTESIS ESPECÍFICA

Hipótesis especifica N° 1:

Formulación de hipótesis:

- **Hipótesis nula (H_0):** La propuesta de implementación de un SGSI en el marco de la norma ISO/IEC 27001 no contribuirá a mejorar la confidencialidad de la información en la notaría García Medina en el año 2025.
- **Hipótesis alternativa (H_1):** La propuesta de implementación de un SGSI en el marco de la norma ISO/IEC 27001 contribuirá a mejorar la confidencialidad de la información en la notaría García Medina en el año 2025.

Prueba estadística:

- ρ (rho de Spearman) = fuerza y dirección de la relación, Si:
  - 0.00–0.19 = muy débil
  - 0.20–0.39 = débil
  - 0.40–0.59 = moderada
  - 0.60–0.79 = fuerte
  - 0.80–1.0 = muy fuerte
- Sig. (p valor) = significancia estadística.
- Si p < 0.05, la relación es significativa.

Tabla 39: Resultado del test de Spearman para validación de la hipótesis especifica N°1

Correlaciones				
			ConfidencialidadPostTest	PromGeneralVarIndep
Rho de Spearman	Confidencialidad PostTest	Coeficiente de correlación	1,000	,939**
		Sig. (bilateral)	.	,000
		N	35	35
	PromGeneralVI	Coeficiente de correlación	,939**	1,000
		Sig. (bilateral)	,000	.
		N	35	35
**. La correlación es significativa en el nivel 0,01 (bilateral).				

Fuente: Elaboración propia con SPSS

Resultados:

- ρ (rho) = 0.939
- p = 0.000 (bilateral, p < 0.001)
- N = 35

El análisis de correlación de Spearman mostró una relación positiva muy fuerte entre la implementación del SGSI y la confidencialidad de la información (ρ = 0.939, p < 0.001). Este hallazgo confirma que un mayor grado de implementación de políticas, controles y buenas prácticas de seguridad se asocia con un incremento significativo en la confidencialidad de la información dentro de la notaría García Medina.

Hipótesis especifica N° 2:

Formulación de hipótesis:

- **Hipótesis nula (H_0):** La implementación de un SGSI en el marco de la norma ISO/IEC 27001 contribuirá a fortalecer la integridad de la información en los sistemas notariales en el año 2025.
- **Hipótesis alternativa (H_1):** La implementación de un SGSI en el marco de la norma ISO/IEC 27001 contribuirá a fortalecer la integridad de la información en los sistemas notariales en el año 2025.

Prueba estadística:

- ρ (rho de Spearman) = fuerza y dirección de la relación, Si:
  - 0.00–0.19 = muy débil
  - 0.20–0.39 = débil
  - 0.40–0.59 = moderada
  - 0.60–0.79 = fuerte
  - 0.80–1.0 = muy fuerte
- Sig. (p valor) = significancia estadística.
- Si p < 0.05, la relación es significativa.

Tabla 40: Resultado del test de Spearman para validación de la hipótesis especifica N°2

Correlaciones				
			IntegridadPostTest	PromGeneralVI
Rho de Spearman	IntegridadPostTest	Coeficiente de correlación	1,000	,954**
		Sig. (bilateral)	.	,000
		N	35	35
	PromGeneralVI	Coeficiente de correlación	,954**	1,000
		Sig. (bilateral)	,000	.
		N	35	35
**. La correlación es significativa en el nivel 0,01 (bilateral).				

Fuente: Elaboración propia con SPSS

Resultados:

- ρ (rho) = 0.954
- p = 0.000 (bilateral, p < 0.001)
- N = 35

El análisis de correlación de Spearman mostró una relación positiva muy fuerte entre la implementación del SGSI y la integridad de la información (ρ = 0.954, p < 0.001). Este resultado confirma que un mayor grado de implementación de políticas, mejora continua y capacitación se asocia con un fortalecimiento significativo de la integridad de los documentos notariales.

Hipótesis especifica N° 3:

Formulación de hipótesis:

- **Hipótesis nula (H_0):** La implementación de un SGSI en el marco de la norma ISO/IEC 27001 contribuirá a mejorar la disponibilidad de la información en los sistemas notariales en el año 2025.
- **Hipótesis alternativa (H_1):** La implementación de un SGSI en el marco de la norma ISO/IEC 27001 contribuirá a mejorar la disponibilidad de la información en los sistemas notariales en el año 2025.

Prueba estadística:

- ρ (rho de Spearman) = fuerza y dirección de la relación, Si:
  - 0.00–0.19 = muy débil
  - 0.20–0.39 = débil
  - 0.40–0.59 = moderada
  - 0.60–0.79 = fuerte
  - 0.80–1.0 = muy fuerte
- Sig. (p valor) = significancia estadística.
- Si p < 0.05, la relación es significativa.

Tabla 41: Resultado del test de Spearman para validación de la hipótesis especifica N°3

Correlaciones				
			DisponibilidadPostTest	PromGeneralVI
Rho de Spearman	DisponibilidadPostTest	Coeficiente de correlación	1,000	,896**
		Sig. (bilateral)	.	,000
		N	35	35
	PromGeneralVI	Coeficiente de correlación	,896**	1,000
		Sig. (bilateral)	,000	.
		N	35	35
**. La correlación es significativa en el nivel 0,01 (bilateral).				

Fuente: Elaboración propia con SPSS

Resultados:

- ρ (rho) = 0.896
- p = 0.000 (bilateral, p < 0.001)
- N = 35

El análisis de correlación de Spearman evidenció una relación positiva muy fuerte entre la implementación del SGSI y la disponibilidad de la información ($\rho = 0.896$, $p < 0.001$). Esto confirma que un mayor nivel de implementación del sistema contribuye a garantizar la accesibilidad y el funcionamiento continuo de la información en los sistemas notariales.

Justificación del uso de las pruebas estadísticas Wilcoxon y Spearman

En la presente investigación se emplearon las pruebas estadísticas Wilcoxon de rangos con signo y Rho de Spearman, debido a que ambas responden a objetivos analíticos distintos, aunque se apliquen sobre variables relacionadas. La prueba de Wilcoxon se utilizó con la finalidad de comparar las mediciones del pretest y postest de la variable dependiente, permitiendo determinar si existen diferencias estadísticamente significativas en el nivel de seguridad de la información antes y después de la aplicación del Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001. Esta prueba resulta adecuada considerando el tamaño de la muestra, la naturaleza ordinal de los datos y la ausencia de supuestos de normalidad.

Por otro lado, el coeficiente de correlación Rho de Spearman se empleó para analizar el grado de relación existente entre la variable independiente y la variable dependiente en la medición postest, con el propósito de establecer la dirección e intensidad de la asociación entre la aplicación del SGSI y el nivel de seguridad de la información. Dado que los datos provienen de escalas tipo Likert y no cumplen con los supuestos de distribución normal, la prueba de Spearman resulta pertinente para evaluar relaciones monotónicas entre variables.

En este sentido, aunque ambas pruebas se aplican sobre variables relacionadas, Wilcoxon y Spearman no cumplen la misma función estadística: la primera evalúa diferencias entre dos mediciones dependientes, mientras que la segunda analiza la relación o asociación entre variables, lo cual justifica el uso complementario de ambas pruebas en la validación de las hipótesis del estudio.

CONCLUSIONES

1. Se determinó que la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO/IEC 27001 influye de manera positiva, significativa y directa en la seguridad de la información en la Notaría García Medina. Este resultado se sustenta en el coeficiente de correlación de Spearman obtenido ($\rho = 0.947$; $p = 0.000$), el cual evidencia una relación positiva muy fuerte entre las variables. En consecuencia, se acepta la hipótesis general de investigación.

2. Se determinó que la implementación del SGSI influye significativamente en la dimensión de confidencialidad de la información, evidenciándose una correlación positiva muy fuerte ($\rho = 0.939$; $p < 0.001$). Estos resultados permiten afirmar que la implementación del sistema fortalece la protección contra accesos no autorizados, por lo que se acepta la hipótesis específica correspondiente.

3. Se determinó que la implementación del SGSI influye significativamente en la dimensión de integridad de la información, presentando una correlación positiva muy fuerte ($\rho = 0.954$; $p < 0.001$). En ese sentido, se evidencia una mejora en la confiabilidad y exactitud de la información, por lo que se acepta la hipótesis específica planteada.

4. Se determinó que la implementación del SGSI influye significativamente en la dimensión de disponibilidad de la información, evidenciando una correlación positiva muy fuerte ($\rho = 0.896$; $p < 0.001$). Esto demuestra que la implementación del sistema mejora el acceso oportuno a la información, por lo que se acepta la hipótesis específica correspondiente.

SUGERENCIAS

1. Reforzar la infraestructura tecnológica de la notaría. Aunque el SGSI ha establecido controles efectivos, la disponibilidad sigue dependiendo de la solidez de los servidores, equipos de red y sistemas de almacenamiento. De igual manera, el monitoreo constante de hardware y software garantizará la detección temprana de fallas.

2. Otra acción clave es fortalecer la conectividad y telecomunicaciones. Dado que los servicios notariales digitales dependen de Internet, resulta conveniente contar con más de un proveedor de conectividad, de manera que, si uno falla, el otro pueda asegurar la continuidad.

3. En cuanto al suministro eléctrico, se sugiere la instalación de UPS y generadores de respaldo, que aseguren la continuidad de los servicios en caso de cortes de energía. Esto debe complementarse con un programa de mantenimiento y pruebas periódicas de dichos sistemas, evitando que fallen en situaciones críticas.

4. Asimismo, se recomienda consolidar un plan de continuidad de negocio y un plan de recuperación ante desastres alineados con el SGSI. Estos planes deben contemplar escenarios como fallas de infraestructura, ataques cibernéticos o desastres naturales, estableciendo protocolos claros de recuperación. Para ello, es indispensable que el personal técnico reciba capacitación específica en gestión de incidentes y procedimientos de restauración rápida de los servicios.

5. Finalmente, es fundamental complementar la tecnología con la concientización del personal. Aunque la disponibilidad puede verse afectada por factores técnicos, los errores humanos también influyen. Por ello, se sugiere realizar simulacros, capacitaciones periódicas y ejercicios prácticos que fortalezcan la cultura de continuidad operativa dentro de la organización.

REFERENCIAS BIBLIOGRAFICAS

[1] International Organization for Standardization, “ISO: Global standards for trusted goods and services”. Cit: 23. júl 2025. [Online]. Available at: https://www.iso.org/home.html

[2] Congreso de la República, “LEY DE PROTECCION DE DATOS PERSONALES - LEY N° 29733”, Lima, 2013.

[3] OEA, “NCS: Lessons Learned and Reflections from the Americas and Other Regions”, jún. 2022. Cit: 16. júl 2025. [Online]. Available at: https://www.oas.org/ext/es/seguridad/prog-ciber

[4] J. J. Lugo Marín, H. E. Carrasquero, a J. O. G. Rivero, “EVALUATION OF INFORMATION SECURITY MANAGEMENT IN MANAGEMENT INFORMATION SYSTEMS AS A TOOL OF COMPETITIVENESS IN COMPANIES OF NON-DESTRUCTIVE TESTING SERVICES IN THE CITY OF LIMA-PERU”, QUALITAS, 2020.

[5] L. S. Rodriguez Baca, C. F. Cruzado Puente de la Vega, C. Mejía Corredor, a M. A. Alarcón Diaz, “Aplicación de ISO 27001 y su influencia en la seguridad de la información de una empresa privada peruana”, roč. 8, s. 786, okt. 2020, doi: 10.20511/pyr2020.v8n3.786.

[6] FORTINET, “La nueva plataforma Fortinet Threat Intelligence Insider Latin America ofrece información local sobre ciberseguridad para varios países de la región”, 2019. Cit: 16. júl 2025. [Online]. Available at: https://www.fortinet.com/lat/corporate/about-us/newsroom/press-releases/2019/new-fortinet-threat-intelligence-insider-latin-america-platform-offers-local-cybersecurity

[7] M. Javier a D. Contreras, “PROPUESTA PARA IMPLEMENTACION DE CONTROLES ESTABLECIDOS POR LA NORMA ISO/IEC 27001:2013 - ANEXO A, APLICABLES EN EL CENTRO DE DIAGNOSTICO AUTOMOTOR - CEDAC LTDA., UBICADO EN LA ZONA INDUSTRIAL DE LA CIUDAD DE CÚCUTA”, Cucuta, 2018.

[8] J. A. Panaqué Dominguez, Y. G. Lizárraga Caipo, a A. Mendoza de los Santos, “Efectos de la implementación de un SGSI basado en la norma ISO 27001 para las organizaciones”, aug. 2022.

[9] ISO27001.ES, “Information security, cybersecurity and privacy protection — Information security management systems — Requirements. ISO.”, 2022.

[10] E. Vega Briceño, “SEGURIDAD DE LA INFORMACIÓN”, Alicante, mar. 2021. doi: https://doi.org/10.17993/tics.2021.4.

[11] M. Toynsé de la Rosa, “AUTOMATIZACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIOÓN BASADO EN LA NORMA ISO/IEC 27001”, Universidad Metropolitana. Ecuador, sep. 2021.

[12] S. Bustamante García, M. Á. Valles Coral, I. E. Cuellar Rodríguez, a D. Lévano Rodríguez, “Políticas basadas en la ISO 27001:2013 y su influencia en la gestión de seguridad de la información en municipalidades de Perú”, Enfoque UTE, roč. 12, č. 2, s. 69–79, apr. 2021, doi: 10.29019/enfoqueute.743.

[13] F. A. Moyano Hernández a D. C. Villamil Sandoval, “Análisis del ciclo PHVA en la gestión de proyectos, una revisión documental”, Revista Politécnica, roč. 17, č. 34, s. 55–69, nov. 2021, doi: 10.33571/rpolitec.v17n34a4.

[14] ISO 27001, “International Organization for Standardization [ISO]”.

[15] A. E. Chica Campuzano, “ANÁLISIS DOCTRINAL Y NORMATIVO DE LA POSIBILIDAD DE INTEGRACIÓN DE LA TECNOLOGÍA BLOCKCHAIN AL SERVICIO NOTARIAL EN LA REPÚBLICA DEL ECUADOR”, Ambato, 2024.

[16] M. E. Alava Cuadra a H. A. Choez Salazar, “DISEÑO DE UN SGSI BASADO EN EL ESTANDAR ISO 27001 PARA LA EMPRESA INVIMEDIC S.A.””, CUENCA, 2023.

[17] O. de J. Pulgarín García, “DISEÑO DEL SISTEMA DE GESTION DE LA SEGURIDAD DE LA INFORMACION BAJO LOS LINEAMIENTOS DEL ESTANDAR ISOIEC 27001 PARA LA NOTARIA UNICA DE LA CIUDAD DE DOSQUEBRADAS”, 2023.

[18] J. C. Cortes Malagon a J. A. Pulido Espinosa, “DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) PARA LOS PROCESOS CRITICOS DE SUMMUM PROJECT BASADO EN LA NORMA NTC-ISO-IEC-270012022”, Universidad Piloto de Colombia, Bogota, 2023.

[19] J. F. Gomez Sanchez, Y. Ochoa Puerta, a L. Patiño Correa, “IMPLEMENTACION SGSI EN LA UNIDAD DE RENTAS BASADO ENLA ISO 27001”, Universidad Catolica de Manizales, Maizales Caldas, 2024.

[20] E. Busto Perez de Mendiguren, “Plan de Implementación del SGSI basado en la ISO/IEC 27001:2022 de la empresa TRADUX”, jún. 2024.

[21] L. E. Esquicha Flores, “ISO 27001: Seguridad de la información y su impacto en el principio de negocio en marcha para empresas que prestan servicios tecnológicos en San Isidro”, júl. 2022.

[22] R. A. García Cruz, “PROPUESTA DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO 27001 PARA LA OFICINA DE TECNOLOGÍAS DE INFORMACIÓN DEL GOBIERNO REGIONAL DE PIURA”, Piura - Perú, 2020.

[23] J. E. Lopez Aguirre, “IMPLEMENTACIÓN DEL SGSI, BASADO EN LA ISO/IEC 27001 PARA DAR TRATAMIENTO AL RIESGO EN UNA EMPRESA CONSTRUCTORA”, Lima, 2022.

[24] M. H. Herrera Velásquez, “Sistema de gestión para la seguridad de la información y la confidencialidad de la información, Hospital II-1 Moyobamba, 2024”, Universidad Nacional de San Martin, Tarapoto, 2024. [Online]. Available at: https://orcid.org/0000-0002-8392-3542

[25] Poder Ejecutivo, “Ley del Notariado”, 2008.

[26] J. M. De Vettori González, “Importancia de la función notarial en la protección de los derechos fundamentales en el contexto del COVID-19”, Ius et Praxis, č. 052, s. 187–196, 2021, doi: 10.26439/iusetpraxis2021.n052.5068.

[27] W. Gutierrez Cabas, “EL NOTARIO DE FE PÚBLICA COMO GARANTE DE LA SEGURIDAD JURÍDICA PREVENTIVA EN LOS DOCUMENTOS NOTARIALES”, jún. 2022.

[28] Ministerio de Justicia, “Decreto Legislativo No 1049”, 2017.

[29] L. Enrique Quintero Parra, “DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) PARA EL DEPARTAMENTO DE INFORMATICA DE LA SUPERINTENDENCIA DE NOTARIADO Y REGISTRO”, Bogotá - Colombia, 2015.

[30] Notaría García Medina, “Notaría Garcia Medina”. Cit: 26. máj 2025. [Online]. Available at: https://notariagarciamedina.com/servicios/

[31] CNL-ATEC, “SISNOT”, 2023, Cit: 12. máj 2025. [Online]. Available at: https://www.notarios.org.pe/#/home

[32] G. De la Cruz Rodriguez, R. A. Mendez Fernandez, a C. Mendez Fernandez, “Seguridad de la información en el comercio electrónico basado en ISO 27001 : Una revisión sistemática”, mar. 2023. [Online]. Available at: https://revistas.ulasalle.edu.pe/innosoft

[33] Organismo de Certificación Global, “ISO 27001:2022 GUÍA DE IMPLEMENTACIÓN DE SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN”, 2022, Cit: 12. máj 2025. [Online]. Available at: www.nqa.com

[34] M. A. Cruz Diaz a S. Fukusaki Infantas, “DISEÑO E IMPLEMENTACION DE UN SISTEMA DEGESTION DE SEGURIDAD DE LA INFORMACION PARA PROTEGER LOS ACTIVOS DE INFORMACION DE LA CLINICA MEDCAM PERU SAC”, Lima, 2017.

[35] M. A. Velepucha Sánchez, J. Morales Carrillo, a M. F. Pazmiño Campuzano, “Análisis y evaluación de riesgos aplicados a la seguridad de la información bajo la norma ISO”, Informática y Sistemas: Revista de Tecnologías de la Informática y las Comunicaciones, roč. 6, č. 1, s. 63–78, jún. 2022, doi: 10.33936/isrtic.v6i1.4473.

[36] ISO 27001, “FASE 2 Análisis del contexto de la Organización y determinación del Alcance”.

[37] A. A. Ávila Coello, “Modelo de SGSI en el Departamento de TI del GADMCN, Aplicando Controles ISO/IEC 27001:2013 e ISO/IEC 27002:2022”, Ciencia Latina Revista Científica Multidisciplinar, roč. 8, č. 5, s. 12000–11210, nov. 2024, doi: 10.37811/cl_rcm.v8i5.14503.

[38] S. A. Cama Jara a G. M. Arellano Bujele, “Implementación de un sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27001 para la mejora de protección de datos personales en la Clínica María del Socorro”, Universidad Tecnológica del Perú, Lima, 2024.

[39] J. J. Cano M., “Ciberataques”, Revista SISTEMAS, č. 157, s. 67–74, okt. 2020, doi: 10.29236/sistemas.n157a6.

[40] F. N. J. Solarte Solarte, E. R. Enriquez Rosero, a M. del C. Benavides Ruano, “Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001”, Revista Tecnológica ESPOL, roč. 28, dec. 2015.

[41] V. Villarreal Morales, K. E. Coro Villarreal, E. G. Fernández Sánchez, a J. P. Cueva Martinez, “Sistema Gestión de Seguridad de la Información y su impacto en el Gobierno y Gestión de las Tecnologías de la Información”, Ciencia Latina Revista Científica Multidisciplinar, roč. 8, č. 5, s. 12956–12979, dec. 2024, doi: 10.37811/cl_rcm.v8i6.14758.

[42] I. Yailín et al., “METODOLOGÍA PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN BASADA EN LOS ASPECTOS MÁS RELEVANTES DE LA NORMA CUBANA NC ISO IEC 27001:2016”, 2020, [Online]. Available at: https://www.eumed.net/rev/rilcoDS/12/gestion-seguridad-informacion.html

[43] ESAN, “La norma ISO 27001 y la mejora continua en la gestión de seguridad de la información”. Cit: 28. júl 2025. [Online]. Available at: https://www.esan.edu.pe/conexion-esan/norma-iso-27001-mejora-continua-en-la-gestion-de-seguridad-informacion

[44] M. A. Porras Ruiz, “SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA GESTIÓN DE RIESGOS EN ACTIVOS DE INFORMACIÓN”, 2019.

[45] W. A. Apaza Chávez, “Propuesta de un plan de seguridad de la información para incrementar la fiabilidad de datos en una financiera”, Trujillo, sep. 2021. [Online]. Available at: https://revistas.ulasalle.edu.pe/innosoft

[46] B. A. Pérez Pira, “IMPORTANCIA DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EMPRESAS DE TECNOLOGÍA”, Universidad Piloto de Colombia., 2020.

[47] J. J. Castro Maldonado, L. K. Gómez Macho, a E. Camargo Casallas, “La investigación aplicada y el desarrollo experimental en el fortalecimiento

de las competencias de la sociedad del siglo XXI", Tecnura, roč. 27, č. 75, s. 140–174, jan. 2023, doi: 10.14483/22487638.19171.

[48] R. H. , C. C. F. , & L. P. B. Sampieri, Metodología de la investigación (6a ed.). McGraw-Hill Education., 2018.

[49] C. De Pelekais, "Métodos cuantitativos y cualitativos: diferencias y tendencias Qualitative and Quantitative Methods: Diferences and Tendencies", 2000.

[50] E. R. Chagoya, "Métodos y técnicas de investigación", Universidad Complutense de Madrid, 2008.

[51] Y. Campos Flores, "TÉCNICAS DE INVESTIGACIÓN", roč. 4, Lima, s. 3–4, 2021.

[52] M. Medina, R. Rojas, W. Bustamante, R. Loaiza, C. Martel, a R. Castillo, Metodología de la investigación: Técnicas e instrumentos de investigación. Instituto Universitario de Innovación Ciencia y Tecnología Inudi Perú, 2023. doi: 10.35622/inudi.b.080.

[53] I. Lopes a P. Oliveira, "Understanding information security culture: A survey in small and medium sized enterprises", v Advances in Intelligent Systems and Computing, Springer Verlag, 2014, s. 277–286. doi: 10.1007/978-3-319-05951-8_27.

[54] D. A. Aguirre Mollehuanca, "Diseño de un Sistema de Gestion de Seguridad de informacion para servicios postales del Perú S.A.", Lima, okt. 2014.

[55] C. D. Torres Chango, "PLAN DE SEGURIDAD INFORMATICA BASADO EN LA NORMA ISO 27001 PARA PROTEGER LA INFORMACION Y ACTIVOS DE LA EMPRESA PRIVADA MAGAPROFER S.A.", jan. 2020.

ANEXOS

Anexo 1: Carta de compromiso de asesor

UNIVERSIDAD NACIONAL AMAZÓNICA DE MADRE DE DIOS
FACULTAD DE INGENIERÍA
"Año de la Recuperación y Consolidación de la Economía Peruana"
"Madre de Dios, capital de la biodiversidad del Perú"

Puerto Maldonado, 26 de mayo del 2025

Carta: Compromiso del Asesor

Señores:
E.P. de Ingeniería de Sistemas e Informática
Facultad de Ingeniería

Por la presente yo, **Néstor Antonio Gallegos Ramos,** identificado con **DNI 0135884,** en mi calidad de docente de la Escuela Profesional de Ingeniería de Sistema e Informática, manifiesto mi compromiso de asesorar el proyecto de tesis titulado:

"Evaluación de riesgos de seguridad en la información de sistemas notariales electrónicos bajo el marco de ISO/IEC 27001, año 2025."

Elaborado por el Bachiller **Pablo Francisco Carrillo Venancino**, identificado con DNI 73113570, en cumplimiento de los lineamientos académicos establecidos por la **Universidad Nacional Amazónica de Madre de Dios (UNAMAD)**, como requisito para la obtención del **Título Profesional de Ingeniero de Sistemas e Informática.**

Me comprometo a brindar la orientación necesaria durante el proceso de elaboración del proyecto, velando por el cumplimiento de los objetivos planteados, el uso adecuado de la metodología de investigación y el respeto a los criterios éticos de la institución.
Asimismo, apoyaré en la revisión y corrección de los avances presentados, de manera que se garantice la calidad y viabilidad del trabajo.

Sin otro particular, quedo a disposición de la institución para cualquier consulta o comunicación relacionada con mi rol como asesor.

Atentamente,

Mg. Néstor Antonio Gallegos Ramos
Docente EP Ingeniería de Sistemas e Informática
Facultad de Ingeniería
UNAMAD

Anexo 2: Matriz de Operacionalización de Variables

DEFINICION CONCEPTUAL	DEFINICION OPERACIONAL	DIMENSIONES	INDICADORES	ESCALA
Variable Independiente: Implementación de un SGSI basado en la norma ISO/IEC 27001 Consiste en la adopción de un conjunto de requisitos, controles y buenas prácticas internacionales para establecer, implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). Su objetivo es proteger la confidencialidad, integridad y disponibilidad de la información, a través de la gestión efectiva de los riesgos de seguridad [9].	Variable Independiente: propuesta de implementación de un SGSI basado en la norma ISO/IEC 27001 La adopción de un SGSI basado en normas como ISO/IEC 27001 implica la implementación documentada de controles técnicos, organizativos (políticas de acceso, capacitación anual obligatoria) y legales, medibles mediante auditorías semestrales, pruebas de recuperación y reducción de incidentes garantizando la protección activa de los documentos notariales digitales [42].	Política de seguridad de la información	Existencia de políticas documentadas y actualizadas	Likert (1-5)
		Gestión de riesgos	Procesos de identificación, análisis y tratamiento de riesgos	
		Mejora continua	Registro de auditorías internas/ acciones correctivas	
		Capacitación y concientización	Programas de formación en seguridad de la información	

Variable Dependiente: Mejora de la seguridad en la Notaría García Medina Conjunto de medidas técnicas, organizativas y normativas implementadas para proteger los procesos y documentos notariales digitales contra amenazas que puedan comprometer su confidencialidad, integridad y disponibilidad. Esto incluye la protección frente a accesos no autorizados, alteraciones indebidas, pérdidas de información y fallos en la continuidad operativa del servicio notarial digital [10].	Variable Dependiente: Mejora de la seguridad en la Notaría García Medina Implementación de protocolos de cifrado, sistemas de backup automatizados, registros de auditoría, firewalls, y normativas de cumplimiento legal para garantizar que los documentos y procesos notariales digitales solo sean accesibles por partes autorizadas, protegidos contra modificaciones no validadas y disponibles sin interrupciones [55].	Confidencialidad	Existencia de mecanismos para prevenir accesos no autorizados	Likert (1-5)
		Integridad	Existencia de mecanismos de validación/ registros de modificaciones	
		Disponibilidad	Accesibilidad y funcionamiento continuo del sistema	

Anexo 3: Matriz de Consistencia

Título: **Propuesta de implementación de un SGSI para la mejora de la seguridad de la información en la notaría garcía medina basado en la norma ISO/IEC 27001, en la ciudad de Puerto Maldonado 2025**
Tesista: Carrillo Venancino, Pablo Francisco

PROBLEMAS	OBJETIVOS	HIPOTESIS	VARIABLES/ INDICADORES	METODOLOGIA
General • ¿En qué medida la propuesta de implementación de un SGSI en el marco ISO/IEC 27001 contribuye con la mejora de la seguridad de la información en la notaría García Medina en el año 2025? **Específicos** • ¿En qué medida la propuesta de implementación de un SGSI en el marco ISO/IEC 27001 contribuye a mejorar la confidencialidad de la información en la notaría García Medina? • ¿En qué medida la propuesta de implementación de un SGSI en el marco ISO/IEC 27001 contribuye a fortalecer la integridad de la información en la notaría García Medina? • ¿En qué medida la propuesta de implementación de un SGSI en el marco ISO/IEC 27001 contribuye a mejorar la disponibilidad de la información en la notaría García Medina?	**General** • Evaluar en qué medida la propuesta de implementación de un SGSI en el marco de la norma ISO/IEC 27001 contribuye a mejorar la seguridad de la información en la notaría García Medina en el año 2025. **Específicos** • Evaluar en qué medida la propuesta de implementación de un SGSI en el marco de la norma ISO/IEC 27001 contribuye a mejorar la confidencialidad de la información en la notaría García Medina. • Evaluar en qué medida la propuesta de implementación de un SGSI en el marco de la norma ISO/IEC 27001 contribuye a fortalecer la integridad de la información en la notaría García Medina. • Evaluar en qué medida la propuesta de implementación de un SGSI en el marco de la norma ISO/IEC 27001 contribuye a mejorar la disponibilidad de la información en la notaría García Medina.	**General** • La propuesta de implementación de un SGSI en el marco de la norma ISO/IEC 27001 contribuirá a mejorar la seguridad de la información en la notaría García Medina en el año 2025 **Específicos** • La propuesta de implementación de un SGSI en el marco de la norma ISO/IEC 27001 contribuirá a mejorar la confidencialidad de la información en la notaría García Medina en el año 2025. • La propuesta de implementación de un SGSI en el marco de la norma ISO/IEC 27001 contribuirá a fortalecer la integridad de la información en los sistemas notariales en el año 2025. • La propuesta de implementación de un SGSI en el marco de la norma ISO/IEC 27001 contribuirá a mejorar la disponibilidad de la información en los sistemas notariales en el año 2025. **Justificación** La propuesta de implementación de la norma ISO/IEC 27001 proporciona una estructura sistemática para identificar, evaluar y tratar los riesgos de seguridad, garantizando la confidencialidad, integridad y disponibilidad de los datos, pilares esenciales para cualquier sistema notarial. Al aplicar esta norma no solo se fortalece la protección de la información crítica, sino que también se mejora la confianza de los ciudadanos en los servicios notariales digitales. **Importancia** Esta investigación es vital para asegurar la autenticidad y protección legal de los documentos notariales digitales frente a ciber amenazas. Establece estándares de seguridad alineados con normativas internacionales, garantizando validez jurídica.	**Variable Independiente:** Implementación de un SGSI basado en la norma ISO/IEC 27001 **Dimensiones:** • Política de seguridad de la información • Gestión de riesgos • Mejora continua • Capacitación y concientización **Indicadores:** • Existencia de políticas documentadas y actualizadas • Procesos de identificación, análisis y tratamiento de riesgos • Registro de auditorías internas/ acciones correctivas • Programas de formación en seguridad de la información **Variable Dependiente:** Mejora de la seguridad en la Notaría García Medina **Dimensiones:** • Confidencialidad • Integridad • Disponibilidad **Indicadores:** • Existencia de mecanismos para prevenir accesos no autorizados • Existencia de mecanismos de validación/ registros de modificaciones • Accesibilidad y funcionamiento continuo del sistema • Registro actualizado de amenazas y vulnerabilidades	**Enfoque:** Cuantitativo **Diseño:** Pre Experimental **Nivel:** Correlacional **Tipo:** Aplicada **Métodos:** Cuantitativo **Técnicas Instrumentales de muestreo:** Entrevistas, **De recolección de datos:** Cuestionarios **De procesamiento de datos:** Pruebas no paramétricas **De análisis:** Análisis estadístico inferencial **Población:** 40 **Muestra:** 35

Anexo 4: Instrumento

INSTRUMENTO DE INVESTIGACIÓN

ENCUESTA: CONTEXTO DE LA ORGANIZACIÓN:

Objetivo: Saber su nivel de comprensión de la importancia del manejo de datos en la organización.

Dirigido a: Personal de la notaría

Indicaciones: Marcar con “X” la opción que considere correcta, tener en cuenta que la encuesta se basa en una evaluación de acuerdo a la siguiente escala:

1 => Deficiente
2 => Insuficiente
3 => Neutral
4 =>Adecuado
5 => Óptimo

PREGUNTA	1	2	3	4	5
1. Mi nivel de conocimiento sobre seguridad de la información es:					
2. Considero que el nivel de importancia que se le da a la seguridad de la información en mi organización es:					
3. La frecuencia con la que recibo capacitaciones sobre seguridad de la información es:					
4. Mi nivel de conocimiento sobre los riesgos a los que está expuesta la información que manejo es:					
5. La claridad y comunicación sobre quién es el responsable de la seguridad de la información en mi organización es:					

VARIABLE INDEPENDIENTE: Aplicación del marco ISO/IEC 27001

Dimensión: Política de seguridad de la información:

PREGUNTA	1	2	3	4	5
1. En la institución existen políticas de seguridad de la información documentadas.					
2. Las políticas de seguridad de la información se actualizan periódicamente					

Dimensión: Gestión de riesgos:

PREGUNTA	1	2	3	4	5
3. Se realiza un proceso formal de identificación de riesgos de seguridad de la información.					
4. Se efectúan análisis y tratamiento de los riesgos de forma sistemática.					

Dimensión: Mejora continua:

PREGUNTA	1	2	3	4	5
5. Se ejecutan auditorías internas sobre seguridad de la información.					
6. Se aplican acciones correctivas tras detectar fallos de seguridad.					

Dimensión: Capacitación y concientización:

PREGUNTA	1	2	3	4	5
7. El personal recibe formación regular en seguridad de la información.					
8. Se promueven campañas internas para concientizar sobre riesgos de seguridad.					

VARIABLE DEPENDIENTE: Evaluación de riesgos de seguridad de la información en sistemas notariales

Dimensión: Confidencialidad

PREGUNTA	1	2	3	4	5
9. Los mecanismos para impedir el acceso no autorizado a los sistemas notariales digitales son:					
10. La limitación del acceso por roles o perfiles de usuario está implementada de la siguiente manera:					

Dimensión: Integridad

PREGUNTA	1	2	3	4	5
11. Los mecanismos para validar la integridad de los documentos digitales son:					
12. El registro de modificaciones realizadas a documentos notariales se lleva a cabo de la siguiente forma:					

Dimensión: Disponibilidad

PREGUNTA	1	2	3	4	5
13. Los mecanismos para verificar que los documentos no han sido alterados sin autorización son:					
14. Las medidas para garantizar la recuperación de información en caso de fallos son:					

Dimensión: Identificación de riesgos

PREGUNTA	1	2	3	4	5
15. El registro actualizado de amenazas y vulnerabilidades del sistema notarial digital es:					
16. La revisión periódica de información sobre riesgos emergentes en seguridad informática se realiza de la siguiente manera:					

Anexo 5: Solicitud de autorización para realización de estudio

UNIVERSIDAD NACIONAL AMAZÓNICA DE MADRE DE DIOS
FACULTAD DE INGENIERÍA
ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

"Año de la recuperación y consolidación de la economía peruana"
"Madre de Dios, Capital de la Biodiversidad del Perú"

Puerto Maldonado, 12 de junio del 2025

OFICIO N°136-2025-UNAMAD-R-VRA-DFI-EPISI

NOTARÍA GARCÍA MEDINA
12 JUN. 2025
RECIBIDO
HORA: 10:00 FIRMA:

Señora:
Mg. Lourdes Madeleine Garcia Medina
TITULAR DE LA NOTARIA PÚBLICA GARCIA MEDINA

Presente. -

ASUNTO: SOLICITO AUTORIZACIÓN PARA REALIZAR INVESTIGACIÓN ACADÉMICA.

REF: SOLICITUD S/N

****

Tengo el agrado de dirigirme a Usted, para saludarlo cordialmente y en atención al documento en referencia, AUTORICE realizar los estudios y aplicación de los instrumentos de investigación, en la Notaria Pública Garcia Medina que usted dignamente dirige, al Bachiller: **Pablo Francisco Carrillo Venancino** de la **Carrera Profesional de Ingeniería de Sistemas e Informática** de la **Universidad Nacional Amazónica de Madre de Dios**.

Información que se requiere para el Proyecto de Tesis Intitulada: **"EVALUACION DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACION EN SISTEMAS NOTARIALES AL MARCO DE LA NORMA ISO/IEC 27001, AÑO 2025"**, con fines únicamente académicos y respetando y actuando conforme a la ley de protección de datos 29733.

Hago propicia la ocasión para expresarle mi consideración más distinguida, estima personal y mi agradecimiento por el apoyo al desarrollo académico y promoción de la investigación.

Sin otro en particular, me suscribo de Usted, no sin antes expresarle los sentimientos de mi especial consideración.

Atentamente,

UNIVERSIDAD NACIONAL AMAZÓNICA DE MADRE DE DIOS
ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

M.Sc. YEAN VILCHEZ NAVARRO
DIRECTOR

CC.
Archivo
DRE/EPISI
FMCM/secret.

UNAMAD Acreditando Calidad

Anexo 6: Solicitud de validación de instrumento

"AÑO DE LA RECUPERACIÓN Y CONSOLIDACIÓN DE LA ECONOMÍA PERUANA EN PERÚ"

SEÑOR: MG. MIGUEL ALATRISTA AGUILAR

SUMILLA: SOLICITO APOYO PARA LA VALIDACIÓN DE INSTRUMENTOS DE INVESTIGACIÓN.

PABLO FRANCISCO CARRILLO VENANCINO, peruano, identificado con DNI N° 73113570, con domicilio en la UPIS Vista Nueva, del distrito de Tambopata, provincia de Tambopata, departamento de Madre de Dios, con correo personal: **pablofvc95@gmail.com**, me presento ante usted y digo:

Que, en mi calidad de egresado de la Carrera Profesional de Ingeniería de Sistemas e Informática, en la actualidad estoy realizando el proyecto de tesis titulado **"Propuesta de implementación de un SGSI para la mejora de la seguridad de la información en la Notaría García Medina basado en la norma ISO/IEC 27001, Puerto Maldonado 2025"**, por lo que recurro a su conocimiento y experiencia en el campo de investigación para solicitarle su opinión y validación respecto al instrumento que se adjunta al presente y que se aplicará con motivo del proceso de investigación, consistentes en:

- Matriz de consistencia
- Operacionalización de variables
- Instrumento
- Ficha de validación

Agradeciendo su oportuna atención, me suscribo de usted.

ATENTAMENTE:

Puerto Maldonado, 09 de junio del 2025



PABLO FRANCISCO CARRILLO VENANCINO
DNI N° 73113570

"AÑO DE LA RECUPERACIÓN Y CONSOLIDACIÓN DE LA ECONOMÍA PERUANA EN PERÚ"

SEÑOR: MG. GLEIZER GREEWICH PANDURO VASQUEZ

SUMILLA: SOLICITO APOYO PARA LA VALIDACIÓN DE INSTRUMENTOS DE INVESTIGACIÓN.

PABLO FRANCISCO CARRILLO VENANCINO, peruano, identificado con DNI N° 73113570, con domicilio en la UPIS Vista Nueva, del distrito de Tambopata, provincia de Tambopata, departamento de Madre de Dios, con correo personal: **pablofvc95@gmail.com**, me presento ante usted y digo:

Que, en mi calidad de egresado de la Carrera Profesional de Ingeniería de Sistemas e Informática, en la actualidad estoy realizando el proyecto de tesis titulado **"Propuesta de implementación de un SGSI para la mejora de la seguridad de la información en la Notaría García Medina basado en la norma ISO/IEC 27001, Puerto Maldonado 2025"**, por lo que recurro a su conocimiento y experiencia en el campo de investigación para solicitarle su opinión y validación respecto al instrumento que se adjunta al presente y que se aplicará con motivo del proceso de investigación, consistentes en:

- Matriz de consistencia
- Operacionalización de variables
- Instrumento
- Ficha de validación

Agradeciendo su oportuna atención, me suscribo de usted.

ATENTAMENTE:

Puerto Maldonado, 09 de junio del 2025



PABLO FRANCISCO CARRILLO VENANCINO
DNI N° 73113570

"AÑO DE LA RECUPERACIÓN Y CONSOLIDACIÓN DE LA ECONOMÍA PERUANA EN PERÚ"

SEÑOR: MG. ALDO ALARCÓN SUCASACA

SUMILLA: SOLICITO APOYO PARA LA VALIDACIÓN DE INSTRUMENTOS DE INVESTIGACIÓN.

PABLO FRANCISCO CARRILLO VENANCINO, peruano, identificado con DNI N° 73113570, con domicilio en la UPIS Vista Nueva, del distrito de Tambopata, provincia de Tambopata, departamento de Madre de Dios, con correo personal: **pablofvc95@gmail.com**, me presento ante usted y digo:

Que, en mi calidad de egresado de la Carrera Profesional de Ingeniería de Sistemas e Informática, en la actualidad estoy realizando el proyecto de tesis titulado **"Propuesta de implementación de un SGSI para la mejora de la seguridad de la información en la Notaría García Medina basado en la norma ISO/IEC 27001, Puerto Maldonado 2025"**, por lo que recurro a su conocimiento y experiencia en el campo de investigación para solicitarle su opinión y validación respecto al instrumento que se adjunta al presente y que se aplicará con motivo del proceso de investigación, consistentes en:

- Matriz de consistencia
- Operacionalización de variables
- Instrumento
- Ficha de validación

Agradeciendo su oportuna atención, me suscribo de usted.

ATENTAMENTE:

Puerto Maldonado, 09 de junio del 2025

PABLO FRANCISCO CARRILLO VENANCINO
DNI N° 73113570

Anexo 7: Ficha de Validación

UNIVERSIDAD NACIONAL AMAZÓNICA DE MADRE DE DIOS
"AÑO DE LA RECUPERACIÓN Y CONSOLIDACIÓN DE LA ECONOMÍA PERUANA"
"MADRE DE DIOS CAPITAL DE LA BIODIVERSIDAD DEL PERÚ"

VALIDACIÓN DE INSTRUMENTOS DE INVESTIGACIÓN

I. DATOS GENERALES

TÍTULO DEL PROYECTO DE TESIS:

"PROPUESTA DE IMPLEMENTACIÓN DE UN SGSI PARA LA MEJORA DE LA SEGURIDAD DE LA INFORMACIÓN EN LA NOTARÍA GARCÍA MEDINA BASADO EN LA NORMA ISO/IEC 27001, PUERTO MALDONADO 2025"

NOMBRE DEL INSTRUMENTO A UTILIZAR EN LA INVESTIGACIÓN:

CUESTIONARIO ESTRUCTURADO PARA LA EVALUACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN, BASADO EN LA NORMA ISO/IEC 27001 Y ORIENTADO A MEDIR LAS DIMENSIONES DE CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD.

II. DATOS DEL EXPERTO

NOMBRES Y APELLIDOS:

Miguel Angel Alarcón Saavedra

LUGAR Y FECHA:

Tambopata, 12 Junio 2025

III. OBSERVACIONES

1. FORMA (Redacción, coherencia, ortografía):

Procede

2. CONTENIDO (El indicador corresponde a los ítems y dimensiones, es coherente):

Procede

3. ESTRUCTURA (Los ítems son detallados):

Procede.....
.....
.....

IV. SUGERENCIAS Y/O APORTES

Procede para su aplicación.....
.....
.....
.....

RESULTADO DE VALIDACIÓN

Por consiguiente, este instrumento:

X	**PROCEDE PARA SU APLICACIÓN**		**DEBE CORREGIRSE**

CIP 130835

FIRMA DEL EXPERTO:

DNI N°: 42536459

UNIVERSIDAD NACIONAL AMAZÓNICA DE MADRE DE DIOS
"AÑO DE LA RECUPERACIÓN Y CONSOLIDACIÓN DE LA ECONOMÍA PERUANA"
"MADRE DE DIOS CAPITAL DE LA BIODIVERSIDAD DEL PERÚ"

VALIDACIÓN DE INSTRUMENTOS DE INVESTIGACIÓN

I. DATOS GENERALES

TÍTULO DEL PROYECTO DE TESIS:

"PROPUESTA DE IMPLEMENTACIÓN DE UN SGSI PARA LA MEJORA DE LA SEGURIDAD DE LA INFORMACIÓN EN LA NOTARÍA GARCÍA MEDINA BASADO EN LA NORMA ISO/IEC 27001, PUERTO MALDONADO 2025"

NOMBRE DEL INSTRUMENTO A UTILIZAR EN LA INVESTIGACIÓN:

CUESTIONARIO ESTRUCTURADO PARA LA EVALUACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN, BASADO EN LA NORMA ISO/IEC 27001 Y ORIENTADO A MEDIR LAS DIMENSIONES DE CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD.

II. DATOS DEL EXPERTO

NOMBRES Y APELLIDOS:

GLEIZER GREENWICH PANDURO VASQUEZ

LUGAR Y FECHA:

TAMBOPATA, 12 JUNIO 2025

III. OBSERVACIONES

1. **FORMA (Redacción, coherencia, ortografía):**

PROCEDE

2. CONTENIDO (El indicador corresponde a los ítems y dimensiones, es coherente):

PROCEDE

3. ESTRUCTURA (Los ítems son detallados):

PROCEDE

IV. SUGERENCIAS Y/O APORTES

PROCEDE PARA SU APLICACIÓN

RESULTADO DE VALIDACIÓN

Por consiguiente, este instrumento:

X	PROCEDE PARA SU APLICACIÓN		DEBE CORREGIRSE

FIRMA DEL EXPERTO:

DNI N°: 70756317

UNIVERSIDAD NACIONAL AMAZÓNICA DE MADRE DE DIOS
"AÑO DE LA RECUPERACIÓN Y CONSOLIDACIÓN DE LA ECONOMÍA PERUANA"
"MADRE DE DIOS CAPITAL DE LA BIODIVERSIDAD DEL PERÚ"

VALIDACIÓN DE INSTRUMENTOS DE INVESTIGACIÓN

I. DATOS GENERALES

TÍTULO DEL PROYECTO DE TESIS:

"PROPUESTA DE IMPLEMENTACIÓN DE UN SGSI PARA LA MEJORA DE LA SEGURIDAD DE LA INFORMACIÓN EN LA NOTARÍA GARCÍA MEDINA BASADO EN LA NORMA ISO/IEC 27001, PUERTO MALDONADO 2025"

NOMBRE DEL INSTRUMENTO A UTILIZAR EN LA INVESTIGACIÓN:

CUESTIONARIO ESTRUCTURADO PARA LA EVALUACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN, BASADO EN LA NORMA ISO/IEC 27001 Y ORIENTADO A MEDIR LAS DIMENSIONES DE CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD.

II. DATOS DEL EXPERTO

NOMBRES Y APELLIDOS:

Aldo Alarcón Sucapuca

LUGAR Y FECHA:

Puerto Maldonado, 18 de junio 2025

III. OBSERVACIONES

1. FORMA (Redacción, coherencia, ortografía):

procede

2. CONTENIDO (El indicador corresponde a los ítems y dimensiones, es coherente):

Procede

3. ESTRUCTURA (Los ítems son detallados):

Procede

IV. SUGERENCIAS Y/O APORTES

Procede para la aplicación

RESULTADO DE VALIDACIÓN

Por consiguiente, este instrumento:

[X] **PROCEDE PARA SU APLICACIÓN** [ ] **DEBE CORREGIRSE**

FIRMA DEL EXPERTO:

DNI N°: 40288129

Anexo 8: Consentimiento informado

NOTARÍA GARCÍA MEDINA

LOURDES MADELEINE GARCÍA MEDINA
NOTARIA ABOGADA DE TAMBOPATA

CONSTANCIA

LOURDES MADELEINE GARCIA MEDINA NOTARIA DE LA PROVINCIA DE TAMBOPATA, DEPARTAMENTO DE MADRE DE DIOS, CON DNI N° 18099990, CON REGISTRO N° 044 DEL COLEGIO DE NOTARIOS DE CUSCO Y MADRE DE DIOS, QUIEN SUSCRIBE HACE CONSTAR:

QUE **PABLO FRANCISCO CARRILLO VENANCINO,** IDENTIFICADO CON DOCUMENTO NACIONAL DE IDENTIDAD N° 73113570, CUENTA CON EL CONSENTIMIENTO EXPRESO DE LA SUSCRITA PARA PODER REALIZAR LA INVESTIGACIÓN ACADÉMICA Y PRACTICAR LAS ENCUESTAS NECESARIAS EN LA SEDE DE ESTA NOTARÍA, CON EL FIN DE APLICAR LO DESARROLLADO EN SU TESIS TITULADA **"PROPUESTA DE IMPLEMENTACIÓN DE UN SGSI PARA LA MEJORA DE LA SEGURIDAD DE LA INFORMACIÓN EN LA NOTARÍA GARCÍA MEDINA BASADO EN LA NORMA ISO/IEC 27001, PUERTO MALDONADO 2025",**

SE EXTIENDE LA PRESENTE **CONSTANCIA,** A SOLICITUD DE PARTE INTERESADA, PARA LOS FINES QUE ESTIME CONVENIENTE.

PUERTO MALDONADO, 12 DE JUNIO DEL 2025

LOURDES MADELEINE GARCÍA MEDINA
NOTARIA ABOGADA DE TAMBOPATA

LOURDES MADELEINE GARCÍA MEDINA
ABOGADA - NOTARIA DE TAMBOPATA

Jr. Puno Nº 745 Puerto Maldonado Telf.: 502258 RPC Claro: 991837369 RPM Movistar 953567692 953567692
Email: notarialourdesga@hotmail.com Horario Corrido: de Lunes a Viernes de 8:00 am. a 7:30 pm. Sábados: 8:00 am. a 1:00 pm.

Anexo 9: Acta de proyecto

Acta de Constitución de Proyecto			
A. Información General			
Nombre del proyecto:	PROPUESTA DE IMPLEMENTACIÓN DE UN SGSI PARA LA MEJORA DE LA SEGURIDAD DE LA INFORMACIÓN EN LA NOTARÍA GARCÍA MEDINA BASADO EN LA NORMA ISO/IEC 27001, EN LA CIUDAD DE PUERTO MALDONADO 2025	Fecha	25/06/2025
Elaborado por:	Carrillo Venancino, Pablo Francisco	Autorizado por:	Notaría García Medina
B. Necesidad del proyecto			
• Determinar en qué medida la implementación de un SGSI en el marco de la norma ISO/IEC 27001 contribuye a mejorar la seguridad de la información en la notaría García Medina en el año 2025.			
C. Objetivos del proyecto			
• Evaluar en qué medida la implementación de un SGSI en el marco de la norma ISO/IEC 27001 contribuye a mejorar la confidencialidad de la información en la notaría García Medina. • Evaluar en qué medida la implementación de un SGSI en el marco de la norma ISO/IEC 27001 contribuye a fortalecer la integridad de la información en la notaría García Medina. • Evaluar en qué medida la implementación de un SGSI en el marco de la norma ISO/IEC 27001 contribuye a mejorar la disponibilidad de la información en la notaría García Medina.			
D. Alcance del proyecto			
• Procesos que involucren seguridad de la información			

Pablo F. Carrillo Venancino

LOURDES MADELEINE GARCÍA MEDINA
ABOGADA - NOTARIA DE TAMBOPATA

Anexo 10: Política general de seguridad de la información

NOTARÍA GARCIA MEDINA	Versión 1.0
	Autor: Pablo Carrillo Venancino
	Fecha: 25/06/2025
Política General de la Seguridad de la Información	

1. Resumen

La presente política establece los lineamientos generales para la gestión de la seguridad de la información en los sistemas notariales. Define el tratamiento de la información según su clasificación, las responsabilidades de los actores involucrados, así como las sanciones aplicables ante incumplimientos. Esta política se basa en los principios de confidencialidad, integridad y disponibilidad, conforme al marco de la norma ISO/IEC 27001.

2. Objetivo

Establecer directrices que garanticen la protección efectiva de los activos de información de las notarías frente a amenazas internas o externas, accidentales o deliberadas, con el fin de asegurar la continuidad del servicio notarial, la confianza de los ciudadanos y el cumplimiento legal, en concordancia con la norma ISO/IEC 27001.

3. Alcance

Esta política es aplicable a todo el personal de la notaría, incluyendo notarios, personal administrativo, técnicos, proveedores de servicios informáticos, contratistas y terceros con acceso a los sistemas o datos notariales.

La política será revisada periódicamente, especialmente ante cambios tecnológicos, normativos o estructurales. Asimismo, considera el cumplimiento de leyes nacionales relacionadas como:

- Ley N.º 29733 – Ley de Protección de Datos Personales
- Ley N.º 27269 – Ley de Firmas y Certificados Digitales
- DL N°1049 – Decreto Legislativo del Notariado
- Estándares internacionales ISO/IEC 27001

4. Principios Generales

- **Importancia de los activos de información:** Los sistemas notariales manejan información crítica como poderes, testamentos, actos jurídicos y datos personales. Su pérdida, alteración o divulgación no autorizada podría comprometer la legalidad y validez de actos públicos notariales.
- **Control de accesos:** Solo el personal debidamente autorizado podrá acceder a la información según su rol.
- **Concientización y formación:** Todo el personal debe conocer y cumplir las políticas de seguridad, así como participar en actividades de concientización.

- **Segregación de funciones:** Cada función o transacción debe estar sujeta a revisiones que permitan auditar quién accedió, cuándo y para qué.
- **Cultura de seguridad:** Se promoverá la seguridad como parte de la cultura organizacional, fortaleciendo comportamientos seguros ante fraudes, errores u omisiones.
- **Clasificación de la información:**
  - **Información Pública:** De libre acceso (ej. datos institucionales).
  - **Información Interna:** Uso exclusivo del personal notarial.
  - **Información Restringida:** Su acceso requiere autorización específica.
  - **Información Confidencial:** Su divulgación causaría daño crítico (ej. testamentos, poderes, escrituras no inscritas).

5. Medidas de Control

- Las áreas de archivo, almacenamiento digital y zonas de servidores deben contar con medidas físicas y lógicas de seguridad.
- Se desactivarán los puertos de medios removibles en equipos críticos. Su uso solo será autorizado previa solicitud documentada.
- Se implementarán controles de acceso, autenticación y gestión segura de contraseñas.
- Se mantendrá un inventario actualizado de los activos de información.
- Toda política o norma modificada deberá comunicarse a los trabajadores de forma clara, señalando los cambios realizados.
- La política general y las políticas específicas serán revisadas al menos una vez al año.

6. Responsabilidades

La Gerencia Notarial será responsable del diseño, implementación y supervisión del SGSI. Cada usuario del sistema debe actuar con responsabilidad frente al uso de la información, cumpliendo las políticas, normas y procedimientos establecidos.

7. Sanciones

La violación de esta política constituye una falta grave. Las sanciones se aplicarán según el reglamento interno de la notaría y pueden ser:

- Amonestación verbal
- Amonestación escrita
- Suspensión laboral
- Cese laboral (en casos graves)

No se requiere aplicar las sanciones de forma progresiva. La gravedad de la falta determinará la sanción correspondiente.

8. Políticas Específicas

Las siguientes políticas complementan y desarrollan esta política general:

- Política de Gestión de Contraseñas
- Política de Escritorio Limpio y Pantalla Segura
- Política de Gestión de Accesos
- Política de Gestión de Incidentes de Seguridad de la Información
- Política de Clasificación y Manejo de la Información
- Política de Continuidad del Negocio y Recuperación ante Desastres

Pablo F. Carrillo Venancino

LOURDES MADELEINE GARCÍA MEDINA
ABOGADA - NOTARIA DE TAMBOPATA

Anexo 11: Políticas complementarias

NOTARÍA GARCIA MEDINA	Versión 1.0
	Autor: Pablo Carrillo Venancino
	Fecha: 25/06/2025
Política de Gestión de Contraseñas	

1. Resumen:

Este documento establece los lineamientos mínimos para la gestión segura de contraseñas dentro de los sistemas notariales electrónicos. Dada la naturaleza crítica de la información manejada en estos entornos, una contraseña débil o comprometida puede representar una amenaza directa a la confidencialidad, integridad y disponibilidad de los activos de información notarial.

2. Objetivo:

Establecer estándares obligatorios para la creación, uso, protección y renovación de contraseñas con el fin de minimizar los riesgos de accesos no autorizados, garantizando la protección de los sistemas notariales y la información jurídica de los ciudadanos.

3. Alcance:

Aplica a todas las cuentas de usuario que tengan acceso a:

- Sistemas de gestión notarial electrónica.
- Correos institucionales.
- Bases de datos, servidores, redes internas y sistemas en la nube.
- Equipos de cómputo con acceso a información clasificada.
- Herramientas administrativas y aplicaciones de firma digital.

4. Creación de Contraseñas:

Las contraseñas de usuarios deben cumplir con los siguientes requisitos:

- Mínimo 8 caracteres.
- Incluir letras mayúsculas, letras minúsculas, números y caracteres especiales (como @, #, %, &).
- No usar palabras obvias o personales como el nombre del usuario, fechas importantes o palabras comunes.
- No se deben reutilizar contraseñas personales para el entorno laboral.

NOTARÍA GARCIA MEDINA	Versión 1.0
	Autor: Pablo Carrillo Venancino
	Fecha: 25/06/2025
Política de Gestión de Contraseñas	

5. Gestión de Contraseñas de Usuarios:

- Las contraseñas deben ser cambiadas al menos cada 90 días.
- Está prohibido activar la opción "Recordar contraseña" en navegadores u otros programas.
- Las contraseñas no deben almacenarse en archivos físicos ni digitales sin protección.
- Está totalmente prohibido compartir contraseñas con cualquier persona, incluyendo personal interno.
- Si se sospecha que una contraseña ha sido comprometida, se debe notificar inmediatamente al área técnica.
- En caso de olvido o pérdida, la contraseña debe ser reestablecida de forma segura por el área técnica designada.

6. Gestión de Contraseñas para Desarrolladores y Técnicos:

- Todas las contraseñas utilizadas en bases de datos o sistemas deben estar encriptadas, nunca almacenadas en texto plano.
- Las interfaces que recojan contraseñas deben ocultar los caracteres mediante símbolos (ej.: ●●●●) y no permitir el almacenamiento automático.

7. Roles y Responsabilidades:

Los roles y responsabilidades respecto a la gestión de contraseñas están alineados con los definidos en la Política General de Seguridad de la Información. Todo el personal con acceso a sistemas notariales debe conocer y cumplir esta política.

8. Sanciones:

Las sanciones por incumplimiento de esta política son las descritas en la **Política General de Seguridad de la Información**, y se aplicarán en función de la gravedad de la falta.

Política de escritorio limpio

NOTARÍA GARCIA MEDINA	Versión 1.0
	Autor: Pablo Carrillo Venancino
	Fecha: 25/06/2025
Política de Escritorio Limpio	

1. Resumen

El presente documento establece la política de escritorio limpio para los entornos notariales. Esta política tiene como finalidad reducir la exposición de información confidencial y sensible cuando un trabajador se ausenta de su estación de trabajo, previniendo así accesos no autorizados, pérdidas o manipulaciones de los activos de información. Se basa en buenas prácticas de seguridad de la información conforme al control 6.9 de la norma ISO/IEC 27001:2022.

2. Objetivo

Garantizar que la información notarial solo sea visible y manipulada por personal autorizado, evitando exposiciones involuntarias en escritorios, pantallas, documentos físicos o dispositivos electrónicos cuando el puesto de trabajo esté desatendido.

3. Alcance

Esta política aplica a todos los trabajadores de la notaría: notarios, personal administrativo, asistentes legales, técnicos informáticos y cualquier tercero con acceso temporal a las estaciones de trabajo, tanto en áreas físicas como virtuales.

4. Criterios de Escritorio Limpio

Para proteger la información en formato físico o digital, el personal deberá cumplir con los siguientes lineamientos:

- **Bloqueo de sesiones:** Toda computadora debe ser bloqueada al momento de dejar la estación de trabajo, incluso por breves períodos. Al finalizar la jornada, los equipos deben apagarse completamente.
- **Gestión de documentos físicos:** Documentos sensibles (escrituras, testamentos, contratos) no deben permanecer expuestos en escritorios. Deben guardarse en cajones cerrados con llave o archivadores autorizados al finalizar el día.

- **Llaves físicas:** Las llaves de gavetas o archivadores con documentos deben mantenerse bajo el control del responsable en todo momento.
- **Anclaje de equipos:** En zonas de atención al público o áreas compartidas, los equipos portátiles deben anclarse físicamente si el trabajador se ausenta.
- **Destrucción de documentos:** Cualquier documento confidencial que deba ser descartado debe ser destruido de forma segura (trituradora o incineración), evitando su reconstrucción.
- **Impresiones:** Todo material impreso debe ser recogido de inmediato. No debe permanecer en bandejas compartidas sin supervisión.
- **Visitas de terceros:** Si un tercero no autorizado se encuentra cerca del escritorio, no debe haber pantallas activas con información sensible ni documentos a la vista.

5. Monitoreo

- Al finalizar la jornada, el responsable designado por la administración notarial verificará el cumplimiento de los criterios de escritorio limpio en cada estación de trabajo.
- Cualquier documento, dispositivo o material expuesto será retirado y almacenado temporalmente por la administración.
- El trabajador podrá recuperarlo al día siguiente, presentando una autorización escrita o validación verbal de su superior directo.

6. Roles y Responsabilidades

Los roles y responsabilidades generales en relación con esta política están definidos en el punto 5 de la **Política General de Seguridad de la Información**. Todos los usuarios con acceso a información notarial son responsables del cumplimiento de estas medidas.

7. Sanciones

Las sanciones por incumplimiento de esta política están contempladas en el punto 6 de la Política General de Seguridad de la Información.

Política de gestión de accesos

NOTARÍA GARCIA MEDINA	Versión 1.0
	Autor: Pablo Carrillo Venancino
	Fecha: 11/09/2025
Política de Gestión de Accesos	

1. Resumen

El presente documento establece las directrices para la gestión de accesos a los sistemas informáticos, aplicaciones y activos de información digital de la notaría. Busca garantizar que solo las personas autorizadas tengan acceso a la información necesaria para el cumplimiento de sus funciones.

2. Objetivo

Definir las normas y procedimientos que regulen el control de accesos a los activos de información de la notaría, asegurando que los usuarios accedan únicamente a la información y recursos necesarios para el desarrollo de sus actividades.

3. Alcance

Esta política aplica a todo el personal de la notaría, así como a consultores, auditores externos o proveedores que, por motivos laborales o contractuales, requieran acceso a los sistemas y documentos notariales, ya sea en soporte físico o digital.

4. Acceso a la Información

- El acceso de los trabajadores a los activos de información estará limitado a las funciones propias de su cargo.
- Todo trabajador que se incorpore a la notaría contará con un usuario individual y una contraseña única para los sistemas asignados. Dichas credenciales deberán cumplir con los lineamientos de la Política de Gestión de Contraseñas.
- Los accesos serán definidos por el área administrativa en coordinación con la jefatura inmediata y aprobados por el responsable de Seguridad de la Información.

- Los terceros (auditores, consultores, proveedores) podrán acceder únicamente con autorización formal de la administración y bajo la firma de un acuerdo de confidencialidad.
- La administración designará a un único administrador de sistemas, responsable de la creación, modificación y eliminación de accesos.

5. Mantenimiento de los Accesos

- Se realizará una revisión periódica de los accesos al menos cada seis meses, para verificar su vigencia y pertinencia.
- Los accesos otorgados a terceros serán eliminados inmediatamente después de culminada la actividad que justificó su autorización.
- En casos de cambios de funciones, se evaluará si los colaboradores mantienen o no sus accesos previos. De no ser pertinentes, deberán ser actualizados o eliminados.
- Todo trabajador que cese funciones deberá entregar la documentación asignada y sus accesos serán retirados de inmediato.

6. Segregación de Funciones

- Los accesos serán estrictamente individuales y no compartidos entre usuarios.
- Ningún trabajador podrá tener acceso a todas las operaciones de un mismo proceso, garantizando la segregación de funciones y evitando conflictos de interés.

7. Roles y Responsabilidades

- **Alta Dirección:** Aprobar la política y garantizar los recursos necesarios.
- **Responsable de Seguridad de la Información (RSI):** Supervisar la correcta aplicación de la política y coordinar auditorías.
- **Administrador de sistemas:** Gestionar la creación, modificación y eliminación de accesos.

- **Trabajadores:** Cumplir con la política y reportar incidentes de seguridad relacionados con accesos.

8. Sanciones

Las sanciones aplicables son las definidas en el punto 7 de la Política General de la Seguridad de la Información.

Política de gestión de incidentes de seguridad

NOTARÍA GARCIA MEDINA	Versión 1.0
	Autor: Pablo Carrillo Venancino
	Fecha: 11/09/2025
Política de Gestión de Incidentes	

1. Resumen

El presente documento establece los lineamientos a seguir en caso de que ocurra un incidente de seguridad de la información en la notaría. Busca garantizar una respuesta oportuna, reducir el impacto sobre los activos digitales y físicos, y proteger la confidencialidad, integridad y disponibilidad de la información notarial.

2. Objetivo

La presente política tiene como objetivo establecer directrices claras para la gestión de incidentes de seguridad en la notaría, con el fin de **minimizar riesgos operativos, legales y reputacionales**, asegurando la continuidad del servicio notarial.

3. Alcance

Esta política aplica a:

- Todos los trabajadores y colaboradores de la notaría.
- Proveedores, consultores o terceros que tengan acceso a los sistemas o documentación digital.
- Todos los procesos y activos de información físicos y electrónicos.

4. Gestión de Incidentes

- Todo trabajador de la notaría tiene la responsabilidad de **reportar de inmediato cualquier incidente de seguridad** (pérdida de información, accesos no autorizados, alteración de documentos, fallos en sistemas, etc.) al responsable de Seguridad de la Información (RSI) y a su jefatura directa.
- Los incidentes reportados serán **clasificados según su gravedad** por el RSI, determinando los procedimientos de respuesta y los planes de acción.

- Se deberán establecer **protocolos de coordinación** con instituciones externas (Policía, Bomberos, servicios técnicos, entidades regulatorias) según la naturaleza del incidente.
- Todo incidente será **registrado en un informe detallado** que deberá contener como mínimo:
  - Activo de información afectado.
  - Descripción del incidente.
  - Riesgo asociado.
  - Controles afectados o comprometidos.
  - Impacto financiero, legal y reputacional.
  - Plan de acción aplicado.
- Los **incidentes graves** deberán ser informados a la Dirección de la notaría, detallando el impacto y los planes de recuperación.
- Todo incidente grave será analizado para verificar si constituye una **infracción legal**, en cuyo caso se procederá con la denuncia o reporte correspondiente a las autoridades competentes.
- Superado el incidente, se deberá **monitorear la efectividad de los controles aplicados** y determinar si el riesgo era conocido o nuevo:
  - Si es un riesgo nuevo, deberá ser incorporado al registro de riesgos.
  - Si es un riesgo conocido, deberá evaluarse si requiere reclasificación (aumentar o disminuir su impacto).

5. Roles y Responsabilidades

- **Alta Dirección:** Aprobar los planes de gestión de incidentes y garantizar los recursos para su atención.
- **Responsable de Seguridad de la Información (RSI):** Coordinar la clasificación, registro, atención y seguimiento de los incidentes.
- **Colaboradores:** Reportar de manera inmediata cualquier incidente de seguridad del que tengan conocimiento.

- **Administradores de sistemas:** Ejecutar las acciones técnicas necesarias para contener y mitigar el incidente.

6. Sanciones

Las sanciones aplicables por el incumplimiento de esta política serán las establecidas en la **Política General de Seguridad de la Información de la notaría**, pudiendo incluir sanciones administrativas internas, suspensión de accesos o acciones legales según corresponda.

Política de gestión de copias de seguridad

NOTARÍA GARCIA MEDINA	Versión 1.0
	Autor: Pablo Carrillo Venancino
	Fecha: 11/09/2025
Política de Gestión de copias de seguridad	

1. Resumen

El presente documento establece los lineamientos para la correcta gestión de copias de respaldo en la notaría, con el fin de asegurar la continuidad del servicio notarial digital y proteger los documentos, bases de datos y aplicativos ante incidentes de pérdida de información, fallos técnicos o ataques informáticos.

2. Objetivo

Definir las directrices generales para la creación, almacenamiento y recuperación de copias de respaldo de los sistemas, aplicaciones, documentos digitales y bases de datos de la notaría, garantizando la **disponibilidad e integridad de la información crítica**.

3. Alcance

Esta política aplica a:

- Todos los sistemas, aplicaciones, bases de datos y documentos digitales generados y administrados en la notaría.
- Todo el personal responsable de la administración de sistemas y de la seguridad de la información.
- Proveedores de servicios tecnológicos que participen en la gestión de respaldos.

4. Gestión de Copias de Respaldo

- Se realizarán copias de seguridad de las **bases de datos notariales** al menos una vez por semana.
- Se realizarán copias de seguridad de los **documentos y trámites digitales** de manera diaria.
- Las copias de seguridad deberán ejecutarse de forma **automática** y no manual, generando versiones diferenciadas por fecha y evitando sobrescribir copias anteriores.

- Las copias de respaldo deberán almacenarse **fuera del servidor principal** y en un **sitio alterno** distinto al local de la notaría, ya sea en servidores externos seguros o en soluciones de nube certificadas.
- Toda copia de respaldo deberá estar **cifrada** para prevenir accesos no autorizados.
- La restauración parcial o total de información deberá ser solicitada al responsable de Seguridad de la Información (RSI) y notificada a la jefatura correspondiente.
- Periódicamente se deberán realizar **pruebas de restauración** para asegurar la validez y usabilidad de las copias generadas.

5. Roles y Responsabilidades

- **Alta Dirección:** Aprobar y supervisar la correcta aplicación de esta política.
- **Responsable de Seguridad de la Información (RSI):** Garantizar la correcta ejecución, almacenamiento y restauración de las copias de seguridad.
- **Administrador de sistemas:** Configurar, monitorear y verificar la generación automática de respaldos.
- **Colaboradores:** Reportar cualquier incidente o necesidad de recuperación de información.

6. Sanciones

El incumplimiento de esta política será sancionado conforme a lo establecido en la **Política General de Seguridad de la Información**, pudiendo incluir medidas disciplinarias internas, suspensión de accesos o acciones legales según la gravedad de la falta.

Política de gestión de activos

NOTARÍA GARCIA MEDINA	Versión 1.0
	Autor: Pablo Carrillo Venancino
	Fecha: 11/09/2025
Política de gestión de activos	

1. Resumen

El presente documento establece los lineamientos para la gestión de los activos de información de la notaría, con el propósito de asegurar su correcta administración, uso responsable y protección frente a riesgos que comprometan su integridad, disponibilidad y confidencialidad.

2. Objetivo

Definir directrices generales para la gestión de los activos de información de la notaría, garantizando su adecuada clasificación, custodia y uso, a fin de prevenir pérdidas, alteraciones o accesos no autorizados que afecten la seguridad de la información.

3. Alcance

Esta política aplica a todos los activos de información físicos y digitales de la notaría, incluyendo:

- Documentos notariales físicos y electrónicos.
- Carpetas compartidas, bases de datos y aplicaciones internas.
- Sistemas informáticos, equipos de cómputo, redes y medios de almacenamiento.
- Personal, proveedores y terceros que administren o utilicen estos activos.

4. Seguridad de Información Digital

- Todo colaborador deberá conocer y cumplir las políticas, normas y procedimientos aplicables al uso de activos digitales.
- Las aplicaciones y sistemas utilizados para la gestión notarial serán provistos y autorizados únicamente por la notaría. No se permitirá la instalación de software adicional sin autorización expresa.
- El intercambio de información con clientes, proveedores o terceros deberá realizarse únicamente a través de las cuentas y medios institucionales.

Está prohibido el uso de correos o servicios personales para fines laborales.

- Está prohibido interceptar, divulgar o acceder a comunicaciones electrónicas sin autorización expresa del dueño de la información.
- El acceso a Internet deberá usarse solo con fines laborales y en función de las responsabilidades asignadas.
- No se deberá almacenar información clasificada como confidencial en dispositivos móviles personales.
- Todo documento notarial catalogado como confidencial deberá estar cifrado.
- Todas las computadoras deberán contar con antivirus, cortafuegos y herramientas de cifrado actualizadas.
- Los puertos de medios removibles deberán estar inhabilitados. En caso de requerirse su uso, será necesaria autorización previa de la administración.
- Los repositorios digitales deberán recibir mantenimiento preventivo al menos cada seis meses.
- Para evitar comprometer información de forma accidental, se deberán observar las siguientes medidas:
    - No abrir correos sospechosos o de remitentes desconocidos.
    - Bloquear la pantalla del equipo cuando no esté en uso.
    - Eliminar de forma segura la documentación digital que ya no sea necesaria.

5. Seguridad Física y de Sitio

- Todo colaborador deberá conocer y cumplir las normas sobre la custodia de activos físicos de la notaría.
- El acceso a áreas administrativas estará restringido al personal autorizado, mientras que las áreas de atención al cliente serán compartidas con usuarios y visitantes bajo supervisión.

- Todo documento físico con datos confidenciales deberá ser destruido de manera segura para que no pueda recuperarse.
- Los escritorios deberán permanecer libres de documentos visibles cuando el colaborador se ausente.
- Las gavetas y archivadores deberán mantenerse bajo llave.
- Los documentos notariales generales (protocolos, registros, archivos históricos) deberán guardarse en almacenes seguros bajo control de acceso.
- Los archivos físicos deberán someterse a revisiones y mantenimiento mínimo una vez al año.

6. Roles y Responsabilidades

- **Alta Dirección:** Aprobar y supervisar la correcta aplicación de esta política.
- **Responsable de Seguridad de la Información (RSI):** Supervisar la clasificación, custodia y protección de los activos.
- **Colaboradores:** Cumplir con las normas establecidas y reportar cualquier incidente o irregularidad.
- **Administración de sistemas:** Garantizar el mantenimiento de los activos digitales y físicos bajo su responsabilidad.

7. Sanciones

El incumplimiento de esta política será sancionado de acuerdo con lo establecido en la Política General de Seguridad de la Información de la notaría, pudiendo incluir medidas disciplinarias, suspensión de accesos o acciones legales según la gravedad de la falta.

Política de uso de redes y comunicaciones

NOTARÍA GARCIA MEDINA	Versión 1.0
	Autor: Pablo Carrillo Venancino
	Fecha: 11/09/2025
Política de uso aceptable de servicios de red y comunicaciones	

1. Objetivo

El objetivo de la presente política es establecer las normas y directrices para el uso seguro, responsable y legal de los servicios de red (Internet, correo electrónico, redes sociales, software, etc.). Esta política busca:

- **Proteger la confidencialidad, integridad y disponibilidad** de la información sensible de la notaría y de sus clientes.
- **Garantizar el cumplimiento** de las leyes y regulaciones aplicables (Ley del Notariado, Ley de Protección de Datos Personales).
- **Preservar la integridad y reputación** de la notaría.
- **Asegurar que los recursos tecnológicos** se utilicen de manera eficiente y para fines profesionales legítimos.

2. Alcance

Esta política aplica a todos los trabajadores de la notaría y a cualquier tercero (proveedores, consultores) que tenga acceso a los sistemas de red y comunicación de la notaría.

3. Principios Generales

El uso de los recursos tecnológicos de la notaría es un privilegio vinculado a la actividad profesional, no un derecho personal ilimitado. Se espera que todos los usuarios actúen con ética, profesionalismo y sentido común.

4. Políticas Específicas de Uso

A. Uso Aceptable:

Los recursos de red deben utilizarse principalmente para actividades relacionadas directamente con las funciones notariales, tales como:

- Comunicación con clientes, colegas, registros y organismos oficiales.
- Investigación jurídica y consulta de bases de datos legales.
- Realización de trámites en sedes electrónicas oficiales.

- Gestión administrativa y contable de la notaría.

B. Uso No Aceptable (Prohibiciones):

Queda estrictamente prohibido utilizar los recursos de la notaría para:

1. **Almacenar o transmitir información confidencial** sin las medidas de cifrado y seguridad apropiadas.
2. **Acceder, descargar, distribuir o almacenar** material ofensivo, obsceno, discriminatorio o ilegal.
3. **Instalar software, hardware o aplicaciones** no autorizadas por el administrador de sistemas.
4. **Realizar descargas personales** (música, películas, software comercial) que no tengan fines profesionales.
5. **Utilizar sistemas peer-to-peer (P2P)**, juegos en línea o streaming para uso personal.
6. **Acceder a cuentas de correo personales** (Gmail, Yahoo, etc.) para el envío o recepción de documentación profesional o sensible. Toda comunicación oficial debe realizarse desde el correo corporativo.
7. **Compartir contraseñas** o credenciales de acceso. Cada usuario es responsable de su cuenta.
8. **Realizar actividades que consuman ancho de banda** de manera excesiva y afecten el rendimiento de la red para fines profesionales.

5. Correo Electrónico

- **Uso Principal:** Herramienta profesional para la comunicación con clientes y organismos.
- **Precaución:** Extreme la cautela al abrir archivos adjuntos o hacer clic en enlaces de remitentes desconocidos para evitar malware y phishing.

- **Firmas:** Todos los correos deben incluir la firma electrónica oficial con los datos de contacto de la notaría.
- **Almacenamiento:** Los correos deben archivarse en las carpetas adecuadas del sistema para garantizar su conservación y fácil recuperación, de acuerdo con la normativa de protocolo notarial.

6. Confidencialidad y Protección de Datos

- **Secreto Profesional:** Todo el personal está sujeto al deber de confidencialidad y secreto profesional notarial. Esta obligación se extiende al manejo de información en formato digital.
- **Datos Personales:** El tratamiento de datos personales de clientes se realizará exclusivamente para la finalidad autorizada.
- **Almacenamiento en la Nube:** Queda prohibido almacenar documentos notariales, minutas o cualquier dato sensible del cliente en servicios de cloud storage públicos o personales (Dropbox, Google Drive personal, WeTransfer sin cifrar, etc.) sin la autorización expresa y el uso de soluciones empresariales aprobadas y seguras.

7. Seguridad de las Contraseñas

- Las contraseñas deben ser robustas, combinando mayúsculas, minúsculas, números y símbolos.
- Deben cambiarse cada 90 días y no se deben reutilizar contraseñas antiguas.
- Bajo ninguna circunstancia se deben anotar en papeles visibles o compartirse.

8. Dispositivos Móviles y Teletrabajo

- Los dispositivos móviles propiedad de la notaría (portátiles, tablets, teléfonos) deben estar protegidos con contraseña y tener habilitado el borrado remoto en caso de pérdida o robo.

- En caso de teletrabajo, el acceso a los sistemas de la notaría se realizará exclusivamente a través de una Red Privada Virtual (VPN) autorizada y con sistemas de autenticación segura.
- Los documentos de trabajo deben almacenarse en los directorios de red de la notaría, no en el disco duro local del equipo personal.

9. Monitoreo y Cumplimiento

- La notaría se reserva el derecho de monitorear, auditar y supervisar el uso de todos sus recursos tecnológicos (tráfico de red, uso de Internet, correos electrónicos, etc.) para garantizar el cumplimiento de esta política, proteger sus activos e investigar posibles incidencias de seguridad. Los usuarios deben tener cero expectativa de privacidad en el uso de estos recursos.
- Las violaciones a esta política serán investigadas y pueden resultar en medidas disciplinarias, que pueden incluir desde una amonestación verbal hasta la terminación de la relación laboral, dependiendo de la gravedad de la infracción. Las actividades ilegales se reportarán a las autoridades competentes.

Anexo 12: Acta de cierre de proyecto

Acta de Cierre y Entrega de proyecto	
Título del proyecto: PROPUESTA DE IMPLEMENTACIÓN DE UN SGSI PARA LA MEJORA DE LA SEGURIDAD DE LA INFORMACIÓN EN LA NOTARÍA GARCÍA MEDINA BASADO EN LA NORMA ISO/IEC 27001, EN LA CIUDAD DE PUERTO MALDONADO 2025.	
Objetivo general: • Determinar en qué medida la implementación de un SGSI en el marco de la norma ISO/IEC 27001 contribuye a mejorar la seguridad de la información en la notaria Garcia Medina en el año 2025. **Objetivo específico:** • Evaluar en qué medida la implementación de un SGSI en el marco de la norma ISO/IEC 27001 contribuye a mejorar la confidencialidad de la información en la notaria García Medina. • Evaluar en qué medida la implementación de un SGSI en el marco de la norma ISO/IEC 27001 contribuye a fortalecer la integridad de la información en la notaria García Medina. • Evaluar en qué medida la implementación de un SGSI en el marco de la norma ISO/IEC 27001 contribuye a mejorar la disponibilidad de la información en la notaria García Medina.	
Inicio: 05/07/2025	Fin: 18/09/2025
Entregables generados por el proyecto: • Política de seguridad de la información • Inventario de activos • Matriz de amenazas y vulnerabilidades • Valoración de activos • Matriz de riesgos • Listado de controles	Costo final del proyecto en Soles: El proyecto no representó costo alguno para la notaría.
Logros del proyecto: • Lograr la mitigación de riesgos a los que estaban expuestos los activos más críticos de la notaría. • Establecer una cultura de seguridad en la notaría.	
Comentarios generales: La importancia de implementar un sistema de gestión de la seguridad de la información (SGSI) basado en estándares de buenas prácticas basado en la familia ISO / IEC 27000, así como un personal de experiencia en lo relacionado a control interno asegura la correcta implementación del mismo.	

Pablo F. Carrillo Venancino

LOURDES MADELEINE GARCÍA MEDINA
ABOGADA - NOTARIA DE TAMBOPATA