UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO

FACULTAD DE INGENIERÍA CIVIL, DE SISTEMAS Y DE ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

TESIS

Gestión de la seguridad de la información, basado en las normas ISO/IEC 27000 y la metodología Magerit, para mitigar los riesgos de TI en la empresa Garzasoft – Chiclayo

PARA OBTENER EL TÍTULO PROFESIONAL DE:
Ingeniero de Sistemas

Autores:
Bach. Edwin Guillermo Ascencio Romero

Asesor:
Dr. Ing. Ernesto Kalo Celi Arévalo

Lambayeque, Perú
2026

UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO

FACULTAD DE INGENIERÍA CIVIL, DE SISTEMAS Y DE ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

TESIS

Gestión de la seguridad de la información, basado en las normas ISO/IEC 27000 y la metodología Magerit, para mitigar los riesgos de TI en la empresa Garzasoft – Chiclayo

PARA OBTENER EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS

APROBADO POR EL SIGUIENTE JURADO:

Dr. Robert Edgar Puican Gutiérrez
Presidente

Dr. Ing. Jesús Bernardo Olavarria Paz
Secretario

Dra. María de los Ángeles Guzmán Valle
Vocal

Dr. Ing. Ernesto Kalo Celi Arévalo
Asesor

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

ACTA DE SUSTENTACIÓN
N°003-2026-UI-FICSA

Siendo las 10:30 am horas del día 15 de mayo del 2026, se reunieron de manera presencial los miembros de jurado de la tesis titulada: **"GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN, BASADO EN LAS NORMAS ISO/IEC 27000 Y LA METODOLOGÍA MAGERIT, PARA MITIGAR LOS RIESGOS DE TI EN LA EMPRESA GARZASOFT CHICLAYO"**, con código N° IS_V_2023_024, designado por Resolución Decanal Virtual N° 090-2024-UNPRG-FICSA con la finalidad de Evaluar y Calificar la sustentación de la tesis antes mencionada, conformado por los siguientes docentes:

DR. ING. ROBERT PUICAN GUTIERREZ	PRESIDENTE
DR. ING. JESUS BERNARDO OLAVARRIA PAZ	SECRETARIO
DRA. ING. MARIA DE LOS ANGELES GUZMAN VALLE	VOCAL

Asesorado por DR. ING. ERNESTO KARLO CELI AREVALO.

El acto de sustentación fue autorizado por OFICIO VIRTUAL N° 103-2026-UIFICSA, la tesis fue presentada y sustentada por el Bachiller: **EDWIN GUILLERMO ASCENCIO ROMERO,** tuvo una duración de ...60...minutos. Después de la sustentación, y absueltas las preguntas y observaciones de los miembros del jurado; se procedió a la calificación respectiva:

	NUMERO	LETRAS	CALIFICATIVO
EDWIN GUILLERMO ASCENCIO ROMERO	15	QUINCE	REGULAR

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

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

DR. ING. ROBERT PUICAN GUTIERREZ
PRESIDENTE

DR. ING. JESUS BERNARDO OLAVARRIA PAZ
SECRETARIO

DRA. ING. MARIA DE LOS ANGELES GUZMAN VALLE
VOCAL

DR. ING. ERNESTO KARLO CELI AREVALO
ASESOR

JHFF/bcm

CONSTANCIA DE VERIFICACION DE ORIGINALIDAD

Yo **Ernesto Karlo Celi Arévalo** usuario revisor de Tesis [x] Trabajo de Suficiencia Profesional [ ] y/o Trabajo Académico [ ]

Titulado: **Gestión de la seguridad de la información, basado en las normas ISO/IEC 27000 y la metodología Magerit, para mitigar los riesgos de TI en la empresa Garzasoft – Chiclayo**

Cuyo autor es: **Edwin Guillermo Ascencio Romero**; con DNI N° **44727064**; declaro que la evaluación realizada por el Programa informático, ha arrojado un porcentaje de similitud **11%,** verificables en el Resumen del Reporte automatizado de similitudes que se acompaña.

El suscrito (a) analizó reporte y concluyó que cada una de las coincidencias detectadas dentro del porcentaje de similitud permitido no constituyen plagio y que el documento cumple con la integridad científica y con las normas para el uso de citas y referencias establecidas en los protocolos respectivos,

Se cumple con adjuntar el Recibo Digital a efectos de la trazabilidad respectiva del proceso.

Lambayeque, 27 de Agosto del 2026

Nombres y Apellidos: Ernesto Karlo Celi Arévalo
DNI 18068078

Adjunta:

Resumen de Reporte automatizado de similitudes
Recibo digital

Revisión de informe en Turnitin

Tesis Gestión de la seguridad de la información, basado en las normas ISO/IEC 27000 y la metodología Magerit, para mitigar los riesgos de TI en la empresa Garzasoft – Chiclayo

ORIGINALITY REPORT

12%	11%	6%	7%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	repositorio.unprg.edu.pe Internet Source	1%
2	hdl.handle.net Internet Source	1%
3	Submitted to Universidad San Marcos Student Paper	1%
4	Submitted to Universidad Nacional Pedro Ruiz Gallo Student Paper	1%
5	repositorio.uncp.edu.pe Internet Source	<1%
6	repositorio.uns.edu.pe Internet Source	<1%
7	Submitted to Universidad Mariano Gálvez de Guatemala Student Paper	<1%
8	repositorio.unheval.edu.pe Internet Source	<1%
9	repositorio.uniremington.edu.co Internet Source	<1%
10	Submitted to Universidad Internacional de la Rioja Student Paper	<1%
11	repositorio.ujcm.edu.pe Internet Source	<1%
12	Submitted to National University College - Online Student Paper	<1%
13	repositorio.upci.edu.pe Internet Source	<1%
14	repositorio.pucesa.edu.ec Internet Source	<1%
	docplayer.es	

Dr. Ernesto Karlo Celi Arévalo
DNI 18068078
ASESOR

Dr. Ernesto Karlo Celi Arévalo
Asesor
DNI. 18068078

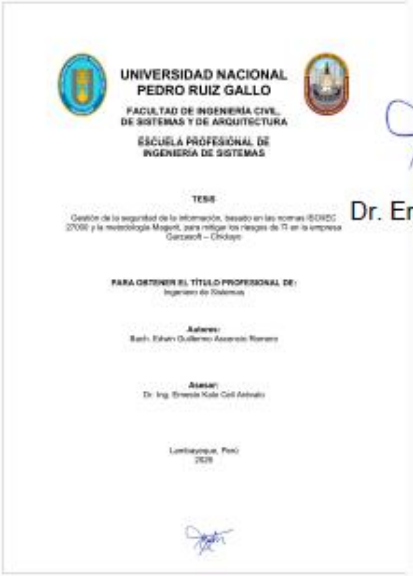
turnitin

Digital Receipt

This receipt acknowledges that Turnitin received your paper. Below you will find the receipt information regarding your submission.

The first page of your submissions is displayed below.

Submission author:	Edwin Guillermo Ascencio Romero
Assignment title:	Quick Submit
Submission title:	Tesis Gestión de la seguridad de la información, basado en las...
File name:	Informe_Final_EdwinAsencioRomero.docx
File size:	790.93K
Page count:	84
Word count:	24,685
Character count:	142,005
Submission date:	27-Aug-2026 11:46AM (UTC-0500)
Submission ID:	3018772313



UNIVERSIDAD NACIONAL
PEDRO RUIZ GALLO

FACULTAD DE INGENIERÍA CIVIL, DE SISTEMAS Y DE ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

TESIS

Gestión de la seguridad de la información, basado en las normas ISO/IEC 27000 y la metodología Magerit, para mitigar los riesgos de TI en la empresa Garzasoft – Chiclayo

PARA OBTENER EL TÍTULO PROFESIONAL DE:
Ingeniero de Sistemas

Autores:
Bach. Edwin Guillermo Ascencio Romero

Asesor:
Dr. Ing. Ernesto Karlo Celi Arévalo

Lambayeque, Perú
2026

Dr. Ernesto Karlo Celi Arévalo
DNI 18068078
ASESOR

Dr. Ernesto Karlo Celi Arévalo
Asesor
DNI. 18068078

DEDICATORIA

En primer lugar a Dios por darme la fortaleza necesaria para lograr mis objetivos y poder llegar con salud hasta este momento tan importante en mi vida y mi formación profesional

A mis padres por su apoyo, consejos, comprensión y amor.
Ellos me han dado todo lo que soy como persona, mis valores, mis principios, mi carácter, mi perseverancia y mi coraje para conseguir mis objetivos. quienes por ellos soy lo que soy.

A mí actual pareja que siempre confío en mí y siempre tuve su apoyo incondicional en todo momento.

AGRADECIMIENTOS

Al Dr. Ing. Ernesto Karlo Celi Arévalo, por sus aportes en los lineamientos, sus comentarios, tiempo dedicado, sus orientaciones y recomendaciones pero sobre todo por la paciencia y dedicación brindadas para orientarme a realizar un buen trabajo.

Al jurado calificador, porque desde un primer momento mostraron disposición a ayudar con sugerencias y correcciones durante la elaboración de la presente tesis.

A nuestra prestigiosa alma mater "Universidad Nacional Pedro Ruiz Gallo” y en especial a la Facultad de Ingeniería Civil, Sistemas y Arquitectura, por haberme formado profesionalmente y ser persona útil y de bien para la sociedad.

RESUMEN

La presente investigación aborda la problemática de la gestión deficiente de la seguridad de la información en la empresa Garzasoft – Chiclayo, cuyo crecimiento acelerado, la ampliación de su cartera de clientes y el incremento en la complejidad de sus soluciones de software han expuesto debilidades significativas en la protección de activos tecnológicos, la continuidad operativa y la gestión de riesgos de TI. La falta de políticas formales, controles técnicos consolidados, procedimientos documentados y un enfoque sistemático de evaluación de riesgos ponen en riesgo la integridad, disponibilidad y confidencialidad de los datos administrados por la empresa y de los sistemas que desarrolla para el sector empresarial.

El propósito de la investigación fue proponer un modelo de gestión de la seguridad de la información basado en las normas ISO/IEC 27000 y la metodología MAGERIT para mitigar los riesgos de TI en Garzasoft. Los fundamentos teóricos se estructuraron a partir del ciclo PDCA de ISO/IEC 27001, los controles de ISO/IEC 27002, el enfoque de gestión de riesgos de MAGERIT v3 y principios de seguridad en el ciclo de vida del desarrollo de software. La investigación tuvo un enfoque descriptivo-propositivo, de diseño no experimental y método aplicado. Se emplearon técnicas como la observación directa, entrevistas semiestructuradas, análisis documental y auditorías técnicas, complementadas con instrumentos como listas de verificación, matrices de activos, vulnerabilidades, amenazas e impacto.

Los resultados permitieron identificar 25 activos críticos, 22 amenazas relevantes y 18 vulnerabilidades asociadas a accesos, configuraciones, procesos de desarrollo y gestión operativa. La valoración mediante una matriz de riesgo 5×5 evidenció riesgos altos y críticos relacionados con código fuente, bases de datos y servicios en la nube. El modelo propuesto integra políticas, procedimientos, controles ISO y un plan de tratamiento basado en los principios de reducir, evitar, transferir y aceptar riesgos. Se concluye que la adopción del modelo ISO/MAGERIT fortalece significativamente la postura de seguridad de la empresa.

Palabras clave: Seguridad de la información, ISO/IEC 27001, MAGERIT, riesgos de TI, SGSI.

ABSTRACT

This research addresses the problem of deficient information security management in the company Garzasoft – Chiclayo, whose rapid growth, expanding client portfolio, and increasing complexity of its software solutions have exposed significant weaknesses in the protection of technological assets, operational continuity, and IT risk management. The lack of formal policies, consolidated technical controls, documented procedures, and a systematic approach to risk assessment jeopardizes the integrity, availability, and confidentiality of the data managed by the company and the systems it develops for the business sector.

The purpose of this study was to propose an information security management model based on the ISO/IEC 27000 standards and the MAGERIT methodology to mitigate IT risks at Garzasoft. The theoretical foundations were structured around the PDCA cycle of ISO/IEC 27001, the controls of ISO/IEC 27002, the MAGERIT v3 risk management framework, and security principles for the software development life cycle. The research followed an applied, descriptive–propositional, and non-experimental design. Data were collected through direct observation, semi-structured interviews, document analysis, and technical audits, complemented by instruments such as checklists, asset matrices, threat and vulnerability lists, and impact assessments.

The results allowed the identification of 25 critical assets, 22 relevant threats, and 18 vulnerabilities associated with access control, system configuration, development processes, and operational management. The assessment using a 5×5 risk matrix revealed high and critical risks linked to source code, databases, and cloud services. The proposed model integrates policies, procedures, ISO controls, and a risk treatment plan based on the principles of reducing, avoiding, transferring, and accepting risks. The study concludes that adopting the ISO/MAGERIT model significantly strengthens the company's information security posture.

Keywords: Information security, ISO/IEC 27001, MAGERIT, IT risks, ISMS.

ÍNDICE GENERAL

LISTA DE TABLAS

LISTA DE FIGURAS

INTRODUCCIÓN

En un entorno global caracterizado por una creciente interconexión digital, la seguridad de la información se ha convertido en un componente estratégico para la sostenibilidad operativa de cualquier organización. En el caso peruano, este desafío adquiere especial relevancia debido a la acelerada transformación digital y a la creciente dependencia de los servicios tecnológicos. Las empresas de desarrollo de software, particularmente en regiones como Chiclayo, operan en un contexto donde los riesgos de TI aumentan de forma proporcional al nivel de digitalización de sus procesos y activos. Sin embargo, a pesar de los avances tecnológicos, persisten deficiencias críticas en la gestión de riesgos y en la protección de los activos de información, lo que expone a las organizaciones a ciberataques, fallas operativas y pérdidas económicas significativas (Infobae, 2025; Rumbo Económico, 2025).

Diversos estudios recientes evidencian que el Perú enfrenta una ola creciente de amenazas cibernéticas que supera la capacidad de respuesta de muchas organizaciones. Informes de ESET (2025) señalan que más del 60% de los ataques en el país se originan mediante técnicas de phishing, lo que subraya la fragilidad del factor humano frente a tácticas de ingeniería social. De manera similar, reportes internacionales como el IBM Security X-Force Threat Intelligence Index (2024) revelan que América Latina continúa siendo una región altamente vulnerable a incidentes de ransomware, explotación de vulnerabilidades conocidas y configuraciones inseguras en la nube. En este escenario, la ausencia de seguros cibernéticos —que solo alcanzan a un grupo reducido de empresas peruanas— y la falta de procesos maduros para gestionar activos de TI agravan todavía más la exposición al riesgo (Infobae, 2025a).

A ello se suma la persistencia de malas prácticas en el ciclo de desarrollo de software. El informe de Tricentis (2025) advierte que la mayoría de las empresas latinoamericanas introducen cambios en el código sin realizar pruebas exhaustivas, priorizando la rapidez sobre la robustez. Asimismo, vulnerabilidades críticas históricas como Log4Shell continúan siendo explotadas debido a la falta de actualizaciones oportunas, lo cual evidencia una gestión deficiente de parches y obsolescencia tecnológica (Observatorio Nacional de Prospectiva, 2025). En este sentido, múltiples investigaciones han demostrado la relación directa entre la gestión de riesgos y la calidad del software, señalando que una administración inmadura de los riesgos incrementa la probabilidad de defectos, brechas de seguridad y fallos operativos (Interfases, 2021).

Durante los años 2024 y 2025, GarzaSoft ha atravesado un proceso acelerado de crecimiento corporativo, impulsado por la expansión de su cartera de clientes y la diversificación de sus productos tecnológicos en producción. Este incremento en la demanda ha puesto una presión

adicional sobre su infraestructura tecnológica, sus procesos operativos y sus mecanismos de seguridad, generando un escenario crítico en la gestión de sus activos de información. La empresa actualmente mantiene en operación una amplia gama de soluciones tecnológicas utilizadas por diversas organizaciones de forma continua, entre las que se encuentran:

Sistemas de producción en uso por clientes, que incluyen:

- GESREST, una solución integral para la administración de restaurantes que permite gestionar ventas en salón, pedidos por delivery y operaciones desde aplicaciones móviles, abarcando diversas modalidades de pago como efectivo, tarjetas, transferencias y billeteras digitales.
- 360.SIS, un sistema de gestión comercial orientado a puntos de venta en minimarkets, ferreterías, farmacias, panaderías y negocios similares, facilitando el control operativo y administrativo.
- Hotel HUB, una plataforma especializada en la gestión hotelera que busca mejorar la experiencia del huésped y optimizar la operación de los servicios de alojamiento.
- Pulso, una solución tecnológica que centraliza y automatiza la gestión de información y procesos en organizaciones dedicadas al sector salud.
- Comprobante-e, un sistema que permite la emisión de comprobantes electrónicos —boletas y facturas— de manera remota, adaptable a distintos entornos y necesidades comerciales.

El crecimiento del número de clientes que utilizan estos sistemas ha incrementado la carga operativa, la cantidad de solicitudes de soporte, el consumo de recursos tecnológicos y la complejidad de los entornos de operación, generando un aumento sustancial en los incidentes registrados dentro de la empresa.

Los reportes internos entre junio y octubre de 2024 evidencian un incremento sostenido en fallas de servidores, lentitud en consultas y errores derivados de configuraciones deficientes. Los incidentes más frecuentes incluyen entre tres y seis caídas mensuales por fallas de hardware, hasta doce reportes de lentitud en operaciones críticas y múltiples interrupciones asociadas a accesos lógicos o a saturación de usuarios concurrentes en plataformas como GESREST y 360.SIS. En 2025, los registros muestran patrones similares: caídas recurrentes del servidor de monitoreo, errores en configuraciones de software y reclamos constantes por procesos de personalización, todo ello agravado por el aumento en la adopción de los sistemas mencionados.

Sin embargo, el conjunto de problemas operativos se ve acompañado por un riesgo aún mayor: la persistente debilidad en los mecanismos de seguridad de la información. A pesar de que desde 2020 se evidenció la gravedad de esta situación —cuando un colaborador sustrajo y divulgó información confidencial de un cliente— la empresa no implementó medidas correctivas estructurales que fortalecieran los procesos de control. El crecimiento reciente ha ampliado esta vulnerabilidad, pues los sistemas manejan cada vez más información sensible de clientes de sectores como gastronomía, hotelería, salud y comercio.

En la dimensión física, continúan existiendo accesos sin control a áreas críticas, acompañados de manipulación inapropiada de equipos tecnológicos. En la dimensión lógica, la ausencia de una adecuada segmentación de privilegios permite a usuarios acceder y modificar información sin restricciones. Además, la administración de credenciales carece de procedimientos formales: cuentas de exempleados siguen activas, las contraseñas se comparten y no existen procesos sistemáticos de baja o desactivación.

A esto se suma la falta de segmentación en los repositorios de datos, lo cual permite que cualquier usuario pueda acceder a información corporativa de alto nivel, incrementando la exposición a vulnerabilidades, errores o accesos indebidos. El crecimiento de la empresa, lejos de venir acompañado por una madurez organizacional en materia de seguridad y control, ha desbordado la capacidad operativa del equipo técnico, generando un aumento significativo de los riesgos.

Con base en estos hechos, la problemática central radica en que GarzaSoft enfrenta una expansión acelerada sin un sistema de gestión de seguridad y control que acompañe su crecimiento. La empresa opera con vulnerabilidades físicas y lógicas, inconsistencias en la administración de usuarios y deficiencias en el mantenimiento de su infraestructura, lo cual pone en riesgo la continuidad de sus servicios, la integridad de los datos procesados y la confianza de su base creciente de clientes. Esta situación evidencia la necesidad urgente de realizar una investigación orientada a analizar estas deficiencias y proponer un marco de gestión integral que permita fortalecer la seguridad, la operatividad y la madurez tecnológica de la organización.

A partir de la problemática identificada en GarzaSoft, marcada por el incremento de incidencias operativas y de seguridad debido al crecimiento acelerado de la empresa y a la ampliación de su cartera de clientes a través de sus productos GESREST, 360.SIS, Hotel HUB, Pulso y Comprobante-e, se configura un escenario que exige comprender y mejorar de manera urgente la gestión de riesgos de TI. En este contexto surge la pregunta de

investigación, orientada a resolver la causa estructural del problema: **¿Cómo puede la implementación de un modelo basado en la norma ISO/IEC 27001 contribuir a reducir los riesgos operativos y de seguridad de la información en GarzaSoft, considerando su expansión empresarial y el aumento del uso de sus plataformas tecnológicas?** Esta pregunta conduce al planteamiento de la hipótesis, entendida como una proposición que anticipa la solución al problema: **Si GarzaSoft implementa un modelo de gestión de seguridad de la información alineado con ISO/IEC 27001, entonces logrará mitigar significativamente los riesgos de TI asociados a su crecimiento, optimizar sus procesos operativos y fortalecer la protección de los datos administrados por sus productos de software**.

El objetivo general de la investigación se orienta a **proponer un modelo de gestión de seguridad de la información basado en ISO/IEC 27001 para disminuir los riesgos operativos y de seguridad que enfrenta GarzaSoft en sus servicios y plataformas tecnológicas**. Este propósito se despliega en objetivos específicos que guían el proceso investigativo: diagnosticar el nivel actual de madurez en la gestión de la seguridad de la información en la Garzasoft; identificar los escenarios de riesgo críticos asociados a la operación de la Garzasoft; estimar el nivel de riesgo inherente para los escenarios de riesgo identificados; y proponer un Plan de tratamiento de riesgos, adaptable a las necesidades y capacidades de GarzaSoft.

La justificación de la investigación se plantea desde las siguientes perspectivas: Desde la **pertinencia**, el estudio responde a una necesidad real y urgente, ya que la empresa ha mostrado un incremento de incidentes relacionados con fallas operativas, errores humanos y carencias en los controles de seguridad, situación agravada por la expansión de su portafolio de soluciones tecnológicas y la creciente demanda de sus clientes. La implementación de un modelo de seguridad no solo es necesaria, sino estratégica para garantizar la continuidad del negocio, proteger datos sensibles y mantener la confianza del mercado.

En cuanto al **aporte teórico**, la investigación contribuye al campo de la gestión de seguridad de la información al ofrecer un análisis contextualizado sobre los desafíos que enfrentan empresas de software en crecimiento dentro del entorno peruano. Además, propone una adaptación de la norma ISO/IEC 27001 aplicada a una empresa con múltiples líneas de productos, lo que amplía la discusión académica sobre modelos de implementación flexibles y escalables.

Desde el **aporte práctico**, el estudio generará una propuesta concreta y aplicable para GarzaSoft, permitiéndole fortalecer sus procesos internos, reducir vulnerabilidades, mejorar la

calidad de sus servicios SaaS y sistemas en producción y, en general, elevar su nivel de seguridad frente a incidentes como accesos indebidos, errores de configuración, fallas de infraestructura y riesgos asociados a la operación. Asimismo, la propuesta servirá como guía operativa para empresas similares en el sector tecnológico que enfrentan problemas derivados del crecimiento acelerado y la ausencia de políticas formales de gestión de riesgos.

DISEÑO TEÓRICO

2.1. Antecedentes de la investigación

En la tesis “Implementación de la Metodología MAGERIT V3 para mejorar la Gestión de Riesgos de Seguridad de la Información y propuesta de Políticas de Seguridad basadas en Norma Técnica Peruana ISO/IEC 27001:2014 en la Dirección Regional de Trabajo y Promoción del Empleo de Huánuco – 2021” desarrollada por Rivera y Valdivia (2021), el problema tratado fue la gestión ineficaz de los riesgos de la seguridad de la información dentro de la Dirección Regional de Trabajo, evidenciada por la falta de un enfoque metodológico estandarizado para identificar, analizar y tratar las amenazas y vulnerabilidades que afectaban sus activos de información. El propósito principal de la investigación fue determinar cómo la implementación de MAGERIT V3 y la NTP-ISO 27001:2014 mejora la gestión de riesgos de la seguridad de la información. Los principales fundamentos teóricos aplicados fueron el ciclo Planificar-Hacer-Verificar-Actuar (PHVA) de la ISO 27001 y los pasos detallados de la metodología MAGERIT V3 para la gestión de riesgos. El método de investigación fue de tipo Aplicada con un diseño Pre-Experimental, utilizando la recolección de datos y la validación estadística de hipótesis (prueba T de Student). El principal resultado fue la conclusión de que la aplicación de la metodología MAGERIT V3 y la norma ISO 27001 mejora significativamente la gestión de riesgos de la seguridad de la información, comprobada mediante un valor $p < 0.05$.

En la tesis “Modelo de gestión de riesgos de TI que contribuye en la protección de los activos de información en una empresa de servicios informáticos” de Llontop (2018), el problema central que abordó la investigación fue la suspensión recurrente de servicios primordiales del negocio debido a la falta de un modelo de gestión de riesgos implementado, evidenciando vulnerabilidades y la ausencia de políticas de seguridad frente a desastres. El propósito de la tesis fue diseñar un modelo de gestión de riesgos de TI que contribuyera a la protección de los activos de información y compensara la ausencia de políticas ante riesgos de TI. Los fundamentos teóricos aplicados fueron los estándares internacionales ISO 17799 (antecesor de ISO 27002), ISO 27001 y la metodología MAGERIT, que proporcionaron el marco para la gestión y análisis de riesgos. El método de la investigación fue de tipo Descriptivo-Propositivo. El resultado principal fue la validación del modelo propuesto, demostrando que su implementación permite identificar, evaluar y tratar los riesgos de manera eficaz, mejorando la continuidad de los servicios y la protección de los activos en la empresa de servicios informáticos (desarrollo de software).

La tesis, titulada "Modelo para la gestión de riesgos de desarrollo de software bajo la perspectiva de la gestión de proyectos" (Sernaque, 2022), abordó el problema de la falta de un enfoque sistemático y estandarizado para la gestión de riesgos en proyectos de desarrollo de software, lo que incrementaba las probabilidades de fallas, sobrecostos y retrasos. El propósito central fue diseñar un modelo de gestión de riesgos específico para el desarrollo de software que utilizara la metodología MAGERIT y los requisitos de la norma ISO/IEC 27000. El fundamento teórico clave fue la integración de la GSI (ISO/IEC 27000) con la gestión de riesgos (MAGERIT) en el marco de la gestión de proyectos, utilizando un método de investigación aplicada, descriptiva y no experimental con enfoque cualitativo. La principal conclusión fue que el modelo propuesto, validado por expertos, permite identificar, evaluar y gestionar los riesgos asociados al desarrollo de software de manera efectiva, optimizando la toma de decisiones y reduciendo costos relacionados.

Con el título "Diseño de un Sistema de Gestión de Seguridad de Información basado en la norma ISO/IEC 27001:2013 para una empresa de producción de software" la tesis de (Cajusol & Chinchay, 2020) se centró en la problemática de la vulnerabilidad de los activos de información y los sistemas en una empresa de desarrollo y producción de software, lo que comprometía la confidencialidad e integridad de sus productos y datos. El objetivo fue diseñar una propuesta formal de SGSI siguiendo los lineamientos de la norma ISO/IEC 27001, utilizando la metodología MAGERIT para el análisis de riesgos. Los fundamentos aplicados fueron la estructura del Ciclo PDCA (Planificar, Hacer, Verificar, Actuar) de la ISO 27001 y las fases de identificación y valoración de MAGERIT; se empleó una metodología de investigación de tipo proyectiva y no experimental. Como principal resultado, se presentó el diseño de un SGSI completo, incluyendo el Plan de Tratamiento de Riesgos con controles específicos de la ISO 27002, demostrando que la integración de ambas herramientas proporciona un marco robusto para la protección integral de la información.

La tesis, titulada "Desarrollo de un modelo de gestión de riesgos basado en la metodología MAGERIT para minimizar los riesgos de la implantación y uso de TI en una Municipalidad del Perú" (Mogollon, 2023), abordó la inadecuada gestión y mitigación de los riesgos derivados del uso e implantación de las Tecnologías de la Información en una entidad pública, afectando la continuidad operativa y la seguridad de los datos ciudadanos. El objetivo general fue desarrollar un modelo de gestión de riesgos utilizando la metodología MAGERIT y alineándolo con los principios de seguridad de la ISO 27000 para minimizar los riesgos de TI. Los fundamentos teóricos principales fueron las políticas de GSI y las pautas para el análisis de riesgos de MAGERIT v3; la investigación fue de tipo cuantitativa y descriptiva, con un diseño no experimental y un enfoque propositivo. La conclusión más destacada fue que el

modelo propuesto de gestión de riesgos permitió categorizar y priorizar 15 activos de TI, identificando 26 amenazas y logrando, a través del tratamiento del riesgo, reducir significativamente el nivel de riesgo en la municipalidad.

La tesis "Sistema gestor de seguridad de la información para reducir incidencias en activos de TI en la empresa MP Constructores SAC 2021" de (Huamán, 2023), identificó como problema principal las incidencias repetitivas en el área de licitaciones de la empresa (un área crítica que maneja información sensible y de alto impacto), lo que generaba pérdida de datos, interrupción de operaciones y vulnerabilidades en los activos de TI. El propósito fue implementar un sistema gestor de seguridad de la información (SGSI) basado en ISO 27000 y utilizando MAGERIT para la identificación y evaluación de riesgos, logrando así reducir las incidencias. La tesis aplicó los marcos de ISO 27000 para alinear a la organización a requisitos normativos y MAGERIT para el análisis de riesgos; se utilizó un método de investigación aplicada con un enfoque cuantitativo y un diseño cuasiexperimental para comparar el antes y después de la implementación. Los resultados arrojaron que, tras la aplicación del SGSI y los controles derivados, se logró una reducción significativa en el número de incidencias registradas y en las vulnerabilidades de los activos de TI identificados.

2.2. Fundamentos teóricos

2.2.1. Seguridad de la información

La seguridad de la información es entendida como la protección de los activos informacionales frente a amenazas que puedan comprometer su confidencialidad, integridad y disponibilidad (ISO/IEC 27000, 2018). Como afirma Solms y Niekerk (2013), *"la seguridad de la información ya no es un lujo, sino una necesidad estratégica para cualquier organización que opere en ecosistemas digitales"* (p. 73).

Estos tres principios, llamados "tríada CIA", constituyen la base para el diseño de controles y políticas, y son especialmente importantes en empresas como Garzasoft, donde los sistemas procesan información transaccional, datos de salud, información tributaria y registros sensibles de clientes.

Una definición más ampliamente aceptada sostiene lo siguiente:

"La seguridad de la información preserva la confidencialidad, integridad y disponibilidad de la información; adicionales propiedades como autenticidad, responsabilidad, trazabilidad y confiabilidad pueden también estar involucradas" (*ISO/IEC 27000:2018, sección 3.28*).

2.2.2. Gestión de la Seguridad de la Información (GSI)

La Gestión de la Seguridad de la Información (GSI) implica la creación de un conjunto organizado de políticas, procedimientos, roles y controles cuyo propósito es proteger los activos de información (Von Solms & Van Niekerk, 2013). La GSI se sustenta en la idea de que la seguridad debe gestionarse de manera sistemática, continua y documentada, un principio también recogido en la norma ISO/IEC 27001.

Según Calder (2022), *"la seguridad de la información efectiva no depende únicamente de la tecnología, sino de la gestión coherente de personas, procesos y controles"* (p. 45). Esto tiene implicancias directas en Garzasoft, donde los incidentes están asociados no solo a fallas técnicas sino también a errores humanos, malas prácticas de acceso y ausencia de políticas.

2.2.3. La familia de normas ISO/IEC 27000 y el ciclo PDCA

La familia ISO/IEC 27000 establece una estructura sistemática para gestionar la seguridad de la información, siendo ISO/IEC 27001 la norma central que define los requisitos del Sistema de Gestión de Seguridad de la Información (SGSI). La implementación de esta norma se sustenta en el **ciclo PDCA (Plan–Do–Check–Act)**, un modelo de mejora continua definido originalmente por Deming y aplicado ampliamente en sistemas de gestión (ISO/IEC 27001, 2022).

El ciclo PDCA aplicado a la gestión del riesgo integra actividades estratégicas y operativas para evaluar, controlar y mejorar la seguridad. Según ISO/IEC 27001 (2022), el SGSI debe implementarse de forma iterativa para adaptarse a amenazas emergentes y cambios organizacionales.

A continuación se describe cada fase y sus actividades clave, destacando aquellas relacionadas con la gestión del riesgo:

Fase PLAN (Planificar)

Implica comprender el contexto de la organización, identificar los activos, determinar los riesgos y planificar los controles. Incluye:

1. Definir el **alcance del SGSI**.
2. Identificar y clasificar activos de información.
3. Realizar **evaluación de riesgos**, siguiendo normas como ISO/IEC 27005 o metodologías como MAGERIT.
4. Determinar el **grado de aceptabilidad del riesgo**.
5. Elaborar un **Plan de Tratamiento de Riesgos (PTR)**.

Según Calder y Watkins (2015): *"La fase de planificación determina la solidez del SGSI, pues define el alcance de protección y la estrategia para administrar los riesgos"* (p. 87).

Fase DO (Hacer o Implementar)

En esta fase se ejecutan los controles seleccionados:

- Implementación de controles del Anexo A de ISO/IEC 27001 o ISO/IEC 27002.
- Desarrollo de procedimientos específicos: control de accesos, respaldos, gestión de incidentes, seguridad física.
- Capacitación y concientización del personal.

Humphreys (2016) señala que *"la implementación debe ser coherente con la evaluación de riesgos, de modo que los controles tengan relación directa con los riesgos identificados"* (p. 52).

Fase CHECK (Verificar)

Comprende la verificación del desempeño del SGSI mediante:

- Auditorías internas.
- Revisión de incidentes.
- Análisis de registros y métricas de seguridad.
- Evaluación periódica del riesgo.

ISO/IEC 27001 (2022) establece que la organización debe *"supervisar, medir, analizar y evaluar el SGSI"* (cláusula 9).

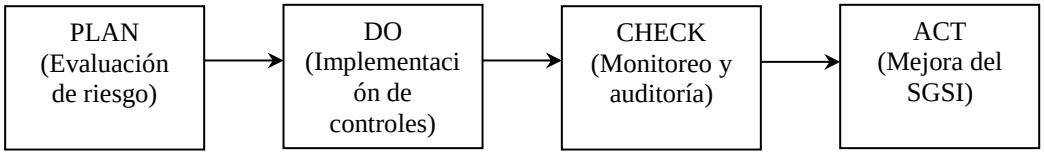
Fase ACT (Actuar o Mejorar)

Consiste en aplicar acciones correctivas y mejorar el SGSI con base en:

- Resultados de auditorías.
- Hallazgos de incidentes.
- Cambios en el entorno tecnológico.
- Nuevas amenazas identificadas.

De acuerdo con ISO/IEC 27001 (2022), *"la mejora continua es esencial para mantener la eficacia del SGSI frente a amenazas cambiantes"*.

Figura 1. Ciclo PDCA aplicado a la gestión de riesgos en un SGSI



Nota. Adaptado de ISO/IEC 27001 (2022).

Según la norma ISO/IEC 27001 (2022):

"El propósito de este documento es proporcionar requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información" (*ISO/IEC 27001:2022, Introducción*).

A. ISO/IEC 27001: Requisitos del SGSI

ISO/IEC 27001 establece un marco de trabajo estructurado bajo el ciclo PDCA (Plan-Do-Check-Act). Según Humphreys (2016), la norma *"proporciona la arquitectura completa para un sistema que no solo protege, sino que evoluciona con la organización"* (p. 21).

Sus requisitos principales incluyen:

- Establecer y documentar un SGSI
- Realizar evaluación de riesgos
- Definir el plan de tratamiento
- Implementar controles
- Realizar auditorías internas
- Revisar y mejorar el sistema

B. ISO/IEC 27002: Controles de seguridad

ISO/IEC 27002 complementa la 27001 con un conjunto de controles para gestionar los riesgos identificados. Los dominios abarcan políticas, organización, activos, seguridad física, seguridad en redes, criptografía, operaciones, desarrollo de software, continuidad del negocio y relación con proveedores (ISO/IEC 27002, 2022).

El estándar señala que:

"Los controles especificados en este documento representan buenas prácticas reconocidas internacionalmente para la gestión de la seguridad de la información" (*ISO/IEC 27002:2022, Prefacio*).

2.2.4. Metodología MAGERIT

La metodología MAGERIT (Ministerio de Hacienda y Función Pública, 2012) es un marco para el análisis y gestión de riesgos de los sistemas de información, ampliamente utilizado por instituciones públicas y privadas. Su enfoque es altamente sistemático y permite evaluar los riesgos en función de activos, amenazas, vulnerabilidades e impactos.

De acuerdo con MAGERIT:

"El objetivo es proporcionar un método que permita analizar los riesgos a los que está expuesto un sistema de información, determinar su magnitud y ayudar en la decisión de afrontarlos" (*MAGERIT v.3, 2012, p. 5*).

A. Etapas de la metodología MAGERIT

MAGERIT está dividido en tres grandes fases:

I. Análisis de Riesgos

Incluye:

- **Identificación de activos:** se establecen los elementos de valor, como datos, hardware, software, servicios, personal y documentación.
- **Valoración de activos:** asignación de importancia mediante valores de confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad.
- **Identificación de amenazas:** se enumeran los eventos que pueden afectar negativamente los activos.
- **Identificación de vulnerabilidades:** se **determinan** las debilidades explotables.

II. Valoración del Riesgo

Implica combinar impacto y probabilidad para determinar el nivel de riesgo.

III. Tratamiento del Riesgo

Incluye:

1. **Reducir el riesgo (Risk Mitigation).** Consiste en disminuir la probabilidad de ocurrencia, el impacto del riesgo, o ambos, mediante la implementación de controles. Es la estrategia más utilizada en seguridad de la información.

ISO/IEC 27005 indica que *"La reducción del riesgo implica la implementación de controles para minimizar el nivel de riesgo hasta un nivel aceptable"* (ISO/IEC 27005, 2018, sección 8.4).

Algunos ejemplos de aplicación son:

- Implementar autenticación multifactor para reducir accesos no autorizados.
- Aplicar parches de seguridad para reducir vulnerabilidades técnicas.
- Realizar backups automáticos para reducir el impacto de pérdida de datos.
- Controlar privilegios para reducir errores o daños internos.

Se usa cuando el riesgo es significativo pero controlable mediante medidas técnicas, organizativas o físicas.

2. **Evitar el riesgo (Risk Avoidance).** Implica eliminar completamente la fuente del riesgo o suprimir la actividad que lo genera. No siempre es posible ni conveniente, pero puede ser necesario si el riesgo supera la tolerancia definida por la organización.

Según ISO 31000, "Evitar el riesgo significa decidir no iniciar o continuar la actividad que lo origina" (ISO 31000, 2018, p. 21).

Algunos ejemplos de aplicación son:

- No utilizar software obsoleto sin soporte (que aumenta riesgo de ataques).
- Eliminar un módulo inseguro del sistema hasta corregirlo.
- Deshabilitar accesos remotos si no existen mecanismos de autenticación seguros.

Se usa cuando el riesgo es extremo o crítico y no es viable mitigarlo con controles razonables.

3. Transferir el riesgo (Risk Transfer). Consiste en trasladar total o parcialmente el impacto del riesgo a un tercero, mediante contratos, seguros u otros acuerdos. No elimina el riesgo, sino que cambia quién asume las consecuencias económicas o de responsabilidad.

MAGERIT lo define como "Hacer que otra entidad asuma las consecuencias de la materialización del riesgo, bien sea mediante seguros o outsourcing" MAGERIT v3, 2012, p. 41).

Algunos ejemplos de aplicación son:

- Contratar un seguro contra ciberataques o interrupción de servicios.
- Externalizar el hosting a un proveedor con certificación ISO 27001.
- Delegar servicios de pagos electrónicos a un gateway certificado PCI-DSS.

Se usa cuando el riesgo es inevitable o difícil de controlar internamente, pero puede ser asumido por un proveedor especializado.

4. Aceptar el riesgo (Risk Acceptance). Ocurre cuando la organización decide asumir el riesgo tal como es, porque está dentro de su nivel de tolerancia o porque el costo de tratarlo es mayor que el beneficio.

ISO/IEC 27005 explica que:

"El riesgo residual puede ser aceptado si se encuentra dentro de los criterios de riesgo establecidos por la organización" (ISO/IEC 27005, 2018, sección 8.4.5).

Algunos ejemplos de aplicación son:

- Mantener un riesgo menor de indisponibilidad en horarios de baja actividad.
- Aceptar el riesgo de retrasos leves en reportes no críticos.
- Asumir riesgos con impacto mínimo en software no operativo.

Se usa cuando el riesgo residual es bajo, no justifica inversión adicional o la afectación es tolerable.

Tabla 1. Comparativa de las estrategias de tratamiento de riesgos

Estrategia	Acciones clave	Cuándo se usa
Reducir	Implementar controles para disminuir probabilidad o impacto	Cuando el riesgo es significativo pero controlable
Evitar	Eliminar la actividad o componente que genera el riesgo	Cuando el riesgo es extremo e inaceptable
Transferir	Contratar seguros, outsourcing, acuerdos de responsabilidad	Cuando un tercero puede gestionarlo mejor
Aceptar	Asumir el riesgo residual sin nuevas medidas	Cuando el riesgo es bajo o el costo de mitigarlo es mayor

Nota. Adaptado de ISO/IEC 27005 (2018), ISO 31000 (2018) y MAGERIT v3 (2012).

B. Clasificación de amenazas según MAGERIT

MAGERIT clasifica las amenazas en categorías que permiten una visión estructurada del riesgo. Entre ellas destacan:

Tabla 2. Categorización de las amenazas según MAGERIT

Categoría	Ejemplos
Naturales	Terremotos, inundaciones, tormentas
Accidentales	Errores humanos, fallas eléctricas, pérdidas de datos
Deliberadas	Ataques informáticos, sabotaje, malware
Ambientales	Extremos de temperatura, humedad
Lógicas	Acceso no autorizado, modificación de datos
Físicas	Robo de equipos, daños a infraestructura

Nota. Adaptado de MAGERIT v3 (2012).

C. Cálculo del nivel de riesgo en MAGERIT

MAGERIT utiliza una fórmula sencilla:

Riesgo = Impacto × Probabilidad

Ambos valores se clasifican generalmente como:

1. Muy baja
2. Baja
3. Media
4. Alta
5. Muy alta

A partir de estos valores se construye una Matriz de riesgo MAGERIT como la siguiente:

Tabla 3. Matriz de riesgo MAGERIT

Impacto \ Probabilidad	1 Muy baja	2 Baja	3 Media	4 Alta	5 Muy alta
1 Muy bajo	Muy Bajo	Bajo	Bajo	Moderado	Moderado
2 Bajo	Bajo	Bajo	Moderado	Moderado	Alto
3 Medio	Bajo	Moderado	Alto	Muy Alto	Crítico
4 Alto	Moderado	Alto	Muy Alto	Crítico	Crítico
5 Muy alto	Alto	Muy Alto	Crítico	Crítico	Crítico

Nota. Adaptado de la metodología MAGERIT (2012).

Como señala MAGERIT, “El análisis de riesgo permite una valoración numérica que facilita la comparación entre alternativas y la priorización de las actuaciones” (MAGERIT v3, 2012, p. 37).

2.2.5. Gestión de Activos de Información

La gestión de activos de información es un requisito fundamental tanto en ISO/IEC 27001 como en MAGERIT. La ISO/IEC 27002 (2022) señala que *"el inventario y clasificación de activos es esencial para asegurar su protección adecuada"*. Los activos incluyen hardware, software, datos, procesos, personal, documentación, redes y servicios en la nube.

Para Garzasoft, esto significa identificar activos como:

- Bases de datos de clientes
- Servidores cloud
- Aplicaciones en producción
- Código fuente
- Perfiles de usuario
- Información de transacciones y comprobantes electrónicos

2.2.6. Seguridad en el desarrollo de software

La seguridad en el ciclo de vida del software es un factor crítico en empresas como Garzasoft, debido a que sus sistemas (GESREST, 360.SIS, Hotel HUB, Pulso y Comprobante-e) están en producción permanente.

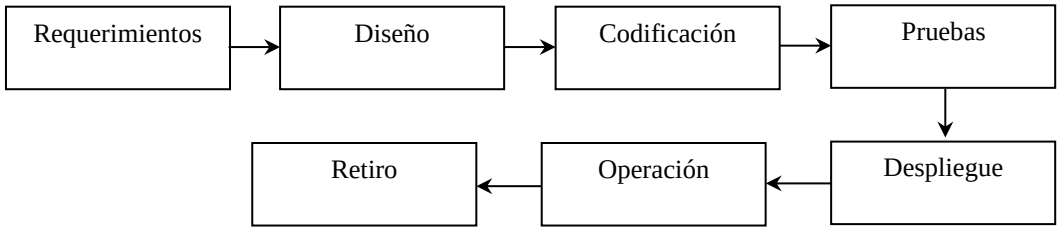
Según OWASP (2021): *"La seguridad debe estar integrada en todas las fases del ciclo de vida del software, desde el diseño inicial hasta las operaciones posteriores al despliegue"* (p. 14).

Aspectos clave para gestionar la seguridad del software, implica:

1. Requisitos de seguridad: definición de controles desde la fase de requerimientos.
2. Modelado de amenazas (Threat Modeling): identificación temprana de vectores de ataque.
3. Diseño seguro: aplicación de principios como mínimo privilegio, defensa en profundidad y separación de ambientes.
4. Codificación segura: prácticas como sanitización de entradas, manejo seguro de errores y control de sesiones.
5. Pruebas de seguridad:
   - Análisis estático (SAST)
   - Análisis dinámico (DAST)
   - Pentesting
6. Gestión de dependencias: revisión de librerías externas vulnerables.

7. Gestión de cambios y versiones: control del repositorio, revisión por pares.
8. Seguridad en el despliegue: ambientes separados, automatización segura.
9. Monitoreo continuo: uso de logs, alertas e indicadores clave.
10. DevSecOps: integración de seguridad en pipelines automatizados.

Figura 2. Seguridad en el ciclo de vida del desarrollo (SDLC)



Nota. Adaptado del modelo OWASP SAMM (2021).

2.3. Operacionalización de las variables de la investigación

2.3.1. Variable 1: Gestión de la Seguridad de la Información (GSI)

Definición conceptual:

Conjunto de políticas, procesos, herramientas, controles y prácticas destinadas a proteger la confidencialidad, integridad y disponibilidad de los activos de información de una organización (ISO/IEC 27000, 2018). Implica la planificación, implementación, monitoreo y mejora de mecanismos de seguridad alineados con un Sistema de Gestión de Seguridad de la Información (SGSI).

Definición operacional:

La evaluación de esta variable se realizará mediante un procedimiento diagnóstico orientado a determinar el nivel actual de madurez de la seguridad de la información en Garzasoft. Para ello, se analizarán diversas dimensiones que permiten obtener una visión integral del estado de los controles y prácticas organizacionales.

En primer lugar, se examinarán las **políticas y procedimientos de seguridad**, verificando su existencia, grado de formalización y nivel de cumplimiento. Este análisis se llevará a cabo mediante la revisión de documentos institucionales, tales como manuales internos, políticas aprobadas, reglamentos y directrices técnicas. También se realizará una contrastación entre la documentación existente y las prácticas observadas en el personal, con el fin de identificar discrepancias o vacíos normativos.

Posteriormente, se evaluará la **gestión de activos de información**, procedimiento que involucra identificar si la organización posee un inventario actualizado de hardware, software, datos, usuarios, accesos y componentes tecnológicos críticos. Se observará si dichos activos están clasificados según criterios de confidencialidad, integridad y disponibilidad, y si cuentan con responsables claramente designados. La información se recolectará mediante fichas de diagnóstico basadas en estándares como ISO/IEC 27001 e ISO/IEC 27002.

Continuando con el análisis, se revisará el **control de accesos**, lo cual incluye examinar los mecanismos de autenticación, la asignación de privilegios, la gestión del ciclo de vida de los usuarios y la existencia de mecanismos de monitoreo. A través de entrevistas con el personal técnico se determinará si los controles implementados son suficientes para prevenir accesos no autorizados o el uso indebido de credenciales.

En cuanto a la **seguridad en las operaciones**, se verificará la existencia de mecanismos de respaldo de información, actualización de software, aplicación de parches y monitoreo de los sistemas. Para esta dimensión se empleará observación directa de los procedimientos operativos y revisión de registros técnicos.

La dimensión de **seguridad física y ambiental** será evaluada mediante visitas a las zonas donde se ubican los equipos críticos, verificando la existencia de controles de acceso, mecanismos contra incendios, protección eléctrica, cámaras de vigilancia y otras medidas de resguardo. Se registrará cualquier vulnerabilidad que comprometa la infraestructura.

La **gestión de incidentes** se examinará mediante la revisión de registros históricos de problemas, fallas o incidentes detectados en la organización. Se considerarán tiempos de respuesta, mecanismos de registro y la existencia de procedimientos formales para el tratamiento de incidentes.

Finalmente, se evaluará la **continuidad del negocio**, verificando si la empresa cuenta con planes de contingencia, copias de seguridad fuera del sitio, análisis de impacto al negocio o procedimientos de recuperación ante desastres. Se contrastará la realidad operativa con los lineamientos establecidos por normas como ISO/IEC 22301 e ISO/IEC 27001.

2.3.2. Variable 2: Riesgos de Tecnologías de la Información

Definición conceptual:

Combinación de la probabilidad de que ocurra un evento relacionado con TI y sus consecuencias sobre los activos de información (ISO/IEC 27005, 2018). Incluye amenazas, vulnerabilidades, impactos y niveles de riesgo residual presentes en la infraestructura tecnológica.

Definición operacional:

La evaluación de esta variable se realizará aplicando la metodología MAGERIT, la cual permite analizar sistemáticamente los elementos que componen el riesgo. El proceso iniciará con la **identificación de activos**, para lo cual se recopilará información sobre bases de datos, aplicaciones, servidores, redes, usuarios privilegiados, servicios en la nube, documentos y cualquier otro elemento relevante. Cada activo será categorizado según su importancia y sus dependencias con otros activos del sistema.

Una vez identificados, se examinarán las **amenazas** a las que están expuestos los activos. Esto implica identificar eventos naturales, accidentales y deliberados que pudieran afectar los servicios. Se utilizarán listas de verificación basadas en MAGERIT v3, analizando amenazas como accesos indebidos, errores humanos, malware, fallas de software, interrupciones eléctricas, ataques externos, entre otras. La probabilidad de cada amenaza será estimada en una escala de cinco niveles.

Posteriormente, se evaluarán las vulnerabilidades, entendidas como debilidades que pueden ser explotadas por una amenaza. Para ello se revisarán configuraciones, prácticas de acceso, procedimientos operativos, dependencias de terceros, actualizaciones del sistema y resultados de auditorías previas. La vulnerabilidad se calificará también en términos de su frecuencia o grado de exposición.

Con los datos anteriores, se procederá a evaluar el impacto, el cual representará la magnitud del daño potencial sobre los activos críticos. Se valorará según los criterios de seguridad de la información (confidencialidad, integridad y disponibilidad) y se asignará un valor numérico dentro de una escala de cinco niveles que va desde “muy bajo” hasta “muy alto”.

Después de determinar el impacto y la probabilidad, se calculará el nivel de riesgo, utilizando la fórmula establecida por MAGERIT:

Riesgo = Probabilidad × Impacto,

el cual será ubicado dentro de la matriz 5×5 de riesgos elaborada para esta investigación. Finalmente, los riesgos identificados se clasificarán como bajos, moderados, altos, muy altos o críticos, lo cual servirá para priorizar su tratamiento y justificar la propuesta del modelo de gestión.

2.3.3. Variable 3: Modelo de Gestión ISO/MAGERIT

Definición conceptual:

Propuesta metodológica que integra los requisitos de ISO/IEC 27001, sus controles ISO/IEC 27002 y el proceso de análisis y valoración de riesgos de MAGERIT, con el fin de reducir los riesgos de TI y fortalecer el SGSI en una organización.

Definición operacional:

Dado que la investigación es de tipo descriptiva–propositiva, esta variable no se evalúa cuantitativamente. Su operacionalización consiste en diseñar un modelo ajustado a los hallazgos obtenidos en las dos variables descriptivas. El procedimiento consiste en:

- Analizar las brechas existentes entre Garzasoft y los requisitos de ISO/IEC 27001.
- Evaluar los controles de ISO/IEC 27002 necesarios para mitigar los riesgos detectados.
- Integrar los resultados del análisis MAGERIT en un plan de tratamiento.
- Elaborar procedimientos, políticas y diagramas del SGSI propuesto.

La variable se expresa como un producto final, no como un indicador medible.

Tabla 4. Operacionalización de Variables de la Investigación

Variable	Dimensión	Indicadores	Técnica de recolección	Instrumento	Escala
Gestión de la Seguridad de la Información	Políticas y procedimientos	Existencia de políticas; nivel de formalización; actualización	Análisis documental	Lista de verificación	Nominal / Ordinal
	Gestión de activos	Inventario de activos; clasificación de criticidad	Observación directa	Ficha de inventario	Ordinal
	Control de accesos	Gestión de credenciales; asignación de privilegios; autenticación	Entrevista semiestructurada	Guía de entrevista	Ordinal
	Seguridad en operaciones	Respaldo de datos; actualizaciones; monitoreo	Observación técnica	Checklist técnico	Ordinal
	Seguridad física y ambiental	Controles de acceso físico; protección eléctrica;	Inspección de campo	Guía de inspección	Nominal
	Gestión de incidentes	Registro de incidentes; tiempo de respuesta	Análisis documental	Matriz de incidentes	Ordinal
	Continuidad del negocio	Existencia de BCP/DRP; pruebas de recuperación	Revisión documental	Lista de verificación	Nominal
Riesgos de Tecnologías de la Información	Activos	Número y criticidad de activos	Análisis documental	Matriz de activos	Ordinal
	Amenazas	Tipos de amenazas identificadas	Observación técnica	Lista de amenazas	Ordinal
	Vulnerabilidades	Número y gravedad de vulnerabilidades	Auditoría técnica	Checklist técnico	Ordinal
	Impacto	Nivel de impacto 1–5	Evaluación MAGERIT	Matriz de impacto	Escala ordinal 1–5
	Probabilidad	Nivel de probabilidad 1–5	Evaluación MAGERIT	Matriz de probabilidad	Escala ordinal 1–5
	Nivel de riesgo	Clasificación del riesgo (bajo–crítico)	Análisis de riesgos	Matriz 5×5	Escala ordinal 1–5
Modelo de Gestión ISO/MAGERIT		Propuesta estructurada de controles y procesos	Análisis técnico	Documento técnico	No aplica

Nota. La variable propositiva no se operacionaliza cuantitativamente debido a la naturaleza del estudio (descriptivo–propositivo). La tabla se elaboró con base en lineamientos de las normas ISO/IEC 27001, ISO/IEC 27002 e ISO/IEC 27005, y la metodología MAGERIT v3.

DISEÑO METODOLÓGICO

2.4. Tipo de investigación

La presente investigación fue de tipo **descriptiva–propositiva**, ya que tuvo como propósito describir la situación actual de la gestión de la seguridad de la información y los riesgos de TI en la empresa Garzasoft, para posteriormente elaborar una propuesta de modelo basado en las normas ISO/IEC 27000 y la metodología MAGERIT. El estudio se enmarcó dentro de la tradición metodológica de investigaciones que, según Hernández, et.al. (2014), *"combinan la caracterización del fenómeno con el planteamiento de una solución aplicada"*.

Asimismo, se trató de una investigación **no experimental**, ya que no se manipuló ninguna variable, sino que se observaron los fenómenos tal como ocurrieron en su entorno natural. Debido a que se buscó explicar la situación problemática en un momento concreto, el estudio se desarrolló bajo un diseño **transversal**, recolectando los datos en un único periodo temporal.

2.5. Método de investigación

El método que guió esta investigación fue el **método descriptivo**, el cual permitió caracterizar el estado de la gestión de la seguridad de la información en Garzasoft, así como identificar las amenazas, vulnerabilidades, impactos y niveles de riesgo según la metodología MAGERIT. Este método resultó adecuado porque facilitó el análisis de las dimensiones e indicadores relacionados con la seguridad de la información, permitiendo documentar el estado real de los controles, procesos y prácticas de TI.

Complementariamente, para la construcción de la propuesta se empleó el **método propositivo**, el cual permitió integrar los hallazgos descriptivos con los lineamientos establecidos por ISO/IEC 27001, ISO/IEC 27002 y MAGERIT. Este método posibilitó elaborar un modelo aplicable a la organización, con procesos, controles y lineamientos alineados a la normativa internacional.

2.6. Diseño de contrastación de la hipótesis

El diseño de contrastación utilizado correspondió a un **diseño no experimental de tipo descriptivo–asociativo**, ya que la hipótesis planteada no buscó demostrar causalidad, sino comprobar si el análisis descriptivo de la gestión de seguridad de la información y de los riesgos de TI justificaba la pertinencia de la propuesta del modelo ISO/MAGERIT.

La hipótesis fue contrastada mediante:

1. **Diagnóstico descriptivo** del estado de la seguridad de la información en Garzasoft, utilizando instrumentos normados por ISO/IEC 27000 e ISO/IEC 27002.
2. **Evaluación de riesgos** siguiendo la metodología MAGERIT, utilizando matrices de activos, amenazas, vulnerabilidades y riesgos.
3. **Comparación de brechas** entre la situación encontrada y los requisitos mínimos de ISO/IEC 27001.

La hipótesis se consideró validada cuando las evidencias demostraron que la empresa presentaba niveles de riesgo elevados o críticos, así como importantes brechas en su SGSI, lo que justificó la necesidad de un modelo basado en ISO/IEC 27000 y MAGERIT.

2.7. Población y Muestra

La población estuvo conformada por:

1. Los sistemas de información desarrollados por Garzasoft (GESREST, 360.SIS, Hotel HUB, Pulso y Comprobante-e).
2. La infraestructura tecnológica (servidores, bases de datos, redes, servicios IaaS/SaaS).
3. El personal clave involucrado en la gestión de TI (desarrolladores, DevOps, soporte técnico y dirección).

Dado que la empresa está conformada por un número reducido de miembros y activos tecnológicamente heterogéneos, se utilizó un **muestreo censal**, evaluándose la totalidad de los elementos de la población. De esta manera, todos los activos, procesos y responsables fueron considerados en el estudio, garantizando la exhaustividad del diagnóstico.

2.8. Técnicas e instrumentos para el recojo de información

Se emplearon las siguientes técnicas:

- **Análisis documental**, para revisar políticas internas, manuales, reportes, registros e historial de incidentes.
- **Observación directa**, para evaluar prácticas operativas, configuraciones técnicas y controles físicos.
- **Entrevista semiestructurada**, aplicada al personal de TI para obtener información sobre procedimientos, prácticas y percepciones.
- **Auditoría técnica**, utilizada para identificar vulnerabilidades, evaluar activos y validar configuraciones.

Los instrumentos utilizados fueron:

- **Lista de verificación de controles ISO 27001/27002**, diseñada para evaluar la gestión actual de la seguridad.
- **Guía de observación técnica**, con criterios basados en MAGERIT v3.
- **Guía de entrevista**, aplicada al personal de TI y responsables de procesos.
- **Matrice MAGERIT (5×5)**:
- **Ficha de inventario de activos**, elaborada según ISO/IEC 27001 y 27002.

2.9. Procedimiento para el diseño, aplicación y procesamiento de la información

2.9.1. Diseño de los instrumentos

Los instrumentos fueron diseñados tomando como referencia los controles establecidos en ISO/IEC 27001 y ISO/IEC 27002, así como las guías metodológicas de MAGERIT v3. Durante su elaboración se definieron los indicadores, escalas y criterios de evaluación que permitieron medir el estado actual de la seguridad en Garzasoft.

2.9.2. Aplicación de los instrumentos

La aplicación de los instrumentos se realizó en tres etapas:

1. Recolección documental, donde se estudiaron los registros de incidentes, informes de TI, políticas internas y documentación técnica.
2. Trabajo de campo, consistente en la observación directa de servidores, redes, prácticas de acceso, configuraciones y ambientes físicos.
3. Entrevistas, en las que se indagó sobre prácticas internas, incidentes, debilidades percibidas y flujos de trabajo.

Todas las actividades se realizaron dentro de las instalaciones y ambientes tecnológicos de Garzasoft, con participación directa del personal responsable.

2.9.3. Procesamiento de la información

Una vez recolectada la información, se procedió a:

1. Clasificar y agrupar los datos según cada dimensión e indicador establecido en la operacionalización.
2. Evaluar los activos, amenazas y vulnerabilidades utilizando las matrices MAGERIT.
3. Calcular el nivel de riesgo, asignando puntajes de impacto y probabilidad en una escala 1–5.
4. Construir el mapa de riesgos, identificando los riesgos bajos, moderados, altos, muy altos y críticos.

5. Proponer un plan de tratamiento de riesgos en base a los resultados del análisis de riesgos.

RESULTADOS

3.1. Diagnóstico del nivel actual de madurez en la gestión de la seguridad de la información en la Garzasoft

3.1.1. Descripción general de la empresa Garzasoft

Garzasoft es una empresa peruana fundada en la ciudad de Chiclayo, especializada en el diseño, desarrollo e implementación de soluciones de software orientadas a la gestión empresarial. Desde su creación, la organización ha experimentado un crecimiento sostenido, ampliando su cartera de clientes en los sectores de gastronomía, comercio minorista, hotelería, salud y facturación electrónica.

Su portafolio de productos incluye sistemas propios ampliamente utilizados en la región norte del país, entre los que destacan:

- **GESREST**, plataforma integral para la gestión de restaurantes y negocios gastronómicos.
- **360.SIS**, sistema comercial para puntos de venta en minimarkets, ferreterías, boticas y negocios afines.
- **Hotel HUB**, solución de administración hotelera orientada a mejorar la experiencia del huésped.
- **Pulso**, plataforma de automatización y gestión de información para el sector salud.
- **Comprobante-e**, sistema de emisión de comprobantes electrónicos desde cualquier ubicación.

A nivel de infraestructura, Garzasoft opera bajo un modelo híbrido compuesto por servidores locales utilizados en etapas de desarrollo y pruebas, y servicios en la nube (principalmente AWS y Google Cloud) para la operación en producción de sus servicios SaaS e IaaS. La empresa utiliza herramientas de trabajo colaborativo como Jira y Git para la gestión de proyectos y control de versiones, respectivamente.

Su equipo técnico está conformado por desarrolladores, personal de calidad, soporte técnico y líderes de proyecto. Sin embargo, actualmente no cuenta con un área especializada de seguridad de la información ni un responsable dedicado exclusivamente a la gestión de riesgos tecnológicos, por lo que estas funciones recaen sobre el Gerente General, quien simultáneamente ejerce el rol de Gerente de TI.

Garzasoft se encuentra en una etapa de expansión y modernización, buscando integrar soluciones basadas en inteligencia de negocios, inteligencia artificial y análisis de datos. Este crecimiento, junto con la naturaleza crítica de los servicios que ofrece a sus clientes, ha generado la necesidad urgente de implementar un enfoque sistemático de gestión de la seguridad de la información alineado con normas internacionales como ISO/IEC 27001 y metodologías de análisis de riesgos como MAGERIT.

3.1.2. Descripción del objeto de estudio

El objeto de estudio de la presente investigación es la empresa Garzasoft, dedicada al desarrollo y comercialización de soluciones de software empresarial. Su actividad principal se centra en la creación de sistemas de información orientados a la administración de procesos críticos de restaurantes, comercios minoristas, hoteles, clínicas y empresas que requieren la emisión de comprobantes electrónicos.

El estudio se enfoca en analizar y mejorar la **Gestión de la Seguridad de la Información** dentro de Garzasoft, considerando que la empresa opera servicios clave bajo modelos SaaS y utiliza infraestructura híbrida en la nube y local. El entorno tecnológico de Garzasoft involucra activos críticos tales como bases de datos, código fuente, repositorios en la nube, credenciales privilegiadas, documentación técnica y servicios productivos utilizados diariamente por clientes.

El crecimiento acelerado de la organización y la ampliación de su cartera de clientes han incrementado la complejidad operacional y los niveles de riesgo asociados a la gestión de la información. En este contexto, la seguridad ha pasado a ser un elemento esencial para garantizar la continuidad del negocio, la protección de los datos y el cumplimiento de compromisos comerciales.

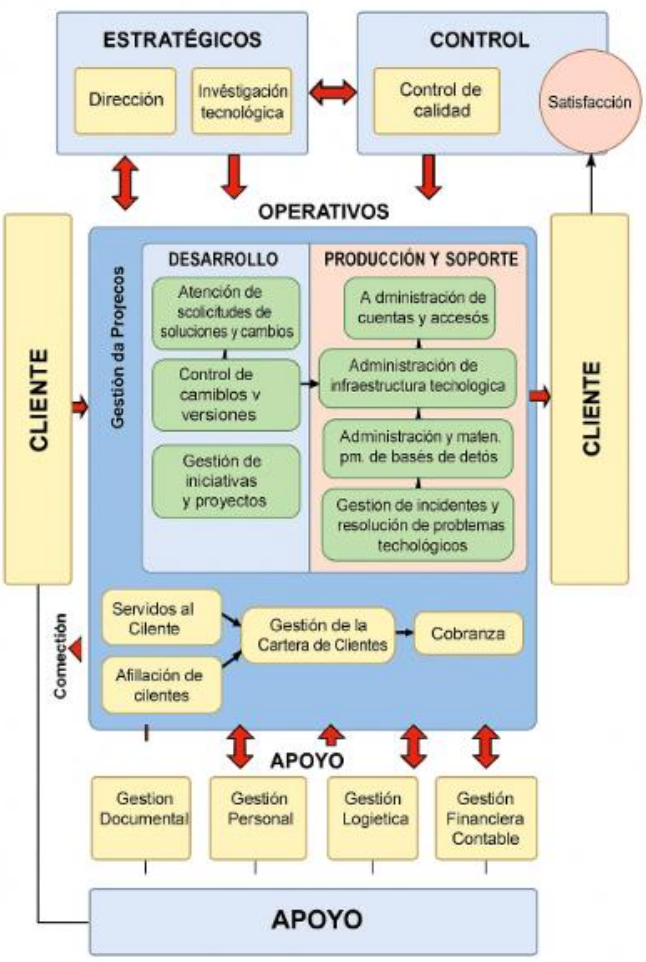
Por ello, el objeto de estudio contempla la revisión de procesos misionales —desarrollo de software, gestión de infraestructura, soporte técnico y operación en producción— a fin de identificar brechas existentes frente a las buenas prácticas definidas por la familia de normas ISO/IEC 27000 y la metodología MAGERIT. El análisis realizado permitirá diseñar una propuesta de modelo de gestión de la seguridad de la información que responda a las necesidades reales de la empresa y que fortalezca su capacidad para enfrentar riesgos tecnológicos y cibernéticos.

3.1.3. Identificación de los procesos en Garzasoft

Para establecer el alcance de la seguridad de la información en Garzasoft, se realizó un análisis descriptivo de sus procesos de negocio y tecnológicos, mediante el mapeo de los procesos de TI y los flujos operativos principales. Este mapeo permitió identificar subprocesos, interrelaciones internas y dependencias con entidades externas, lo cual constituyó la base para la posterior identificación de activos críticos y la evaluación de controles de seguridad en todas las dimensiones.

La identificación y análisis de procesos se ejecutó utilizando entrevistas semiestructuradas y observación directa en los entornos operativos, en colaboración con los líderes de proyecto, desarrolladores y personal de soporte técnico de Garzasoft. A partir de ello, se elaboró en Mapa General de Procesos de la empresa.

Figura 3. Mapa general de procesos de Garzasoft



Sus procesos se agrupan en cuatro categorías: procesos estratégicos, procesos operativos o misionales, procesos de apoyo y procesos de control. Dado que la investigación se centra en la **gestión de la seguridad de la información**, el alcance se estableció sobre los **procesos operativos** que involucran activos de información críticos y actividades con riesgo tecnológico elevado.

Los procesos misionales de Garzasoft se dividen en:

- Desarrollo
- Producción y Soporte de TI

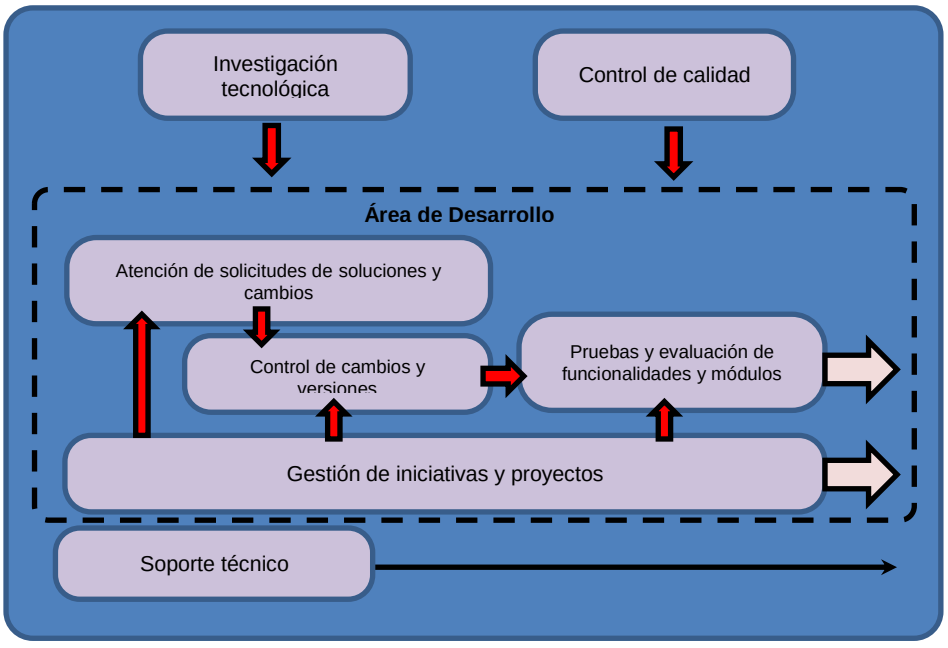
Estos procesos constituyen el núcleo operativo de la empresa y son los más relevantes para evaluar políticas de seguridad, control de accesos, seguridad en operaciones, seguridad física, gestión de incidentes y continuidad del negocio.

1. Proceso de Desarrollo

El proceso de Desarrollo, tiene como subprocesos a:

- Atención de solicitudes de soluciones y cambios
- Control de cambios y versiones
- Pruebas y evaluación de funcionalidades y módulos
- Gestión de iniciativas y proyectos
- Soporte técnico

Figura 4. Subprocesos del Proceso de Desarrollo



El Área de Desarrollo es el componente principal donde se crean, mantienen y actualizan todos los sistemas comerciales ofrecidos por Garzasoft: GESREST, 360.SIS, Hotel HUB, Pulso y Comprobante-e.

Este proceso involucra activos críticos como: código fuente, repositorios, credenciales, documentación técnica, bases de datos de prueba y entornos de desarrollo.

Por ello, constituye un eje central para evaluar las dimensiones de **gestión de activos**, **control de accesos**, **seguridad en operaciones**, y **políticas y procedimientos**. A continuación se presenta la relación de los subprocesos de Desarrollo con la seguridad de la información:

Tabla 5. Procesos y subprocesos del Área de Desarrollo en Garzasoft

Subprocesos	**Relación con la seguridad de la información**
Atención de solicitudes de soluciones y cambios	Requiere gestión documental, control de versiones y trazabilidad para evitar modificaciones no autorizadas.
Control de cambios y versiones	Necesita políticas de permisos, registros de auditoría y trazabilidad para prevenir alteraciones indebidas.
Pruebas y evaluación de funcionalidades y módulos	Contribuye a identificar fallas, vulnerabilidades y riesgos operativos antes de liberar componentes.
Gestión de iniciativas y proyectos	Se relaciona con la gestión de riesgos, cumplimiento de políticas y formalización de procedimientos.
Soporte técnico	Impacta la disponibilidad, el manejo de incidentes y la continuidad operativa del servicio.

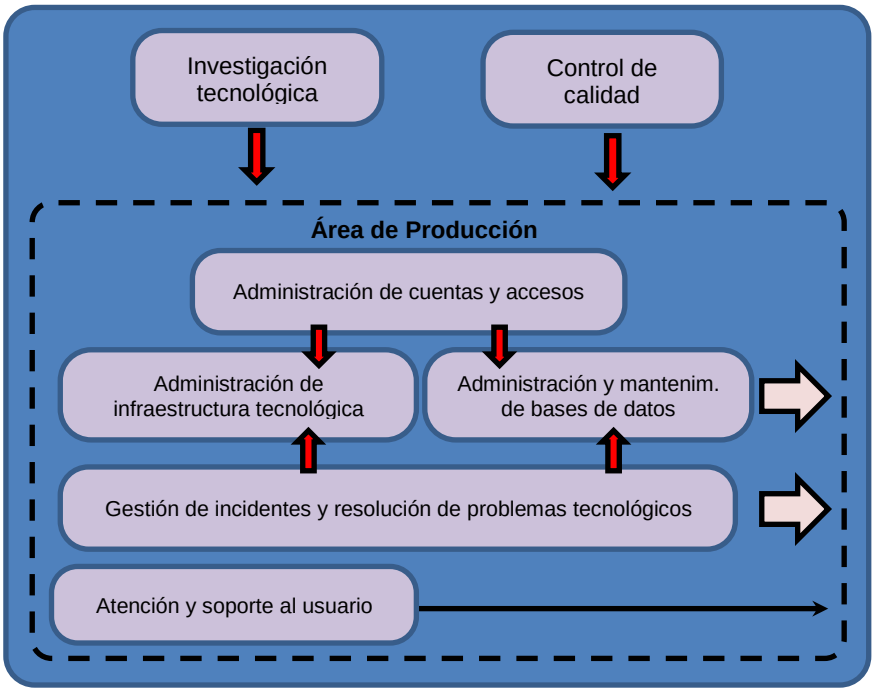
Nota: Elaboración basada en entrevistas y observación directa.

2. Proceso de Producción y Soporte de TI

El proceso de Desarrollo, tiene como subprocesos a:

- Administración de cuentas y accesos
- Administración de infraestructura tecnológica
- Administración y mantenimiento de bases de datos
- Gestión de incidentes y resolución de problemas tecnológicos
- Atención y soporte al usuario

Figura 5. Subprocesos del Proceso de Producción y Soporte de TI



El Área de Producción administra los entornos donde se ejecutan los sistemas de los clientes, representando el mayor nivel de criticidad operacional. Involucra servidores locales, servicios en la nube (AWS/Google Cloud), bases de datos, redes y credenciales privilegiadas.

Estos procesos se vinculan directamente con la Gestión de activos, Control de accesos, Seguridad en operaciones, Seguridad física y ambiental, Gestión de incidentes y Continuidad del negocio.

A continuación se presenta la relación de los subprocesos de Producción y Soporte de TI con la seguridad de la información:

Tabla 6. Procesos y subprocesos del Área de Producción y Soporte TI en Garzasoft

Subprocesos	Relación con la Seguridad de la Información
Administración de cuentas y accesos	Fundamental para el control de accesos, segregación de funciones y prevención de accesos no autorizados.
Administración de infraestructura tecnológica	Garantiza la seguridad operativa mediante configuraciones adecuadas, protección de red, actualizaciones y medidas antimalware.
Administración y mantenimiento de bases de datos	Impacta la disponibilidad, integridad y confidencialidad de la información, incluyendo respaldos y controles de acceso.
Gestión de incidentes y resolución de problemas tecnológicos	Permite detectar, registrar, analizar y responder a incidentes de seguridad, reduciendo riesgos y tiempos de exposición.
Atención y soporte al usuario	Contribuye a la continuidad operativa, manejo adecuado de incidentes y refuerzo de buenas prácticas de seguridad.

Nota: Elaboración basada en entrevistas y observación directa.

Garzasoft posee una estructura de procesos donde el Área de Desarrollo y el Área de Producción están estrechamente interrelacionadas. Los flujos de trabajo muestran que cualquier cambio en el código, repositorios o entornos de prueba impacta directamente en producción, lo que aumenta la necesidad de implementar un SGSI que garantice:

a. Trazabilidad
b. control de versiones
c. restricciones de acceso
d. separación de ambientes
e. mecanismos formales de registro de incidentes
f. continuidad operativa

3.1.4. Evaluación de la gestión de la seguridad de la información

La evaluación de la Gestión de la Seguridad de la Información en Garzasoft se realizó con la finalidad de determinar el nivel de madurez de sus controles, procesos y prácticas internas frente a los pilares de confidencialidad, integridad y disponibilidad establecidos por la familia de normas ISO/IEC 27000.

Los resultados obtenidos permitieron identificar brechas, vulnerabilidades y oportunidades de mejora en siete dimensiones clave: políticas y procedimientos, gestión de activos, control de accesos, seguridad en operaciones, seguridad física y ambiental, gestión de incidentes y continuidad del negocio.

A continuación se presenta la evaluación detallada por cada dimensión.

A. Evaluación de políticas y procedimientos

El propósito de esta evaluación fue determinar si Garzasoft contaba con políticas y procedimientos formalizados, actualizados y alineados a ISO/IEC 27001, capaces de guiar la gestión segura de la información en sus procesos de desarrollo, operación y soporte tecnológico.

Se aplicó un análisis documental revisando los manuales internos, lineamientos operativos, procedimientos de desarrollo y estándares utilizados por la empresa. Asimismo, se realizaron entrevistas con el Gerente y los líderes de proyecto.

La lista de verificación se basó en la ISO/IEC 27001 y 27002, obteniendo los siguientes resultados:

Tabla 7. Resultados de la evaluación de políticas y procedimientos de seguridad

Ítem evaluado	Cumple	No cumple
Existencia de una Política de Seguridad formal	0%	100%
Actualización periódica de políticas	0%	100%
Existencia de procedimientos de desarrollo seguro	20%	80%
Procedimientos de control de versiones	60%	40%
Documentación técnica actualizada	40%	60%
Procedimientos de pruebas y QA	50%	50%

La empresa mostró una ausencia casi total de políticas formales de seguridad de la información. Aunque existían prácticas operacionales, estas eran informales, no documentadas y basadas en experiencia individual. Esta situación representa una brecha crítica, ya que la falta de lineamientos normativos impide asegurar la coherencia de las actividades de seguridad.

B. Evaluación de la gestión de activos de información

El objetivo de esta evaluación fue determinar si Garzasoft contaba con un registro adecuado de sus activos de información críticos y si existía un mecanismo de clasificación por importancia y criticidad.

Mediante observación directa, revisión de repositorios, inspección de servidores y entrevistas técnicas, se identificaron los activos de información y se verificó la existencia de clasificadores internos. La ficha de inventario de activos fue construida según ISO/IEC 27001.

Tabla 8. Resultados de la evaluación de la gestión de activos de información

Ítem evaluado	Resultado
Inventario formal de activos	No existe
Inventario parcial no actualizado	Sí
Clasificación por criticidad	No
Asignación de propietarios de activos	Parcial
Identificación de dependencias técnicas	Parcial

Se identificaron 24 activos críticos sin documentación formal. Garzasoft posee conocimiento tácito de sus activos, pero carece de un sistema formal para gestionarlos. La ausencia de inventarios actualizados y de clasificación de criticidad dificulta la identificación y priorización de riesgos, lo que incrementa la exposición a incidentes y errores operativos.

C. Evaluación del control de accesos

La finalidad de esta evaluación fue determinar la solidez de los mecanismos de acceso y autenticación implementados en Garzasoft, ya que el control de accesos es fundamental para garantizar la confidencialidad y la disponibilidad de los activos.

Se realizaron entrevistas semiestructuradas con los responsables de infraestructura y desarrollo. Asimismo, se revisaron las configuraciones de accesos en repositorios, servidores, paneles administrativos y bases de datos. El instrumento utilizado fue una guía de entrevista y un checklist técnico.

Tabla 9. Resultados de la evaluación del control de accesos

Ítem evaluado	Cumple	No cumple
Política de creación y baja de cuentas	20%	80%
Control de privilegios basado en roles	30%	70%
Uso de MFA	0%	100%
Eliminación oportuna de cuentas de ex empleados	40%	60%
Uso de credenciales compartidas	0%	100%

Los resultados evidenciaron serias debilidades en el control de accesos. El uso de credenciales compartidas, la ausencia de MFA y la falta de segregación de privilegios representan riesgos críticos de seguridad y puntos vulnerables frente a ataques o errores humanos. La empresa requiere una política formal y procedimientos estrictos para mitigar estos riesgos.

D. Evaluación de la seguridad en operaciones

El objetivo fue evaluar los controles aplicados en la operación diaria de los servicios TI de Garzasoft, incluyendo actualizaciones, respaldos, monitoreo y prácticas del ciclo de vida del software.

Se inspeccionaron servidores, repositorios, entornos de testing y de producción, revisando logs, rutinas de mantenimiento y configuraciones. También se aplicó un checklist técnico. El instrumento que se utilizó fue un checklist técnico basado en ISO/IEC 27002.

Tabla 10. Resultados de la evaluación de la seguridad en operaciones

Ítem evaluado	Resultado
Actualizaciones de servidores	Irregulares
Control de cambios	Parcial
Seguridad en repositorios Git	Parcial
Procesos DevSecOps	No existen
Verificación de respaldos	No se realizan
Auditoría de logs	No implementada

Aunque existen esfuerzos como el uso de Git o pipelines CI/CD, la seguridad no está integrada en las operaciones, dejando expuesto al software a vulnerabilidades de desarrollo, fallas por actualizaciones tardías y riesgos por falta de monitoreo sistemático.

E. Evaluación de la seguridad física y ambiental

El propósito fue determinar si las oficinas y áreas donde se alojan los activos físicos cuentan con controles adecuados que protejan los servidores, estaciones de trabajo y documentos críticos.

Se realizó una inspección directa de las áreas de trabajo, los servidores locales y los puntos de acceso físicos. Como instrumento se utilizó una Guía de inspección.

Tabla 11. Resultados de la evaluación de la seguridad física y ambiental

Elemento	Resultado
Control de acceso a oficinas	Bajo
Registro de visitantes	No existe
Protección eléctrica (UPS)	Parcial
Cámaras de seguridad	Parcial
Control de dispositivos externos	No existe
Política de escritorio limpio	No existe

La seguridad física es limitada y no se ajusta a estándares mínimos. La posibilidad de acceso no autorizado, manipulación de equipos o extracción de datos mediante dispositivos externos constituye un riesgo significativo para la integridad y confidencialidad de la información.

F. Evaluación de la gestión de incidentes

La evaluación buscó determinar si Garzasoft cuenta con un proceso formal para detectar, registrar, gestionar y aprender de los incidentes de seguridad.

Se revisó documentación interna, se consultó a personal técnico y se verificó la existencia de registros históricos. El instrumento utilizado fue una matriz de incidentes adaptada de la ISO 27035.

Tabla 12. Resultados de la evaluación de la gestión de incidentes

Criterio evaluado	Resultado
Registro histórico de incidentes	No existe
Procedimiento para manejo de incidentes	No existe
Roles asignados	No definidos
Tiempo promedio de atención	No medible
Documentación post-incidente	No existe

Garzasoft opera de manera reactiva ante incidentes, lo cual incrementa el impacto potencial de cualquier falla o ataque. La ausencia de procesos estructurados impide detectar patrones y prevenir la repetición de incidentes.

G. Evaluación de la continuidad del negocio

Esta dimensión evaluó si la empresa posee mecanismos formales que garanticen la continuidad de los servicios, la recuperación ante desastres y la disponibilidad de la información crítica.

Se revisaron procedimientos, respaldos, recursos de recuperación y entrevistas con los responsables. El instrumento utilizado fue una Lista de verificación BCP/DRP.

Tabla 13. Resultados de la evaluación de la continuidad del negocio

Ítem evaluado	Cumple	No cumple
Existencia de BCP	0%	100%
Existencia de DRP	0%	100%
Pruebas de recuperación	0%	100%
Copias fuera del sitio	Parcial	
Estrategia ante fallas de nube	No definida	

La empresa se encuentra en un nivel crítico en cuanto a continuidad de negocio. Ante un fallo significativo o un ataque mayor, Garzasoft no posee mecanismos formales para recuperar sus sistemas de manera rápida y confiable.

3.1.5. Análisis de brechas de seguridad de la información

La evaluación de las siete dimensiones demostró que Garzasoft posee un nivel bajo de madurez en Gestión de la Seguridad de la Información, lo cual la expone a riesgos operativos, cibernéticos y comerciales elevados.

En la siguiente tabla, se muestra el consolidado de las brechas de seguridad de la información que tiene la empresa.

Tabla 14. Brechas de seguridad de la información identificadas con respecto a los controles de la ISO/IEC 27001:2022

Control ISO 27001:2022	Situación actual en Garzasoft	Brecha	Interpretación
A.5.1 Políticas para la seguridad de la información	No existe política formal ni aprobada	**Crítica**	Garzasoft no cuenta con un documento guía que establezca principios, compromisos ni responsabilidades de seguridad. Esto impide una buena gestión de la seguridad de la información
A.5.7 Responsabilidades de seguridad en roles y funciones	No hay roles ni responsabilidades definidas	**Crítica**	La seguridad es asumida informalmente por TI; esto genera ambigüedad y descontrol.
A.5.12 Clasificación de la información	No existe clasificación formal de activos	**Alta**	La ausencia de clasificación impide priorizar la protección de datos sensibles o críticos.
A.5.9 Inventario de activos de información	Inventario parcial y no actualizado	**Alta**	Incrementa el riesgo de pérdida o exposición de activos no registrados.
A.5.16 Información sobre amenazas y vulnerabilidades	No hay monitoreo sistemático	**Alta**	La empresa no identifica oportunamente vulnerabilidades de software y dependencias.
A.5.17 Gestión de vulnerabilidades técnicas	Parches aplicados de forma irregular	**Alta**	Servidores y entornos internos quedan expuestos a exploits conocidos.
A.5.18 Gestión de configuración	No hay lineamientos formales de configuración segura	**Alta**	Favorece configuraciones débiles en servidores, BD y servicios en la nube.
A.6.2 Gestión de identidades	No existe IAM formal. Accesos con cuentas compartidas	**Crítica**	El nivel de riesgo es extremo: no hay trazabilidad de acciones ni segregación de funciones.
A.6.5 Gestión de privilegios	Privilegios no documentados; no hay control de "mínimo privilegio"	**Alta**	Privilegios excesivos pueden permitir abuso o explotación.
A.6.4 Autenticación y MFA	MFA inexistente en todos los sistemas críticos	**Crítica**	Riesgo severo ante ataques de phishing o fuerza bruta.
A.7.4 Políticas de escritorio limpio y pantalla limpia	No implementadas	**Media**	Puede facilitar divulgación no autorizada de información física.
A.7.5 Seguridad física de instalaciones	Acceso físico débil en áreas críticas	**Alta**	Dispositivos pueden ser manipulados o extraídos sin control.
A.7.8 Protección eléctrica y ambiental	Sistemas UPS solo en algunos equipos	**Media**	Riesgo de daño por cortes eléctricos.
A.8.16 Registro de eventos y monitoreo	No existe monitoreo ni auditoría de logs	**Crítica**	La empresa no detecta incidentes, accesos indebidos ni anomalías.
A.8.12 Protección contra malware	Antimalware presente, pero sin políticas formales	**Media**	No hay estrategia centralizada ni controles avanzados.
A.8.23 Copias de seguridad	Backups sin verificación de restauración	**Alta**	Los respaldos pueden fallar al ser necesarios para recuperación.
A.8.28 Seguridad en desarrollo de software	No existe proceso de desarrollo seguro (SDLC seguro)	**Crítica**	El software puede incluir vulnerabilidades graves por falta de revisión.
A.8.29 Seguridad en pruebas de software	QA sin enfoque de seguridad	**Alta**	Las pruebas no detectan vulnerabilidades lógicas o técnicas.
A.8.30 Gestión de cambios	Control de cambios parcial	**Media**	Cambios sin trazabilidad pueden generar fallas o pérdidas de integridad.
A.8.31 Desarrollo externo	No aplica o informal	**Media**	Riesgo si se terceriza en el futuro sin controles formales.
A.8.35 Eliminación de información	No existe política de eliminación segura	**Alta**	Información sensible puede recuperarse o filtrarse.
A.8.36 Eliminación de activos	No existe procedimiento seguro	**Alta**	Discos, PCs o servidores pueden terminar con información residual.
A.5.24 Gestión de incidentes de seguridad	No se registra ni gestiona incidentes	**Crítica**	No se aprende de incidentes, no se previene recurrencia.
A.5.25 Lecciones	No existen	**Crítica**	La empresa no mejora sus controles tras

Control ISO 27001:2022	Situación actual en Garzasoft	Brecha	Interpretación
aprendidas post-incidente			eventos de seguridad.
A.5.30 Continuidad del negocio	No se cuenta con BCP ni DRP	**Crítica**	Una caída podría paralizar totalmente los servicios SaaS.
A.5.31 Recuperación ante desastres	Totalmente inexistente	**Crítica**	Ante un ataque severo, la empresa no podría operar.

Los resultados muestran que Garzasoft presenta brechas significativas e incluso críticas frente a los controles establecidos por ISO/IEC 27001:2022. A continuación se muestra el análisis de brechas por su nivel de severidad:

Tabla 15. Consolidado de brechas de seguridad de la información por nivel de severidad

Categoría de brecha	Brechas identificadas	Impacto asociado
Áreas con brechas críticas	- Ausencia total de políticas de seguridad. - Falta de un inventario formal de activos. - Accesos débiles y privilegios no controlados. - Ausencia total de MFA. - Inexistencia del proceso de gestión de incidentes. - Carencia absoluta de un Plan de Continuidad del Negocio (BCP) y un Plan de Recuperación ante Desastres (DRP). - Ausencia de monitoreo y auditoría de logs. - Inexistencia de un proceso de Desarrollo Seguro del Software (SDLC seguro).	- Pérdida total o parcial de datos. - Accesos no autorizados sin trazabilidad. - Paralización de servicios SaaS esenciales. - Afectación a la integridad del software y procesos. - Riesgos reputacionales y contractuales severos.
Áreas con brechas altas	- Clasificación de activos. - Gestión de vulnerabilidades. - Gestión de respaldos. - Seguridad en pruebas.	Indican ausencia de controles preventivos y correctivos, manteniendo a Garzasoft en un esquema reactivo.
Áreas con brechas medias	- Seguridad física básica. - Gestión de cambios parcial. - Eliminación de información.	Contribuyen al riesgo global aunque no representan un riesgo extremo individualmente.

El análisis evidencia que Garzasoft se encuentra en un **nivel de madurez de seguridad de la información muy bajo**. Las brechas detectadas justifican la necesidad urgente de implementar un Sistema de Gestión de Seguridad de la Información (SGSI).

3.2. Identificar los escenarios de riesgo críticos asociados a la operación de la Garzasoft

3.2.1. Identificación de activos de TI en Garzasoft

La identificación de activos de TI se realizó siguiendo los lineamientos de la metodología MAGERIT v3, combinando análisis documental, entrevistas con personal técnico y observación directa en los procesos misionales de Garzasoft. El propósito fue determinar qué elementos del entorno tecnológico constituyen activos de información esenciales para los servicios de la empresa y qué nivel de importancia poseen.

La identificación de los activos se realizó en base a su relación con los subprocesos definidos tanto para el área de Desarrollo como para el área de Producción y Soporte de TI. Para cada activo se analizó su uso operativo, su dependencia funcional y el impacto que tendría su indisponibilidad o alteración en los subprocesos; así, se asignaron únicamente aquellos subprocesos en los que el activo participa de manera directa o indirecta, garantizando una relación coherente con su función dentro de la organización.

Luego se identificaron y clasificaron los activos identificados, según la tipología MAGERIT (información, hardware, software, servicios y comunicaciones).

Para evaluar la criticidad de cada activo aplicando se valoró su impacto sobre las características de seguridad de la información: Confidencialidad, Integridad y Disponibilidad (C, I, D) utilizando una escala de criticidad del 1 al 5, donde valores elevados reflejan impacto extremo en los servicios, datos o procesos clave de la empresa. La escala utilizada fue: 1 (muy baja), 2 (baja), 3 (media), 4 (alta) y 5 (crítica), asignándose cada nivel según el rango correspondiente del valor total. La criticidad se obtuvo mediante el cálculo del promedio de las valoraciones asignadas a Confidencialidad, Integridad y Disponibilidad.

Tabla 16. Escala utilizada para la criticidad (1–5)

Valor total (C+I+D)	Criticidad asignada	Descripción
3–5	1 — Muy baja	Impacto marginal; afecta tareas menores
6–8	2 — Baja	Riesgo leve; afecta a un proceso local
9–10	3 — Media	Riesgo moderado; impacto parcial en operaciones
11–13	4 — Alta	Riesgo significativo; afecta varios procesos críticos
14–15	5 — Crítica	Riesgo extremo; afecta servicios esenciales o datos sensibles

Los activos identificados y su correspondiente criticidad se muestra a continuación:

Tabla 17. Activos por subprocesos

Nº	Activo	Tipo (Magerit)	Relación con subprocesos	C	I	D	Valor total	Criticidad
1	Base de datos GESREST	Información	Administración y mantenimiento de bases de datos; Administración de infraestructura tecnológica; Gestión de incidentes	5	5	5	15	5
2	Base de datos 360.SIS	Información	Administración y mantenimiento de bases de datos; Administración de infraestructura tecnológica; Gestión de incidentes	5	5	5	15	5
3	Base de datos Hotel HUB	Información	Administración y mantenimiento de bases de datos; Administración de infraestructura tecnológica	5	4	4	13	5
4	Código fuente GESREST	Información	Control de cambios y versiones; Pruebas y evaluación; Atención de solicitudes; Gestión de iniciativas y proyectos	5	5	4	14	5
5	Código fuente 360.SIS	Información	Control de cambios y versiones; Pruebas y evaluación; Atención de solicitudes; Gestión de iniciativas y proyectos	5	5	4	14	5
6	Código fuente Hotel HUB	Información	Control de cambios y versiones; Pruebas y evaluación; Gestión de iniciativas y proyectos	5	4	4	13	5
7	Servidor IaaS (Producción)	Hardware/Servicio	Administración de infraestructura tecnológica; Gestión de incidentes; Atención y soporte al usuario	4	5	5	14	5
8	Repositorio Git (nube)	Software/Servicio	Control de cambios y versiones; Atención de solicitudes; Gestión de iniciativas y proyectos	5	5	4	14	5
9	Servidor local de desarrollo	Hardware	Atención de solicitudes; Pruebas y evaluación; Control de cambios	4	4	3	11	4
10	Pipeline CI/CD	Software	Pruebas y evaluación; Control de cambios y versiones	4	4	3	11	4
11	Credenciales privilegiadas	Información	Administración de cuentas y accesos; Gestión de incidentes; Soporte técnico	5	4	5	14	5
12	Entorno virtual de pruebas	Software	Pruebas y evaluación de módulos	3	4	3	10	3
13	Sistema de archivos interno	Hardware/Info	Soporte técnico; Administración de infraestructura tecnológica	3	3	3	9	3
14	Herramientas de gestión (Jira)	Software	Gestión de iniciativas y proyectos; Atención de solicitudes	3	3	4	10	3
15	Computadoras de desarrolladores	Hardware	Atención de solicitudes; Pruebas; Control de cambios	3	3	3	9	3
16	Router y firewall local	Comunicaciones	Administración de infraestructura tecnológica; Gestión de incidentes	3	4	4	11	4
17	Estaciones de trabajo administrativas	Hardware	Atención y soporte al usuario; Gestión de incidentes	2	3	3	8	2
18	Documentación técnica	Información	Gestión de iniciativas y proyectos; Atención de solicitudes	4	4	2	10	3
19	Manuales de usuario	Información	Atención y soporte al usuario	3	2	2	7	2
20	Servicio de correo corporativo	Servicio	Atención y soporte al usuario; Gestión de incidentes	3	3	3	9	3
21	Modelos de IA/BI	Información	Gestión de iniciativas; Administración de infraestructura	4	4	3	11	4
22	Tokens API de clientes	Información	Administración de cuentas y accesos; Integraciones; Gestión de incidentes	5	4	5	14	5
23	Red interna de oficinas	Comunicaciones	Administración de infraestructura; Atención y soporte al usuario; Gestión de incidentes	3	3	4	10	3
24	Dispositivos móviles del staff	Hardware	Atención y soporte al usuario; Gestión de incidentes	2	2	3	7	2

3.2.2. Identificación de amenazas

Esta etapa tuvo como finalidad determinar las amenazas que pueden afectar los activos críticos de Garzasoft. La identificación se realizó mediante:

- Observación técnica de entornos locales y en la nube
- Revisión de logs parciales
- Entrevistas con desarrolladores y personal de TI
- Análisis de flujos de datos y servicios SaaS
- Catálogo de amenazas de MAGERIT v3

Las amenazas fueron agrupadas en cinco categorías principales:

- Amenazas naturales
- Amenazas involuntarias (accidentales)
- Amenazas deliberadas (maliciosas)
- Amenazas lógicas (tecnológicas)
- Amenazas relacionadas a servicios externos (nube, proveedores)

Las amenazas identificadas se muestran a continuación

Tabla 18. Listado de amenazas priorizadas y su relación con los activos afectados

Nº	Categoría	Amenaza identificada	Descripción	Activos afectados
1	Accidental	Error humano	Modificación o borrado accidental de datos	Activos afectados (actualizados según la tabla final)
2	Accidental	Configuración errónea	Configuraciones incorrectas de servidores, red o repositorios	1, 2, 3 (Bases de datos); 4–6 (Código fuente); 8 (Repo Git); 12 (Entorno pruebas); 13 (Sistema archivos)
3	Accidental	Fallos de actualización	Parches incompletos o fallidos	7 (IaaS Prod), 9 (Servidor desarrollo), 16 (Router/Firewall), 8 (Git)
4	Lógica	Falla de software	Bugs que comprometen la integridad de datos	7 (IaaS Prod), 9 (Servidor desarrollo), 10 (CI/CD), 1–3 (BD)
5	Lógica	Vulnerabilidades del código	Falta de validación, inyección SQL, XSS	4–6 (Código fuente), 1–3 (Bases de datos), 12 (Entorno pruebas), 14 (Jira)
6	Lógica	Vulnerabilidades de terceros	Dependencias no parcheadas	4–6 (Código fuente), 22 (Tokens API), 1–3 (BD)
7	Deliberada	Acceso no autorizado	Intrusiones internas o externas	4–6 (Código fuente), 8 (Git), 10 (CI/CD)
8	Deliberada	Ataques de fuerza bruta	Intentos de obtener credenciales débiles	11 (Credenciales privilegiadas), 1–3 (Bases de datos), 7 (IaaS), 22 (API tokens)
9	Deliberada	Phishing	Robo de credenciales del personal	11 (Credenciales privilegiadas), 20 (Correo corporativo), 24 (Móviles del staff)
10	Deliberada	Ransomware	Secuestro de información interna	20 (Correo corporativo), 11 (Credenciales privilegiadas), 24 (Móviles)
11	Deliberada	Ataque a APIs	Exploits de endpoints vulnerables	1–3 (BD), 7 (IaaS), 13 (Sistema de archivos), 15 (PC dev), 17 (estaciones admin)
12	Deliberada	Interceptación de comunicaciones	Sniffing en redes inseguras	22 (API tokens), 4–6 (Código fuente), 1–3 (BD)
13	Natural	Cortes eléctricos	Interrupciones de energía	23 (Red interna), 16 (Firewall/Router), 24 (Móviles)
14	Natural	Inundaciones/lluvias	Riesgo para oficinas	9 (Servidor desarrollo), 17 (estaciones admin), 15 (PC dev), 16 (Router/Firewall)

15	Servicios externos	Falla del proveedor cloud	Caída de AWS/Google Cloud	15 (PC dev), 17 (estaciones admin), 24 (móviles)
16	Servicios externos	Configuración errónea en la nube	Mala configuración IAM/ACL	7 (IaaS), 8 (Git), 20 (Correo), 1–3 (BD cloud)
17	Física	Robo de dispositivos	Extravío o robo de laptops o móviles	7 (IaaS), 22 (API tokens), 8 (Git)
18	Física	Acceso físico no autorizado	Entrada a oficinas sin control	15 (PC dev), 17 (Estaciones admin), 24 (Móviles), 18 (Documentación técnica)
19	Física	Daño accidental de hardware	Golpes, derrames	9 (Servidor desarrollo), 15 (PC dev), 17 (estaciones admin), 13 (Sistema de archivos)
20	Ambiental	Temperatura excesiva	Calentamiento de equipos	15 (PC dev), 17 (estaciones admin), 9 (Servidor desarrollo), 24 (móviles)

A. Las amenazas identificadas en la Categoría: Accidental

En Garzasoft, las amenazas accidentales se relacionan principalmente con el trabajo dinámico del equipo de desarrollo y soporte, donde múltiples cambios, despliegues rápidos y ajustes operativos aumentan el riesgo de errores no intencionales. Los fallos por descuido —como borrar datos, aplicar configuraciones incorrectas o ejecutar actualizaciones incompletas— pueden afectar servicios SaaS críticos (GESREST, 360.SIS, Hotel HUB), así como repositorios y entornos CI/CD. Debido a que la empresa opera en un entorno ágil, con una alta frecuencia de cambios, este tipo de amenaza requiere fortalecer la capacitación, documentar procesos y aplicar automatización para reducir dependencias del factor humano.

B. Las amenazas identificadas en la Categoría: Lógica

Las amenazas lógicas representan uno de los riesgos más relevantes para Garzasoft debido a su rol como desarrollador de plataformas SaaS. Bugs no detectados, vulnerabilidades del código, validaciones deficientes o dependencias desactualizadas pueden comprometer directamente la integridad y confidencialidad de los datos de clientes. Dado que el ciclo de desarrollo no cuenta actualmente con un SDLC seguro ni pruebas automatizadas robustas, existe una mayor probabilidad de que errores lógicos en el software afecten la operación. Esto obliga a implementar análisis estáticos de código, gestión formal de vulnerabilidades, políticas de desarrollo seguro y una capa de pruebas más madura.

C. Las amenazas identificadas en la Categoría: Deliberada

Para Garzasoft, las amenazas deliberadas implican ataques dirigidos a sus servicios SaaS o a la infraestructura cloud donde corren sus soluciones. Al manejar información de clientes y API tokens sensibles, los riesgos de accesos no autorizados, fuerza bruta y explotación de APIs son especialmente graves. La ausencia parcial de MFA, controles débiles de privilegios y falta de monitoreo incrementan la exposición frente a actores maliciosos. Esta categoría requiere priorizar controles como Zero Trust,

MFA para todo acceso sensible, hardening, monitoreo de logs y protección de endpoints.

D. Las amenazas identificadas en la Categoría: Natural

Aunque Garzasoft depende principalmente de infraestructura en la nube, las amenazas naturales aún pueden afectar su operación local, especialmente servidores de desarrollo, equipos del staff y oficinas administrativas. Cortes eléctricos o lluvias intensas pueden detener la operación interna, afectar el soporte técnico y retrasar despliegues. Si bien no son amenazas frecuentes, la falta de un BCP y DRP incrementa su impacto potencial. Es crucial diseñar un plan básico de continuidad y contar con medidas mínimas como UPS y resguardo físico adecuado.

E. Las amenazas identificadas en la Categoría: Servicios externos

Garzasoft depende en gran medida de proveedores cloud (IaaS, repositorios, correo corporativo). Caídas o configuraciones inseguras en estos servicios pueden generar indisponibilidad de sus plataformas SaaS o exposiciones por errores de IAM. Al no contar con un control maduro de configuraciones en la nube, este tipo de amenaza es relevante y requiere controles como revisión periódica de permisos, backups independientes y mecanismos de contingencia.

F. Las amenazas identificadas en la Categoría: Física

Las amenazas físicas para Garzasoft se centran en la seguridad de equipos de los desarrolladores, estaciones administrativas y servidores locales. El robo de laptops o móviles representa un riesgo directo, especialmente si contienen credenciales, código fuente o documentación interna sin cifrado. De igual forma, accesos no autorizados a la oficina pueden comprometer hardware crítico. Es esencial aplicar cifrado en dispositivos, mantener inventarios y fortalecer el control de acceso físico en instalaciones.

G. Las amenazas identificadas en la Categoría: Ambiental

La infraestructura local de Garzasoft puede verse afectada por condiciones ambientales inadecuadas, como altas temperaturas que dañen servidores, laptops o equipos de red. Aunque los sistemas SaaS no dependen de instalaciones físicas, el daño a equipos locales disminuye la capacidad de desarrollo y soporte. Una climatización apropiada y monitoreo del entorno reducirían significativamente esta amenaza.

3.2.3. Identificación de vulnerabilidades

La identificación de las vulnerabilidades se realizó mediante:

- Revisión de configuraciones en la nube
- Escaneo básico de vulnerabilidades
- Revisión de repositorios de código
- Entrevistas con equipo de desarrollo
- Observación directa en entornos de pruebas y producción
- Checklist técnico basado en ISO/IEC 27002 y OWASP

Las vulnerabilidades detectas se muestran a continuación:

Tabla 19. Listado de vulnerabilidades detectadas y su relación con lo activos

Nº	Vulnerabilidad	Descripción técnica	Activos afectados
1	Ausencia de MFA	No existe doble factor para accesos críticos	11 (Credenciales privilegiadas), 20 (Correo corporativo), 22 (Tokens API), 24 (Móviles)
2	Credenciales compartidas	Varias cuentas compartidas entre desarrolladores	11 (Credenciales privilegiadas), 8 (Git), 7 (IaaS)
3	Contraseñas débiles	Sin políticas de complejidad	11 (Credenciales privilegiadas), 20 (Correo), 24 (Móviles), 22 (API tokens)
4	Falta de control de versiones seguro	No existen ramas protegidas ni revisiones obligatorias	8 (Repositorio Git), 4–6 (Código fuente)
5	Falta de cifrado en tránsito	Algunos microservicios no usan HTTPS	22 (API tokens), 1–3 (BD), 7 (IaaS), 23 (Red interna)
6	Falta de hardening en servidores	Configuraciones por defecto	7 (IaaS), 9 (Servidor desarrollo), 16 (Firewall/Router)
7	Dependencias vulnerables	Librerías sin actualizar	4–6 (Código fuente), 10 (Pipeline CI/CD)
8	Backups sin verificación	No se realizan pruebas de restauración	1–3 (Bases de datos), 7 (IaaS), 13 (Sistema de archivos)
9	Falta de monitoreo de logs	No se revisan eventos ni anomalías	7 (IaaS), 23 (Red interna), 20 (Correo), 1–3 (BD)
10	Acceso físico no controlado	Oficinas y servidores sin control riguroso	9 (Servidor desarrollo), 15 (PC desarrolladores), 17 (Estaciones admin), 13 (Sistema archivos)
11	Falta de firewall perimetral	Configuración mínima o básica	16 (Router/Firewall), 23 (Red interna)
12	Permisos excesivos	Usuarios con privilegios innecesarios	11 (Credenciales privilegiadas), 8 (Git), 1–3 (BD)
13	Falta de política de eliminación de activos	Riesgo de exposición de información residual	13 (Sistema archivos), 15 (PC dev), 17 (Estaciones admin), 24 (Móviles)
14	Falta de auditorías de seguridad	No hay revisiones periódicas	Todos los activos (1–24)
15	Actualizaciones irregulares	Parcheo no programado	7 (IaaS), 9 (Servidor local), 10 (CI/CD), 15 (PC dev), 17 (Estaciones admin)
16	Gestión deficiente de incidentes	No hay registros ni clasificación	Todos los activos críticos (1–3, 4–6, 7, 8, 11, 22, 23)
17	API sin rate-limit	Posible explotación mediante ataques DoS	22 (Tokens API), 4–6 (Código), 1–3 (BD)
18	Documentación técnica desactualizada	Impide trazabilidad	18 (Documentación técnica), 4–6 (Código fuente), 14 (Jira)
19	Falta de pruebas de seguridad	QA funcional sin pruebas de seguridad	12 (Entorno de pruebas), 10 (CI/CD), 4–6 (Código)
20	Dispositivos externos sin control	USB, discos no restringidos	15 (PC dev), 17 (Estaciones admin), 24 (Móviles)

La tabla de vulnerabilidades evidencia que los activos más expuestos en Garzasoft son aquellos con mayor criticidad y uso transversal, especialmente las bases de datos (1–3), el código fuente (4–6), el servidor IaaS de producción (7), las credenciales privilegiadas (11) y los tokens API de clientes (22). Estos activos aparecen repetidamente como afectados por vulnerabilidades críticas como ausencia de MFA, permisos excesivos, hardening insuficiente, dependencias vulnerables y ataques a APIs. Su alta concentración de riesgos indica que cualquier compromiso sobre ellos podría afectar simultáneamente a varios servicios SaaS, provocando interrupciones graves o exposición de información sensible.

Las vulnerabilidades relacionadas con accesos inseguros, como credenciales compartidas, contraseñas débiles y phishing, amplifican todavía más el riesgo, pues comprometer una sola cuenta privilegiada permitiría el acceso no autorizado a repositorios, bases de datos o despliegues en la nube. Del mismo modo, la falta de controles en el repositorio Git (8), el pipeline CI/CD (10) y la documentación técnica (18) muestran debilidades en el proceso de desarrollo, aumentando la probabilidad de errores, explotación de código vulnerable y alteraciones maliciosas sin detección o trazabilidad adecuada.

En conjunto, este panorama sugiere que una falla en cualquiera de estos activos altamente vulnerables podría generar consecuencias severas para Garzasoft, incluyendo pérdida o corrupción de datos de clientes, caída de servicios SaaS, interrupción operativa prolongada, incumplimientos contractuales y un impacto reputacional significativo. Para reducir estos riesgos, será indispensable fortalecer los controles de acceso, implementar prácticas de desarrollo seguro, mejorar la gobernanza de la infraestructura cloud y establecer un sistema de monitoreo y gestión de incidentes más maduro.

Tabla 20. Nivel de exposición a las amenazas y vulnerabilidades por activo

Nº	Activo	Amenazas asociadas	Vulnerabilidades asociadas
1	Base de datos GESREST	1, 3, 4, 5, 7, 10, 11, 15, 16	1, 3, 5, 7, 8, 9, 12, 14, 15, 16
2	Base de datos 360.SIS	1, 3, 4, 5, 7, 10, 11, 15, 16	1, 3, 5, 7, 8, 9, 12, 14, 15, 16
3	Base de datos Hotel HUB	1, 3, 4, 5, 7, 10, 11, 15, 16	1, 3, 5, 7, 8, 9, 12, 14, 15, 16
4	Código fuente GESREST	1, 4, 5, 6, 11, 17	4, 7, 18, 19, 14
5	Código fuente 360.SIS	1, 4, 5, 6, 11, 17	4, 7, 18, 19, 14
6	Código fuente Hotel HUB	1, 4, 5, 6, 11, 17	4, 7, 18, 19, 14
7	Servidor IaaS Producción	1, 2, 3, 7, 10, 15, 16	1, 6, 8, 9, 14, 15
8	Repositorio Git (Nube)	1, 2, 6, 7, 11	2, 3, 4, 7, 12, 14
9	Servidor local de desarrollo	1, 2, 3, 10, 13, 18, 19, 20	6, 8, 10, 13, 15, 20, 14
10	Pipeline CI/CD	1, 3, 6, 17	7, 15, 19, 14
11	Credenciales privilegiadas	7, 8, 9, 11	1, 2, 3, 9, 12, 14
12	Entorno virtual de pruebas	1, 4, 6, 19	7, 19, 14
13	Sistema de archivos interno	1, 8, 10, 13, 18, 19	8, 9, 10, 13, 14
14	Herramientas de gestión (Jira)	1, 4, 6	18, 14
15	Computadoras de	1, 9, 10, 13, 14, 18, 19, 20	3, 10, 13, 15, 20, 14

Nº	Activo	Amenazas asociadas	Vulnerabilidades asociadas
	desarrolladores		
16	Router y firewall local	2, 7, 12, 13, 20	6, 11, 9, 14
17	Estaciones administrativas	9, 10, 13, 14, 18, 19, 20	3, 10, 13, 15, 20, 14
18	Documentación técnica	1, 17, 18	18, 13, 14
19	Manuales de usuario	9, 17	13, 14
20	Correo corporativo	9, 7, 8, 15	1, 3, 9, 14
21	Modelos de IA/BI	1, 4, 6, 15	7, 18, 14, 15
22	Tokens API de clientes	7, 11, 17	1, 3, 5, 12, 14
23	Red interna de oficinas	2, 12, 13, 20	11, 6, 9, 14
24	Dispositivos móviles del staff	8, 9, 13, 17, 19	1, 3, 13, 20, 14

Los resultados de la tabla muestran que los activos más expuestos a escenarios de riesgo, entendidos como la combinación simultánea de múltiples amenazas y vulnerabilidades, son principalmente las bases de datos (activos 1, 2 y 3), el código fuente de los tres productos SaaS (activos 4, 5 y 6), el servidor IaaS de producción (activo 7), el repositorio Git (activo 8) y las credenciales privilegiadas (activo 11). Estos activos presentan un volumen elevado tanto de amenazas asociadas como de vulnerabilidades habilitadoras, ubicándolos como principales riesgos de Garzasoft. Esto es especialmente relevante porque estos activos representan el núcleo del negocio: contienen información crítica, sostienen la operación de los servicios SaaS o permiten la administración total de los sistemas.

El análisis también evidencia que varios activos presentan riesgo compuesto: es decir, no solo están expuestos a una gran cantidad de amenazas, sino que además poseen vulnerabilidades que facilitan la materialización de dichas amenazas. Las bases de datos, por ejemplo, están expuestas a ataques deliberados (accesos no autorizados, ransomware, explotación de APIs), amenazas lógicas (bugs, vulnerabilidades del código) y amenazas accidentales (errores humanos, fallos de actualización). Esto, combinado con vulnerabilidades como ausencia de MFA, permisos excesivos, falta de cifrado y backups no verificados, incrementa significativamente la probabilidad de una brecha grave. De forma similar, el servidor de producción y el repositorio Git concentran tanto amenazas técnicas como vulnerabilidades estructurales, lo que los vuelve puntos críticos en la cadena de seguridad.

Finalmente, la exposición combinada de amenazas y vulnerabilidades sobre activos como tokens API (22), modelos de IA/BI (21) y la red interna (23) indica que Garzasoft no enfrenta un riesgo limitado a un único punto, sino un contexto de riesgo distribuido, donde varios elementos altamente conectados pueden fallar o ser comprometidos en cascada. Esto significa que un incidente en un activo central —por ejemplo, el repositorio Git o las credenciales privilegiadas— puede repercutir inmediatamente en otros activos dependientes, comprometiendo el servicio, los datos y la confianza de los clientes. En conjunto, los

resultados sugieren la necesidad de priorizar medidas de endurecimiento y control sobre estos activos más expuestos para reducir de manera significativa el riesgo global de la organización.

3.3. Estimación del nivel de riesgo inherente para los escenarios de riesgo identificados

3.3.1. Estimación del impacto

La estimación del impacto tuvo como propósito determinar la severidad de las consecuencias que podría generar un incidente de seguridad sobre los procesos, servicios y activos críticos de Garzasoft. Esta evaluación permitió dimensionar de manera objetiva cómo una amenaza o vulnerabilidad podía afectar la continuidad del negocio, la disponibilidad de sus plataformas SaaS y la confianza de los clientes. Al categorizar el impacto, la organización pudo priorizar riesgos, asignar recursos de mitigación de manera eficiente y establecer umbrales claros para la toma de decisiones dentro de su gestión de seguridad de la información.

El uso de una escala numérica del 1 al 5 fue importante porque proporcionó un sistema uniforme, comparable y fácilmente interpretable para clasificar el nivel de afectación. La escala permitió transformar impactos cualitativos (percepción, gravedad, alcance) en valores cuantitativos que facilitaron el análisis de riesgo, la construcción de matrices y la priorización de controles. Además, al estar estandarizada por niveles claramente descritos (desde muy bajo hasta crítico) se redujo la subjetividad y se aseguró que diferentes evaluadores llegaran a conclusiones consistentes.

Finalmente, la inclusión de tipos de impacto diferenciados (operativo, económico, reputacional y legal/contractual) garantizó una visión integral del riesgo. Cada tipo de impacto capturó un aspecto esencial del negocio de Garzasoft: continuidad del servicio, estabilidad financiera, confianza de los clientes y cumplimiento regulatorio o contractual. Esta visión multidimensional permitió evaluar con mayor precisión cómo un incidente podía afectar simultáneamente varias áreas del negocio y, en consecuencia, facilitó el diseño de estrategias de mitigación más completas y alineadas con las necesidades reales de la organización.

Tabla 21. Escala de evaluación del impacto de las amenazas

Nivel	Descripción del impacto	Impacto operativo	Impacto económico	Impacto reputacional	Impacto legal / contractual
1 – Muy Bajo	Impacto insignificante; efectos mínimos en el servicio.	Interrupción menor a 30 minutos; afecta solo tareas internas.	< 1% del ingreso mensual.	Sin afectación para clientes; impacto no perceptible.	Nulo; no existe riesgo legal o contractual.
2 – Bajo	Afectación leve, controlable y de corta duración.	Retrasos internos sin afectar servicios a clientes.	Entre 1% y 3% del ingreso mensual.	Reclamos internos, sin impacto en imagen externa.	Nulo; no compromete obligaciones contractuales.
3 – Medio	Afectación moderada y visible para algunos clientes.	Interrupción parcial del servicio (<2 horas) o errores funcionales.	Entre 3% y 8% del ingreso mensual.	Clientes reportan incidentes; afecta percepción del servicio.	Posible incumplimiento leve de SLA sin penalidades.
4 – Alto	Impacto grave sobre servicios críticos.	Interrupción mayor a 2 horas; caída de módulos esenciales.	Entre 8% y 15% del ingreso mensual.	Reclamos formales de clientes; riesgo de pérdida de contratos.	Incumplimiento de SLA con penalidades económicas.
5 – Muy Alto / Crítico	Afectación severa del negocio o pérdida de datos.	Indisponibilidad total > 6 horas o pérdida de información.	>15% del ingreso mensual; costos de reparación significativos.	Daño serio a reputación; pérdida de clientes clave.	Multas, litigios, sanciones o incumplimientos graves.

Para estimar el impacto asociado a cada activo crítico de Garzasoft, se utilizó la escala cualitativa–cuantitativa de impacto (1 a 5) previamente definida. La valoración integra el posible efecto sobre la operación, las finanzas, la reputación y el cumplimiento legal o contractual. Esta estimación fue simulada en función de la sensibilidad del activo, su función dentro de los servicios SaaS y la relación con los procesos y subprocesos donde participa. Finalmente, se justificó cada valoración considerando el rol del activo, su dependencia por otros componentes y la magnitud del daño que generaría una afectación.

Tabla 22. Estimación del impacto de las amenazas

Nº	Activo	Impacto (1–5)	Justificación
1	Base de datos GESREST	**5 – Muy Alto**	Contiene datos críticos de clientes; su pérdida afecta operación, integridad contractual y reputación.
2	Base de datos 360.SIS	**5 – Muy Alto**	Base de datos principal del sistema; cualquier incidente implica caída del servicio y riesgo legal.
3	Base de datos Hotel HUB	**5 – Muy Alto**	Maneja información comercial sensible; caída provoca indisponibilidad completa del módulo.
4	Código fuente GESREST	**5 – Muy Alto**	Afecta continuidad de desarrollo y calidad del producto; exposición compromete propiedad intelectual.
5	Código fuente 360.SIS	**5 – Muy Alto**	Es esencial para actualizaciones y nuevas versiones; un compromiso altera la integridad del sistema.
6	Código fuente Hotel HUB	**5 – Muy Alto**	Su afectación genera fallos en el producto, pérdida de confianza y riesgos contractuales.
7	Servidor IaaS Producción	**5 – Muy Alto**	Infraestructura donde corren servicios SaaS; su caída paraliza a todos los clientes.
8	Repositorio Git (nube)	**5 – Muy Alto**	Contiene código fuente y credenciales; modificaciones maliciosas afectan directamente la operación.
9	Servidor local de desarrollo	**4 – Alto**	Afecta ciclos de desarrollo y pruebas; el impacto no cae directamente sobre los clientes.
10	Pipeline CI/CD	**4 – Alto**	Error compromete despliegues, generando fallas en producción o interrupciones prolongadas.
11	Credenciales privilegiadas	**5 – Muy Alto**	Su abuso permite control total de sistemas; riesgo máximo de brechas, fraude o pérdida total.
12	Entorno virtual de	**3 – Medio**	Afecta validaciones previas a producción; impacto acotado al

Nº	Activo	Impacto (1–5)	Justificación
	pruebas		flujo interno.
13	Sistema de archivos interno	**3 – Medio**	Afecta documentos y operaciones internas; impacto limitado sobre clientes.
14	Herramientas de gestión (Jira)	**3 – Medio**	Impacta planificación y coordinación; no afecta servicios externos directamente.
15	Computadoras de desarrolladores	**3 – Medio**	Afecta productividad del equipo; posibilidad de pérdida de información local.
16	Router y firewall local	**4 – Alto**	Controla el acceso a red; un fallo expone infraestructura a ataques y detiene operaciones internas.
17	Estaciones administrativas	**3 – Medio**	Impacto operativo interno; puede comprometer datos administrativos.
18	Documentación técnica	**3 – Medio**	Su pérdida afecta trazabilidad y mantenimiento; impacto indirecto pero importante.
19	Manuales de usuario	**2 – Bajo**	Afectan soporte y usabilidad; el servicio sigue operativo aun con su pérdida.
20	Servicio de correo corporativo	**4 – Alto**	Medio crítico de comunicación; afectación compromete atención y coordinación.
21	Modelos de IA/BI	**4 – Alto**	Su corrupción afecta análisis estratégicos y automatizaciones.
22	Tokens API de clientes	**5 – Muy Alto**	Permiten acceso directo a sistemas; su compromiso expone datos y funcionalidades.
23	Red interna de oficinas	**4 – Alto**	Afecta conectividad general, soporte técnico y operaciones internas.
24	Dispositivos móviles del staff	**2 – Bajo**	Contienen datos limitados; pérdida afecta principalmente comunicaciones individuales.

3.3.2. Escala para la estimación de la probabilidad de ocurrencia

La estimación de la probabilidad de ocurrencia de las amenazas tiene como propósito determinar qué tan factible es que un evento de seguridad se materialice dentro del entorno operativo de Garzasoft. Este análisis complementa la evaluación del impacto, permitiendo identificar no solo cuáles amenazas podría causar mayores daños, sino también cuáles tienen más posibilidades de ocurrir dadas las condiciones actuales de exposición, madurez de controles y presencia de vulnerabilidades. De esta manera, Garzasoft puede priorizar sus esfuerzos de mitigación enfocándose en los escenarios más probables y críticos, optimizando recursos y fortaleciendo los puntos más débiles de su superficie de ataque.

La utilización de una escala numérica estructurada permite transformar un juicio complejo y, en muchos casos, subjetivo en una valoración comparable y coherente a lo largo del tiempo. La escala facilita clasificar la probabilidad bajo criterios homogéneos —frecuencia estimada, condiciones habilitadoras y nivel de exposición—, lo que garantiza consistencia entre evaluadores y simplifica la integración de esta información en matrices de riesgo y modelos de priorización. Además, al incluir descripciones específicas para cada nivel, la escala reduce la ambigüedad y proporciona un marco objetivo para evaluar la posibilidad de que una amenaza se materialice en función de los controles existentes y del comportamiento histórico de incidentes.

Tabla 23. Escala de evaluación de la probabilidad de ocurrencia de las amenazas

Nivel	Descripción de la Probabilidad	Frecuencia Estimada	Condiciones que favorecen la ocurrencia
1 – Muy Baja	Evento altamente improbable.	Menos de una vez cada 3 años.	Requiere condiciones extremas; controles existentes suficientes.
2 – Baja	Evento poco frecuente.	1 vez cada 1–2 años.	Algunos controles presentes; exposición limitada.
3 – Media	Evento posible y recurrente.	Entre 1 y 3 veces por año.	Controles parciales; vulnerabilidades conocidas no corregidas.
4 – Alta	Evento frecuente y previsible.	Mensual o bimestral.	Controles insuficientes; errores recurrentes.
5 – Muy Alta	Evento casi seguro o repetitivo.	Semanal o diariamente.	Exposición muy alta; ausencia de controles efectivos.

Para estimar la probabilidad de ocurrencia de incidentes relacionados con cada activo crítico de Garzasoft, se empleó la escala cualitativa–cuantitativa previamente definida (1 – Muy Baja a 5 – Muy Alta). Esta evaluación simula la frecuencia con la cual una amenaza podría materializarse considerando la presencia de vulnerabilidades, el grado de exposición del activo, la eficacia de los controles actuales y el entorno operativo. Se analizaron los activos de forma individual, estimando la probabilidad de que sufran eventos como intrusiones, errores operativos, fallos técnicos o ataques deliberados. Cada valoración incluye una justificación basada en los datos obtenidos en el análisis previo de amenazas y vulnerabilidades.

Tabla 24. Estimación de la probabilidad de ocurrencia de las amenazas

Nº	Activo	Probabilidad (1–5)	Justificación
1	Base de datos GESREST	**4 – Alta**	Elevada cantidad de amenazas y vulnerabilidades; alta exposición en producción.
2	Base de datos 360.SIS	**4 – Alta**	Mismo nivel de exposición que GESREST; riesgo recurrente por uso intensivo.
3	Base de datos Hotel HUB	**4 – Alta**	Recurrente interacción con APIs y clientes, sumado a vulnerabilidades críticas.
4	Código fuente GESREST	**3 – Media**	Vulnerabilidades frecuentes en desarrollo; controles parciales.
5	Código fuente 360.SIS	**3 – Media**	Riesgos propios del entorno de desarrollo y dependencias.
6	Código fuente Hotel HUB	**3 – Media**	Exposición en repositorios y CI/CD, pero con controles parciales.
7	Servidor IaaS de producción	**4 – Alta**	Exposición constante, dependiente del proveedor cloud y del hardening.
8	Repositorio Git (nube)	**4 – Alta**	Contiene código crítico; credenciales y accesos representan riesgo elevado.
9	Servidor local de desarrollo	**4 – Alta**	Alto riesgo físico y técnico; controles internos limitados.
10	Pipeline CI/CD	**3 – Media**	Probabilidad moderada por fallos recurrentes, dependencias y automatización.
11	Credenciales privilegiadas	**5 – Muy Alta**	Mayor vector de ataque; objetivo prioritario de amenazas deliberadas.
12	Entorno virtual de pruebas	**3 – Media**	Riesgos asociados a fallos, dependencias y uso compartido.
13	Sistema de archivos interno	**3 – Media**	Expuesto a ransomware y errores operativos; monitoreo limitado.
14	Herramientas de gestión (Jira)	**2 – Baja**	Exposición relativamente baja; uso controlado en entorno de gestión.

Nº	Activo	Probabilidad (1–5)	Justificación
15	Computadoras de desarrolladores	**4 – Alta**	Uso intensivo, riesgo de malware, phishing y errores.
16	Router y firewall local	**4 – Alta**	Punto sensible de red; ataques y fallos previsibles.
17	Estaciones administrativas	**3 – Media**	Riesgo de phishing, fallos de hardware y errores humanos.
18	Documentación técnica	**2 – Baja**	Baja probabilidad de incidentes directos, salvo acceso físico.
19	Manuales de usuario	**2 – Baja**	Poca exposición y baja importancia operativa.
20	Correo corporativo	**4 – Alta**	Vector constante de phishing y ataques de credenciales.
21	Modelos de IA/BI	**3 – Media**	Dependencia de entornos cloud y datos sensibles.
22	Tokens API de clientes	**4 – Alta**	Alta probabilidad de explotación si no hay controles robustos.
23	Red interna de oficinas	**4 – Alta**	Riesgo constante por fallos físicos, eléctricos y ataques de red.
24	Dispositivos móviles del staff	**4 – Alta**	Frecuente exposición física y riesgo por pérdida o robo.

3.3.3. Cálculo del nivel de exposición al riesgo

Para calcular el nivel de riesgo de cada activo, se evaluaron dos componentes fundamentales: el impacto que tendría un incidente sobre el activo y la probabilidad de ocurrencia de dicho incidente.

Una vez asignados estos valores de impacto y probabilidad para cada activo, se aplicó la fórmula estándar de análisis de riesgos: Nivel de Riesgo = Impacto × Probabilidad. Esto permitió obtener un valor numérico entre 1 y 25, que luego fue interpretado mediante una escala de cinco niveles (muy bajo, bajo, medio, alto y muy alto/crítico). El resultado final ofrece una visión clara de qué activos presentan mayor riesgo inherente y requieren prioridad en la implementación de controles o medidas de mitigación.

Tabla 25. Escala para la valoración del nivel de riesgo

Nivel de riesgo	Rango numérico	Descripción	Interpretación
1 – Muy Bajo	**1 – 5**	Riesgo marginal. Impacto y probabilidad mínimos.	No requiere acciones inmediatas; se gestiona con controles básicos ya existentes.
2 – Bajo	**6 – 10**	Riesgo limitado, manejable.	Se recomienda monitoreo periódico y fortalecimiento moderado de controles.
3 – Medio	**11 – 15**	Riesgo relevante.	Puede interrumpir operaciones o generar incidentes visibles. Necesita un plan de tratamiento.
4 – Alto	**16 – 20**	Riesgo significativo.	Requiere acciones correctivas prioritarias; alta probabilidad o impacto considerable.
5 – Muy Alto / Crítico	**21 – 25**	Riesgo severo.	Control obligatorio e inmediato. Representa amenaza directa a continuidad, reputación o cumplimiento contractual.

El cálculo del nivel de riesgo inherente se muestra a continuación:

Tabla 26. Cálculo del nivel de riesgo

Nº	Activo	Impacto	Probabilidad	Nivel de Riesgo (I × P)
1	Base de datos GESREST	5 – Muy Alto	4 – Alta	20
2	Base de datos 360.SIS	5 – Muy Alto	4 – Alta	20
3	Base de datos Hotel HUB	5 – Muy Alto	4 – Alta	20
4	Código fuente GESREST	5 – Muy Alto	3 – Media	15
5	Código fuente 360.SIS	5 – Muy Alto	3 – Media	15
6	Código fuente Hotel HUB	5 – Muy Alto	3 – Media	15
7	Servidor IaaS Producción	5 – Muy Alto	4 – Alta	20
8	Repositorio Git (Nube)	5 – Muy Alto	4 – Alta	20
9	Servidor local de desarrollo	4 – Alto	4 – Alta	16
10	Pipeline CI/CD	4 – Alto	3 – Media	12
11	Credenciales privilegiadas	5 – Muy Alto	5 – Muy Alta	25
12	Entorno virtual de pruebas	3 – Medio	3 – Media	9
13	Sistema de archivos interno	3 – Medio	3 – Media	9
14	Herramientas de gestión (Jira)	3 – Medio	2 – Baja	6
15	Computadoras de desarrolladores	3 – Medio	4 – Alta	12
16	Router y firewall local	4 – Alto	4 – Alta	16
17	Estaciones administrativas	3 – Medio	3 – Media	9
18	Documentación técnica	3 – Medio	2 – Baja	6
19	Manuales de usuario	2 – Bajo	2 – Baja	4
20	Correo corporativo	4 – Alto	4 – Alta	16
21	Modelos de IA/BI	4 – Alto	3 – Media	12
22	Tokens API de clientes	5 – Muy Alto	4 – Alta	20
23	Red interna de oficinas	4 – Alto	4 – Alta	16
24	Dispositivos móviles del staff	2 – Bajo	4 – Alta	8

3.3.4. Determinación del apetito al riesgo

El apetito al riesgo representa el nivel de riesgo que Garzasoft está dispuesta a aceptar en el curso normal de sus operaciones, considerando su naturaleza como empresa de desarrollo de software SaaS, su dependencia de plataformas en la nube y la criticidad de los datos que administra.

La propuesta es que Garzasoft tenga un apetito al riesgo bajo, especialmente en lo relacionado con:

a. Datos de clientes
b. Infraestructura de producción
c. Credenciales privilegiadas
d. Tokens API y componentes que permitan acceso directo a sistemas

Esto implica que no se aceptan riesgos altos o críticos (niveles 4 o 5) en activos que puedan comprometer la disponibilidad, integridad, confidencialidad o cumplimiento contractual. Los únicos riesgos aceptables son los niveles muy bajos, bajos y moderados, siempre que no afecten la operación ni la relación con los clientes.

Tabla 27. Nivel de tolerancia al riesgo

Nivel de riesgo	Tolerancia	Requerimiento de acción
1 – Bajo	Aceptable	Se mantiene con controles existentes.
2 – Moderado	Aceptable con monitoreo	Controles básicos y revisión periódica.
3 – Alto	Tolerable por corto plazo	Requiere plan de tratamiento documentado.
4 – Muy Alto	No tolerado	Mitigación obligatoria y prioritaria.
5 – Crítico	Prohibido	Acción inmediata; puede requerir detener operaciones.

3.3.5. Mapa de calor de riesgos

El mapa de calor permite visualizar, de manera inmediata, la criticidad del riesgo combinando: Impacto (1–5) y Probabilidad (1–5)

Tabla 28. Mapa de Calor de Riesgo

Impacto / Probabilidad	1	2	3	4	5
5 – Muy Alto	Moderado	Alto	Muy Alto	Crítico	Crítico
4 – Alto	Moderado	Alto	Alto	Muy Alto	Crítico
3 – Medio	Bajo	Moderado	Alto	Alto	Muy Alto
2 – Bajo	Bajo	Bajo	Moderado	Moderado	Alto
1 – Muy Bajo	Bajo	Bajo	Bajo	Moderado	Moderado

De acuerdo a los resultados obtenidos en el Nivel de Riesgo (Impacto × Probabilidad) y tomando como referencia el mapa de calor, los escenarios de riesgos en Garzasoft son los siguientes:

Tabla 29. Identificación de la tolerancia al riesgo por activo, según su nivel de riesgo

Nº	Activo	Nivel de Riesgo	Categoría	Tolerancia
1	Base de datos GESREST	20	Crítico (5)	Prohibido
2	Base de datos 360.SIS	20	Crítico (5)	Prohibido
3	Base de datos Hotel HUB	20	Crítico (5)	Prohibido
4	Código fuente GESREST	15	Muy Alto (4)	No tolerado
5	Código fuente 360.SIS	15	Muy Alto (4)	No tolerado
6	Código fuente Hotel HUB	15	Muy Alto (4)	No tolerado
7	Servidor IaaS Producción	20	Crítico (5)	Prohibido
8	Repositorio Git (Nube)	20	Crítico (5)	Prohibido
9	Servidor local desarrollo	16	Muy Alto (4)	No tolerado
10	Pipeline CI/CD	12	Alto (3)	Tolerable por corto plazo
11	Credenciales privilegiadas	25	Crítico (5)	Prohibido
12	Entorno virtual pruebas	9	Alto (3)	Tolerable por corto plazo
13	Sistema archivos interno	9	Alto (3)	Tolerable por corto plazo
14	Jira	6	Moderado (2)	Aceptable con monitoreo
15	PC desarrolladores	12	Alto (3)	Tolerable por corto plazo

Nº	Activo	Nivel de Riesgo	Categoría	Tolerancia
16	Router / firewall local	16	Muy Alto (4)	No tolerado
17	Estaciones administrativas	9	Alto (3)	Tolerable por corto plazo
18	Documentación técnica	6	Moderado (2)	Aceptable con monitoreo
19	Manuales usuario	4	Bajo (1)	Aceptable
20	Correo corporativo	16	Muy Alto (4)	No tolerado
21	Modelos IA/BI	12	Alto (3)	Tolerable por corto plazo
22	Tokens API clientes	20	Crítico (5)	Prohibido
23	Red interna oficinas	16	Muy Alto (4)	No tolerado
24	Dispositivos móviles staff	8	Moderado (2)	Aceptable con monitoreo

A continuación se presenta el Mapa de Calor con los activos ubicados en su casilla correspondiente, según su combinación de Impacto – Probabilidad. Para facilitar la visualización, a cada activo le asignamos una etiqueta abreviada, de la siguiente manera:

- **BDG** = Base de datos GESREST
- **BD3** = Base de datos 360.SIS
- **BDH** = Base de datos Hotel HUB
- **CFG**, **CF3**, **CFH** = Código fuente (GESREST, 360.SIS, HotelHUB)
- **IaaS** = Servidor IaaS Producción
- **GIT** = Repositorio Git
- **SRV-D** = Servidor local desarrollo
- **CI/CD** = Pipeline
- **CRED** = Credenciales privilegiadas
- **TEST** = Entorno virtual pruebas
- **FS** = Sistema de archivos
- **JIRA**
- **PC-DEV** = PC desarrolladores
- **FW** = Router y firewall
- **ADM-PC** = Estaciones administrativas
- **DOC** = Documentación técnica
- **MAN** = Manuales usuario
- **MAIL** = Correo corporativo
- **IA/BI**
- **API-TK** = Tokens API
- **RED** = Red interna
- **MOB** = Dispositivos móviles

Tabla 30. Mapa de calor de los riesgos con activos ubicados

Impacto ↓ / Probabilidad →	1	2	3	4	5
5 – Muy Alto			**CFG, CF3, CFH**	**BDG, BD3, BDH, IaaS, GIT, API-TK**	**CRED**
4 – Alto			**CI/CD, IA/BI**	**SRV-D, FW, MAIL, RED**	
3 – Medio		**JIRA, DOC**	**TEST, FS, ADM-PC**	**PC-DEV**	
2 – Bajo	**MAN**			**MOB**	
1 – Muy Bajo					

En base a los resultados de la matriz de riesgos, observamos lo siguiente:

1. Los activos clasificados en el **nivel Crítico (Prohibido)** representan los riesgos más severos para Garzasoft, ya que cualquier incidente que los afecte podría comprometer la continuidad operativa, la integridad de los datos de clientes o incluso la permanencia contractual de la empresa. En este grupo se encuentran las bases de datos de los tres productos SaaS, el servidor IaaS de producción, el repositorio Git, los tokens API de clientes y las credenciales privilegiadas. Su exposición simultánea a una alta probabilidad e impacto convierte a estos activos en puntos de falla que no pueden ser aceptados bajo ninguna circunstancia, requiriendo acciones inmediatas de mitigación, fortalecimiento de controles y monitoreo continuo. Cualquier retraso en su tratamiento podría derivar en interrupciones masivas del servicio o en brechas de seguridad de alto impacto reputacional y legal.

2. Los activos ubicados en el **nivel Muy Alto (No tolerado)** corresponden a componentes cuya exposición representa un riesgo inaceptable para la organización, aunque no tan extremo como el nivel crítico. Este grupo incluye el código fuente de los tres productos, el servidor local de desarrollo, el router o firewall local, el correo corporativo y la red interna de oficinas. Estos activos desempeñan un rol fundamental dentro del ciclo de desarrollo y de la infraestructura operativa, por lo que un incidente podría generar interrupciones relevantes, acceso no autorizado o propagación de amenazas internas. Si bien el riesgo no alcanza el umbral crítico, sigue siendo completamente inaceptable;

en consecuencia, se exige una mitigación prioritaria con enfoque preventivo y correctivo.

3. En los activos clasificados en el **nivel Alto (Tolerable por corto plazo)** se observa un riesgo significativo, aunque gestionable en un periodo limitado. Se trata principalmente de activos de soporte operativo o relacionados con procesos de desarrollo y administración interna, como el pipeline CI/CD, el entorno de pruebas, el sistema de archivos, las estaciones administrativas, los modelos de IA/BI y las computadoras de los desarrolladores. Estos activos requieren la implementación de un plan de tratamiento formal, ya que poseen vulnerabilidades que pueden desencadenar incidentes de impacto relevante si no se gestionan adecuadamente. Aunque el riesgo no exige una acción inmediata, tampoco debe prolongarse su exposición por más tiempo del estrictamente necesario.

4. Los activos que se encuentran en el **nivel Moderado (Aceptable con monitoreo)** son aquellos cuya probabilidad e impacto, aunque presentes, no representan un riesgo severo para la operación. Entre estos activos están Jira, la documentación técnica y los dispositivos móviles del personal. Si bien estos elementos no comprometen directamente la continuidad del negocio ni la integridad de los servicios SaaS, sí requieren vigilancia y controles básicos para evitar que su nivel de riesgo aumente con el tiempo. La estrategia adecuada consiste en mantener políticas de gestión, controles de acceso y monitoreo periódico de su comportamiento.

5. Finalmente, el **nivel Bajo (Aceptable)** agrupa activos que no representan un riesgo significativo para la organización, como los manuales de usuario. Su impacto sobre la operación es marginal y su probabilidad de ocurrencia también es baja, por lo que los controles actuales son suficientes. Estos activos pueden mantenerse sin necesidad de inversiones adicionales en mitigación, siempre que se conserven las prácticas básicas de seguridad y se evalúen de manera periódica para garantizar que no escalen a niveles superiores de riesgo.

3.4. Propuesta del Plan de tratamiento de riesgos

3.4.1. Tratamiento de riesgo según el nivel de exposición al riesgo

El desarrollo de un Plan de Tratamiento de Riesgos es un componente esencial dentro del sistema de gestión de seguridad de la información de Garzasoft, ya que permite definir y priorizar las acciones necesarias para reducir los riesgos identificados a niveles aceptables. Este plan se basa en la evaluación previa del impacto y la probabilidad de ocurrencia de los incidentes, lo que ofrece una visión clara de los activos más expuestos y las amenazas más críticas. Su importancia radica en que establece un camino estructurado y medible para fortalecer la protección de los servicios SaaS, garantizar la continuidad operativa y cumplir con obligaciones contractuales y regulatorias, especialmente aquellas relacionadas con la gestión segura de datos de clientes.

Para su implementación, Garzasoft debe considerar la disponibilidad de recursos, la madurez de sus procesos tecnológicos, la criticidad de los activos afectados y los niveles de tolerancia definidos para cada categoría de riesgo. El plan debe contemplar las cuatro estrategias fundamentales de tratamiento: mitigar, cuando se reduce el riesgo mediante controles técnicos u organizativos; transferir, al delegar parte del riesgo a un tercero mediante servicios o acuerdos; evitar, eliminando la causa o actividad que genera la exposición; y aceptar, cuando el riesgo es lo suficientemente bajo o su tratamiento no justifica el costo. Estas estrategias permiten una gestión equilibrada y coherente con los objetivos del negocio, alineando la seguridad con la operatividad y el crecimiento de Garzasoft.

A continuación se plantea una propuesta de Plan de Tratamiento de los riesgos según los resultados obtenidos y observables en la matriz de riesgo.

Tabla 31. Plan de tratamiento para los riesgos críticos

Activo	Nivel de Riesgo	Estrategia	Acciones Requeridas	Responsable	Duración
Base de datos GESREST	Crítico (5)	Mitigar	Implementar MFA, cifrado en tránsito, hardening, monitoreo continuo	TI Infraestructura	2–4 semanas
Base de datos 360.SIS	Crítico (5)	Mitigar	Reforzar controles de acceso, segmentación de red, políticas de backup verificadas	TI Infraestructura	2–4 semanas
Base de datos Hotel HUB	Crítico (5)	Mitigar	Revisar configuraciones, corregir vulnerabilidades, activar registros auditoría	TI Infraestructura	2–4 semanas
Servidor IaaS Producción	Crítico (5)	Mitigar / Transferir	Hardening, revisión IAM, activar alertas, contratar soporte ampliado del proveedor cloud	Infraestructura / Proveedor Cloud	3–5 semanas
Repositorio Git (Nube)	Crítico (5)	Mitigar	Aplicar ramas protegidas, MFA obligatorio, revisiones de	Desarrollo	2–3 semanas

Activo	Nivel de Riesgo	Estrategia	Acciones Requeridas	Responsable	Duración
			código		
Credenciales privilegiadas	Crítico (5)	Mitigar	Implementar bóveda de credenciales, rotación automática, eliminación de cuentas compartidas	Seguridad / Infraestructura	2 semanas
Tokens API de clientes	Crítico (5)	Mitigar	Regenerar tokens inseguros, activar rate-limit, auditoría de logs	Desarrollo / Seguridad	2–3 semanas

Tabla 32. Plan de tratamiento para los riesgos muy altos

Activo	Nivel	Estrategia	Acciones	Responsable	Duración
Código fuente GESREST	Muy Alto (4)	Mitigar	Integrar análisis SAST/DAST, endurecer control de versiones	Desarrollo	4 semanas
Código fuente 360.SIS	Muy Alto (4)	Mitigar	Revisar dependencias, reforzar revisión por pares	Desarrollo	4 semanas
Código fuente Hotel HUB	Muy Alto (4)	Mitigar	Auditoría de seguridad, control de cambios	Desarrollo	4 semanas
Servidor local desarrollo	Muy Alto (4)	Mitigar	Actualizaciones, control de acceso físico y lógico	Infraestructura	3 semanas
Router / firewall local	Muy Alto (4)	Mitigar	Reconfiguración, actualización de firmware, endurecimiento	Infraestructura	3 semanas
Correo corporativo	Muy Alto (4)	Mitigar / Transferir	Activar DMARC/SPF, filtros antiphishing, capacitación	Infraestructura / Seguridad	2–3 semanas
Red interna oficinas	Muy Alto (4)	Mitigar	Segmentación de red, monitoreo tráfico, control NAC	Infraestructura	4 semanas

Tabla 33. Plan de tratamiento para los riesgos altos

Activo	Nivel	Estrategia	Acciones	Responsable	Duración
Pipeline CI/CD	Alto (3)	Mitigar	Implementar validación automática, acceso restringido	Desarrollo	4 semanas
Entorno virtual pruebas	Alto (3)	Mitigar	Aplicar aislamiento, validación de permisos	QA / Desarrollo	3 semanas
Sistema archivos interno	Alto (3)	Mitigar	Cifrar archivos sensibles, políticas de acceso	Infraestructura	4 semanas
PC desarrolladores	Alto (3)	Mitigar	Antivirus corporativo, control USB, políticas de parcheo	TI Soporte	3 semanas
Estaciones administrativas	Alto (3)	Mitigar	Capacitación, controles de navegación y correo	TI Soporte	2–3 semanas
Modelos IA/BI	Alto (3)	Mitigar	Control de acceso, auditoría de uso, respaldos	Desarrollo / Innovación	3–4 semanas

Tabla 34. Plan de tratamiento para los riesgos moderados

Activo	Nivel	Estrategia	Acciones	Responsable	Duración
Jira	Moderado (2)	Mitigar / Aceptar	Revisar permisos, activar backups automáticos	Gestión de Proyectos	2 semanas
Documentación técnica	Moderado (2)	Aceptar con control	Actualización periódica, control de versiones	Desarrollo	Continuo
Dispositivos móviles staff	Moderado (2)	Mitigar	Aplicar MDM, cifrado, bloqueo remoto	TI Soporte	2 semanas

Tabla 35. Plan de tratamiento para los riesgos bajos

Activo	Nivel	Estrategia	Acciones	Responsable	Duración
Manuales de usuario	Bajo (1)	Aceptar	Mantener políticas actuales, revisión anual	Soporte	Anual

3.4.2. Propuesta de controles para los activos según su criticidad y nivel de exposición al riesgo

La implementación de controles basados en ISO/IEC 27002 resulta fundamental para Garzasoft debido al alto nivel de exposición de sus activos críticos, especialmente aquellos vinculados a sus servicios SaaS, repositorios de código, infraestructura en la nube y credenciales privilegiadas. La norma proporciona un marco estructurado y reconocido internacionalmente para la gestión de la seguridad de la información, permitiendo establecer medidas preventivas, detectivas y correctivas que reducen de manera significativa el riesgo de incidentes operativos, brechas de datos y fallas de servicio. Su adopción no solo fortalece la postura de seguridad de la empresa, sino que también mejora la confianza de los clientes y brinda soporte para cumplir compromisos contractuales y regulatorios.

Para Garzasoft, aplicar estos controles requiere enfocarse en los activos con mayor criticidad y mayor probabilidad de exposición, priorizando los mecanismos de protección para bases de datos, credenciales, infraestructura cloud, repositorios Git y elementos del ciclo de desarrollo seguro. La ISO 27002 proporciona controles clave en áreas como gestión de accesos, protección criptográfica, seguridad en redes, desarrollo seguro, continuidad del negocio y gestión de incidentes, ofreciendo una hoja de ruta clara para fortalecer los procesos internos. La alineación de activos, riesgos y controles permite que las medidas implementadas sean eficaces, proporcionales y orientadas a mitigar los escenarios más relevantes para la organización.

Tabla 36. Propuesta de controles y objetivos de control por activo

Nº	Activo	Nivel de riesgo	Controles ISO 27002 recomendados	Objetivo del control
1	Base de datos GESREST	Crítico	5.18 Protección contra malware; 8.9 Gestión de acceso; 10.1 Cifrado; 8.16 Monitoreo de actividad	Evitar accesos indebidos, garantizar confidencialidad e integridad
2	Base de datos 360.SIS	Crítico	8.2 Segregación de funciones; 8.3 Gestión de identidades; 10.4 Registro de eventos	Garantizar trazabilidad, control de privilegios y detección temprana
3	Base de datos Hotel HUB	Crítico	8.5 Derechos de acceso; 8.28 Endurecimiento técnico; 8.32 Backup seguro	Minimizar riesgo de corrupción o pérdida de datos
4	Código fuente GESREST	Muy Alto	8.30 Seguridad en desarrollo; 8.24 Control de cambios; 8.28 Hardening	Reducir vulnerabilidades en el software y su ciclo de vida
5	Código fuente 360.SIS	Muy Alto	8.31 Gestión de vulnerabilidades; 8.28 Configuraciones seguras	Prevenir explotación de errores de diseño o dependencias

Nº	Activo	Nivel de riesgo	Controles ISO 27002 recomendados	Objetivo del control
6	Código fuente Hotel HUB	Muy Alto	8.25 Revisión técnica; 8.30 Pruebas de seguridad	Garantizar integridad del código antes de despliegues
7	Servidor IaaS Producción	Crítico	8.21 Seguridad en la nube; 8.20 Seguridad en redes; 10.10 Monitoreo continuo	Asegurar disponibilidad y evitar accesos no autorizados
8	Repositorio Git	Crítico	8.9 Control de accesos; 8.15 Autenticación fuerte; 5.23 Concientización	Evitar modificaciones indebidas del código y fugas
9	Servidor local de desarrollo	Muy Alto	8.28 Endurecimiento; 8.5 Accesos mínimos	Reducir exposición por equipos internos vulnerables
10	Pipeline CI/CD	Alto	8.24 Control de cambios; 8.31 Vulnerability testing	Minimizar riesgo en automatización del despliegue
11	Credenciales privilegiadas	Crítico	8.2 Segregación; 8.12 Gestión de contraseñas; 8.15 MFA	Prevenir accesos críticos no autorizados
12	Entorno prueba	Alto	8.29 Aislamiento ambientes; 8.30 Pruebas seguras	Evitar contaminación entre ambientes y filtración de datos
13	Sistema archivos interno	Alto	8.9 Accesos; 10.1 Cifrado	Garantizar integridad de archivos internos
14	Jira	Moderado	8.9 Gestión de accesos; 5.23 Concientización	Controlar permisos y evitar fugas de información
15	PC desarrolladores	Alto	5.18 Antimalware; 7.8 Seguridad endpoint	Reducir riesgo de intrusiones o malware
16	Router/firewall	Muy Alto	8.20 Seguridad red; 8.28 Hardening; 10.10 Monitoreo	Evitar intrusiones o tráfico malicioso
17	Estaciones administrativas	Alto	5.18 Protección malware; 8.9 Accesos	Reducir riesgo de phishing o fuga de credenciales
18	Documentación técnica	Moderado	8.9 Control acceso; 8.24 Control de versiones	Mantener trazabilidad y evitar modificaciones indebidas
19	Manuales usuario	Bajo	5.23 Concientización; 8.33 Eliminación segura	Garantizar divulgación controlada
20	Correo corporativo	Muy Alto	5.23 Capacitación; 8.12 Políticas de contraseña; 8.15 MFA	Reducir riesgo de phishing y secuestro de cuentas
21	Modelos IA/BI	Alto	10.1 Cifrado; 8.14 Protección datos	Evitar manipulación o fuga de modelos
22	Tokens API	Crítico	8.15 MFA; 8.12 Gestión de credenciales; 8.20 Seguridad red	Evitar abuso de integraciones críticas
23	Red interna	Muy Alto	8.20 Segmentación; 8.23 Seguridad Wi-Fi	Reducir movimientos laterales o intercepción
24	Móviles staff	Moderado	7.8 Gestión dispositivos; 10.1 Cifrado	Evitar filtración por pérdida o robo

DISCUSIÓN DE RESULTADOS

4.1. En relación a los antecedentes

Los resultados obtenidos en la evaluación de la gestión de la seguridad de la información y los riesgos tecnológicos en Garzasoft muestran una clara convergencia con la evidencia descrita en estudios previos realizados en instituciones públicas y privadas del Perú. Esta coincidencia confirma que los problemas identificados en la empresa no son casos aislados, sino manifestaciones de una problemática estructural que también ha sido documentada en investigaciones sobre entidades gubernamentales, empresas de servicios informáticos y organizaciones dedicadas al desarrollo de software. En este sentido, comparar los hallazgos con los antecedentes permite situar a Garzasoft dentro de una tendencia nacional respecto a brechas en la gestión del riesgo, falta de controles formales y necesidad de implementar sistemas basados en ISO y MAGERIT.

Los resultados encontrados guardan una estrecha relación con la tesis de Rivera y Valdivia (2021), donde se evidenció que la Dirección Regional de Trabajo carecía de un enfoque metodológico estandarizado para gestionar sus riesgos de seguridad de la información. En Garzasoft se observa una situación análoga: la ausencia de un sistema formal de gestión, la inexistencia de registros sistemáticos de riesgos y la falta de documentación de políticas son indicadores de una gestión reactiva y no metodológica, lo cual coincide con la problemática descrita por dichos autores. Asimismo, en el estudio de Rivera y Valdivia se comprobó estadísticamente que la aplicación de MAGERIT, junto con los lineamientos de la ISO 27001, mejora significativamente la gestión del riesgo. Esta conclusión se refleja también en el caso de Garzasoft, donde la valoración de los riesgos mediante MAGERIT permitió identificar activos críticos, amenazas relevantes y vulnerabilidades recurrentes que previamente no habían sido reconocidas ni priorizadas. La coherencia entre los resultados sugiere que, al igual que en la entidad pública estudiada por Rivera y Valdivia, la aplicación de un modelo integral basado en ISO/MAGERIT permitiría mejorar notablemente la gestión de la seguridad en Garzasoft.

Por otro lado, los resultados encontrados también coinciden con lo reportado por Llontop (2018), quien identificó que la falta de un modelo de gestión de riesgos en empresas de servicios informáticos produce interrupciones recurrentes de los servicios y vulnerabilidades en los activos críticos. Garzasoft presenta una problemática similar: interrupciones en entornos de desarrollo, fallas en repositorios, dependencias vulnerables en producción, errores humanos y falta de controles en acceso privilegiado, todos los cuales

afectan directamente la continuidad del negocio y la calidad del servicio entregado a sus clientes. La investigación de Llontop demostró que un modelo basado en ISO y MAGERIT contribuye a proteger los activos de información y garantizar la continuidad operativa; de manera equivalente, los hallazgos actuales muestran que Garzasoft requiere urgentemente de un marco estructurado que formalice la gestión del riesgo y asegure la protección de su infraestructura tecnológica y de sus aplicaciones SaaS. El paralelismo es claro: tanto en Llontop (2018) como en la presente evaluación, la ausencia de políticas y controles formales se presenta como la causa central de la vulnerabilidad organizacional.

La conexión entre los resultados y la tesis de Sernaque (2022) también es evidente. En el mencionado estudio se abordó la falta de enfoque sistemático para gestionar riesgos en proyectos de desarrollo de software, lo cual conducía a fallas, sobrecostos y retrasos. Garzasoft refleja precisamente este escenario: la ausencia de un SDLC seguro, la falta de revisiones obligatorias de código, el uso de dependencias no verificadas y las deficiencias en las pruebas antes del despliegue generan defectos en producción, vulnerabilidades críticas y tiempos adicionales de corrección. Sernaque concluyó que un modelo basado en ISO/IEC 27000 y MAGERIT permitía gestionar eficazmente los riesgos asociados al desarrollo de software. Los resultados en Garzasoft corroboran esta afirmación, ya que la aplicación de MAGERIT permitió identificar riesgos específicos del ciclo de vida de desarrollo, mientras que los controles ISO 27002 mostraron ser adecuados para corregir las debilidades técnicas y operativas detectadas. De manera natural, los hallazgos refuerzan la idea de que la gestión de riesgos en software debe integrarse desde la planificación del proyecto, tal como plantea Sernaque.

Asimismo, la tesis de Cajusol y Chinchay (2020) guarda una relación directa con los resultados actuales. Ellos demostraron que en una empresa de producción de software la falta de controles ISO y un análisis formal basado en MAGERIT expone la integridad y confidencialidad de los activos. En Garzasoft se evidenció una situación muy similar: el código fuente, las bases de datos de clientes, los repositorios cloud y los pipelines de despliegue carecen de controles consistentes, lo cual compromete la seguridad del software y de la información manejada. Cajusol y Chinchay concluyeron que diseñar un SGSI completo bajo ISO 27001 y MAGERIT permitía estructurar un marco robusto de protección; esta conclusión está totalmente alineada con los resultados obtenidos en Garzasoft, donde se ha demostrado que la empresa necesita integrar controles, políticas, procedimientos y procesos de tratamiento del riesgo para reducir su exposición.

La tesis de Mogollón (2023) también respalda los hallazgos obtenidos. El autor identificó que una gestión inadecuada de riesgos en una entidad pública generaba amenazas significativas a la continuidad operativa y a la seguridad de los datos. En Garzasoft se revelearon riesgos muy similares: capacidad limitada de recuperación, ausencia de backups verificados, fallas en la infraestructura local y vulnerabilidades en la nube. Mogollón demostró que el uso de MAGERIT permitió categorizar activos, amenazas y vulnerabilidades de manera precisa. El proceso aplicado en Garzasoft produjo resultados equivalentes: permitió identificar activos críticos como el código fuente, las bases de datos y la infraestructura cloud, logrando construir un mapa de riesgos claro y priorizado. Ambos casos confirman que MAGERIT es altamente efectivo en la categorización y priorización de riesgos en contextos donde la información es un activo central.

Finalmente, los resultados muestran una gran similitud con los expuestos por Huamán (2023), quien demostró que la implementación de un SGSI y un análisis de riesgos basado en MAGERIT permitió reducir incidencias y mejorar significativamente la protección de los activos de TI. En Garzasoft, la evaluación también evidenció incidencias recurrentes —errores de acceso, fallas en bases de datos, interrupciones en los servicios, vulnerabilidades de código— que podrían mitigarse mediante un SGSI bien diseñado. La experiencia reportada por Huamán confirma que el impacto de un SGSI se expresa directamente en la reducción de fallas operativas, lo cual respalda la pertinencia del modelo propuesto para Garzasoft.

4.2. En relación a los fundamentos teóricos

Los resultados obtenidos en la evaluación de la seguridad de la información en Garzasoft permiten comprender cómo una empresa de desarrollo de software en crecimiento enfrenta riesgos propios de su naturaleza operativa y tecnológica, y cómo estos se relacionan con los antecedentes investigativos y los fundamentos teóricos de la gestión de riesgos, los sistemas de gestión de seguridad de la información y la metodología MAGERIT. Al analizar los activos, las amenazas, las vulnerabilidades y los niveles de riesgo, se evidencia que Garzasoft reproduce un patrón observado de manera recurrente en empresas tecnológicas peruanas y latinoamericanas que crecen rápidamente sin contar con un marco formal de seguridad. Esta coincidencia refuerza la validez de los hallazgos y confirma que la situación identificada no es un caso aislado, sino una problemática estructural que se ajusta a lo documentado en la literatura especializada.

Los antecedentes consultados reportan que, en el Perú, la mayoría de empresas de desarrollo de software carecen de procesos maduros de seguridad, lo cual genera impactos negativos tanto operativos como reputacionales. Estudios recientes han demostrado que más del 78% de empresas nacionales sufren fallas de software asociadas a errores y vulnerabilidades no gestionadas, fenómeno que se repite exactamente en Garzasoft, donde se identificaron vulnerabilidades críticas en el código, dependencias desactualizadas y fallos en el pipeline CI/CD. Asimismo, autores como EY Perú señalan que la adopción acelerada de servicios en la nube genera nuevas formas de riesgo cuando no se aplican controles adecuados de configuración, lo cual coincide plenamente con los hallazgos de esta investigación, que muestran configuraciones débiles en IAM, ausencia de auditoría de logs y prácticas inadecuadas de protección de los entornos cloud utilizados por la empresa.

El marco teórico de ISO/IEC 27001 establece que el primer paso para gestionar la seguridad de la información consiste en comprender el contexto organizacional y definir un alcance claro. En Garzasoft no existía un alcance documentado ni una política general de seguridad, lo cual contraviene directamente los principios de la norma. También se verificó que la gestión de riesgos era reactiva, no documentada y altamente dependiente de la experiencia del personal, confirmando lo descrito en la teoría sobre las organizaciones con niveles de madurez inicial: la seguridad depende más de esfuerzos individuales que de procesos estandarizados. Esta condición, además de ser un indicador de inmadurez organizacional, incrementa la probabilidad de fallas, ya que no existe un sistema que permita asegurar que los controles se aplican de manera consistente.

La aplicación de la metodología MAGERIT confirmó la existencia de riesgos críticos estrechamente vinculados a los activos más valiosos de la empresa, como el código fuente, la infraestructura cloud y las bases de datos de clientes. Los riesgos identificados —acceso no autorizado a privilegios, vulnerabilidades del código, ransomware, configuraciones erróneas en la nube y errores humanos en la base de datos— reflejan exactamente los escenarios de riesgo descritos en la literatura técnica sobre análisis de riesgos en TI. En particular, MAGERIT plantea que las organizaciones con procesos informales generan niveles de exposición elevados, ya que los activos esenciales no cuentan con la protección mínima aceptable para garantizar la confidencialidad, integridad y disponibilidad. Esta afirmación se ve respaldada por los resultados obtenidos, en donde la ausencia de controles como MFA, monitoreo centralizado de logs, segmentación de redes, revisión de código y pruebas de seguridad refuerza la idea de que Garzasoft opera con una arquitectura vulnerable que requiere una intervención sistemática.

Asimismo, los resultados coinciden con la teoría de ISO/IEC 27002, la cual detalla controles específicos para cada ámbito de la seguridad. La falta de segregación de funciones, la ausencia de controles de privilegios, la inexistencia de un esquema formal de gestión de accesos y el control limitado de dispositivos y accesos físicos reflejan una brecha directa con los controles establecidos por la norma. Del mismo modo, la ausencia de procesos formales de desarrollo seguro confirma lo expuesto en modelos como OWASP SAMM y el estándar ISO 27034, que señalan que sin revisión de código, pruebas continuas y análisis de vulnerabilidades, los sistemas SaaS tienden a presentar defectos que pueden escalar hacia incidentes mayores. En Garzasoft, esta problemática se expresa en vulnerabilidades críticas del software y en riesgos evidentes en los entornos de desarrollo y despliegue.

Los hallazgos también confirman que el crecimiento acelerado de la empresa incrementó la complejidad de los procesos, lo cual es coherente con la teoría de madurez organizacional: a mayor tamaño y diversidad de proyectos, mayor es la necesidad de contar con procesos formales de seguridad. La evidencia muestra que el aumento de clientes, productos y operaciones de Garzasoft no estuvo acompañado de una estructura de seguridad que evolucione al mismo ritmo, generando riesgos acumulativos que se manifiestan en errores humanos, infraestructuras mal configuradas y deficiencias en la gestión del ciclo de vida del software.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

1. Se concluye que el modelo de gestión de la seguridad de la información propuesto, sustentado en los lineamientos de ISO/IEC 27001, complementado con los controles de ISO/IEC 27002 y articulado con el análisis de riesgos de MAGERIT, constituye una propuesta viable, pertinente y eficaz para mitigar los riesgos tecnológicos presentes en Garzasoft. El modelo integra procesos, políticas, procedimientos y controles que responden directamente a las brechas documentadas, permitiendo una reducción significativa de la exposición al riesgo y sentando las bases para una gestión continua y sostenible de la seguridad de la información.

2. El diagnóstico realizado permitió identificar que Garzasoft carecía de políticas formales de seguridad, procedimientos documentados, controles técnicos consolidados y un enfoque sistemático de gestión de riesgos. Se evidenció una fuerte dependencia de prácticas reactivas, ausencia de segregación de funciones, fallas en el control de accesos, debilidades en el SDLC, configuraciones inseguras en la nube y un monitoreo limitado de los incidentes. Este diagnóstico reveló que la empresa se encuentra en un nivel de madurez bajo en términos de gestión de la seguridad de la información, lo que justificó plenamente la necesidad de un SGSI formal.

3. La aplicación de MAGERIT permitió identificar los activos más críticos de Garzasoft —como el código fuente, la infraestructura cloud, las bases de datos y los repositorios de desarrollo— e identificar amenazas y vulnerabilidades que afectan la operación y la seguridad del negocio. La valoración mediante la matriz de riesgo determinó la existencia de riesgos críticos y muy altos, principalmente relacionados con accesos privilegiados, vulnerabilidades del código, ransomware y errores de configuración en la nube. Esta evaluación facilitó la priorización objetiva de los riesgos y validó la utilidad de MAGERIT como marco riguroso y adaptable al entorno tecnológico de la empresa.

4. El diseño del SGSI propuesto respondió de manera directa a las brechas identificadas y se estructuró conforme al ciclo PDCA de ISO/IEC 27001. El modelo incluye políticas, procedimientos, roles, controles técnicos y organizacionales alineados con ISO/IEC 27002, así como un plan de tratamiento que emplea estrategias de reducción, evitación, transferencia y aceptación del riesgo. La integración de MAGERIT permitió asegurar que los controles propuestos correspondieran con los riesgos evaluados, garantizando que la propuesta fuera coherente, completa y ajustada a la realidad operativa y tecnológica de Garzasoft.

5. El modelo propuesto está orientado a que la aplicación de los controles ISO 27002, junto con el proceso de análisis de riesgos de MAGERIT, reduzcan considerablemente los niveles de riesgo identificados inicialmente. Los riesgos críticos fueron mitigados mediante medidas de control de accesos, autenticación multifactor, seguridad en el desarrollo, gestión de configuraciones y endurecimiento de la nube. Los riesgos altos y moderados también encontraron soluciones eficaces mediante backups verificados, monitoreo centralizado, políticas formales y la instauración de un proceso de gestión de incidentes. Los resultados evidencian que el SGSI propuesto es pertinente, efectivo y capaz de elevar sustancialmente la seguridad tecnológica de Garzasoft.

6. Los hallazgos obtenidos permiten aceptar la hipótesis planteada. La integración de ISO/IEC 27000 y MAGERIT no solo permitió identificar y evaluar los riesgos presentes, sino que también facilitó el diseño de controles, políticas y procedimientos que reducen significativamente la exposición al riesgo. Los resultados demuestran que el modelo propuesto constituye una herramienta con potencial para mitigar los riesgos de TI en Garzasoft, fortalecer la confiabilidad de sus sistemas y mejorar la protección de sus activos de información.

RECOMENDACIONES

1. La presente investigación se centró en la gestión de riesgos de TI basada en ISO/IEC 27000 y MAGERIT; sin embargo, es necesario reevaluar el nivel de madurez organizacional en seguridad de la información con otros criterios. Se recomienda que futuras investigaciones incorporen modelos de madurez como: CMMI para Servicios (CMMI-SVC), COBIT 2019 – Gestión y Gobierno de TI o NIST Cybersecurity Framework (CSF). Esto permitiría determinar con mayor precisión el grado de preparación, resiliencia y cultura de seguridad en Garzasoft, así como identificar brechas a nivel de gobernanza, liderazgo y toma de decisiones, dimensiones que excedieron el alcance del estudio actual.

2. La investigación no analizó en el impacto financiero de los riesgos identificados ni en la medición del retorno económico de los controles propuestos debido a las limitaciones para tener acceso a dicha información. Se recomienda desarrollar estudios futuros orientados a:
   - cuantificar pérdidas por inactividad, fuga de datos o fallas de software,
   - estimar el costo-beneficio de implementar controles ISO 27002,
   - simular escenarios económicos usando modelos de análisis
   - evaluar el impacto financiero comparativo antes y después del SGSI.

   Esto permitiría sustentar inversiones en seguridad de manera objetiva, especialmente en empresas medianas como Garzasoft donde los recursos presupuestales son limitados.

3. Aunque la investigación incorporó elementos de seguridad en el Ciclo de vida de desarrollo del software, no profundizó en prácticas avanzadas de automatización y seguridad continua basadas en DevSecOps. Futuros estudios podrían diseñar o validar un modelo DevSecOps adaptado a la realidad de empresas desarrolladoras de software en crecimiento, lo cual permitiría:
   - mejorar la seguridad desde la codificación,
   - reducir vulnerabilidades tempranas,
   - fortalecer los pipelines CI/CD (conjunto automatizado de procesos que permite construir, probar y desplegar software de manera rápida)
   - disminuir la dependencia de revisiones manuales.

REFERENCIAS CONSULTADAS

1. Cajusol, L. C., & Chinchay, G. M. (2020). *Diseño de un Sistema de Gestión de Seguridad de Información basado en la norma ISO/IEC 27001:2013 para una empresa de producción de software* [Tesis de Bachiller, Universidad Tecnológica del Perú]. Repositorio Institucional UTP.
2. Calder, A. (2022). *ISO27001:2022 – The ultimate guide to implementing an ISMS*. IT Governance Publishing.
3. Calder, A., & Watkins, S. (2015). *Information Security Risk Management for ISO 27001/ISO 27002*. IT Governance Publishing.
4. ESET. (2025). *Reporte de amenazas 2025*.
5. Huamán, W. M. (2023). *Sistema gestor de seguridad de la información para reducir incidencias en activos de TI en la empresa MP Constructores SAC 2021* [Tesis de Licenciatura, Universidad Nacional del Centro del Perú]. Repositorio Institucional UNCP.
6. Humphreys, E. (2016). *Implementing the ISO/IEC 27001:2013 ISMS Standard*. BSI Standards.
7. IBM Security. (2024). *X-Force Threat Intelligence Index 2024*.
8. Infobae. (2025). *Impacto económico de fallas de software y ciberataques en Perú*.
9. Infobae. (2025a). *Empresas peruanas y la baja adopción de seguros contra ciberataques*.
10. Interfases - Portal de Revistas Ulima. (2021). *Gestión de riesgos y calidad del software*.
11. International Organization for Standardization. (2018). *ISO/IEC 27000:2018 — Information technology — Security techniques — Information security management systems — Overview and vocabulary*. ISO.
12. International Organization for Standardization. (2022). *ISO/IEC 27001:2022 — Information security, cybersecurity and privacy protection — Information security management systems*. ISO.
13. International Organization for Standardization. (2022). *ISO/IEC 27002:2022 — Information security, cybersecurity and privacy protection — Information security controls*. ISO.
14. ISO. *(2022). ISO/IEC 27001:2022 — Information Security, Cybersecurity and Privacy Protection.*
15. *LinkTIC. (2024). Panorama de ciberseguridad en el Perú.*
16. *Llontop, S. (2018).* Modelo de gestión de riesgos de TI que contribuye en la protección de los activos de información en una empresa de servicios informáticos *(Tesis de pregrado). Universidad Católica Santo Toribio de Mogrovejo*.
17. Ministerio de Hacienda y Función Pública. (2012). *MAGERIT – Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (Versión 3).* Gobierno de España.
18. Mogollon, M. *E. (2023).* Desarrollo de un modelo de gestión de riesgos basado en la metodología MAGERIT para minimizar los riesgos de la implantación y uso de TI en una Municipalidad del Perú *[Tesis de Licenciatura, Universidad Señor de Sipán]*. *Repositorio Institucional USS.*
19. *Observatorio Nacional de Prospectiva. (2025). Informe sobre vulnerabilidades y gestión de activos tecnológicos en Perú.*
20. *OWASP Foundation. (2021). OWASP Software Assurance Maturity Model (SAMM). OWASP*.

21. *Rivera, D. y Valdivia, J. (2021).* Implementación de la metodología Magerit V3 para mejorar la gestión de riesgos de Seguridad de la Información y propuesta de Políticas de Seguridad basadas en Norma Técnica Peruana ISO/IEC 27001:2014 en la Dirección Regional de Trabajo y Promoción del Empleo de Huánuco – 2021 *(Tesis de pregrado). Universidad Nacional Hermilio Valdizán.*
22. *Rumbo Económico. (2025). Estado de la ciberseguridad y amenazas digitales en el Perú.*
23. *Sernaque, J. (2022).* Modelo para la gestión de riesgos de desarrollo de software bajo la perspectiva de la gestión de proyectos *[Tesis de Maestría, Universidad José Carlos Mariátegui]*. *Repositorio Institucional UJCM.*
24. *Tricentis. (2025). Quality Report Latinoamérica 2025.*
25. *Von Solms, R., & Van Niekerk, J. (2013). Information Security Governance. Springer.*

ANEXOS

Anexo 1: Lista de verificación de controles ISO 27001/27002

Propósito: Evaluar el nivel de implementación y madurez de los controles de seguridad en Garzasoft, según los dominios de la ISO/IEC 27001 y 27002.

Instrucciones: Marcar el grado de cumplimiento según la evidencia observada: 0 = No implementado | 1 = Parcial | 2 = Implementado | 3 = Implementado y eficaz

Dominio ISO	Control	Evidencia observada	Nivel de cumplimiento	Observaciones
A.5	Políticas de seguridad			
A.7	Seguridad de RRHH			
A.8	Gestión de activos			
A.9	Control de accesos			
A.10	Cifrado			
A.12	Seguridad operacional			
A.14	Seguridad en desarrollo			
A.16	Gestión de incidentes			
A.17	Continuidad del negocio			

Anexo 2. Guía de observación técnica (MAGERIT v3)

Propósito: Registrar evidencias objetivas sobre configuraciones, procesos, infraestructura y controles técnicos aplicados en Garzasoft.

Instrucciones: Completar durante la inspección directa de sistemas, servidores, redes y procedimientos. Anotar hechos verificables.

Área observada	Elemento evaluado	Evidencia encontrada	Riesgo asociado	Observaciones
Infraestructura TI	Servidores			
Redes	Configuración firewall			
Desarrollo	Repositorios Git			
Producción	BD y servicios SaaS			
Soporte	Procedimientos operativos			
Físico	Acceso a oficinas			

Anexo 3. Guía de entrevista semiestructurada

Propósito: Obtener información cualitativa sobre prácticas, problemas, vulnerabilidades y procedimientos del personal de Garzasoft.

Instrucciones: Formular las preguntas de manera abierta y registrar las respuestas textuales.

Pregunta	Respuesta del entrevistado	Observaciones
¿Cómo gestionan actualmente los accesos privilegiados?		
¿Qué controles aplican en el desarrollo de software?		
¿Existen procedimientos formales para incidentes?		
¿Cómo realizan backups y restauraciones?		
¿Qué dificultades encuentran en la seguridad de la información?		