UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO

Facultad de Ingeniería Civil, Sistemas y de Arquitectura

Escuela Profesional de Ingeniería de Sistemas

TESIS

Sistema de Gestión de la Seguridad de la Información para los procesos de soporte y desarrollo de software SaaS de la empresa Iteprevengo

PARA OBTENER EL TÍTULO PROFESIONAL DE:

Ingeniero de sistemas

Autores:

Bach. Guerrero Diaz Lalita

Bach. Alberca Cubas Kevin

Asesor:

Mg. Ing. Arteaga Lora, Roberto Carlos

Lambayeque – Perú

12 de junio del 2026

UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO

Facultad de Ingeniería Civil, Sistemas y de Arquitectura

Escuela Profesional de Ingeniería de Sistemas

TESIS

Sistema de Gestión de la Seguridad de la Información para los procesos de soporte y desarrollo de software SaaS de la empresa Iteprevengo

PARA OBTENER EL TÍTULO PROFESIONAL DE:

Ingeniero de sistemas

Autores:

Bach. Guerrero Diaz Lalita

Bach. Alberca Cubas Kevin

Asesor:

Mg. Ing. Arteaga Lora, Roberto Carlos

Lambayeque – Perú

2026

UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO

Facultad de Ingeniería Civil, Sistemas y de Arquitectura

Escuela Profesional de Ingeniería de Sistemas

TESIS

Sistema de Gestión de la Seguridad de la Información para los procesos de soporte y desarrollo de software SaaS de la empresa Iteprevengo

PARA OBTENER EL TÍTULO PROFESIONAL DE:

Ingeniero de sistemas

APROBADO POR EL SIGUIENTE JURADO

Msc. Ing. Omar Wilton Saavedra Salazar
Presidente

Dr. Ing. Juan Villegas Cubas
Secretario

Msc. Ing. Oscar Efrain Capuñay Uceda
Vocal

UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO

Facultad de Ingeniería Civil, Sistemas y de Arquitectura

Escuela Profesional de Ingeniería de Sistemas

TESIS

Sistema de Gestión de la Seguridad de la Información para los procesos de soporte y desarrollo de software SaaS de la empresa Iteprevengo

PARA OBTENER EL TÍTULO PROFESIONAL DE:

Ingeniero de sistemas

Msc. Ing. Roberto Carlos Arteaga Lora
Asesor

Lalita Guerrero Diaz
Bach. en Ingeniería de Sistemas

Kevin Alberca Cubas
Bach. en Ingeniería de Sistemas

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

ACTA DE SUSTENTACIÓN N°008-2026-UI-FICSA

Siendo las 10:30 am horas del día 12 de junio del 2026, se reunieron de manera presencial los miembros de jurado de la tesis titulada: **"SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN PARA LOS PROCESOS DE SOPORTE Y DESARROLLO DE SOFTWARE SAAS DE LA EMPRESA ITEPREVENGO", con código N° IS_V_2024_013,** designado por **Resolución Decanal Virtual N° 461-2024-UNPRG-FICSA** con la finalidad de Evaluar y Calificar la sustentación de la tesis antes mencionada, conformado por los siguientes docentes:

MSC. ING. OMAR WILTON SAVEDRA SALAZAR	PRESIDENTE
DR.ING.JUAN ELIAS VILLEGAS CUBAS	SECRETARIO
MSC. ING. OSCAR EFRAIN CAPUÑAY UCEDA	VOCAL

Asesorado por MSC. ING. ROBERTO CARLOS ARTEAGA LORA.

El acto de sustentación fue autorizado por **OFICIO VIRTUAL N° 138-2026-UIFICSA**, la tesis fue presentada y sustentada por los Bachilleres: **LALITA GUERRERO DIAZ Y KEVIN ALBERCA CUBAS,** tuvo una duración de ...70.....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
LALITA GUERRERO DIAZ	18	DIECIOCHO	MUY BUENO
KEVIN ALBERCA CUBAS	18	DIECIOCHO	MUY BUENO

Por lo que quedan **APTOS** para obtener el Título Profesional de **INGENIERO (A) 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 ..11:50 an.. Se dio por concluido el presente acto académico, dándose conformidad al presente acto, con la firma de los miembros del jurado.

MSC. ING. OMAR WILTON SAVEDRA SALAZAR
PRESIDENTE

DR.ING.JUAN ELIAS VILLEGAS CUBAS
SECRETARIO

MSC. ING. OSCAR EFRAIN CAPUÑAY UCEDA
VOCAL

MSC. ING. ROBERTO CARLOS ARTEAGA LORA
ASESOR

JHFF/bcm

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

"Año de la Esperanza y el Fortalecimiento de la Democracia"

CONSTANCIA DE APROBACIÓN DE ORIGINALIDAD DE TESIS

Según Res. N° 659-2020-R

Yo, ARTEAGA LORA ROBERTO CARLOS, asesor de la Tesis de los bachilleres:

GUERRERO DIAZ LALITA
ALBERCA CUBAS KEVIN

Titulada:

"SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN PARA LOS PROCESOS DE SOPORTE Y DESARROLLO DE SOFTWARE SAAS DE LA EMPRESA ITEPREVENGO"

Luego de la revisión exhaustiva del documento constato que la misma tiene un índice de similitud de 17**%** verificable en el reporte de similitud del programa TURNITIN.

El suscrito analizó dicho reporte y concluyó que, cada una de las coincidencias detectadas NO CONSTITUYEN PLAGIO. A mi leal saber y entender, la tesis cumple con todas las normas para el uso de citas y referencias establecidas por la Universidad Nacional Pedro Ruiz Gallo. Se expide la presente según lo dispuesto en la Resolución Nº 659-2020-R, de fecha 8 de setiembre de 2020, que aprueba la directiva para la evaluación de originalidad de los documentos académicos, de investigación formativa y para la obtención de Grados y Títulos de la UNPRG.

Lambayeque, 14 de abril de 2026

Atentamente,

MAG. ING. ROBERTO CARLOS ARTEAGA LORA
DNI: 16755764

Se adjunta:

- Recibo digital
- Revisión de informe en Turnitin

SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN PARA LOS PROCESOS DE SOPORTE Y DESARROLLO DE SOFTWARE SAAS DE LA EMPRESA ITEPREVENGO

INFORME DE ORIGINALIDAD

17%	15%	10%	8%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	hdl.handle.net Fuente de Internet	5%
2	Submitted to Universitat Oberta de Catalunya Trabajo del estudiante	2%
3	repositorio.unal.edu.co Fuente de Internet	1%
4	fonseca-guajira.gov.co Fuente de Internet	1%
5	repositorio.undac.edu.pe Fuente de Internet	1%
6	bffrepositorio.unal.edu.co Fuente de Internet	1%
7	www.adinelsa.com.pe Fuente de Internet	1%
8	pdfcoffee.com Fuente de Internet	1%
9	www.congreso.gob.pe Fuente de Internet	1%
10	Submitted to Universidad Nacional Pedro Ruiz Gallo Trabajo del estudiante	<1%
11	repositorio.unprg.edu.pe Fuente de Internet	<1%
12	Submitted to Universidad Politécnica de Madrid Trabajo del estudiante	<1%
13	qdoc.tips Fuente de Internet	<1%
	repository.unad.edu.co	

Mag. Ing. Roberto Carlos Arteaga Lora
DNI: 16755764
Asesor

14	Fuente de Internet	<1 %
15	Guamán Muela, Franklin Vinicio. "Desarrollo de un Sistema de Gestión de Seguridad de la Información (SGSI) utilizando la norma ISO/27001 para la protección de datos en la Unidad Educativa La Inmaculada de la ciudad de Ambato.", Universidad Católica de Cuenca (Ecuador) Publicación	<1 %
16	upc.aws.openrepository.com Fuente de Internet	<1 %
17	repositorio.upse.edu.ec Fuente de Internet	<1 %
18	Santos Llanos, Daniel Elías. "Gestión de Riesgos de Seguridad de Información, Bajo el Estándar ISO/IEC 27005:2022, Aplicando Ontologías de Dominio.", Pontificia Universidad Catolica del Peru (Peru), 2024 Publicación	<1 %
19	Submitted to Universidad Nacional de Colombia Trabajo del estudiante	<1 %
20	ERM PERU S.A.. "EIA para la Ampliación del Programa de Exploración y Desarrollo en el Lote 88-IGA0000175", R.D. N° 035-2014-MEM/AAE, 2020 Publicación	<1 %
21	Submitted to Universidad Privada del Norte Trabajo del estudiante	<1 %
22	Submitted to Universidad de Santiago de Chile Trabajo del estudiante	<1 %
23	María Palacios Guillem. "Propuesta de un nuevo procedimiento basado en la norma ISO 9001 para la gestión conjunta de la norma ISO 31000, la filosofía Kaizen y la herramienta Lean Manufacturing en pymes industriales de la Comunidad Valenciana.", Universitat Politecnica de Valencia, 2021 Publicación	<1 %

Mag. Ing. Roberto Carlos Arteaga Lora
DNI: 16755764
Asesor

24	Pedro Pablo Poveda Orjuela. "Configuración de un modelo conceptual para los sistemas de gestión "qhse3+", con perspectiva de rendimiento energético y administración integral de riesgos", Universitat Politecnica de Valencia, 2021 Publicación	<1 %
25	Submitted to Universidad Internacional de la Rioja Trabajo del estudiante	<1 %
26	Llatasi, Fanny Luz Calizaya. "Propuesta e implementación de un sistema de gestión de seguridad para reducir los riesgos y peligros según ISO 45001 en la corporación Caliz S.A.C. - Puno", Universidad Nacional del Altiplano de Puno (Peru) Publicación	<1 %
27	Venegas Carazas, Lizbeth Lucy. "Implementación de un sistema de gestión ambiental en la empresa constructora SICMA S.A.C. - Región Puno", Universidad Nacional del Altiplano de Puno (Peru) Publicación	<1 %
28	Jennifer Jomaira Loayza Castro, Daniel Jacobo Andrade Pesántez. "Modelo de madurez de seguridad de información de Sistemas Integrales de Gestión de Riego y Drenaje", Religación, 2025 Publicación	<1 %
29	Vargas Barrios, Pedro Julio. "Modelo de Seguridad Para Plataformas Colaborativas de E-Ciencia Sobre Cloud Computing", Universidad Distrital Francisco José de Caldas (Colombia), 2024 Publicación	<1 %
30	"Gestión del cambio para la sostenibilidad socioeconómica de las naciones", Alianza de Investigadores Internacionales SAS, 2025 Publicación	<1 %
31	ECOLOGIA Y TECNOLOGIA AMBIENTAL S.A.C. "MEIA para la Implementación del Proyecto	<1 %

Mag. Ing. Roberto Carlos Arteaga Lora
DNI: 16755764
Asesor

	Implementar Línea de Cal, Mejoras Ambientales e Integración de Instrumentos Ambientales en la Planta Condorcocha-IGA0006877", R.D. N° 081-2018-PRODUCE/DVMYPE-I/DIGGAM, 2020 Publicación	
32	Ruiz Márquez, José A.. "Eslabones internos y externos de la cadena de distribución de datos como causa de brechas en entidades reguladas por HIPAA en Puerto Rico, Louisiana y Nevada.", Inter-American University of Puerto Rico (Puerto Rico) Publicación	<1 %
33	Submitted to Universidad San Marcos Trabajo del estudiante	<1 %
34	Submitted to utn Trabajo del estudiante	<1 %
35	Navira Angulo-Murillo, Jhoanna Cárdenas-Encalada, Francisco Bolaños-Burgos. "LA CONTINUIDAD DE NEGOCIO EN LAS INSTITUCIONES DE EDUCACIÓN SUPERIOR DEL ECUADOR. CASO DE ESTUDIO.", REVISTA CIENTÍFICA MULTIDISCIPLINARIA ARBITRADA "YACHASUN", 2020 Publicación	<1 %
36	Submitted to Universidad Carlos III de Madrid - EUR Trabajo del estudiante	<1 %
37	repositorio.upn.edu.pe Fuente de Internet	<1 %
38	Humpiri Flores, Milton Edward. "Modelo de convención con controles de auditoría y seguridad de base de datos relacionales, 2023", Universidad Nacional del Altiplano de Puno (Peru) Publicación	<1 %
39	Submitted to consultoriadeserviciosformativos Trabajo del estudiante	<1 %

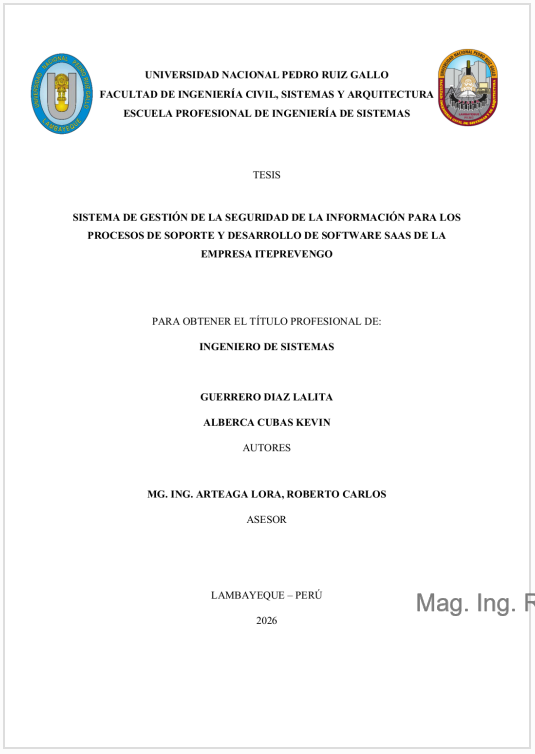
Mag. Ing. Roberto Carlos Arteaga Lora
DNI: 16755764
Asesor

Recibo digital

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

La primera página de tus entregas se muestra abajo.

Autor de la entrega:	Lalita Guerrero Diaz; Kevin Alberca Cubas
Título del ejercicio:	Proyectos de tesis
Título de la entrega:	SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN...
Nombre del archivo:	INFORME_FINAL_DE_TESIS_2026.pdf
Tamaño del archivo:	6.71M
Total páginas:	263
Total de palabras:	53,369
Total de caracteres:	314,304
Fecha de entrega:	14-abr-2026 12:09p. m. (UTC-0500)
Identificador de la entrega:	2931905861



UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO
FACULTAD DE INGENIERÍA CIVIL, SISTEMAS Y ARQUITECTURA
ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

TESIS

SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN PARA LOS PROCESOS DE SOPORTE Y DESARROLLO DE SOFTWARE SAAS DE LA EMPRESA ITEPREVENGO

PARA OBTENER EL TÍTULO PROFESIONAL DE:

INGENIERO DE SISTEMAS

GUERRERO DIAZ LALITA

ALBERCA CUBAS KEVIN

AUTORES

MG. ING. ARTEAGA LORA, ROBERTO CARLOS

ASESOR

LAMBAYEQUE – PERÚ

2026

Mag. Ing. Roberto Carlos Arteaga Lora
DNI: 16755764
Asesor

DEDICATORIA

A mis padres,
por ser mi pilar, mi guía y mi refugio constante.
Por su amor incondicional y sus sacrificios silenciosos.
A mi hermano,
por enseñarme, con su ejemplo,
que los grandes logros nacen del sacrificio y la constancia.
Este logro también les pertenece.

Lalita Guerrero Diaz

A mis padres,
por ser el cimiento de todo lo que soy.
Por cada sacrificio silencioso,
cada palabra de aliento y
cada acto de amor que hizo posible este camino.
Este logro también es suyo.

Kevin Alberca Cubas

AGRADECIMIENTOS

A Dios, por ser mi guía en cada paso de este camino y por concederme la sabiduría y la perseverancia necesarias para no rendirme cuando este proceso se tornó difícil.

A mi familia, por acompañarme y esforzarse cada día a lo largo de estos años de carrera para que esta meta fuera posible. Solo nosotros conocemos el esfuerzo y la historia que hay detrás de este título.

A mi compañero de tesis y enamorado, Kevin Alberca, porque más allá del resultado, este camino nos permitió aprender a trabajar juntos, crecer y apoyarnos mutuamente, tanto en lo académico como en lo personal.

A nuestro asesor, el Mg. Ing. Roberto C. Arteaga L. por su orientación y acompañamiento a lo largo de este proceso de investigación.

Al Ing. Herbert Parimango, gerente de Iteprevengo, por su apertura, disposición y apoyo para facilitar el desarrollo de este estudio dentro de su organización.

Un agradecimiento especial al Dr. Ing. Ernesto K. Celi A., la Dra. Ing. Jessie L. Bravo J. y el Bach. Cristian M. Guevara R., por su rol como expertos validadores y por sus valiosos aportes que enriquecieron esta investigación y que esperamos sea un referente útil para futuros colegas.

A los miembros del jurado, el Msc. Ing. Omar W. Savedra S., el Dr. Ing. Juan Villegas C. y el Msc. Ing. Oscar E. Capuñay U., por sus aportes y su evaluación.

Finalmente, agradezco a todas las personas que de una u otra manera contribuyeron a la realización de esta investigación.

Lalita Guerrero Diaz

En primer lugar, agradezco a Dios por la fortaleza, la sabiduría y la perseverancia que me concedió a lo largo de este proceso.

A mis padres y familia, quienes con su apoyo constante hicieron posible que llegue hasta aquí. Cada esfuerzo realizado en este trabajo lleva impresa su dedicación y su fe en nosotros.

A Lalita Guerrero, compañera de tesis y enamorada. Gracias por cada hora compartida, por tu paciencia, tu inteligencia y tu entrega en cada etapa de este proyecto. Recorrer este camino juntos lo hizo más significativo y más nuestro.

A nuestro asesor de tesis, Ing. Roberto Carlos Arteaga Lora, por su orientación experta y su compromiso; asimismo, a los ingenieros Msc. Ing. Omar Wilton Saavedra Salazar, Dr. Ing. Juan Villegas Cubas y Msc. Ing. Oscar Efraín Capuñay Uceda, cuyas observaciones y recomendaciones han permitido mejorar sustancialmente esta investigación.

A los ingenieros, Dr. Ing. Ernesto Karlo Celi Arevalo, la Dra. Ing. Jessie Leila Bravo Jaico y el Bach. Cristian Miguel Guevara Ramirez por su valioso aporte y apoyo como expertos validadores de la presente tesis.

Expresamos nuestro sincero agradecimiento al Ing. Herbert Parimango Rodríguez, CEO de Iteprevengo, por abrirnos las puertas de su empresa y facilitar el acceso a la información, los procesos y el entorno necesarios para llevar a cabo esta investigación. Su confianza y disposición fueron fundamentales para el desarrollo y la viabilidad de este trabajo.

A todos mis amigos y compañeros quienes, de una u otra forma, formaron parte de este camino: mi sincero agradecimiento.

Kevin Alberca Cubas

RESUMEN

El acelerado avance tecnológico ha impulsado el uso de entornos en la nube y del modelo Software as a Service (SaaS) para la prestación de servicios. Si bien este escenario ha facilitado la continuidad y eficiencia de los procesos empresariales también ha incrementado la exposición a riesgos de seguridad, los cuales podrían comprometer la estabilidad financiera y el prestigio institucional de las organizaciones. Bajo este contexto, Iteprevengo una microempresa peruana dedicada a la consultoría y desarrollo de software SaaS especializado en Seguridad y Salud en el Trabajo (SST), opera bajo una modalidad íntegramente remota y basada en entornos cloud, este escenario hace indispensable la adopción de un marco de gestión estructurado que salvaguarde los pilares fundamentales de la información: confidencialidad, integridad y disponibilidad.

La presente investigación tuvo como objetivo diseñar un Sistema de Gestión de la Seguridad de la Información basado en la NTP ISO/IEC 27001:2022, para los procesos de soporte y desarrollo de software SaaS de la empresa Iteprevengo. Se empleó una metodología estructurada en cinco fases, alineadas a las directrices de la ISO/IEC 27003:2010. La gestión de riesgos se desarrolló conforme a la NTP ISO/IEC 27005:2022 en conjunto con la NTP ISO/IEC 27002:2022. El diseño del SGSI fue validado mediante juicio de expertos, quienes evaluaron criterios de pertinencia, suficiencia, coherencia, claridad y la alineación normativa.

El modelo desarrollado en la investigación es descriptivo no experimental, en el cual se emplearon entrevistas semiestructuradas, grupos de enfoque y revisión documental como instrumentos de recolección de datos.

Como resultado se obtuvo un diseño de SGSI validado por expertos, aplicable a empresas de desarrollo de software SaaS con entornos de trabajo remoto, que permite gestionar riesgos de seguridad de información y sirve como referencia metodológica para organizaciones con características similares que buscan alinearse con la NTP ISO/IEC 27001:2022.

Palabras clave: Sistema de Gestión de la Seguridad de la Información, NTP ISO/IEC 27001, NTP ISO/IEC 27003, NTP ISO/IEC 27005, NTP ISO/IEC 27002, Software as a Service.

ABSTRACT

Rapid technological advancement has driven the use of cloud environments and the Software as a Service (SaaS) model for service delivery. Although this scenario has facilitated the continuity and efficiency of business processes, it has also increased exposure to security risks, which could compromise the financial stability and institutional prestige of organizations. In this context, Iteprevengo, a Peruvian micro-enterprise dedicated to the consulting and development of SaaS software specialized in occupational health and safety (OSH), operates under a fully remote modality and based on cloud environments, this scenario makes it essential to adopt a structured management framework that safeguards the fundamental pillars of information: confidentiality, integrity and availability.

The objective of this research was to design an Information Security Management System based on NTP ISO/IEC 27001:2022, for the support and development processes of SaaS software of the company Iteprevengo. A methodology structured in five phases was used, aligned with the guidelines of ISO/IEC 27003:2010. Risk management was developed in accordance with NTP ISO/IEC 27005:2022 in conjunction with NTP ISO/IEC 27002:2022. The design of the ISMS was validated through expert judgment, who evaluated criteria of relevance, sufficiency, coherence, clarity and regulatory alignment.

The model developed in the research is descriptive and non-experimental, in which semi-structured interviews, focus groups and documentary review were used as data collection instruments.

As a result, an ISMS design validated by experts was obtained, applicable to SaaS software development companies with remote work environments, which allows managing information security risks and serves as a methodological reference for organizations with similar characteristics that seek to align with NTP ISO/IEC 27001:2022.

Keywords: Information Security Management System, NTP ISO/IEC 27001, NTP ISO/IEC 27003, NTP ISO/IEC 27005, NTP ISO/IEC 27002, Software as a Service.

INDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

INTRODUCCIÓN

La transformación digital acelerada en los últimos años ha convertido a la información en uno de los activos más valiosos de las organizaciones. El incremento del uso de tecnologías de la información, servicios en la nube y plataformas digitales ha permitido optimizar procesos y ampliar mercados; sin embargo, también ha incrementado de manera significativa los riesgos asociados a la seguridad de la información. En este contexto, la protección de la confidencialidad, integridad y disponibilidad de la información se ha vuelto un factor crítico para garantizar la continuidad del negocio, la confianza de los clientes y el cumplimiento de requisitos legales y contractuales.

La pandemia del Covid-19 generó una disrupción económica global que impactó de manera significativa en el Perú, con la caída de hasta un 60% del producto bruto interno (PBI), según la investigación de Hernandez (2021). El sector empresarial más afectado fueron las micro, pequeñas y medianas empresas (MiPymes), la mayoría de estas organizaciones se vieron obligadas a adoptar modelos digitales y remotos para asegurar su supervivencia. Según una investigación realizada por Edelman, 9 de cada 10 empresas consideran que la pandemia aceleró su proceso de transformación digital.

Las microempresas que operan bajo el modelo de Software as a Service (SaaS) y esquemas de trabajo remoto enfrentan desafíos particulares en la gestión de la seguridad de la información. Según el informe global sobre amenazas 2024 realizado por Crowdstrike, las intrusiones en la nube aumentaron en un 75 % en el 2023 y los ataques orientados a la nube aumentaron en un 110 %. Estas dificultades se ven agravadas por la limitada disponibilidad de recursos financieros y especializados, convirtiendo a las microempresas en uno de los sectores más vulnerables frente a incidentes de ciberseguridad. De hecho, el 43% de todos los ciberataques están dirigidos a este sector empresarial, según un estudio de Accenture.

P & M SUPPORT S.R.L., cuyo nombre comercial es Iteprevengo, es una microempresa peruana dedicada a la consultoría, capacitación y desarrollo de software orientados a la gestión de la Seguridad y Salud en el Trabajo (SST). A fin de adaptarse a los cambios generados en el entorno empresarial posteriores a la pandemia, adoptó un modelo de trabajo 100 % remoto para sus áreas de soporte y desarrollo de software, junto con una infraestructura tecnológica basada en servicios en la nube.

En entornos SaaS y cloud, la seguridad no depende únicamente del proveedor de servicios, implica una responsabilidad compartida, puesto que los clientes deben asumir responsabilidad en aspectos como la configuración, gestión de accesos, la encriptación, etc. El informe "estado de ciberseguridad 2023" (State of Cybersecurity 2023) emitido por ISACA, expuso las causas de ataques más comunes entre los que sobresalieron: configuraciones inadecuadas, sistema sin parches, defectos de inyección, registro y monitoreo insuficientes, etc. En este contexto, la ausencia de un sistema integral no solo puede comprometer la continuidad del servicio y la reputación organizacional, también puede derivar en incumplimientos normativos, impactos financieros, pérdida de confianza de grupos de interés entre otros.

Frente a esta realidad, la presente investigación tiene como propósito diseñar un Sistema de Gestión de la Seguridad de la Información (SGSI) adaptado a las características, necesidades y modelo de negocio de la empresa Iteprevengo. El diseño del SGSI se basa en las directrices de la NTP ISO/IEC 27001:2022, con el fin de establecer un marco estructurado que permita fortalecer la gestión de la seguridad de la información.

El proyecto de investigación se estructura en cinco capítulos. El primer capítulo corresponde al análisis del objeto de estudio, donde se describe el contexto organizacional y se identifica la problemática existente. En el segundo capítulo se desarrolla el marco teórico, abordando los conceptos, modelos y normativas relacionadas con la seguridad de la

información y los sistemas de gestión. En el tercer capítulo se presenta el marco metodológico, detallando la tipificación del estudio, las técnicas de recolección de datos y el despliegue de la metodología propuesta. El cuarto capítulo expone el desarrollo del diseño del SGSI. Finalmente, en el quinto capítulo se presenta la validación de los resultados mediante la aplicación de juicio de expertos.

Con base en los hallazgos de la investigación, se formularon las conclusiones y recomendaciones pertinentes. El documento concluye con la relación de la bibliografía consultada y los anexos que sustentan el estudio.

ANÁLISIS DEL OBJETO DE ESTUDIO

Situación Problemática

La emergencia sanitaria provocada por la pandemia del Covid-19, representó un punto de inflexión para Iteprevengo. La empresa experimentó un auge en la demanda de servicios de Seguridad y Salud en el Trabajo, así como la necesidad de redefinir su arquitectura tecnológica. Para asegurar la continuidad de sus operaciones, Iteprevengo no sólo adoptó un modelo de trabajo 100 % remoto para los procesos de soporte y desarrollo de software, sino que también tuvo que adaptarse a trabajar en entornos digitales altamente dependientes de servicios en la nube.

Este proceso de transición se caracterizó por tomar decisiones reactivas que respondan a las nuevas demandas del mercado, lo que conllevó a que muchos aspectos relacionados con la seguridad de la información se gestionen sobre la marcha, sin realizar un análisis formal de la efectividad de las medidas implementadas durante la transición al trabajo remoto y al uso de servicios en la nube.

Actualmente, los colaboradores de Iteprevengo acceden a los sistemas corporativos desde dispositivos personales y redes domésticas. Si bien la empresa no ha registrado incidentes de seguridad críticos materializados, esta situación no es garantía de que los riesgos asociados a la seguridad de la información se encuentren adecuadamente gestionados. La ausencia de eventos graves puede responder a factores circunstanciales o a la aplicación de medidas técnicas aisladas, sin que ello implique un conocimiento completo y confiable del estado real de la seguridad de la información en la organización.

La falta de visibilidad sobre posibles brechas de seguridad coloca a la empresa en una situación de inestabilidad, ya que determinados riesgos podrían materializarse en cualquier momento. Por otro lado, este desconocimiento impide anticiparse a incidentes de seguridad,

priorizar riesgos de manera adecuada y tomar decisiones informadas. Si bien las buenas prácticas de seguridad aplicadas han resultado efectivas hasta el momento, se sustentan de manera informal, sin la adecuada documentación y sin un enfoque integral de gestión.

Por otro lado, Iteprevengo tiene como clientes a importantes empresas del sector retail en el país y de otros rubros, las cuales exigen mayores niveles de seguridad, cumplimiento de estándares y protección de la información al contratar servicios tecnológicos. En un entorno de alta competitividad, la capacidad de demostrar una gestión adecuada de la información se convierte en un factor diferenciador y en un requisito clave para la permanencia y crecimiento en el mercado. La ausencia de un Sistema de Gestión de la Seguridad de la Información (SGSI) formalmente establecido limita la capacidad de la organización para responder a estas exigencias.

En este contexto, el problema central no radica en la inexistencia de medidas técnicas de seguridad, sino en la falta de un enfoque estructurado, documentado y alineado a un estándar reconocido, como lo es la NTP ISO/IEC 27001:2022, que permita gestionar de manera sistemática la seguridad de la información.

Formulación del Problema

¿El diseño de un Sistema de Gestión de la Seguridad de la Información basado en la NTP ISO/IEC 27001:2022 reducirá significativamente los riesgos asociados a la seguridad de la información de los procesos de soporte y desarrollo de software SaaS en la empresa Iteprevengo?

Objetivos de la Investigación

Objetivo General

Diseñar un Sistema de Gestión de la Seguridad de la Información basado en la NTP ISO/IEC 27001:2022 que garantice la confidencialidad, integridad y disponibilidad de la información en los procesos de soporte y desarrollo de software SaaS en la empresa Iteprevengo.

Objetivos Específicos

- Analizar la situación actual de la seguridad de la información en los procesos de desarrollo y soporte de software SaaS de la empresa Iteprevengo.
- Evaluar los riesgos de seguridad de la información a los que están expuestos los procesos de soporte y desarrollo de software SaaS de la empresa Iteprevengo.
- Proponer el diseño de un Sistema de Gestión de Seguridad de la Información basado en la NTP ISO/IEC 27001:2022, adecuado a los procesos de soporte y desarrollo de software SaaS de la empresa Iteprevengo.
- Validar el diseño del SGSI propuesto mediante juicio de expertos.

Justificación del Problema

La presente investigación se justifica socialmente dado que contribuye a fortalecer la confianza de los clientes, colaboradores y partes interesadas mediante el diseño de un SGSI que garantice el manejo seguro y responsable de la información en Iteprevengo. Al promover una cultura organizacional orientada a la prevención, la transparencia y el uso ético de datos, la investigación aporta al bienestar colectivo y al fortalecimiento de relaciones basadas en la confianza y la seguridad.

Desde el ámbito tecnológico, la investigación es pertinente debido al crecimiento acelerado de servicios digitales y al uso de infraestructura en la nube dentro de Iteprevengo. Diseñar un SGSI basado en normativas reconocidas internacionalmente como lo es la familia de la ISO 27000, permite mejorar el control sobre los sistemas de información, establecer procedimientos formales para la gestión del riesgo, reducir vulnerabilidades, responder a incidentes y asegurar la disponibilidad, integridad y confidencialidad de los datos.

En el ámbito económico, la investigación se justifica dado que ofrece a Iteprevengo un enfoque preventivo que permite minimizar costos asociados a incidentes de seguridad, interrupciones del servicio y pérdidas de información. El diseño del SGSI, basado en un análisis de riesgos adaptado a la realidad de una microempresa remota, optimiza la asignación de recursos y fortalece la competitividad de la organización, permitiéndole mejorar su posición en el mercado y asegurar un crecimiento sostenible a largo plazo.

MARCO TEÓRICO

Antecedentes

Antecedentes Internacionales

Tabla 1.

Primer Antecedente Internacional

TÍTULO	Plan de contingencia informático para el área de TI en base a la norma de calidad ISO 27001:2013 para la fundación cultural y educativa Ambato - Unidad Educativa Atenas
PAÍS	Ecuador
UNIVERSIDAD	Universidad Técnica de Ambato
AÑO	2020
AUTORES	Burgos Gordon Christian Andres
OBJETIVO	Diseñar un plan de contingencia informático para el área de TI en base a la norma de calidad ISO 27001:2013 para la Fundación Cultural y Educativa Ambato - Unidad Educativa Atenas.
RESUMEN	La investigación fue tipificada como descriptiva, aplicada y de campo. Se emplearon técnicas como la observación, encuestas y entrevistas para la recolección de datos. Se utilizó la metodología Octave-S para la evaluación de los riesgos y el método Delphi para validar el diseño plan de contingencia; el cual constó de 5 etapas: definición del alcance, análisis de los recursos de TI, escenarios de riesgo, evaluación de los riesgos y la identificación de controles según las directrices de la ISO 27001:2013. El autor define acciones a realizar antes, durante y posterior a la aplicación del plan, incluyendo la creación de grupos de trabajo y la asignación de roles específicos dentro del departamento de TI.
ANÁLISIS DE RELACIÓN CON LA PRESENTE INVESTIGACIÓN	Se toma en consideración este trabajo de investigación, debido a que da lugar a una declaración de aplicabilidad, proceso inicial que se tiene contemplado realizar para poder medir el grado de madurez de la seguridad de información en nuestro caso de estudio.

Nota. Elaborado por los investigadores en base a Burgos (2020).

Tabla 2.

Segundo Antecedente Internacional

TÍTULO	Diseño de un SGSI bajo norma ISO/IEC 27001:2013 aplicado a un caso de estudio.
PAÍS	Ecuador
UNIVERSIDAD	Escuela Politécnica Nacional
AÑO	2020
AUTORES	Guano Zapata Marilyn J.& Jaramillo Vinueza Michelle N.
OBJETIVO	Diseñar un sistema de gestión de la seguridad de la información aplicado a un caso de estudio compatible en la norma ISO/IEC 27001:2013
RESUMEN	La investigación tuvo como unidad de análisis al Hospital de las Fuerzas Armadas N°1 (H.E-1) El levantamiento de información se realizó mediante la observación directa y entrevistas al personal del hospital. La metodología se definió en tres fases: el estudio diagnóstico, la viabilidad y el diseño del SGSI tomando como guías la norma ISO/IEC 27001:2013 y la metodología Magerit para la gestión de riesgos. Los autores concluyeron que el SGSI diseñado resultó eficaz en la identificación de activos valiosos, procesos críticos, vulnerabilidades y amenazas, incluyendo su origen. Se sugiere que el equipo de implementación esté compuesto por individuos que posean las habilidades y experiencia descritas en la sección "Roles y Responsabilidades" del informe de investigación.
ANÁLISIS DE RELACIÓN CON LA PRESENTE INVESTIGACIÓN	Esta investigación resulta relevante dado que proporciona una tabla comparativa entre las distintas metodologías utilizadas para la gestión de riesgos, evidenciándose que Magerit es la metodología más completa. Siguiendo los lineamientos de esta investigación, se utilizará la metodología Magerit para la gestión de riesgos.

Nota. Elaborado por los investigadores en base a Guano y Jaramillo (2020)

Antecedentes Nacionales

Tabla 3.

Primer Antecedente Nacional

TÍTULO	Implementación de un Sistema de Gestión de Seguridad de la Información para mejorar la Seguridad de la Información en una empresa MYPE – 2021
PAÍS	Lima – Perú
UNIVERSIDAD	Universidad Tecnológica del Perú
AÑO	2022
AUTORES	Alex Richar Silva Guerrero
OBJETIVO	Implementar un SGSI para mejorar la seguridad de la información en una empresa MYPE – 2021
RESUMEN	La investigación se llevó a cabo en una MYPE de Lima. Se emplearon entrevistas, cuestionarios y fichas de observación para recopilar información. La NTP-ISO/IEC 27001:2014 fue la base metodológica para diseñar el SGSI, mientras que la guía PMBOK se utilizó para la gestión del proyecto; el cual se dividió en cinco fases con actividades detalladas y entregables específicas para cada una. El autor concluye que la implementación del SGSI permitió gestionar activos, amenazas, vulnerabilidades, incidencias, controles, políticas y procedimientos de manera efectiva. Se enfatizó la importancia del compromiso de la alta dirección para el éxito de esta implementación y sugirió extender el alcance del SGSI a otros procesos de la empresa, así como revisar y actualizar periódicamente la política de seguridad y los procedimientos.
ANÁLISIS DE RELACIÓN CON LA PRESENTE INVESTIGACIÓN	Se toma como antecedente esta investigación ya que implementa un SGSI en una MYPE aplicando también la metodología ISO/IEC 27001:2014 y demostrando que es viable a pesar de los recursos limitados de una empresa de este tipo y se resalta la importancia de involucrar a la alta dirección.

Nota. Elaborado por los investigadores en base a Silva (2022)

Tabla 4.

Segundo Antecedente Nacional

TÍTULO	Diseño de un sistema de gestión de seguridad de la información basada en la norma técnica peruana -ISO/IEC 27001:2014 para la municipalidad distrital de Huácar 2022

PAÍS	Perú, Huánuco
UNIVERSIDAD	Universidad Nacional Hermiliovaldizán
AÑO	2022
AUTORES	Villadeza Romero Karen L. & Condor Simon, Reynaldo D.
OBJETIVO	Proponer el diseño de un Sistema de Gestión de Seguridad de la Información basado en la NTP ISO/IEC 27001:2014, para mejorar la seguridad de la información de la Municipalidad Distrital de Huácar 2022.
RESUMEN	El estudio fue de tipo descriptiva aplicada no experimental. La metodología se dividió en tres fases: el diagnóstico del estado de los sistemas de la información, proponer políticas de seguridad basadas en la Norma Técnica Peruana ISO/IEC 27001:2014 e identificar los riesgos de la SI usando MAGERIT V3; todo esto con el fin de proponer un SGSI que se adapte a la entidad en cuestión. La investigación concluye que la municipalidad se encontraba en una etapa inicial respecto a los controles implementados. El uso de la metodología MAGERIT versión 3 permite identificar peligros internos y externos, determinando que la mayoría de los activos estaban en un nivel intolerable de riesgo.
ANÁLISIS DE RELACIÓN CON LA PRESENTE INVESTIGACIÓN	El desarrollo de la investigación aplica también la metodología de gestión de riesgos Magerit en su versión 3 la cual es la adecuada para entidades en etapa inicial de control de sus activos como lo es Iteprevengo, se toma en cuenta también la declaración de aplicabilidad y el plan de tratamiento de riesgos.

Nota. Elaborado por los investigadores en base a Villadeza y Condor (2022)

Antecedentes Locales

Tabla 5.

Primer Antecedente Local

TÍTULO	Modelo de Gestión de Riesgos de TI que da soporte a los procesos de evaluación, financiamiento y cobranza de la empresa CHANCAFE NORTE S.A.C. basada en la metodología MAGERIT
PAÍS	Perú, Lambayeque
UNIVERSIDAD	Universidad Nacional Pedro Ruiz Gallo

AÑO	2022
AUTORES	Davila Puicon Soledad Milagros
OBJETIVO	Desarrollar un modelo de gestión de riesgos de TI como soporte de la SI de los procesos de evaluación, financiamiento y cobranza en la empresa CHANCAFE NORTE SAC
RESUMEN	El diseño del modelo de gestión de riesgos se basó en los estándares ISO/IEC (31001, 27001, 27002 y 27005) y la metodología MAGERIT y tuvo como alcance los procesos de evaluación, financiamiento y cobranza. La investigación se desarrolló en tres etapas: identificación del riesgo, análisis y evaluación del riesgo y tratamiento del riesgo. Para validar el modelo, se contó con la opinión de tres expertos, quienes determinaron que el modelo cumple con los criterios de claridad, coherencia y relevancia. La autora recomendó poner en marcha la implementación en un corto plazo con la finalidad de dar soporte a la seguridad de TI de los procesos críticos de la empresa.
ANÁLISIS DE RELACIÓN CON LA PRESENTE INVESTIGACIÓN	Este estudio contribuye a nuestra investigación al describir detalladamente a través de un gráfico la secuencia de actividades involucradas en la gestión de riesgos, lo que permite comprender claramente el proceso paso a paso.

Nota. Elaborado por los investigadores en base a Dávila (2022)

Tabla 6.

Segundo Antecedente Local

TÍTULO	La seguridad de la información y su relación con la gestión de los riesgos de negocio en las empresas agroindustriales azucareras.
PAÍS	Lambayeque, Perú
UNIVERSIDAD	Universidad Nacional Pedro Ruiz Gallo
AÑO	2020
AUTORES	Tapia Carrillo Jhoely M. & Vidal Castillo Josue L.
OBJETIVO	Desarrollar un modelo de gestión de los riesgos de TI que mejore la gestión de la seguridad de la información en las empresas agroindustriales azucareras.

RESUMEN	La investigación tuvo como unidad de análisis las áreas de desarrollo y producción de la Empresa Agroindustrial Pomalca SAA. El modelo de gestión de riesgos propuesto se basa en los estándares ISO 27001, 27003 y la metodología Magerit y se desarrolló en cinco fases: Inicio del proyecto, determinación del alcance del SGSI propuesto, análisis y evaluación de los escenarios de riesgo de TI, tratamiento de los riesgos de TI y estructuración de las políticas de la seguridad de la información. Los autores resaltan la importancia de la evaluación de riesgos, al ser esencial para identificar y analizar los riesgos potenciales, lo que permite a su vez seleccionar las medidas de protección adecuadas para cada escenario de riesgo.
ANÁLISIS DE RELACIÓN CON LA PRESENTE INVESTIGACIÓN	La investigación proporciona una fórmula para estimar el nivel de exposición al riesgo, considerando no sólo la probabilidad de ocurrencia y el impacto potencial, sino que adiciona al producto de estos la criticidad del activo. Haciendo de la evaluación de activos, una etapa fundamental dentro del proceso de gestión de riesgos. Esta fórmula será aplicada en la gestión de riesgos de nuestro caso de estudio por considerarla pertinente.

Nota. Elaborado por los investigadores en base a Tapia y Vidal (2020)

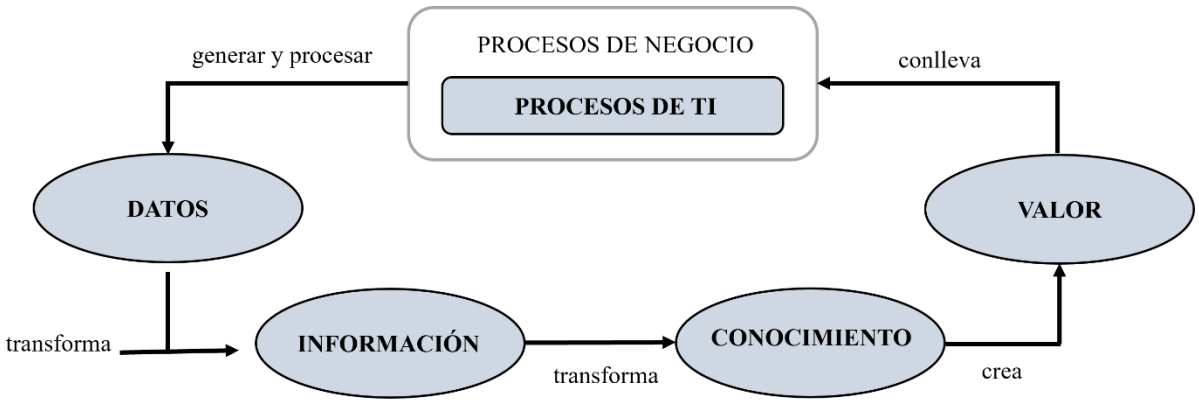
Base Teórica

Valor Estratégico de la Información en el Contexto Empresarial

Valencia (2021) refiere que un dato es un elemento que carece de significado intrínseco por sí solo. No obstante, cuando lo situamos en un contexto relevante (solo o en conjunto con otros datos) de tal forma que tiene significado en el tiempo y lugar indicado, se convierte en información. Esta, al ser analizada, discriminada, validada y sintetizada se convierte en conocimiento (de modo que crea valor para la empresa), el cual es fundamental para poder tomar decisiones que aseguren el buen funcionamiento operativo, táctico y estratégico de la organización, lo que conlleva a optimizar sus operaciones, mejorar su eficiencia, identificar nuevas oportunidades y obtener ventajas competitivas.

Figura 1.

Ciclo de la información



Nota. Elaborado por los investigadores en base a F. J. Valencia, 2021

Para Gallardo y Valdez (2022), como se citó en Valles (2023), “la información es un activo estratégico muy importante que permite garantizar la continuidad de la operatividad a corto, mediano y largo plazo”. Esto hace indispensable, que se implementen todas las medidas

necesarias para asegurar la confidencialidad, integridad y disponibilidad de la información, identificando vulnerabilidades y amenazas para corregirlas o minimizarlas (García et al., 2018).

Seguridad de la Información

La seguridad de la información son el conjunto de medidas de carácter preventivo y reactivo, que realiza una persona, una organización o un sistema, según corresponda, con la finalidad de resguardar y proteger la información que está bajo su gestión, tratando de mantener los niveles de confidencialidad, disponibilidad e integridad aceptables (Aguirre y Palacios, 2014).

Seguridad de la Información y Seguridad Informática.

Valencia y Orozco (2017) explican la diferencia entre seguridad informática y seguridad de la información de la siguiente manera:

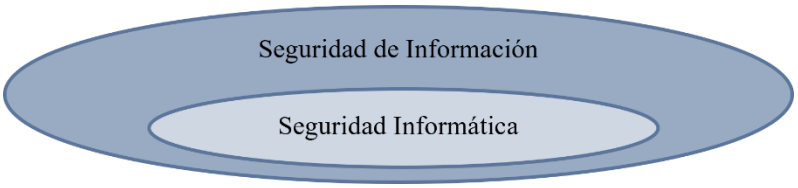
> La diferencia entre seguridad informática y seguridad de información radica en el tipo de recursos sobre los que actúa cada una. La primera se enfoca en la tecnología propiamente dicha, en las infraestructuras tecnológicas que sirven para la gestión de la información en una organización, mientras que la segunda está relacionada con la información en sí misma, como activo estratégico para la adecuada toma de decisiones empresariales en las organizaciones modernas. (p.74)

Garre et al. (2020) ponen énfasis en diferenciar los términos "seguridad de información" y "seguridad informática", refiere que el primero embarca al otro, siendo el último un término más restrictivo, como se muestra en la Figura 2. Argumentan que la seguridad informática es aquella que se centra exclusivamente en la seguridad de los sistemas de información y, por lo tanto, se limita al ámbito de la información automatizada, mientras que, la seguridad de información se encarga de proteger la información en todas sus formas

(oral, escrita, impresa, electrónica, etc) y en cualquier etapa de su ciclo de vida (creación, captura, mantenimiento, distribución y uso, almacenamiento, archivo y destrucción).

Figura 2.

Relación entre la seguridad de información y la seguridad informática



Nota. Elaborado por los autores en base a Garre et al., 2020

Principios de la Seguridad de Información.

De acuerdo con la NTP ISO/IEC 27001, la seguridad de la información consiste en preservar tres propiedades fundamentales: confidencialidad, integridad y disponibilidad, conocidas también como la tríada CID (o CIA, por sus siglas en inglés).

Valencia y Orozco (2017) describen las principales propiedades de la seguridad de la información de la siguiente manera:

- **Confidencialidad**, es la propiedad asociada con el acceso y el uso de la información sólo por parte de personas, entidades o mecanismos que se encuentran autorizados y tienen la necesidad de conocerla.
- **Integridad**, es la propiedad de salvaguardar la exactitud, precisión y la completitud de la información y de los activos tecnológicos ante su modificación o destrucción no autorizada.
- **Disponibilidad**, es la propiedad de que la información sea accesible y utilizable a petición de una entidad autorizada cuando lo requiera.

Existen otros atributos que complementan los conceptos de seguridad. Entre estos se destacan:

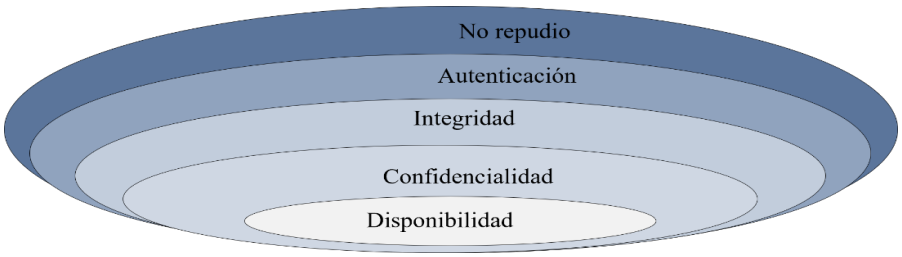
- **Autenticidad**, es la propiedad por la cual se garantiza que una entidad es la que dice ser; busca asegurar la validez de la información en tiempo, forma y distribución.
- **No repudio**, es la propiedad que permite garantizar la autoría de un mensaje y/o su envío, de forma tal que un emisor no niegue su autoría.

Costas (2014) explica cómo las distintas propiedades de seguridad se relacionan jerárquicamente, relación que se ilustra en la Figura 3:

> Están interrelacionadas jerárquicamente, de modo que cada una depende de la anterior; si una propiedad de nivel inferior no está presente, la de nivel superior no puede ser aplicada. De esta manera, la disponibilidad se convierte en el primer requisito de seguridad, cuando existe ésta, se puede disponer de confidencialidad, que es imprescindible para conseguir integridad, imprescindible para poder obtener autenticación y, por último, el no repudio, que solo se obtiene si se produce previamente la autenticación. (p. 13)

Figura 3.

Relación entre las propiedades de la seguridad de la información



Nota Elaborado por los autores en base a J. Costas, 2014

La Organización como Sistema

Concepto de Sistema

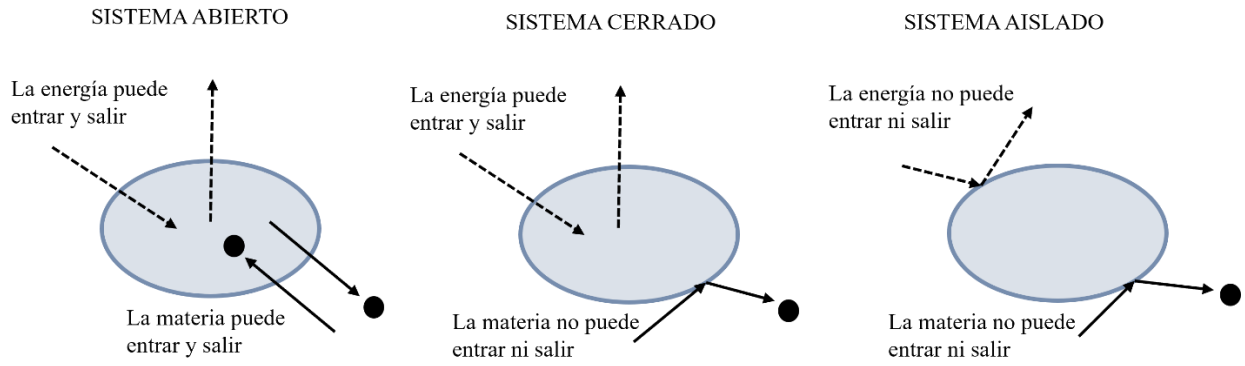
Johansen (1982) define un sistema como un conjunto de entidades o elementos interrelacionados, caracterizados por determinados atributos, que interactúan entre sí dentro de un ambiente específico para alcanzar un objetivo común. Estas interacciones se desarrollan dinámicamente mediante una corriente de entradas (inputs) que, a través de un proceso de conversión, se transforman en salidas (outputs), reguladas por mecanismos de retroalimentación que permiten ajustar y mejorar continuamente el funcionamiento del sistema.

En este contexto, los sistemas pueden clasificarse según su nivel de intercambio con el entorno. Navarro (2001) distingue tres tipos principales de sistemas en función del intercambio de energía y/o materia, estos son:

- **Sistemas abiertos:** presentan intercambios tanto de energía como de materia con el entorno.
- **Sistemas cerrados:** intercambian energía con el entorno, pero no materia.
- **Sistemas aislados**: no presentan intercambio de energía ni de materia con el exterior.

Figura 4.

Tipos de sistemas



Nota. Elaborado por los investigadores en base a J. L. Navarro, 2001.

La organización desde un enfoque sistémico

Desde la perspectiva sistémica, las organizaciones pueden entenderse como un sistema compuesto por partes interdependientes que interactúan entre sí y con el entorno, generando un comportamiento colectivo que le confiere entidad propia (Navarro, 2001).

Esta caracterización se sustenta en diversos aspectos. En primer lugar, la interacción entre los individuos de una organización genera un comportamiento global que no puede explicarse únicamente mediante el análisis de sus partes, lo que hace necesario un enfoque holístico. Así mismo, una organización presenta propiedades emergentes, como la cultura organizacional, los estilos de liderazgo o el clima laboral, las cuales surgen de la interacción entre sus componentes y no pueden explicarse únicamente a partir de cada elemento de forma aislada. Además de que, existe una fuerte interdependencia entre sus componentes, de modo que cualquier cambio en uno de ellos puede afectar el funcionamiento del sistema en su conjunto.

De igual manera una organización forma parte de un suprasistema mayor, como el sistema sociocultural, y a su vez se estructura en subsistemas internos que interactúan entre sí, tales como: el subsistema ambiental, técnico, estructural, psicosocial, de metas y valores, gerencial, etc.

En consecuencia, debido a estas interacciones, interdependencias y propiedades emergentes, una organización es considerada como un sistema, ya que su comportamiento y resultados surgen del conjunto de relaciones entre sus partes y con el entorno.

La organización como sistema abierto

Diversos autores coinciden en que las organizaciones deben comprenderse como sistemas abiertos, debido a su permanente interacción con el entorno. En este sentido, Katz y Kahn (1996) señalan que “las organizaciones son notoriamente sistemas abiertos, pues el

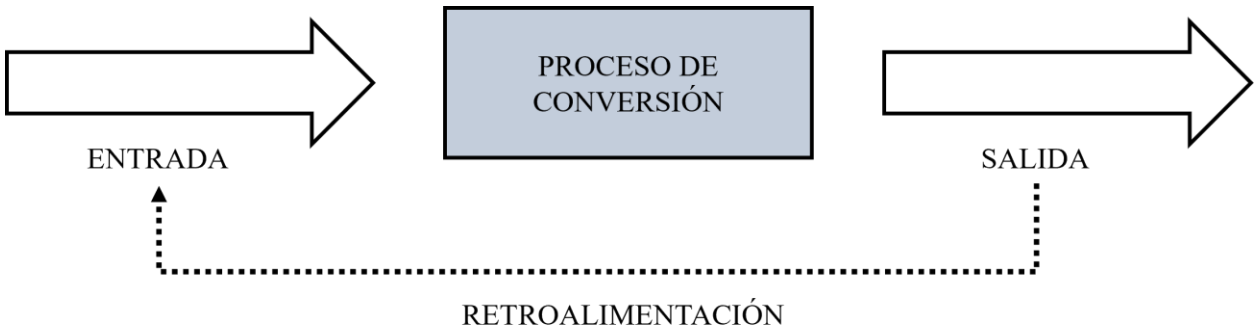
insumo de energías y la conversión del resultado en insumo energético adicional consisten en transacciones entre la organización y su ambiente" (p. 25).

Johansen (1982) señala que los sistemas abiertos están conformados por diversos elementos fundamentales que permiten comprender su funcionamiento. Estos se presentan en la Figura 5 y se describen a continuación:

- **Entrada** (inputs): recursos, datos o elementos que ingresan al sistema desde su entorno y que constituyen la base para el desarrollo de sus procesos internos.
- **Proceso de conversión:** conjunto de actividades o mecanismos mediante los cuales el sistema transforma las entradas en resultados, permitiendo cumplir el objetivo para el cual fue diseñado.
- **Salidas (outputs):** resultados o productos generados por el sistema después del proceso de conversión, los cuales pueden manifestarse en forma de bienes, servicios, información o decisiones.
- **Retroalimentación (feedback),** es el mecanismo mediante el cual el sistema recibe información sobre los resultados obtenidos, permitiendo evaluar su desempeño y realizar ajustes para mejorar su funcionamiento.

Figura 5.

Elementos de un sistema abierto



Nota. Elaborado por los investigadores en base a O. Johansen, 1982.

Atributos estructurales y funcionales de los sistemas

Los sistemas también pueden analizarse a partir de sus atributos, los cuales permiten comprender tanto su configuración como su funcionamiento. En este sentido, es posible distinguir dos tipos principales:

- **Atributos estructurales:** se relacionan con la organización interna del sistema, incluyendo sus componentes, relaciones y elementos que definen su configuración.
- **Atributos funcionales:** describen las actividades y procesos mediante los cuales el sistema opera y cumple los objetivos para los cuales fue diseñado.

La organización como macrosistema

Bajo este enfoque sistémico, la organización puede comprenderse como un macro sistema compuesto por diversos subsistemas que interactúan entre sí para alcanzar los objetivos organizacionales.

En este contexto, las organizaciones implementan diversos sistemas de gestión orientados a controlar, coordinar y mejorar sus procesos internos. Uno de ellos es el Sistema de Gestión de Seguridad de la Información (SGSI), cuyo propósito es proteger los activos de información de la organización mediante un enfoque sistemático basado en estándares internacionales.

Sistema de Gestión

Gatell y Pardo (2014), definen un sistema de gestión como un conjunto de elementos (políticas, procesos, productos/servicios, estructura organizacional y recursos) que se encuentran interrelacionados y permiten a una organización desarrollar su misión corporativa, garantizando la satisfacción de cualquier parte interesada.

En una línea similar, Magerit (2012), señala a un sistema de gestión como "lo que hace la organización para gestionar sus procesos o actividades, de forma que los productos que fabrica o los servicios que presta satisfagan los objetivos que la propia organización se ha marcado" (p.114).

Sistema de Gestión de la Seguridad de la Información.

Un Sistema de Gestión de la Seguridad de la Información (SGSI) es un enfoque sistemático y estructurado que integra un conjunto de políticas, procedimientos, guías, recursos y actividades asociadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información de una organización. Su propósito principal es minimizar los riesgos de seguridad de la información y, con ello, garantizar la protección de los activos de información, lo que permite alcanzar los objetivos estratégicos y comerciales de la organización (ISO, 2018).

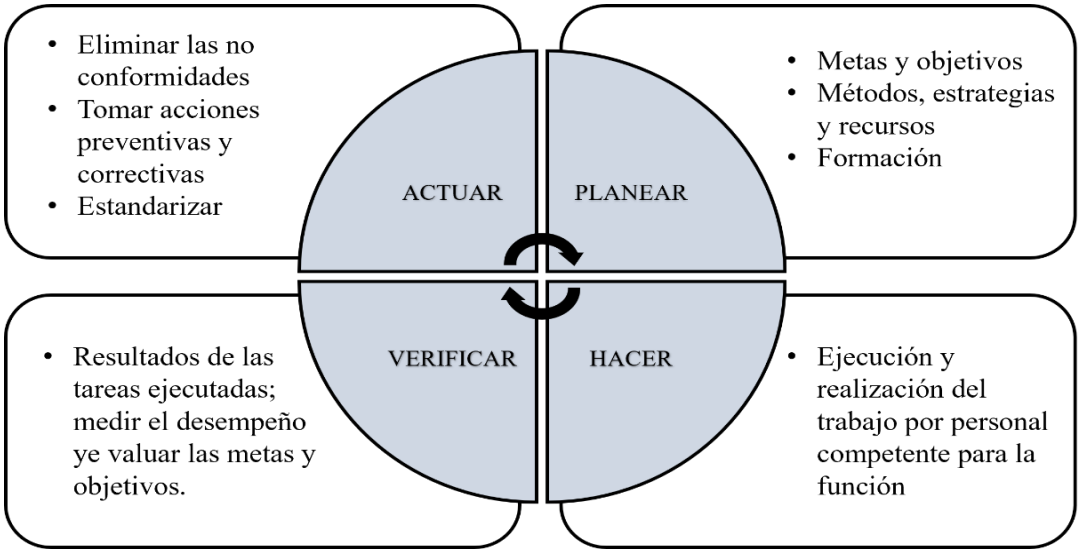
Ciclo PHVA.

Zapata (2015) define el ciclo PHVA como "un ciclo que contribuye a la ejecución de los procesos de forma organizada y a la comprensión de la necesidad de ofrecer altos estándares de calidad en el producto o servicio; por lo tanto, puede ser utilizado en las empresas, ya que permite la ejecución eficaz de las actividades" (p.14).

El PHVA, también conocido como ciclo de la mejora continua o ciclo Deming (en honor a su creador, Edward Deming), es una herramienta en el cual se basan los sistemas de gestión de las organizaciones y se fundamenta en cuatro fases: planificar (Plan), hacer (Do), verificar (Check) y actuar (Act).

Figura 6.

Despliegue del ciclo PHVA



Nota. Adaptado de *Despliegue del ciclo PHVA* (p.4), de A. Zapata, 2015.

Zapata (2015) proporciona un detalle de cada fase:

- **Planificar:** En esta fase se establecen las metas y los métodos para cumplirlas, se definen los objetivos y se establecen las técnicas para lograrlos, se precisan los indicadores para comprobar que fueron alcanzados. Se enfatiza en qué hacer y cómo hacerlo.
- **Hacer:** En esta fase se impulsa la implementación de acuerdo a lo planificado; es decir se desarrollan los planes estratégicos, operativos y tácticos de la calidad, se implementan y se realiza el trabajo acorde con los requisitos de la ley, los clientes y las normas técnicas establecidas.
- **Verificar**: En esta fase se monitorean los procesos, los productos y los servicios; y se realiza el seguimiento para confirmar que las actividades se ejecutaron según lo planificado. Se plantean las estrategias para mantener o mejorar las acciones de acuerdo con los resultados obtenidos.

- **Actuar**: En esta fase se desarrolla la mejora, se eliminan las no conformidades y se establecen acciones correctivas, preventivas y de mejora. Se gira de nuevo el ciclo mediante la ejecución de una nueva planificación que permita ajustar las directrices y objetivos de calidad según los nuevos acontecimientos del entorno.

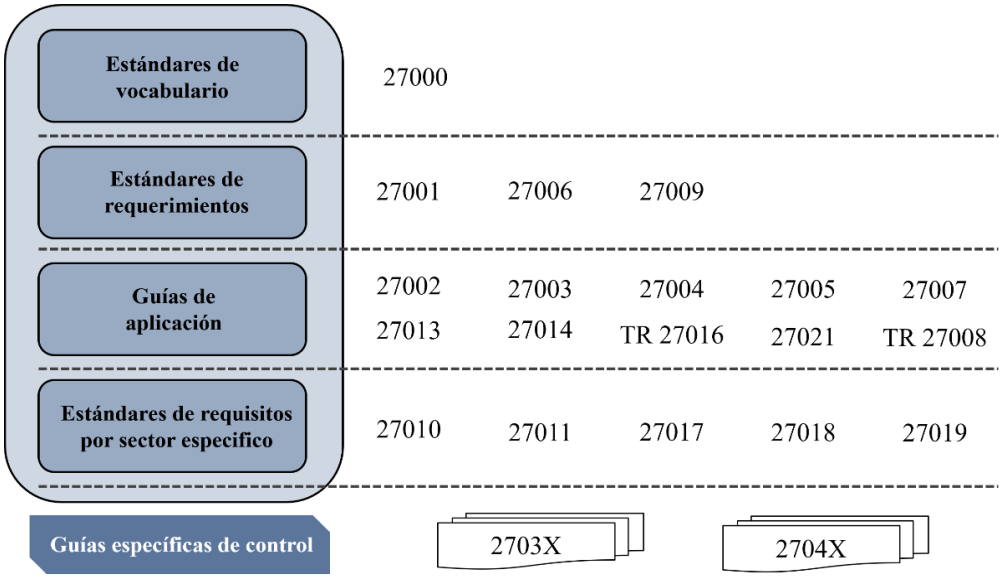
Estándares y Marcos Internacionales de Seguridad de la Información

En el ámbito de la seguridad de la información, se han desarrollado numerosos estándares, marcos y guías de referencia con el propósito de establecer cómo se debe implementar la seguridad de la información dentro de una organización. Sin embargo, "la familia de estándares ISO 27000 es el conjunto de estándares más reconocido y ampliamente aceptado a nivel mundial" (Prislan et al., 2017, p.8).

La familia 27000, lo componen, aproximadamente, 19 normas principales, clasificadas en cuatro categorías, tal como se puede apreciar en la Figura 7.

Figura 7.

Relación entre las normas de la familia ISO/IEC 27000

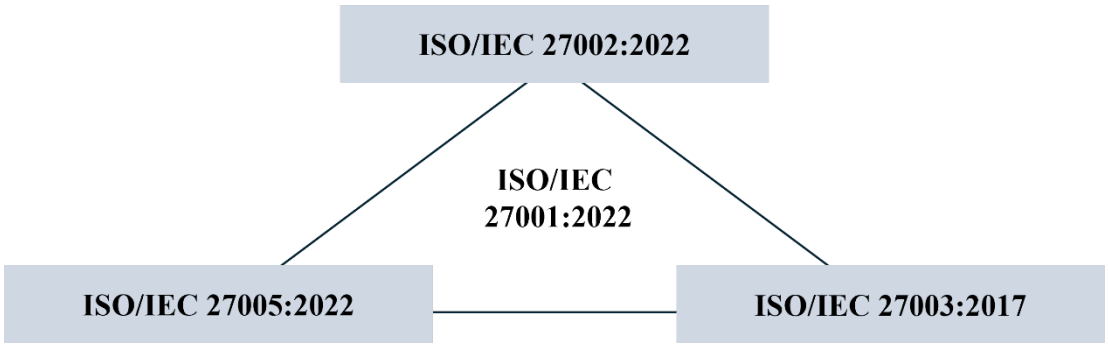


Nota. Adaptado de *Relaciones de la familia de estándares SGSI,* (p.19)*,* de ISO, 2018.

A pesar de la cantidad de normas de la serie ISO/IEC 27000, aquellas que sirven de referente directo para la implementación de un SGSI en una organización, se enmarcan en cuatro de ellas, las cuales podemos reconocer en la Figura 8.

Figura 8.

Normas ISO/IEC para la implementación de un SGSI



Nota. Elaborado por los investigadores.

A continuación, se presenta un desglose detallado de estas normas, explicando cómo cada una contribuye a la solidez y eficacia de un SGSI:

ISO/IEC 27000

La norma internacional ISO/IEC 27000, actualmente denominada *Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información - Descripción general y vocabulario*, es un estándar introductorio que describe los fundamentos de un SGSI. Proporciona un glosario de términos y definiciones clave empleados en los demás estándares de esta serie. A continuación, se detallan los conceptos más relevantes para la comprensión de un SGSI:

- **Activo,** cualquier elemento que tiene valor para la organización y que por lo tanto requiere protección.
- **Control,** cualquier medida, política, procedimiento, dispositivo o práctica que se implementa para modificar, reducir o mantener el riesgo a un nivel aceptable.
- **Evento, ocurrencia** identificada que indica una posible violación de la seguridad de la información.
- **Incidente,** evento no deseado o inesperado que tienen una probabilidad significativa de comprometer las operaciones comerciales de la organización y amenazar la seguridad de la información.
- **Amenaza,** causa potencial de un incidente no deseado o inesperado que puede resultar en daño a un sistema o a la organización.
- **Vulnerabilidad,** debilidad de un activo o control que puede ser explotada por una o más amenazas.
- **Riesgo,** combinación de la probabilidad de que un incidente ocurra y el impacto que dicho evento tendría en la organización.
- **Impacto,** resultado o consecuencia de la materialización de un riesgo.
- **Probabilidad,** posibilidad de que una amenaza explote una vulnerabilidad específica y cause un incidente.

NTP ISO/IEC 27001:2022

La NTP ISO/IEC 27001:2022, adopción nacional del estándar internacional ISO/IEC 27001:2022, denominada: *Seguridad de la información, ciberseguridad y protección de la privacidad - Sistemas de gestión de la seguridad de la información – Requisitos*, es el único estándar certificable de la familia ISO/IEC 27000.

Proporciona a las organizaciones, independientemente de su tipo, tamaño o naturaleza, un marco de trabajo sólido con los requisitos necesarios para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un SGSI (ISO, 2018).

A la fecha, la norma ha tenido tres versiones. A continuación, en la Tabla 7, se presenta una comparativa que destaca los aspectos clave de cada versión:

Tabla 7.

Cuadro comparativo entre las versiones de la ISO/IEC 27001

CARACTERÍSTICA	VERSIONES DE LA ISO/IEC 27001		
	ISO/IEC 27001:2005	**ISO/IEC 27001:2013**	**ISO/IEC 27001:2022**
Estructura de alto nivel	No aplicable	Introducida	Mantenida
Controles de seguridad	133 controles en 11 grupos	114 controles en 14 grupos	93 controles en 4 grupos
Gestión de riesgos	Fundamental	Reforzada	Enfoque renovado
Contexto de la organización	No específicamente abordado	Introducido	Ampliado
Liderazgo de la alta dirección	Implícito	Explicado	Enfatizado
Evaluación del desempeño	Menos enfocado	Introducido	Reforzado
Flexibilidad y personalización	Limitada	Mejorada	Significativamente ampliada

Nota. Elaborado por los investigadores.

La NTP ISO/IEC 27001 se divide en 11 secciones (resumidas en la Tabla 8) e incluye un “Anexo A”; las secciones 0 a 3 son generalidades, proporcionan una base sólida para comprender los conceptos y principios fundamentales de la seguridad de la información (y no son obligatorias para la implementación), mientras que las secciones 4 a 10, establecen los requisitos fundamentales para un SGSI y deben ser cumplidos obligatoriamente para poder obtener la certificación. (Instituto Nacional de Calidad [INACAL], 2022c).

El anexo A, es un documento normativo que proporciona 93 controles de seguridad de información, directamente derivados y alineados con los listados en NTP ISO/IEC 27002:2022.

Tabla 8.

Estructura de la norma NTP ISO/IEC 27001:2022

0. Introducción		
1. Alcance		
2. Referencias normativas		
3. términos y condiciones		
4. Contexto de la organización	4.1	Comprender la organización y su contexto
	4.2	Comprender las necesidades y expectativas de las partes interesadas
	4.3	Determinar el alcance del sistema de gestión de seguridad de la información
	4.4	Sistema de gestión de seguridad de la información
5. Liderazgo	5.1	Liderazgo y compromiso
	5.2	Política
	5.3	Roles, responsabilidades y autoridades organizacionales
6. Planificación	6.1	Acciones para tratar los riesgos y las oportunidades
	6.2	Objetivos de seguridad de la información y planificación para conseguirlos
	6.3	Planificación de cambios
7. Soporte	7.1	Recursos
	7.2	Competencia
	7.3	Toma de conciencia
	7.4	Comunicación
	7.5	Información documentada
8. Operación	8.1	Planificación y control operacional
	8.2	Evaluación de riesgos de seguridad de la información
	8.3	Tratamiento de riesgos de seguridad de la información
9. Evaluación del desempeño	9.1	Monitoreo, medición, análisis y evaluación
	9.2	Auditoría interna
	9.3	Revisión de la dirección
10. Mejoras	10.1	Mejora continua

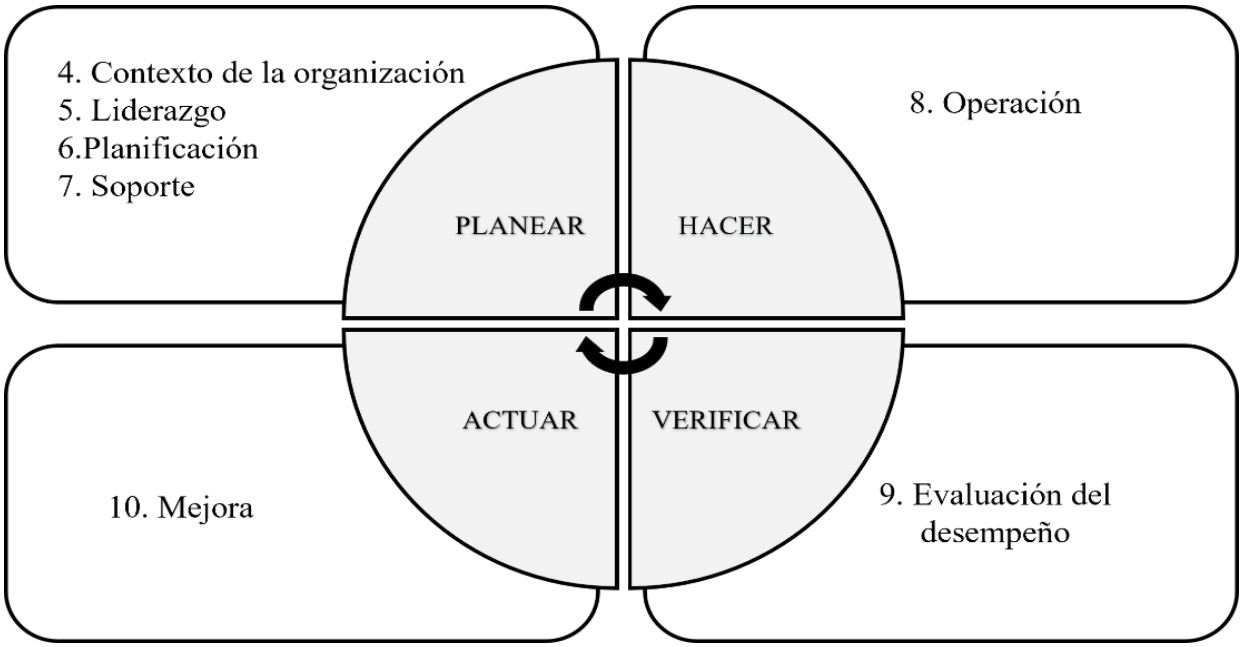
	10.2	No conformidad y acción correctiva
11. Anexo A.	Resumen de los objetivos de control y controles de la ISO/IEC 27002	

Nota. Elaborado por los investigadores tomando como referencia la NTP ISO/IEC 27001

La estructura de los requisitos de la NTP ISO/IEC 27001, se alinean perfectamente con las cuatro fases del ciclo PHVA. Esta correspondencia puede observarse en la Figura 9.

Figura 9.

Secciones de la NTP ISO/IEC 27001 en función del Ciclo Deming



Nota. Adaptado de *Numerales de la norma en función del ciclo Deming* (p.71), por Valencia, 2021

NTP ISO/IEC 27002:2022

La Norma Técnica Peruana NTP ISO/IEC 27002:2022, adopción nacional del estándar internacional ISO/IEC 27002:2022, denominada: *Seguridad de la información, ciberseguridad y protección de la privacidad: controles de seguridad de la información*, es una guía de

referencia para determinar e implementar controles para el tratamiento de riesgos de seguridad de la información en un SGSI (INACAL, 2022a).

La norma internacional surgió originalmente en el 2000 como ISO/IEC 17799, posteriormente fue actualizada como ISO/IEC 27002 en octubre del año 2005. A la fecha, la norma ha tenido tres versiones, la versión válida actual es la ISO/IEC 27002:2022.

Esta última versión de la NTP ISO/IEC 27002 clasifica los controles de seguridad de la información en 4 grupos (a diferencia de la versión 2013, que los clasificaba en 14 dominios): 37 controles organizacionales, 8 controles de personas, 14 controles físicos y 34 controles tecnológicos; haciendo un total de 93 controles definidos.

A continuación, en la Tabla 9 se presenta una comparativa que destaca los aspectos clave de las dos últimas versiones:

Tabla 9.

Cuadro comparativo entre las versiones de la NTP ISO/IEC 27002

CARACTERÍSTICA	VERSIONES DE LA NTP ISO/IEC 27002	
	NTP IEC/ISO 27002: 2013	NTP IEC/ISO 27002:2022
Dominios / Grupos	14 dominios	4 grupos
N° de controles	114 controles	93 controles
Objetivos de control	35 objetivos	-
Controles nuevos	-	11 nuevos controles
Controles fusionados	-	24 controles fusionados
Controles eliminados	-	Ningún control eliminado

Nota. Elaborado por los investigadores.

Al respecto, la International Organization for Standardization, refiere que la organización es quien determina que controles implementar, previo a una evaluación de

riesgos. Esta determinación debe basarse en los criterios de aceptación del riesgo, las opciones de tratamiento del riesgo y la metodología de gestión del riesgo aplicado por la organización.

NTP ISO/ IEC 27003:2019

La Norma Técnica Peruana NTP ISO/IEC 27003:2019, adopción nacional del estándar internacional ISO/IEC 27003:2017, denominada: *Tecnología de la información — Técnicas de seguridad — Sistemas de gestión de la seguridad de la información — Orientación*, sirve de "referencia para la especificación y diseño de un SGSI, desde su inicio hasta los planes de implementación" (Valencia, 2021, p.74).

La primera versión de la norma internacional se publicó en el año 2010. A la fecha, se han publicado dos versiones, la versión válida actual es la ISO/IEC 27003:2017. A continuación, en la Tabla 10 se compara los aspectos clave de ambas versiones:

Tabla 10.

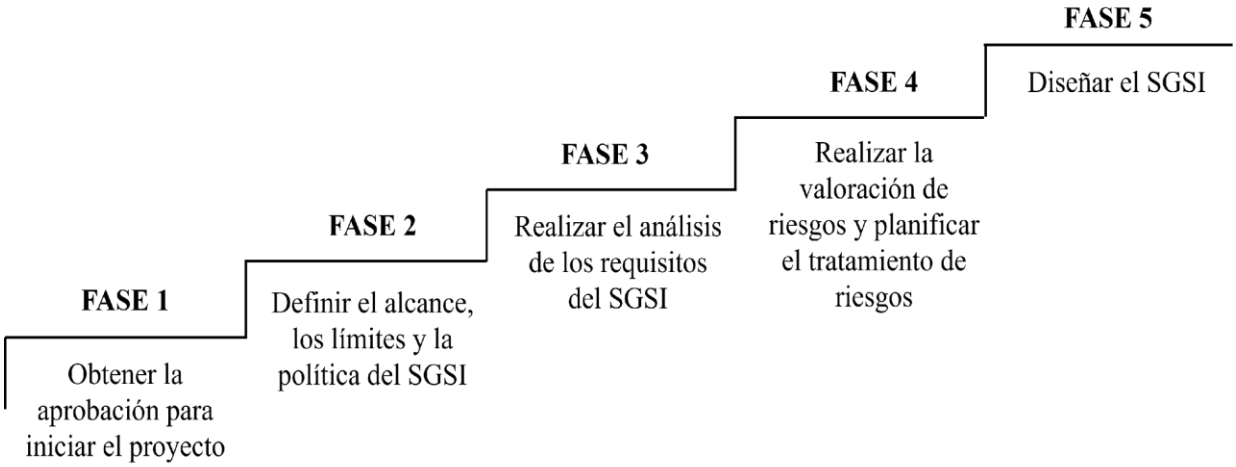
Cuadro comparativo entre las versiones de la ISO/IEC 27003

ASPECTO	VERSIONES DE LA ISO/IEC 27003	
	ISO/IEC 27003:2010	ISO/IEC 27003:2017
Propósito	Proveer guía para la implementación de un SGSI según ISO 27001:2005	Proveer guía para la implementación de un SGSI según ISO 27001:2013
Estructura del documento	Basado en los requisitos de ISO 27001:2005	Sigue la estructura de ISO 27001:2013
Flexibilidad	Menos flexible, enfoque más secuencial en la implementación	Más flexible, permite adaptaciones específicas a cada organización
Cláusulas	No sigue exactamente las cláusulas de ISO 27001	Cláusulas 4 a 10 alineadas directamente con ISO 27001:2013
Enfoque en la implementación	Proceso de diseño e implementación de SGSI desde el inicio hasta la producción de la documentación	Incluye obtención de aprobación de la gerencia, definición del proyecto y planificación del SGSI

Nota. Elaborado por los investigadores.

Figura 10.

Fases del proceso de diseño e implementación de un SGSI



Nota. Adaptado de *Fases para implementar un SGSI con base en la norma ISO/IEC 27003:2010* (p.78), Valencia, 2021.

Valencia (2021) proporciona una guía detallada del proceso de diseño de un SGSI, basada en la metodología propuesta por la ISO/IEC 27003:2010, la cual organiza el proceso en 5 fases secuenciales (Observe Figura 10). Aunque esta norma fue actualizada en 2017, el autor justifica el uso de la versión original debido a su relevancia metodológica. Las fases contempladas son las siguientes:

- **FASE I: Obtener la aprobación de la dirección para iniciar el proyecto.** Valencia (2021) refiere que un proyecto de SGSI no se limita únicamente al área de tecnología, sino que debe abordarse como un proyecto organizacional, ya que abarca todas las áreas de la empresa. Por ello, es fundamental contar con la aprobación, el respaldo y el compromiso de la alta dirección para garantizar su efectividad y éxito.

  El objetivo de esta fase es "obtener la aprobación de la dirección para iniciar el proyecto de SGSI mediante la definición de un caso de negocio y un plan de proyecto" (Valencia, 2021, p. 81).

- **FASE II: Definir el alcance, los límites y la política del SGSI.** El propósito de esta fase es establecer los factores clave de un SGSI: "la definición detallada del alcance y los límites, el desarrollo de la política, y el respaldo de la alta dirección" (Valencia, 2021, p. 85).
- **FASE III: Realizar el análisis de los requisitos de seguridad de información.**

  En esta fase se definen tareas como:

  a. Definir los requisitos de seguridad de la información para el proceso SGSI.
  b. Identificar los activos dentro del alcance del SGSI.
  c. Realizar una evaluación de la seguridad de la información.
- **FASE IV: Realizar la valoración de riesgos y planear el tratamiento de riesgos.** En esta fase se define la metodología a emplear para gestionar los riesgos de la seguridad de la información. La gestión del riesgo es el eje central del SGSI, siendo la norma ISO/IEC 27005 el principal referente en este ámbito (Valencia, 2021).
- **FASE IV: Diseñar el SGSI.** Valencia (2021), refiere que el diseño del SGSI contempla, básicamente, tres componentes:

  a. Documentación. La documentación es una de las etapas más extensas en un proyecto de SGSI. Esta se genera a lo largo de las distintas fases del diseño e implementación del SGSI y debe contemplar todos los requisitos establecidos en la norma ISO/IEC 27001 (Valencia, 2021). A continuación, en la Tabla 11 se lista la documentación obligatoria según la mencionada norma.

Tabla 11.

Documentos obligatorios de la NTP ISO/IEC 27001:2022

CLÁUSULA	NOMBRE DE DOCUMENTO	DESCRIPCIÓN

4.3	Alcance del SGSI	Documento que define los límites y la aplicabilidad del SGSI. Su propósito es definir qué partes de la organización están cubiertas por el SGSI, asegurando que sea relevante y manejable.
5.2	Política de seguridad de la información	Documento estratégico que establece el compromiso de la alta dirección con la seguridad de la información. Establece los principios, objetivos generales y el marco para la gestión de riesgos y cumplimiento normativo.
6.1.2	Proceso de evaluación de riesgos de seguridad de la información	Documento que describe la metodología para identificar, analizar y evaluar los riesgos de seguridad de información. Incluye los criterios de evaluación, herramientas (matrices), etc.
6.1.3	Proceso de tratamiento de riesgos de seguridad de la información	Documento que describe el procedimiento para tratar los riesgos de seguridad de información. Define cómo se eligen controles y se asignan responsabilidades para su implementación.
6.1.3 d	Declaración de Aplicabilidad - SoA	Documento que lista los controles del Anexo A, indicando cuales son aplicables o no, con justificaciones basadas en la evaluación de riesgos.
6.2	Objetivos de seguridad de información	Documento que establece metas específicas, medibles y alineadas con la política de seguridad de información.
7.2	Evidencia de la competencia	Registros documentados que demuestran las cualificaciones, formación, habilidades y experiencia del personal involucrado en el SGSI.
8.2	Resultados de las evaluaciones de riesgos	Registros de los resultados de las evaluaciones de riesgos de seguridad de la información, incluyendo riesgos identificados, su análisis y evaluación.
8.3	Plan de tratamiento de riesgos	Documento que detalla las acciones seleccionadas para tratar riesgos, controles implementados y el riesgo residual resultante.
9.1	Evidencia de monitoreo, medición, análisis y evaluación	Registros de los métodos, resultados y análisis de monitoreo y medición del desempeño del SGSI, incluyendo la efectividad de controles.

		Su propósito es evaluar si el SGSI logra sus objetivos y proporcionar datos para mejoras continuas.
9.2	Programa de auditoría interna y resultados	Documento que incluye el programa de auditorías internas (criterios, alcance, métodos, frecuencia) y los resultados de las auditorías realizadas.
9.3	Resultados de revisiones por la dirección	Registros de las revisiones periódicas por la alta dirección, incluyendo entradas (desempeño, cambios, oportunidades) y salidas (decisiones, acciones).
10.2	Evidencia de no conformidades y acciones correctivas.	Registros de no conformidades identificadas, sus causas, acciones correctivas tomadas y verificación de su efectividad.

Nota. Elaborado por los investigadores tomando como referencia la NTP ISO/ IEC 27001.

b. Implementación del plan de tratamiento de riesgos. Valencia (2021) señala que, el plan de tratamiento de riesgos, este debe ser formalmente aprobado por la alta dirección antes de su implementación, teniendo en cuenta los recursos necesarios y definiendo un cronograma detallado para su ejecución.

c. Monitoreo constante de la seguridad de la información. Según Valencia (2021), este proceso resulta fundamental en un SGSI, pues garantiza la supervisión continua de la SI. Se puede realizar a través de dos instrumentos:

- Implementación de un proceso de gestión de incidentes de la SI.
- Desarrollo de auditorías periódicas al sistema (Pruebas del SGSI).

NTP ISO/IEC 27004:2018

La Norma Técnica Peruana NTP ISO/IEC 27004:2018, adopción nacional del estándar internacional ISO/IEC 27004:2016, denominada: *Tecnología de la información — Técnicas de seguridad — Gestión de la seguridad de la información — Monitoreo, medición, análisis y evaluación*, proporciona "directrices destinadas a ayudar a las organizaciones a evaluar el

rendimiento en seguridad de la información y la eficacia de un sistema de gestión de seguridad de la información para cumplir con los requisitos de ISO/IEC 27001:2013, 9.1: monitorización, medición, análisis y evaluación" (INACAL, 2018, p.1).

La norma establece que, a partir de las necesidades de información identificadas por la organización, deben definirse métricas e indicadores que permitan generar datos objetivos mediante procesos de seguimiento y medición. Estos datos serán posteriormente analizados y evaluados con el propósito de determinar si satisfacen los requerimientos informativos y si evidencian el nivel de desempeño y eficacia del SGSI.

La relevancia de este proceso radica en que los resultados obtenidos sustentan la toma de decisiones estratégicas y operativas, fortalecen la gobernanza de la seguridad de la información y favorecen la mejora continua del sistema.

El monitoreo, la medición, el análisis y la evaluación de un SGSI comprenden una serie de procesos que se presentan en la Figura 11, estos son:

a) **Identificar las necesidades de información**, consiste en determinar qué información requiere la organización para evaluar el desempeño y la eficacia del SGSI, a fin de priorizar y documentar adecuadamente.

b) **Crear y mantener medidas**, implica diseñar y actualizar sistemáticamente las medidas que respondan a las necesidades de información del SGSI, especialmente ante cambios en su entorno o requisitos.

c) **Establecer procedimientos;** consiste en definir los procedimientos necesarios para implementar las medidas priorizadas, incluyendo la recopilación, verificación, análisis y presentación de los datos. Se definen herramientas, métodos y formatos de reporte para comunicar los resultados de forma clara y oportuna.

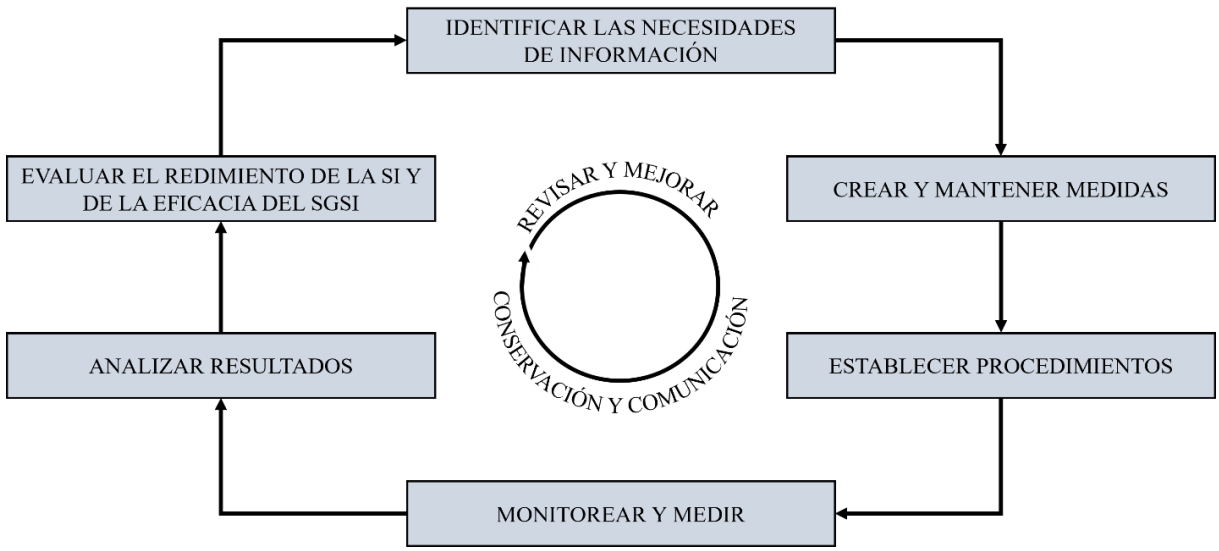
d) **Supervisar y medir,** consiste en ejecutar las actividades de monitoreo y medición conforme a los procedimientos establecidos, ya sea de forma manual o automatizada, asegurando la correcta recopilación, almacenamiento y verificación de los datos para garantizar su fiabilidad.

e) **Analizar los resultados**, consiste en examinar e interpretar los datos recopilados en función del objetivo de cada medida, considerando el contexto en el que fueron obtenidos. El análisis permite identificar brechas entre los resultados esperados y reales.

f) **Evaluar el rendimiento de la SI y la eficacia del SGSI,** Consiste en interpretar los resultados con el fin de evaluar si el sistema alcanza los objetivos definidos y si las acciones implementadas son adecuadas para lograr los resultados previstos.

Figura 11.

Proceso de monitoreo, medición, análisis y evaluación de un SGSI



Nota. Adaptado de *Procesos de monitorización, medición, análisis y evaluación* (p.10), INACAL, 2018.

Gestión del Riesgo

Valencia (2021) señala la importancia de la gestión de riesgos dentro de la seguridad de la información:

> Entre los aspectos clave de la seguridad de la información, los procesos de gestión de riesgos son el eje central que integra y vuelve operativos los diferentes elementos que hacen parte de un modelo de seguridad. En este sentido, los modelos de gestión de riesgos son la base sobre la que se construye la seguridad de la información de una organización (p. 30).

En el ámbito de la gestión de riesgos de seguridad de la información, existen diversas metodologías que ofrecen enfoques estructurados para identificar, analizar y tratar riesgos. A continuación, en la Tabla 12 se analizan las metodologías más reconocidas a nivel internacional:

Tabla 12.

Matriz comparativa de metodologías para la gestión de riesgos

CRITERIO		**METODOLOGÍAS**				
		ISO 27005	**OCTAVE**	**NIST SP 800-30**	**CRAMM**	**MAGERIT**
Ámbito de aplicación		Todo tipo de organización	Grandes empresas	Grandes empresas	Grandes Empresas	Todo tipo de organización
Tipo de análisis	Cualitativo	Completo	Incompleto	Completo	Completo	Completo
	Cuantitativo	Incompleto	Incompleto	Completo	Completo	Completo
Elementos del modelo	Procesos	Completo	Completo	No tiene	-	Completo
	Activos	Completo	Completo	No tiene	Completo	Completo
	Vulnerabilidades	Completo	Completo	Completo	Completo	Incompleto
	Amenazas	Completo	Completo	Completo	Completo	Completo
	Salvaguardas	Completo	Completo	Completo	Completo	Completo

Objetivos de seguridad	Confidencialidad	Completo	Completo	Completo	Completo	Completo
	Integridad	Completo	Completo	Completo	Completo	Completo
	Disponibilidad	Completo	Completo	Completo	Completo	Completo
	Autenticidad	-	No tiene	No tiene	Completo	Completo
	Trazabilidad	-	No tiene	No tiene	No tiene	Completo
Ayuda de implementación	Herramientas	No tiene	Completo	No tiene	Completo	Completo
	Plan de proyecto	-	Completo	No tiene	No tiene	Completo
	Técnicas	No tiene	Completo	No tiene	No tiene	Completo
	Roles	-	Completo	-	No tiene	Completo
	Comparativas	No tiene	No tiene	No tiene	No tiene	Completo

Nota. Elaborado por los autores en base a Guano y Jaramillo (2020).

En los siguientes apartados se exponen las metodologías más utilizadas para la gestión de riesgos, las cuales son:

NTP ISO/IEC 27005

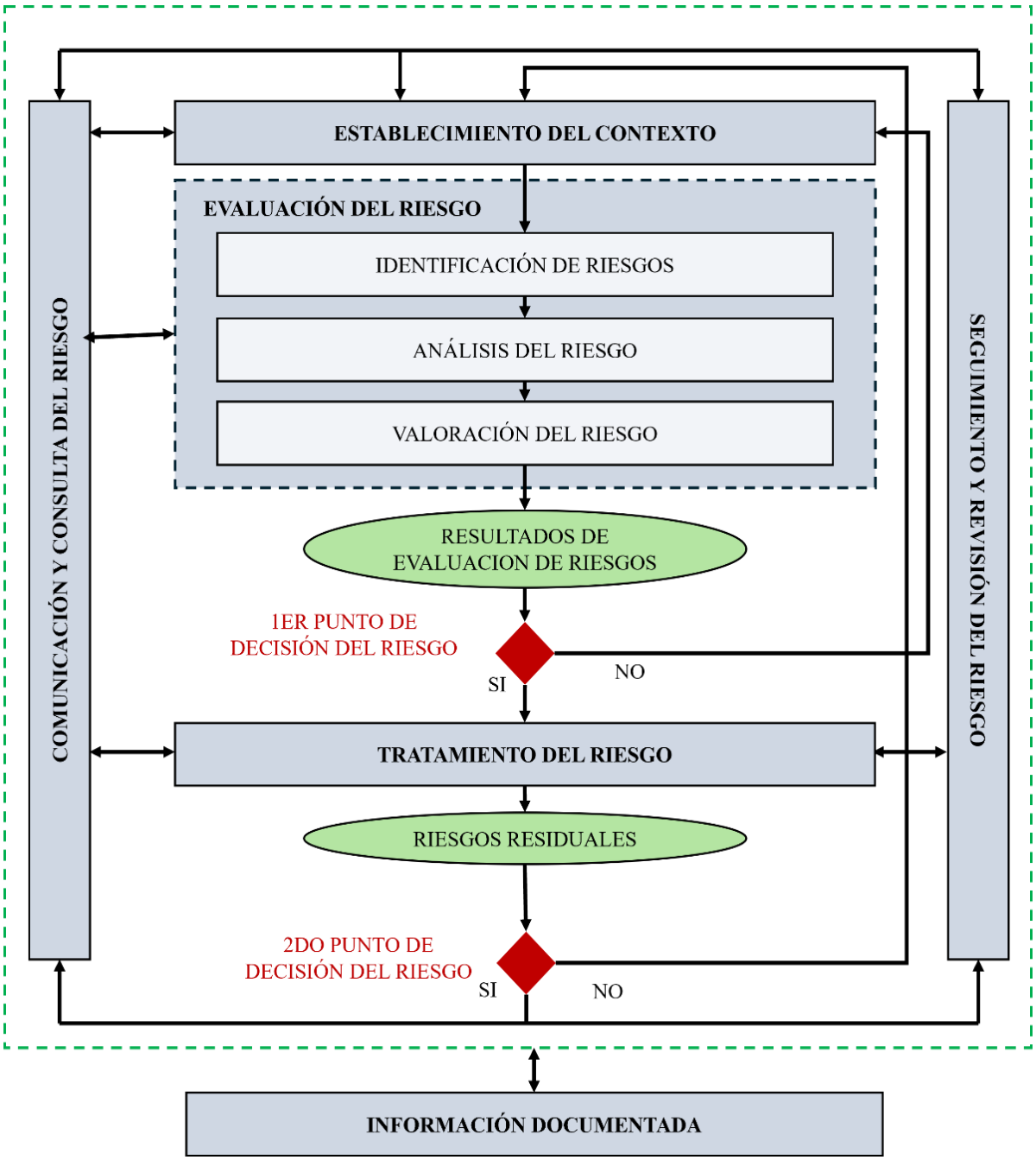
La Norma Técnica Peruana NTP ISO/IEC 27005:2022, adopción nacional del estándar internacional ISO/IEC 27005:2022, denominada *Seguridad de la información, ciberseguridad y protección de la privacidad: Orientación sobre la gestión de riesgos de seguridad de la información*, proporciona las directrices para la "gestión del riesgo de seguridad de la información en una organización, sin embargo, no establece metodologías específicas para tal fin" (Valencia, 2021, p. 75).

Según la norma NTP ISO/IEC 27005, "la gestión del riesgo analiza qué puede suceder y cuáles pueden ser las consecuencias posibles, antes de decidir qué debería ser hecho y cuándo, para reducir el riesgo a un nivel aceptable" (INACAL, 2022b, p.4).

En la Figura 12, se muestra el proceso de gestión de riesgos de la seguridad de la información según la ISO/IEC 27005.

Figura 12.

Proceso de gestión de riesgos según la ISO/ IEC 27005



Nota. Adaptado *de Proceso de gestión de riesgos de seguridad de información* (p.13), INACAL, 2022b.

A continuación, se detalla las actividades del proceso de gestión de riesgos de la seguridad de la información:

1. ***Establecimiento del contexto.*** Se establece los criterios básicos necesarios para la gestión del riesgo de seguridad de la información, los cuales son de dos tipos:

    a. **Criterios de aceptación del riesgo,** estos pueden ser uno o más valores (umbrales) que permiten tomar decisiones clave en el proceso de gestión del riesgo, la primera durante la valoración del riesgo, para determinar si el riesgo es aceptable; y la segunda, durante el tratamiento del riesgo, para decidir si el tratamiento propuesto es suficiente para alcanzar un nivel aceptable, o se necesita un tratamiento de riesgo adicional. Entre estos tenemos:

        i. ***Apetito de riesgo:*** Cantidad y tipo de riesgo que la organización decide asumir en la búsqueda del cumplimiento de sus objetivos estratégicos y la creación de valor (Instituto de Auditores Internos de España, s.f.).

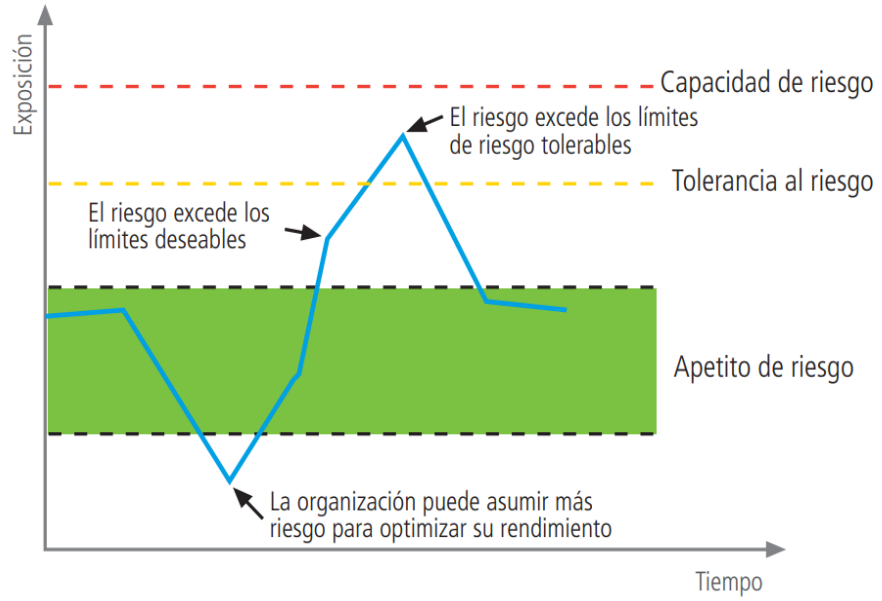
        ii. ***Tolerancia al riesgo:*** Es el límite de variación de riesgo respecto al apetito de riesgo que la organización está dispuesta a aceptar a fin de alcanzar sus objetivos. Proporciona métricas claras para determinar cuándo los niveles de riesgo requieren una intervención (Instituto de Auditores Internos de España, s.f.).

        iii. ***Capacidad de riesgo:*** Es el nivel máximo de riesgo que la es capaz de soportar en el cumplimiento de sus objetivos. (Instituto de Auditores Internos de España, s.f.).

    En la Figura 13 se puede observar la relación entre los términos apetito, tolerancia y capacidad del riesgo.

Figura 13.

Relación entre apetito, tolerancia y capacidad de riesgo



Nota. Adaptación de *Apetito, tolerancia y capacidad de riesgo* (p.17), del Instituto de Auditores Internos de España (s.f.)

b. **Criterios para la evaluación de riesgos de la seguridad de la información,** estos criterios especifican mediante escalas cualitativas o cuantitativas cómo se determina la importancia de un riesgo en términos de:

   i. ***Criterios de consecuencias (impacto),*** las escalas deben expresarse en términos del nivel de daño o pérdida que podría sufrir la organización o una persona debido a la afectación de la confidencialidad, integridad o disponibilidad de la información.

   ii. ***Criterios de probabilidad,*** las escalas pueden expresarse en términos probabilísticos (la posibilidad de que un evento ocurra en un periodo de tiempo determinado) o en términos frecuentistas (el número promedio de ocurrencias en un periodo de tiempo determinado).

iii. ***Criterios para determinar el nivel del riesgo (Criterios de valoración del riesgo)***, las escalas deben expresarse en base a los criterios de consecuencia y de probabilidad. Estos son necesarios para valorar los riesgos analizados y su propósito es ayudar a los propietarios del riesgo a decidir sobre la retención o tratamiento de los riesgos y priorizar el tratamiento del riesgo.

2. ***Evaluación de riesgos de seguridad de la información.*** Según la NTP ISO/IEC 27005:2022, en esta etapa se describe cualitativa o cuantitativamente el riesgo. La evaluación de riesgos consta de las siguientes actividades:

   a. **Identificación del riesgo,** proceso que consiste en encontrar, reconocer y describir los riesgos. Hay dos enfoques comúnmente utilizados para realizar la identificación de los riesgos:

      - Enfoque basado en eventos, identifica escenarios de riesgos estratégicos a partir de sucesos que preocupan a la alta dirección y las partes interesadas.
      - Enfoque basado en activos, parte de los activos de información y construye escenarios operativos combinando amenazas y vulnerabilidades, anticipando escenarios que podrían derivar en incidentes. Es más técnico y detallado.

   b. **Análisis del riesgo,** consiste en analizar las consecuencias y la probabilidad de cada riesgo identificado, con el fin de determinar su nivel de riesgo, utilizando metodologías de análisis cualitativo o cuantitativo, o semicuantitativo, dependiendo de las circunstancias. Comprende subactividades, las cuales son:

      - Evaluar las consecuencias
      - Evaluar la probabilidad
      - Determinar el nivel de riesgo.

c. **Valoración del riesgo**, el propósito es comparar el nivel del riesgo estimado frente a los criterios de aceptación del riesgo, con el fin de determinar si dicho riesgo puede ser aceptado de lo contrario debe ser priorizado para su tratamiento.

3. ***Tratamiento del riesgo de seguridad de la información.*** En esta etapa se busca gestionar los riesgos identificados aplicando estrategias adecuadas para su tratamiento; las cuales son:

   - Evitar el riesgo, al decidir no iniciar o continuar la actividad que da origen al riesgo.
   - Modificar el riesgo, reduciendo la probabilidad de ocurrencia o el impacto del riesgo, mediante controles o mejoras en el proceso.
   - Retener el riesgo, aceptar el riesgo sin tomar medidas inmediatas, asumiendo sus consecuencias por elección informada.
   - Compartir el riesgo, distribuir el riesgo con otras partes, ya sea interna o externamente.

   En función de la estrategia de tratamiento seleccionada, se definen el (los) control (es) necesario(s) para su cumplimiento, estos pueden ser de tipo preventivo, de detección o correctivo.

   Una vez definido el plan de tratamiento del riesgo, se determinan los riesgos residuales, los cuales surgen de la actualización de la evaluación de riesgos tras los efectos esperados del tratamiento del riesgo propuesto.

4. ***Comunicación y consulta del riesgo de seguridad de la información.*** La información acerca de los riesgos debería ser intercambiada y/o compartida entre los tomadores de decisiones y otros interesados.

5. ***Seguimiento y revisión del riesgo de seguridad de la información.*** Se debería hacer el seguimiento y revisión de los riesgos y sus factores para identificar cualquier cambio en el contexto de la organización en una etapa temprana, y para mantener una visión completa de los riesgos.

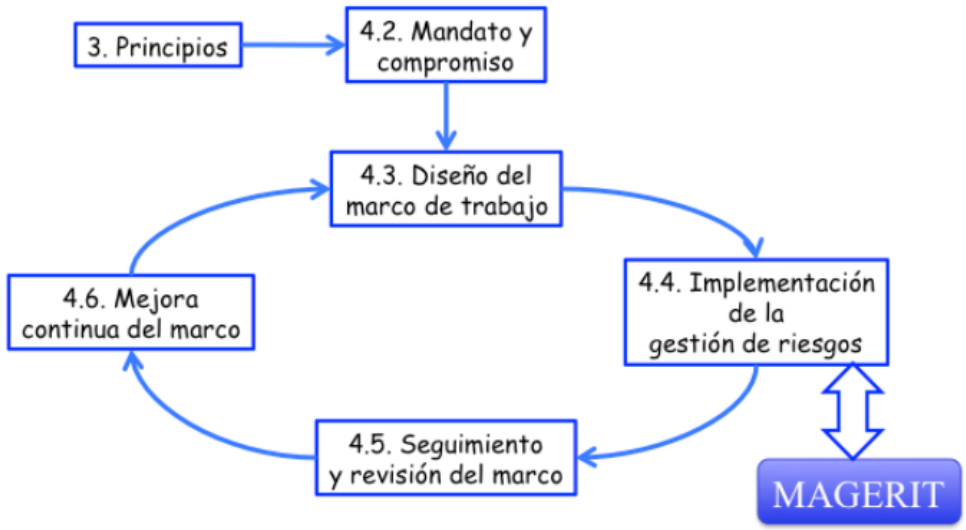
MAGERIT

MAGERIT, es una metodología integral de análisis y gestión de riesgos, cuya estructura se encuentra alineada a los principios establecidos en la norma ISO 31000.

La ISO 31000, proporciona directrices generales para la gestión sistemática de riesgos organizacionales, ofrece un esquema adaptable a cualquier sector, tamaño o estructura corporativa. MAGERIT, adopta el modelo propuesto por la norma, pero focaliza su atención específicamente en los riesgos derivados de los sistemas de información y las tecnologías de la comunicación (Observe Figura 14).

Figura 14.

Gestión de riesgos según ISO 31000



Nota. Adaptación de *ISO 31000 - Marco de trabajo para la gestión de riesgos*, (p.7), del Ministerio de Hacienda y Administraciones Públicas, 2012.

El proceso de gestión de riesgos según MAGERIT comprende tres componentes (Observe Figura 15):

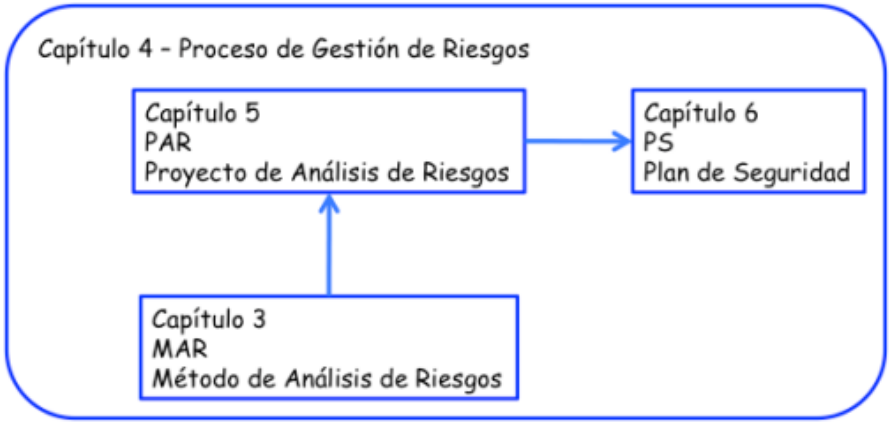
1. **Método de Análisis de Riesgos (MAR),** es el método técnico que define cómo realizar el análisis de riesgos (fase de análisis). Incluye subactividades como:
    - Caracterización de activos.
    - Caracterización de amenazas.
    - Caracterización de salvaguardas.
    - Estimación del nivel del riesgo.

2. **Proyecto de Análisis de Riesgos (PAR),** es la aplicación práctica del MAR en un proyecto concreto. Incluye actividades como:
    - Actividades preliminares (estudio de oportunidad, definición del alcance y planificación del proyecto).
    - Elaboración del análisis de riesgos siguiendo el método MAR.
    - Comunicación de resultados y documentación.

3. **Plan de Seguridad (PS),** es el resultado que surge tras realizar un PAR y consiste en un conjunto de proyectos y acciones para tratar los riesgos identificados. Incluye actividades como:
    - Identificación de proyectos de seguridad.
    - Planificación de proyectos de seguridad.
    - Ejecución del plan.

Figura 15.

Actividades del proceso de gestión de riesgos de MAGERIT



Nota. Adaptación de *Actividades formalizadas*, (p.13), del Ministerio de Hacienda y Administraciones Públicas, 2012.

Estos componentes se relacionan en un ciclo coherente: el MAR proporciona el método, el PAR es la aplicación práctica y el PS es la respuesta organizada para gestionar los riesgos detectados.

MARCO METODOLÓGICO

Tipificación de la Investigación

La investigación se ha tipificado como ***descriptiva tecnológica no experimental de tipo mixta***, a continuación, se detalla la fundamentación:

a. ***Según su alcance.*** Será de tipo descriptiva. Los autores Hernandez et al. (2014), refieren que las investigaciones descriptivas "únicamente pretenden medir o recoger información de manera independiente sobre los conceptos o las variables a las que se refiere, su objetivo no es indicar cómo se relacionan éstas" (p.92).

   En la presente investigación se pretende observar y describir la realidad actual del proceso de soporte y desarrollo de software SaaS de la empresa Iteprevengo con respecto a la seguridad de la información.

b. Por su propósito: Será de tipo tecnológica aplicada. Según Espinoza (2014) este tipo de investigación "tiene como propósito transformar conocimientos existentes o modelos en objetos útiles a la sociedad. Buscan que las soluciones generen efectividad o productividad" (p.106).

Por otra parte, Ñaupas et al. (2018) señalan que la investigación tecnológica surge como respuesta a la necesidad de mejorar y optimizar los sistemas y procedimientos existentes:

> Surge de la necesidad de mejorar, perfeccionar y optimizar el funcionamiento de los sistemas, los procedimientos, normas, reglas tecnológicas actuales a la luz de los avances de la ciencia y la tecnología. Por tanto, este tipo de investigación no se presta a la calificación de verdadero, falso o probable sino a la de: eficiente, deficiente, eficaz o ineficaz. (pág. 138)

La presente investigación pretende dar solución a la problemática expuesta con el diseño de un SGSI en base a la familia de estándares internacionales ISO/IEC 27000.

c. ***Por la contrastación de hipótesis.*** Será de tipo no experimental - transversal. Según Hernandez et al. (2014), las investigaciones no experimentales sólo observan al fenómeno en su ambiente natural para analizarlo. Además, las clasifican en: transversales y longitudinales, siendo la transversal aquella que recopila datos en un único momento.

   En la presente investigación no se pretende implementar el SGSI propuesto debido a las limitaciones presentadas, pero se someterá a un juicio de expertos para evaluar su efectividad. La recopilación de datos se hará en un momento concreto de la investigación.

d. ***Por la naturaleza de la información,*** será de tipo mixta. Para Lieber y Weisner (2010), como se citó en Hernandez et al. (2014), "los métodos mixtos caracterizan a los objetos de estudio mediante números y lenguaje e intentan recabar un rango amplio de evidencia para robustecer y expandir nuestro entendimiento de ellos". Es decir, conjugar los procedimientos de investigación cualitativa y cuantitativa.

   En la presente investigación se obtendrán datos de naturaleza cualitativa, como las perspectivas de los participantes, información de tipo textos, narrativas y elementos visuales. Esta información será representada en forma numérica para ser analizada matemáticamente.

Población y Muestra

Arias (2012) define a la población como "un conjunto finito o infinito de elementos con características comunes para los cuales serán extensivas las conclusiones de la investigación" (p.81), mientras que la muestra "es un subconjunto representativo y finito que se extrae de la población accesible" (p.83).

Se determinó que, debido a la cantidad limitada de elementos, la población y la muestra serán idénticas. Esta estará compuesta por todos los activos de información del proceso de soporte y desarrollo de software SaaS.

Técnicas de Recopilación de Información

La recopilación de la información es un proceso fundamental en toda investigación, ya que permite obtener datos que, al ser analizados e interpretados generan conocimiento.

En la presente investigación se recurrirá a diversas técnicas de recopilación de información, que facilitarán la identificación de aspectos relevantes sobre la seguridad de la información en la organización contribuyendo así al desarrollo del diseño del SGSI. Las técnicas y sus respectivos instrumentos son:

- *Entrevista semiestructurada,* consiste en formular preguntas en forma verbal al encuestado basándose en una guía no tan formal y rígida, permite al entrevistador introducir preguntas para esclarecer vacíos en la información; es decir no todas las preguntas están predeterminadas. Se tendrá como instrumento una Guía de preguntas en base a los requisitos de la NTP ISO/ IEC 27001 y al Anexo A de la norma.
- *Grupos de enfoque,* consiste en una reunión grupal focalizada, conducida por un moderador encargado de hacer preguntas y dirigir la discusión. El fin del investigador es conocer cómo los participantes construyen una perspectiva de un problema a través de la interacción colectiva. Para su aplicación se utilizará como instrumento un plan de trabajo, desarrollado en conjunto con los colaboradores de distintos niveles de la organización.
- *Revisión documental*, consiste en recopilar y analizar información procedente de documentos, registros, materiales, etc., lo que permite tener conocimientos previos sobre el tema de investigación. Para su aplicación, se emplearán fichas de registro de información que facilitarán la sistematización y el análisis de los documentos revisados.

Metodología Propuesta

Con base en los fundamentos teóricos expuestos en el Capítulo II, se adoptó como marco metodológico general para el diseño del Sistema de Gestión de la Seguridad de la Información (SGSI), la NTP ISO/IEC 27001:2022, por tratarse de un estándar internacional que ofrece los requisitos para establecer, implementar, mantener y mejorar un SGSI, siendo además la única norma certificable en materia de seguridad de la información.

Es necesario señalar que la NTP ISO/ IEC 27001 adopta un enfoque basado en la gestión de riesgos, aunque no define una metodología específica para llevarla a cabo. En este sentido, la selección metodológica se sustentó en el análisis comparativo de Guano y Jaramillo (2020), quienes identifican a la ISO/IEC 27005 y MAGERIT como las alternativas más completas y adaptables a distintos contextos organizacionales. En coherencia con estos hallazgos y considerando el objeto de estudio, se optó por la NTP ISO/IEC 27005:2022 como base para la gestión de riesgos, complementándola con herramientas de MAGERIT a fin de fortalecer el proceso de análisis.

Respecto a la estructura metodológica del proyecto, se adoptó la propuesta de Valencia (2021), autor que plantea una metodología basada en la ISO/IEC 27003:2010, por proporcionar una orientación práctica para el diseño de un SGSI. En base a esta propuesta, el proyecto se estructuró en cinco fases secuenciales, cada una con actividades y entregables específicos.

Finalmente, se precisa que el presente trabajo de investigación se limita únicamente al diseño del SGSI, sin incluir su implementación operativa. Esta decisión responde a las condiciones actuales de la organización; no obstante, el modelo propuesto constituye una base metodológica alineada a estándares internacionales, que podrá servir como hoja de ruta para una futura implementación y eventual proceso de certificación.

A continuación, se detallará cada fase, actividad y entregable:

Fase I : Contexto Organizacional y Compromiso de la Alta Dirección

- **Actividad 1: Determinar el Contexto de la Organización**

  El objetivo de esta actividad es analizar y comprender el entorno interno y externo en el que opera la organización, para identificar factores relevantes que influyen en la gestión de la seguridad de información. Para ello, se llevará a cabo una revisión documental orientada a obtener y sistematizar la información necesaria que permita describir adecuadamente el contexto organizacional.

  Entregable:

  - Historia, misión y visión.
  - Organigrama.
  - Tabla de análisis PESTEL.
  - Necesidades y expectativas de las partes interesadas.

- **Actividad 2: Elaborar el Plan del Proyecto**

  Esta actividad tiene como fin obtener la aprobación formal de la alta dirección para iniciar y ejecutar el proyecto. Para ello, se elaborará un Plan de Proyecto que contenga los rubros necesarios para facilitar a la alta dirección la toma de decisiones sobre la viabilidad del proyecto.

  Entregable:

  - Plan del proyecto.

Fase II - Definición del Alcance y la Política del SGSI

- **Actividad 3: Identificar y Caracterizar los Procesos del Negocio**

Esta actividad tiene como finalidad identificar y caracterizar los procesos del negocio de la organización, con el propósito de comprender su funcionamiento, su interacción y su relación con la información.

Para ello se elaborará un mapa de procesos de la organización, diferenciando los procesos estratégicos, operacionales (misionales) y de soporte.

Posteriormente se caracterizará cada proceso, teniendo en cuenta los siguientes criterios:

- Descripción del proceso: explicación general del propósito del proceso dentro de la organización.
- Entradas: recursos, información o insumos necesarios para ejecutar el proceso.
- Actividades clave: conjunto de actividades principales que permiten transformar las entradas en salidas.
- Salidas: resultados o productos generados por el proceso, pueden ser servicios, entregables o información.

Esta actividad permitirá contar con una visión estructurada de los procesos del negocio y servirá como base para el análisis de criticidad posterior orientado a la definición del alcance del SGSI.

Entregable:

- Mapa general de los procesos de la organización.
- Tabla de caracterización descriptiva de los procesos de la organización.

- **Actividad 4: Definir el Alcance del SGSI**

Según Valencia (2021), el alcance "define dónde y para qué es exactamente aplicable el SGSI, puede ser un proceso, un conjunto de procesos, una sede, un servicio o un conjunto de servicios" (p.86). Este debe ser claro y preciso, evitando que sea tan amplio

que comprometa la viabilidad del proyecto, o tan limitado que no aporte un valor real a la empresa ni facilite una eventual certificación.

En esta actividad, se realizará un análisis de criticidad de los procesos previamente identificados en la Actividad 3, con el objetivo de determinar de manera objetiva el alcance del SGSI.

El análisis de criticidad se basará en la evaluación comparativa de cada proceso utilizando los siguientes criterios:

- Nivel de sensibilidad de la información gestionada.
- Nivel de dependencia tecnológica.
- Influencia en la generación de ingresos.

Cada criterio será valorado mediante una escala ordinal, permitiendo asignar un puntaje cuantitativo a variables cualitativas. La suma de los puntajes permitirá determinar el nivel de criticidad relativa de cada proceso. En las Tablas 13, 14 y 15 se muestran las escalas utilizadas para el análisis:

Tabla 13.

Nivel de sensibilidad de información que gestiona un proceso

TIPO	DESCRIPCIÓN	VALOR
Baja	Información pública o de libre difusión sin impacto relevante.	1
Media	Información interna cuyo acceso no autorizado puede generar inconvenientes operativos.	2
Sensible	Información interna o de clientes cuya divulgación o alteración puede afectar reputación o cumplimiento contractual.	3
Crítica	Información altamente confidencial, estratégica o regulada (datos personales, código fuente, bases de datos productivas, credenciales, información de salud, etc.).	4

Nota. Elaborado por los investigadores.

Tabla 14.

Nivel de dependencia tecnológica del proceso

NIVEL	DESCRIPCIÓN	VALOR
Bajo	El proceso puede ejecutarse manualmente sin afectar significativamente su continuidad.	1
Medio	Utiliza herramientas digitales de apoyo, pero puede continuar parcialmente sin ellas.	2
Alto	Requiere sistemas tecnológicos para su ejecución normal; la interrupción genera paralización significativa.	3
Muy Alto	Depende totalmente de infraestructura tecnológica; sin sistemas TI el proceso no puede operar.	4

Nota. Elaborado por los investigadores.

Tabla 15.

Tipo de influencia en la generación de ingresos de la organización

NIVEL	DESCRIPCIÓN	VALOR
No genera	No tiene relación directa con ingresos.	1
Indirecta	Contribuye al funcionamiento de procesos que generan ingresos.	2
Directa	El proceso produce servicios o productos facturables.	3

Nota. Elaborado por los investigadores.

En la Tabla 16 se expone la escala de utilizada para valorar la criticidad de los procesos de la organización.

Tabla 16.

Escala de valoración de criticidad de los procesos

RANGO DE PUNTAJE	NIVEL DE CRITICIDAD	INTERPRETACIÓN
3-5	Baja	Proceso con limitada exposición a riesgos de SI, baja dependencia tecnológica y menor impacto en el modelo de negocio desde la perspectiva del SGSI
6-8	Media	Proceso con exposición moderada a riesgos de SI. Requiere controles, pero su nivel de criticidad no lo posiciona como prioritario para el alcance inicial del SGSI.
9-11	Alta	Proceso estratégico con alta exposición a riesgos de SI; prioritario para el alcance del SGSI.

Nota. Elaborado por los investigadores

Los procesos clasificados con nivel de criticidad alta serán incluidos dentro del alcance del SGSI.

Entregable:

- Alcance del SGSI.

- **Actividad 5: Definir los Roles y Responsabilidades**

  En esta actividad se identificará y documentará los roles y responsabilidades necesarios para el diseño, implementación y gestión del SGSI, garantizando que cada colaborador asignado comprenda de manera clara sus tareas y funciones relacionadas con la seguridad de información.

  Entregable:

  - Roles y responsabilidades.

- **Actividad 6: Definir la Política de la Seguridad de la Información**

  De acuerdo con Valencia (2021), la política de la Seguridad de la Información es un documento normativo de cumplimiento obligatorio, por medio del cual la alta dirección manifiesta su compromiso con la seguridad de la información. Este documento orienta las decisiones y acciones relacionadas con dicho ámbito y, debe ser aprobado, publicado y comunicado por la alta dirección a todas las partes interesadas del SGSI.

  Entregable:

  - Política de la Seguridad de la Información.

Fase III: Análisis de los Requisitos de la Seguridad de Información

- **Actividad 7: Realizar un análisis de brechas**

Antes de abordar de manera directa un análisis de riesgos, es fundamental conocer el estado actual de la organización en materia de seguridad de la información. Para ello, se llevará a cabo un análisis de brechas, mediante la aplicación de guías de entrevista , diseñadas en base a los requisitos establecidos en la NTP ISO/IEC 27001:2022 y los 93 controles del Anexo A de dicha norma.

La aplicación de los instrumentos se llevará a cabo mediante entrevistas semiestructuradas al personal de TI y al CEO de la organización. Los datos obtenidos serán analizados utilizando una versión adaptada del modelo de madurez de procesos de COBIT 5, con el fin de determinar el nivel de cumplimiento de cada requisito y control evaluado. El modelo de madurez adaptado se muestra en la Tabla 17.

Tabla 17.

Modelo de madurez utilizado en análisis de brechas

ESTADO	DESCRIPCIÓN
NO APLICA	El control no es relevante para la organización debido a su contexto, modelo de negocio o estructura.
INEXISTENTE	No hay evidencia de que el control se aplique en la organización. Puede o no haber conocimiento sobre él.
INICIAL	Se reconoce la importancia del control, se aplican algunas buenas prácticas de manera reactiva e informal, pero sin estructura ni documentación.
LIMITADO	El control se aplica de un modo totalmente informal. Existen documentos preliminares (políticas, procedimientos, configuraciones), pero sin estandarización, ni aprobación.
DEFINIDO	El control está formalmente establecido (documentado, aprobado y comunicado) y se aplica. Puede tratarse de un procedimiento, una política o una configuración técnica.
GESTIONADO	Se aplica y se mide la efectividad del control mediante auditorías, métricas o revisiones periódicas. Se aplican mejoras basadas en datos.
OPTIMIZADO	El control está en mejora continua, se ajusta según resultados y nuevas amenazas o regulaciones.

Nota. Elaborado por los investigadores tomando como referencia COBIT 5.

Entregable:

- Informe de análisis de brechas.

- **Actividad 8: Identificar los Activos de Información**

  En la presente investigación se decidió aplicar un enfoque basado en activos para lograr identificar los riesgos de seguridad de la información.

  Para el cumplimiento de esta actividad, se trabajará de manera conjunta con el personal de TI, con el objetivo de identificar, clasificar y registrar todos los activos de información comprendidos en el alcance del SGSI. La información recopilada será documentada según el formato descrito en la Tabla 18, el cual permitirá consolidar el Registro de Inventario de Activos y servirá como insumo principal para las etapas posteriores del análisis de riesgos.

Tabla 18.

Catalogación de activos de información

CAMPO	DESCRIPCIÓN
ID ACTIVO	Identificador único asignado a cada activo para facilitar su registro y trazabilidad dentro del SGSI.
NOMBRE DEL ACTIVO	Denominación breve del activo de información.
DESCRIPCIÓN DEL ACTIVO	Detalle que especifica las características, funcionalidades o propósito del activo dentro de la organización.
PROPIETARIO DEL ACTIVO	Persona responsable de la gestión y protección del activo.
CATEGORÍA	Si es primario o de soporte, según lo definido en la metodología.
TIPO	Sub clasificación del activo si es información, software, hardware, personal, red, etc.

Nota. Elaborado por los investigadores.

Entregable:

- Tabla de Registro de inventario de activos.

- **Actividad 9: Definir Criticidad de los Activos de Información**

  Una vez identificados los activos involucrados en el alcance, se procederá a valorar cada uno de ellos en base a las tres dimensiones básicas de la seguridad de la información: confidencialidad, integridad y disponibilidad.

  Siguiendo los lineamientos metodológicos propuestos por MAGERIT, cada dimensión será valorada cuantitativamente utilizando una escala común y homogénea del 1 al 3. La Tabla 19 detalla esta escala, donde 1 representa un nivel bajo de afectación, 2 un nivel medio y 3 un nivel alto de afectación.

Tabla 19.

Escala de valoración de las dimensiones de la SI

CRITERIO	VALOR	DESCRIPCIÓN
DISPONIBILIDAD	1	La disponibilidad del activo no es crítica, y una interrupción no tendría un impacto grave.
	2	La interrupción podría causar inconvenientes o daños moderados, pero los procesos pueden ser restaurados rápidamente.
	3	El activo debe estar disponible en todo momento, la interrupción causaría un impacto crítico.
INTEGRIDAD	1	La alteración no tiene consecuencias graves, los procesos pueden seguir funcionando sin grandes problemas.
	2	La alteración podría causar interrupciones moderadas en las operaciones o daños financieros menores.
	3	La alteración no autorizada del activo podría causar un daño crítico (interrupción de operaciones clave, daño financiero considerable).
CONFIDENCIALIDAD	1	La información es pública o poco sensible. La divulgación no tendría un impacto significativo.
	2	La divulgación no autorizada causaría un impacto moderado (impacto en operaciones internas, posible daño reputacional).
	3	La información es extremadamente sensible. La divulgación no autorizada causaría un impacto grave (pérdida de ventaja competitiva, daño legal, etc.).

Nota. Elaborado por los investigadores tomando como referencia la NTP ISO/IEC 27005.

Tras valorar cada activo de información según la tríada CID, se estimará su criticidad promediando los valores asignados a cada dimensión (Ver Fórmula 1). El resultado obtenido será redondeado al número entero más cercano, y en función de este, se asignará un nivel de criticidad, de acuerdo a la escala expuesta en la Tabla 20.

Fórmula 1:

$$\text{NIVEL DE CRITICIDAD} = \frac{\text{VALOR DE CONFIDENCIALIDAD} + \text{VALOR DE INTEGRIDAD} + \text{VALOR DE DISPONIBILIDAD}}{3}$$

Tabla 20.

Nivel de criticidad de los activos de información

VALOR DE CRITICIDAD	NIVEL DE CRITICIDAD
1	Baja
2	Media
3	Alta

Nota. Elaborada por los investigadores.

Entregable:

- Tabla de catalogación de activos de información.

Fase IV: Evaluación y Tratamiento de Riesgos

- **Actividad 10: Identificar amenazas y vulnerabilidades**

  Las vulnerabilidades, por sí solas, no causan daño, son condiciones que podrían ser aprovechadas por una amenaza y afectar a un activo de información, dando lugar a un incidente (Valencia, 2021). Comprender esta relación es esencial en el análisis de riesgos, siendo clave formularse la siguiente pregunta: ¿Qué amenaza podría explotar determinada vulnerabilidad de un activo?

El propósito de esta actividad es identificar las vulnerabilidades internas y las amenazas potenciales asociadas a cada activo de información, con el fin de identificar los posibles "escenarios de riesgo", que a partir de ahora serán denominados "riesgos intrínsecos".

Para realizar esta actividad, se trabajará con el personal de TI a través de un grupo de enfoque, utilizando como insumos: el catálogo de amenazas (Anexo C) y el catálogo de vulnerabilidades (Anexo D) de la norma NTP ISO/ IEC 27005, así como los resultados obtenidos en el análisis de brechas de la Actividad 7.

Entregable:

- Tabla de amenazas y vulnerabilidades por activo.

- **Actividad 11: Analizar el riesgo**

  En esta actividad se busca comprender la naturaleza del riesgo, con el fin de determinar el nivel de riesgo mediante la evaluación conjunta de dos variables fundamentales:

  a. **Estimación del impacto**, consiste en estimar el grado de afectación que tendría la materialización de un riesgo intrínseco sobre los activos de información.

     Siguiendo las directrices de la metodología de MAGERIT y con el fin de asegurar un enfoque integral, se han definido tres criterios de evaluación para la estimación del impacto, los cuales son: continuidad de los servicios, economía y seguridad.

     Cada criterio se valorará mediante una escala numérica del 1 al 5, la cual se presenta en la Tabla 21, facilitando el análisis, la interpretación y la comparación entre los diferentes niveles.

     MAGERIT (2012), señala que la criticidad de un activo tiene influencia directa en la estimación del impacto, ya que esta se utiliza como base para valorar las posibles consecuencias de la materialización de un riesgo; es decir, mientras

mayor sea la criticidad del activo de información, mayor será el impacto que podría generar en la organización.

Tabla 21.

Criterios de evaluación para la estimación del impacto

VALOR	NIVEL	CONTINUIDAD DE SERVICIOS	ECONOMÍA	SEGURIDAD
1	MUY BAJO	Las interrupciones tienen un efecto marginal sobre actividades poco relevantes.	Las afectaciones económicas son mínimas y sin consecuencias contractuales significativas.	Se presentan eventos de seguridad sin efectos considerables sobre la organización o sus activos.
2	BAJO	Ocurren interferencias menores que no impiden continuar con procedimientos de emergencia u operatividad básica.	Se producen pequeñas pérdidas o leves incumplimientos en contratos sin mayor trascendencia.	Se dan incidentes con repercusión limitada sobre la seguridad de los activos de información.
3	MEDIO	Afecta la eficiencia de las operaciones por condiciones adversas, aunque sin paralizar la actividad completamente.	Las pérdidas son notables y algunos compromisos contractuales pueden verse afectados de forma relevante.	Se detectan problemas de seguridad que pueden ser analizados y gestionados sin mayores dificultades.
4	ALTO	Se generan cortes importantes en los servicios, paralizando ciertas áreas operativas y requiriendo altos costos de recuperación.	Las pérdidas económicas son serias, acompañadas de fallos en el cumplimiento de compromisos contractuales relevantes.	Existen incidentes importantes de seguridad, con complicaciones para su investigación o rastreo.
5	MUY ALTO	Se generan fallas críticas en las operaciones, lo que impacta de manera significativa en la reputación y ocasiona daños en equipos o infraestructuras.	Se generan pérdidas financieras muy significativas y se incumplen obligaciones contractuales de alta importancia.	Se presentan incidentes graves en seguridad, imposibilitando el seguimiento o análisis de los eventos.

Nota. Elaborado por los investigadores en base a MAGERIT (2012).

El impacto final se calculará promediando los valores asignados a cada criterio de evaluación, para cada riesgo intrínseco (Ver Fórmula 2). El valor resultante será redondeado al número entero más cercano, y con base en este se determinará un nivel de impacto final, de acuerdo a la escala expuesta en la Tabla 22.

Fórmula 2:

$$\text{IMPACTO FINAL} = \frac{\text{CRITERIO 1} + \text{CRITERIO 2} + \text{CRITERIO 3}}{3}$$

Tabla 22.

Escala de valoración de impacto final

VALOR	NIVEL	DESCRIPCIÓN
1	MUY BAJO	El riesgo tendría un efecto marginal sobre la organización. Las interrupciones serían mínimas, sin afectar significativamente las operaciones, las finanzas ni la seguridad de la información. No se requerirían medidas extraordinarias para su resolución.
2	BAJO	El riesgo ocasiona perturbaciones menores que podrían gestionarse sin impacto significativo en la continuidad operativa, la economía ni la confidencialidad o integridad de los activos. Las consecuencias serían controlables y de baja trascendencia.
3	MEDIO	El riesgo generaría afectaciones visibles y moderadas en al menos uno de los tres criterios. Podría impactar la eficiencia operativa, provocar pérdidas relevantes o causar incidentes de seguridad gestionables pero que requieren atención.
4	ALTO	El riesgo tendría un impacto importante en la organización. Podría comprometer la continuidad operativa, generar pérdidas económicas considerables o desencadenar incidentes de seguridad con efectos duraderos y difíciles de rastrear o mitigar.

5	MUY ALTO	El riesgo podría causar daños críticos y generalizados en múltiples dimensiones: operaciones paralizadas, pérdidas financieras graves e incidentes de seguridad severos que afectan la reputación, la infraestructura o la capacidad de respuesta.

Nota. Elaborado por los investigadores en base a MAGERIT (2012).

b. Probabilidad de ocurrencia, consiste en estimar la frecuencia con la que un riesgo intrínseco podría llegar a materializarse.

Para estimar la probabilidad de ocurrencia se considerarán tres criterios: el tipo de exposición al riesgo, la existencia o ausencia de controles y la experiencia previa del sector frente a amenazas similares.

Esta valoración se realizará mediante una escala numérica única detallada en la Tabla 23.

Tabla 23.

Escala de valoración de probabilidad

VALOR	NIVEL	DESCRIPCIÓN
1	REMOTO	No existe exposición directa al riesgo. Existen múltiples controles preventivos eficaces. Las amenazas asociadas son muy raras en el sector empresarial.
2	IMPROBABLE	La exposición al riesgo es limitada o restringida a entornos internos. Existen controles, aunque estos no son totalmente eficaces. La amenaza es ocasional o en contextos muy específicos.
3	POSIBLE	Exposición al riesgo conocida. Existen controles parcialmente implementados. La amenaza es común en el sector y, aunque no hay antecedentes internos, el riesgo es latente.
4	PROBABLE	Existe una exposición significativa. Los controles son inexistentes o ineficaces. La amenaza es conocida y recurrente en entornos similares.
5	MUY PROBABLE	Hay una exposición directa sin ningún tipo de protección. Los controles son inexistentes o ineficaces. La amenaza es automatizada o masiva.

Nota. Elaborado por los investigadores en base a MAGERIT (2012).

A partir de estas dos estimaciones previas (impacto y probabilidad), se procederá a calcular la exposición al riesgo, para cada riesgo intrínseco, utilizando la Fórmula 3.

Fórmula 3:

EXPOSICIÓN AL RIESGO = PROBABILIDAD * IMPACTO

Posterior a ello se determinará el Nivel de Exposición al Riesgo (NER) utilizando la escala expuesta en la Tabla 24, la cual muestra una escala ponderada que agrupa los posibles valores de la exposición al riesgo en cuatro niveles.

Tabla 24.

Escala de valoración de exposición al riesgo

RANGO	NIVEL	DESCRIPCIÓN	CONDICIÓN
1 – 4	Bajo	El riesgo es mínimo; el impacto o la probabilidad son bajos. Es poco probable que afecte significativamente a la organización.	Riesgo aceptable por Iteprevengo
5 – 9	Medio	El riesgo es moderado. Podría afectar a la organización en ciertas condiciones, pero no compromete funciones críticas.	Riesgo aceptable por Iteprevengo. (Condicionalmente)
10 – 15	Alto	El riesgo es significativo; existe una probabilidad o impacto considerable. Podría generar una afectación importante a la organización. Requiere monitoreo y evaluación.	Riesgo inaceptable por Iteprevengo
16 – 25	Crítico	El riesgo elevado; impacto o probabilidad graves. Puede afectar gravemente los activos críticos de la organización. Necesita medidas inmediatas.	Riesgo inaceptable por Iteprevengo

Nota. Elaborado por los investigadores tomando como referencia la NTP ISO/IEC 27005.

Para facilitar el análisis e interpretación visual de los resultados, en la Tabla 25 se expone una matriz de calor, que muestra cada NER asociado por color a su categoría correspondiente.

Tabla 25.

Matriz de calor para la valoración del NER

		MUY BAJO	BAJO	MEDIO	ALTO	MUY ALTO
		1	2	3	4	5
MUY PROBABLE	5	5	10	15	20	25
PROBABLE	4	4	8	12	16	20
POSIBLE	3	3	6	9	12	15
IMPROBABLE	2	2	4	6	8	10
REMOTO	1	1	2	3	4	5

Nota. Elaborado por los investigadores tomando como referencia la NTP ISO/IEC 27005.

Entregable:

- Tabla de análisis del riesgo/ Cálculo del NER.

- **Actividad 12: Valorar el riesgo**

  Como parte del proceso de gestión del riesgo, es necesario establecer los "criterios de aceptación del riesgo", umbrales que orientarán la toma de decisiones respecto al tratamiento de los riesgos identificados. En este sentido, se definirán dos criterios fundamentales:

  a. **Apetito del riesgo**, se refiere a todos aquellos riesgos intrínsecos clasificados como "nivel bajo", es decir, con un valor de NER entre 1 y 4.
  b. **Tolerancia al riesgo**, se extiende hasta aquellos riesgos intrínsecos clasificados como "nivel medio", es decir, con un valor de NER entre 5 y 9. Estableciéndose como umbral de tolerancia un NER con valor igual a 9.

La valoración del riesgo es el primer punto de decisión crítica dentro del proceso de gestión del riesgo, consiste en comparar los resultados del análisis del riesgo contra los criterios de aceptación del riesgo definidos.

En este punto se evaluará si el NER supera el umbral de tolerancia definido para la presente investigación. Aquellos riesgos cuya magnitud exceda dicho umbral deberán ser incorporados al Plan de Tratamiento del Riesgo (PTR).

Para los riesgos cuyo NER no supere el umbral, se procederá a determinar si la información disponible es suficiente para considerarlos aceptables.

Entregable:

- Tabla de análisis del riesgo/Valoración del riesgo.

- **Actividad 13: Definir el Plan de Tratamiento del Riesgo**

  El objetivo de esta actividad es reducir el NER de cada riesgo no aceptado a un valor o nivel inferior al umbral de tolerancia definido, mediante la aplicación de estrategias de tratamiento de riesgos.

  Para ello, se seleccionará la estrategia de tratamiento más adecuada junto con las acciones específicas requeridas para implementar la estrategia seleccionada. Finalmente se determinarán las salvaguardas (controles) relacionados a la acción a implementar, utilizando como fuente el Anexo A de la norma NTP ISO/IEC 27001:2022 y la NTP ISO/IEC 27002:2022.

  Entregable:

  - Tabla del Plan de Tratamiento del Riesgo.

Fase V: Diseño del Sistema de Gestión de la Seguridad de la Información

- **Actividad 14: Definir estructura documental del SGSI**

  La documentación es la columna vertebral de un SGSI. En esta actividad se elaborarán únicamente los documentos exigidos por la NTP ISO/IEC 27001 que correspondan a la etapa de diseño del SGSI, según lo indicado en la Tabla 11 del marco teórico. La documentación generada en esta etapa resulta fundamental para facilitar la futura implementación, auditoría y mejora continua del SGSI.

  Entregables:

  - Documentación obligatoria por la ISO/IEC 27001.

- **Actividad 15: Plan de Concientización de Seguridad de Información**

  El factor humano constituye uno de los principales riesgos para la seguridad de la información en las organizaciones, por ende se requiere asegurar que su personal conozca, comprenda y aplique adecuadamente los lineamientos del SGSI.

  En esta actividad se elaborará un plan destinado a fomentar la cultura de seguridad de la información dentro de la organización. El diseño incluirá objetivos del programa, contenidos mínimos alineados con las amenazas y riesgos identificados, modalidades de capacitación (presencial, virtual y campañas internas) e indicadores para evaluar la eficacia del programa.

  Entregable:

  - Plan de concientización y sensibilización de la Seguridad de la Información.

- **Actividad 16: Definir indicadores de desempeño del SGSI**

  La presente actividad tiene como finalidad definir los indicadores de desempeño del SGSI, con el propósito de evaluar de manera sistemática la eficacia y nivel de cumplimiento del sistema, en concordancia con los requisitos de la NTP ISO/IEC 27001:2022, cláusula 9.1.

  Para la definición de los indicadores se tomará como referencia la NTP ISO/IEC 27004, la cual establece directrices para la medición y evaluación del desempeño del SGSI.

  Previamente, se determinarán las dimensiones de medición, entendidas como áreas del SGSI que agrupan aspectos relacionados de la gestión de seguridad de la información. Estas dimensiones se determinan considerando la estructura de la ISO/IEC 27001:2022, los controles aplicables del Anexo A, el análisis de riesgos realizado y el alcance definido del sistema.

  A partir de cada dimensión se definen indicadores, los cuales constituyen medidas cuantificables que permiten evaluar el cumplimiento de los objetivos del SGSI y la eficacia de los controles implementados. Para cada indicador se determinará el objetivo de la medición, tipo de indicador (KPI o KRI), métrica asociada, fórmula de cálculo, fuente de datos, frecuencia de medición, meta y el responsable de seguimiento.

  Entregables:

  - Tablas de métricas e indicadores

RESULTADOS

El presente capítulo desarrolla la propuesta de diseño del Sistema de Gestión de la Seguridad de la Información (SGSI) para los procesos de soporte y desarrollo de software de la empresa Iteprevengo. La propuesta se estructura bajo el enfoque del ciclo PDCA, garantizando la coherencia sistémica del modelo y su orientación hacia la mejora continua.

Dado el carácter propositivo de la investigación, el alcance del presente trabajo se centra en el diseño metodológico y estructural de los componentes del SGSI, sin contemplar su implementación. No obstante, el modelo incorpora lineamientos proyectados para su ejecución y seguimiento, a fin de asegurar su viabilidad y consistencia técnica.

La arquitectura general del SGSI propuesto se presenta en la Figura16, donde se observa la interacción de sus componentes bajo el enfoque PHVA y el rol central de la gestión de riesgos como eje transversal del sistema.

Posteriormente, en la Tabla 26 se detallan los componentes del SGSI propuesto, junto con la metodología empleada para su desarrollo y la naturaleza estructural o funcional de cada elemento que lo conforma.

Figura 16.

Diseño del Sistema de Gestión de la Seguridad de la Información propuesto

Nota. Elaborado por los investigadores

Tabla 26.

Componentes del SGSI propuesto

COMPONENTE	METODOLOGÍA UTILIZADA	TIPO DE ELEMENTO
Contexto de la organización	Se desarrolló mediante revisión documental institucional, entrevistas semiestructuradas a personal clave y análisis de partes interesadas. Asimismo, se aplicó un análisis PESTEL para identificar factores externos relevantes. El componente se formuló en coherencia con los lineamientos establecidos en la cláusula 4.1 de la ISO/IEC 27001, relativa al contexto de la organización.	**Estructural.** Se define el marco base del SGSI.
Alcance del SGSI	Se realizó un análisis de procesos para comprender el funcionamiento interno y los flujos de información de la organización. Posteriormente, se aplicó un Análisis de Impacto al Negocio (BIA) que permitió identificar procesos críticos. Con base en estos resultados, se delimitó objetivamente el alcance del SGSI, en coherencia con lo establecido en la cláusula 4.3 de la ISO/IEC 27001:2022.	**Estructural.** Se delimitan los límites y la aplicabilidad del sistema.
Política de la Seguridad de la Información	La Política de Seguridad de la Información fue estructurada en una política general y políticas específicas. Para su organización se tomó como referencia la clasificación de los 14 dominios de seguridad de la ISO/IEC 27001:2013, por considerarse una estructura temática que facilita un desarrollo ordenado del documento. Su formulación se realizó en concordancia con la cláusula 5.2 de la ISO/IEC 27001:2022.	**Estructural.** Se establecen lineamientos en materia de seguridad de la información.
Objetivos de la Seguridad de la Información	Se definieron en coherencia con la Política de Seguridad de la Información, el contexto organizacional y el alcance del SGSI. Su formulación se realizó conforme a lo establecido en la cláusula 6.2 de la ISO/IEC 27001:2022	**Estructural.** Se establecen metas que guían el desempeño del SGSI. El seguimiento de cumplimiento de metas es funcional.
Roles y responsabilidades	Se definieron a partir del análisis del organigrama institucional, las funciones existentes y el alcance del SGSI,	**Estructural.** Se define la estructura organizativa del SGSI.

	asignando responsabilidades específicas relacionadas con la gestión de la seguridad de la información. La estructuración de roles se realizó en concordancia con la cláusula 5.3 de la ISO/IEC 27001:2022.	
Modelo de Gestión de Riesgos	Se estructuró tomando como base la ISO/IEC 27005 como marco metodológico para la identificación, análisis, evaluación y tratamiento de riesgos de seguridad de la información. Asimismo, se incorporaron herramientas técnicas de MAGERIT para fortalecer la valoración de activos, amenazas e impactos. El modelo fue diseñado en coherencia con las cláusulas 6.1.2 y 6.1.3 de la ISO/IEC 27001:2022.	**Estructural.** Define el marco metodológico para la gestión del riesgo dentro del SGSI. Su aplicación se materializa de manera funcional
Plan de Tratamiento de Riesgos	Se elaboró a partir de los resultados de la evaluación de riesgos, definiendo para cada riesgo identificado la opción de tratamiento correspondiente y seleccionando controles alineados al Anexo A de la ISO/IEC 27001:2022. Para el análisis detallado de los controles seleccionados, se utilizó como referencia la ISO/IEC 27002. Su formulación se realizó en concordancia con la cláusula 6.1.3 de la ISO/IEC 27001:2022.	**Funcional.** Es el resultado de la evaluación del riesgo.
SOA	Se elaboró con base en los resultados del análisis y tratamiento de riesgos, justificando la inclusión o exclusión de los controles del Anexo A de la ISO/IEC 27001:2022. La ISO/IEC 27002 se utilizó como guía para el análisis técnico de los controles. Su formulación se realizó en concordancia con la cláusula 6.1.3 d) de la norma.	**Estructural.** Se formaliza la selección y justificación de controles.
Implementación de controles	Se plantearon acciones propuestas para la implementación de los controles definidos en el PTR. Para la definición de dichas acciones se utilizó como guía la ISO/IEC 27002. Este componente se desarrolló en concordancia con la cláusula 6.1.3 y el enfoque operativo de la cláusula 8 de la ISO/IEC 27001:2022.	**Funcional.** Comprende las acciones orientadas al aplicar los controles definidos.
Plan de concientización	El Plan de Concientización se diseñó considerando el contexto organizacional,	**Estructural** Se plantean actividades

	los procesos incluidos en el alcance del SGSI, los resultados del análisis de riesgos y la documentación del sistema, incluida la Política de Seguridad de la Información. Asimismo, se tuvo en cuenta los roles definidos y los requisitos de competencia y toma de conciencia establecidos en las cláusulas 7.2 y 7.3 de la ISO/IEC 27001:2022.	orientadas a fortalecer la toma de conciencia, contribuyendo a la operación del SGSI.
Documentación del SGSI	Se elaboró conforme a los requisitos obligatorios de la ISO/IEC 27001:2022, desarrollándose únicamente los documentos correspondientes al diseño del sistema.	**Estructural.** Proporciona soporte formal y normativo al SGSI
Métricas e indicadores	Las métricas e indicadores del SGSI fueron definidos en concordancia con la cláusula 9.1 de la ISO/IEC 27001:2022, utilizando como guía metodológica la ISO/IEC 27004 para su estructuración. Para la organización de los indicadores se tomó como referencia los objetivos del SGSI y las cláusulas pertinentes de la ISO/IEC 27001:2022.	**Funcional.** Permite evaluar el desempeño, eficacia y mejora del SGSI.

Nota. Elaborado por los investigadores

En los apartados siguientes se desarrolla cada componente de manera detallada, siguiendo la estructura metodológica propuesta en base a la NTP ISO/IEC 27003. A continuación, se presenta el desarrollo de cada fase, sus respectivas actividades y entregables relacionados:

FASE I: Contexto Organizacional y Compromiso de la Alta Dirección

- **Actividad 1: Determinar el Contexto de la Organización**

Para el desarrollo de esta actividad, se realizó una revisión exhaustiva de la documentación interna de la organización, lo cual permitió comprender el entorno interno y externo de Iteprevengo. Como resultado, se definieron los entregables asociados a esta actividad, los cuales se detallan a continuación:

Historia

La empresa fue fundada en el año 2013 bajo el nombre de P&M HSEQ, por iniciativa del Ing. Herbert Parimango y un equipo de especialistas en prevención de accidentes y enfermedades ocupacionales. Desde sus inicios la empresa se ha especializado en la prestación de servicios de consultoría, capacitación y desarrollo de software, todos ellos enfocados en la Seguridad y Salud en el Trabajo (SST). Posteriormente, con el objetivo de reflejar mejor su identidad y propósito, la empresa cambió su nombre comercial a Iteprevengo.

En el año 2020, como respuesta a la pandemia, la empresa adoptó un modelo de trabajo 100% remoto. Este periodo marcó un punto de inflexión para la empresa, ya que la SST cobró mayor relevancia en los entornos laborales, lo que generó una mayor demanda en los servicios y consolidó su presencia en el mercado. Actualmente su principal giro de negocio es el desarrollo de software a medida, orientado a brindar soluciones tecnológicas eficaces y adaptables a las necesidades del entorno empresarial en SST.

Misión

Brindar soluciones tecnológicas especializadas en la gestión de la Seguridad y Salud en el Trabajo, a través del desarrollo de software, consultoría y capacitación, con el fin de contribuir a entornos laborales más seguros, eficientes y sostenibles.

Visión

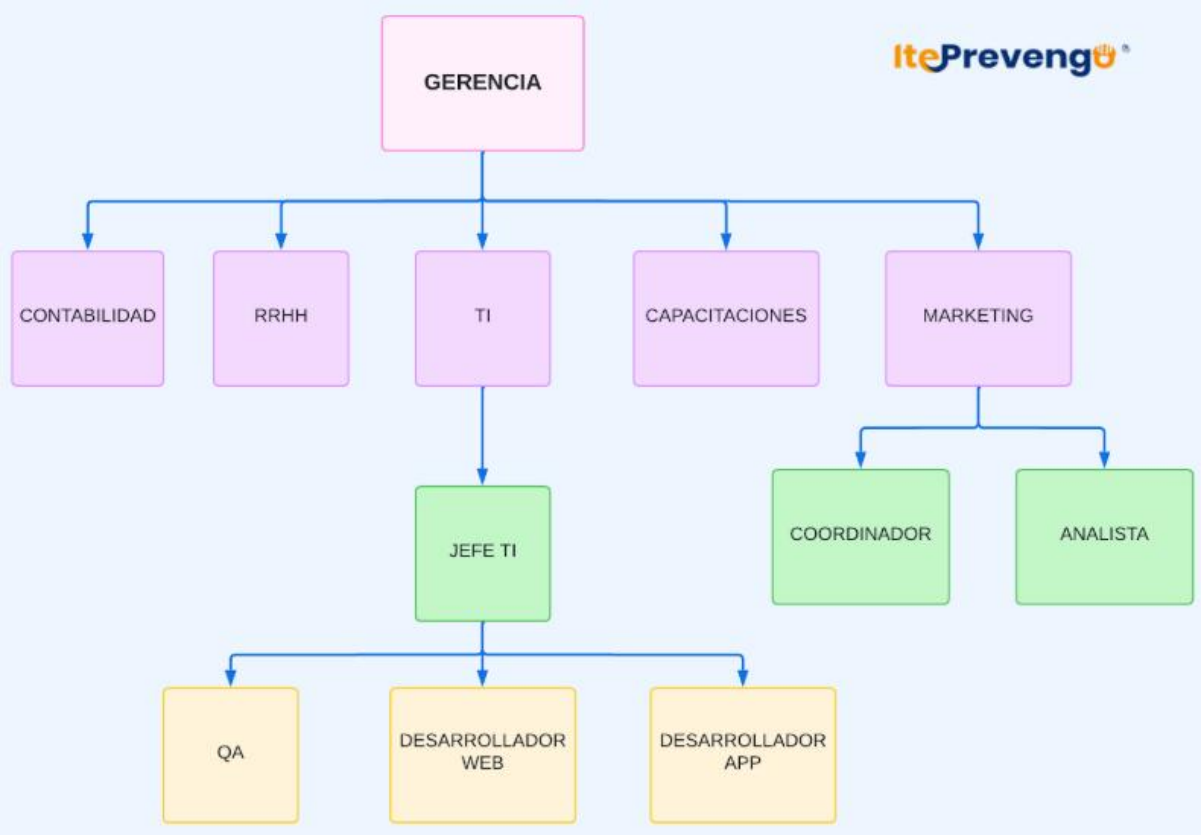
Al 2030, consolidarse como el principal referente a nivel nacional en el desarrollo de soluciones digitales para la gestión de la Seguridad y Salud en el Trabajo.

Organigrama

A continuación en la Figura 17 se expone la distribución organizacional de la empresa:

Figura 17.

Organigrama de Iteprevengo



Nota. Elaborado por los investigadores.

Análisis PESTEL

El presente análisis PESTEL tiene como propósito identificar y comprender los factores externos que influyen en las operaciones de Iteprevengo. A continuación, se detallan los factores considerados:

- Factores políticos: Estabilidad Gubernamental y políticas de formalización laboral.
- Factores económicos: Estabilidad económica, fluctuaciones en el tipo de cambio y Limitado acceso para las PYMES.
- Factores sociales: Conciencia en SST y trabajo remoto e híbrido.
- Factores tecnológicos*:* Nivel de implementación tecnológica en empresas del sector SST, Ciberseguridad e Innovación tecnológica (Inteligencia artificial).
- Factores ecológicos: Cambio climático y preferencias por soluciones sostenibles (SaaS).
- *Factores legales:* Propiedad intelectual y protección de software, cumplimiento de normativas de seguridad y salud laboral (Ley N° 29783) y Ley de protección de datos personales (Ley N° 29733).

Necesidades y expectativas de las partes interesadas

A continuación, en la Tabla 27 se exponen las necesidades y expectativas de las partes interesadas identificadas.

Tabla 27.

Necesidades y expectativas de las partes interesadas

PARTES INTERESADAS		**REQUERIMIENTO**	
		NECESIDAD	**EXPECTATIVA**
CONTEXTO EXTERNO	**CLIENTES**	▪ Cumplimiento de las cláusulas en el Acuerdo de Seguridad de la Información. ▪ Disponibilidad y confiabilidad de los servicios contratados.	Contar con Certificación ISO/IEC 27001 como garantía de un sistema seguro y confiable.
	PROVEEDORES		
	Amazon Web Services	▪ Manejo confidencial de la información contractual y técnica.	Recepción de requerimientos técnicos y operativos
	Go Daddy		
	Google		

	Namecheap		precisos, claros y oportunos.
	.pe		
	Bitbucket		
	Digital Ocean		
	ORGANISMOS LEGALES		
	Ministerio de Trabajo	▪ Cumplir con la Ley de Protección de Datos Personales - Ley N° 29733 ▪ Ley N° 29783 - Ley de Seguridad y Salud en el Trabajo ▪ Cumplir con la Ley de Delitos Informáticos - Ley N° 30096	Colaborar con organizaciones alineadas al régimen legal vigente
	INDECOPI		
	Ministerio de Justicia		
CONTEXTO INTERNO	**ALTA DIRECCIÓN**		
	Gerente General	▪ Cumplimiento normativo y legal. ▪ Información precisa para la toma de decisiones.	Acceso a información íntegra, oportuna y actualizada para el direccionamiento estratégico.
	Socios		
	COLABORADORES		
	Jefe de TI	▪ Acceso a información disponible y segura para el desarrollo de sus funciones. ▪ Protección de información personal y corporativa.	Recibir capacitación e incentivos vinculados al cumplimiento del SGSI.
	Desarrolladores		
	Otros empleados		

Nota. Elaborado por los investigadores.

- **Actividad 2: Elaborar el Plan de Constitución del Proyecto**

  En esta actividad, se elaboró el plan del proyecto, documento que formaliza el inicio del proyecto. A través de este documento se obtuvo la aprobación formal por parte de la alta dirección, lo que permitió continuar con el desarrollo de las siguientes actividades del proyecto.

  El entregable de esta actividad "Plan de proyecto", consúltese en el Anexo 1.

Fase II: Definición del Alcance y la Política del SGSI

- **Actividad 3: Identificar los Procesos del Negocio**

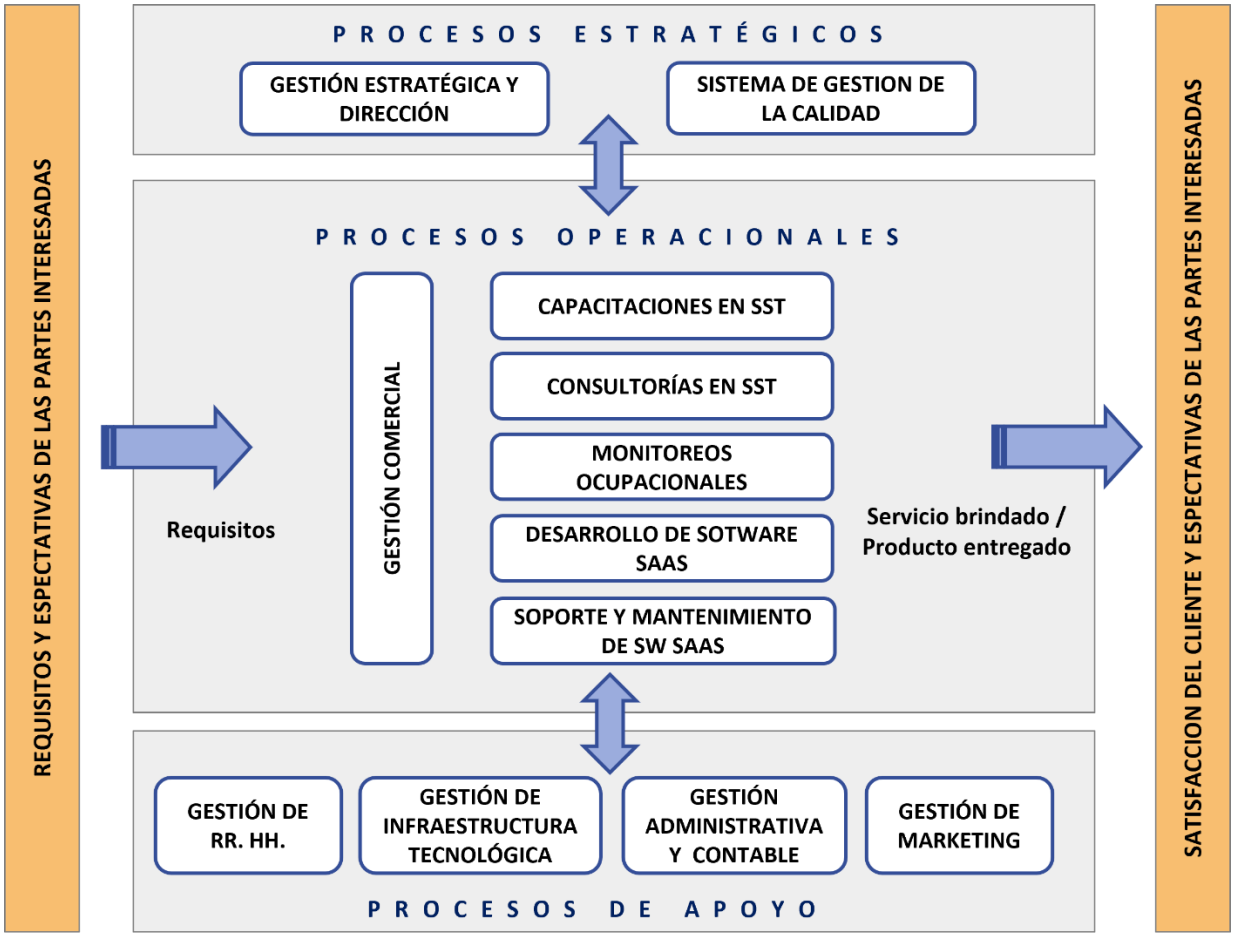
En esta actividad, se procedió a identificar los procesos del negocio de Iteprevengo, clasificándolos en estratégicos, misionales y de soporte. Como resultado, se elaboró el mapa general de procesos, el cual se presenta en la Figura 18.

Posteriormente, se realizó la caracterización descriptiva de cada proceso, considerando su propósito, entradas, actividades clave y salidas, la cual se muestra en la Tabla 28.

Este análisis permitió comprender la estructura operativa de la organización y establecer la base para la posterior evaluación de criticidad de los procesos de Iteprevengo desde la perspectiva de la seguridad de la información.

Figura 18.

Mapeo general de los procesos de la empresa Iteprevengo



Nota. Elaborado por los investigadores.

Tabla 28.

Caracterización de procesos de la empresa Iteprevengo

PROCESO	DESCRIPCIÓN	ENTRADAS	ACTIVIDADES CLAVE	SALIDAS
PROCESOS ESTRATÉGICOS				
Gestión Estratégica y Dirección	Proceso orientado a la definición de la planificación estratégica, establecimiento de objetivos organizacionales, toma de decisiones y supervisión del desempeño general de la empresa.	- Información financiera. - Indicadores de desempeño. - Retroalimentación de clientes. - Contexto normativo	- Definición de objetivos estratégicos. - Planificación empresarial. - Asignación de recursos.	- Políticas organizacionales - Directrices operativas - Planes estratégicos
Sistema de Gestión de la Calidad	Proceso encargado de asegurar la conformidad de los servicios brindados mediante el seguimiento de indicadores, control documental y acciones de mejora continua.	- Requisitos del cliente - Resultados de auditoría. - Indicadores de procesos	- Gestión documental - Seguimiento de indicadores - Auditorías internas	- Registros del SGC - Informes de auditoría - Planes de mejora
PROCESOS OPERACIONALES				
Gestión Comercial	Proceso responsable de la captación de clientes, elaboración de propuestas técnicas y económicas, negociación contractual y seguimiento postventa.	- Estrategia comercial organizacional - Requerimientos de los clientes Información del mercado	- Prospección de clientes - Presentación de servicios - Elaboración de propuestas - Negociación - Formalización contractual	- Contratos concretados - Órdenes de servicios - Cartera de clientes

Capacitaciones en SST	Proceso orientado diseño, planificación y ejecución de actividades formativas dirigidas a trabajadores y organizaciones clientes, con el propósito de fortalecer conocimientos y competencias en materia de prevención de riesgos laborales y cumplimiento normativo.	- Requerimientos de los clientes - Normativas SST - Material informativo - Información de participantes	- Diseño de contenido - Elaboración de material didáctico - Programación de sesiones - Ejecución de participaciones - Evaluación de participantes	- Sesiones de capacitación - Material informativo entregado - Registros de asistencia - Certificados emitidos - Informes de capacitación
Consultorías en SST	Proceso comprende las actividades orientadas a brindar asesoramiento técnico especializado a organizaciones clientes para la implementación, mejora o cumplimiento de requisitos normativos en materia de SST.	- Requerimientos del cliente - Información organizacional del cliente - Documentación interna del cliente - Normativa aplicable SST	- Diagnóstico de la organización cliente - Revisión documental - Identificación de brechas - Elaboración de informes - Propuesta de planes de acción	- Informes técnicos - Planes de mejora - Documentación SST elaborada o actualizada - Reportes de cumplimiento
Monitoreos Ocupacionales	Proceso relacionado con la planificación y ejecución de evaluaciones técnicas relacionadas con las condiciones de trabajo en las organizaciones clientes. Permite a los clientes identificar niveles de exposición a riesgos y adoptar medidas correctivas conforme a la normativa vigente.	- Información de la organización cliente - Parámetros técnicos normativos aplicables - Contrato de prestación de servicio	- Planificación de monitoreos - Recolección de datos - Registro de mediciones - Análisis de resultados - Elaboración de informes	- Informes técnicos de monitoreo - Registros y resultados de evaluaciones - Recomendaciones técnicas

Desarrollo de Software SaaS	Proceso encargado del análisis, diseño, programación, pruebas y despliegue de soluciones tecnológicas orientadas a la gestión de SST bajo modalidad Software como Servicio. Opera en modalidad 100 % remota.	- Requerimientos funcionales y no funcionales - Especificaciones técnicas	- Análisis - Diseño - Programación - Pruebas - Despliegue	- Versiones de software - Funcionalidades implementadas - Código fuente actualizado
Soporte y Mantenimiento SaaS	Proceso orientado a garantizar la disponibilidad, estabilidad, seguridad y correcto funcionamiento de la plataforma tecnológica ofrecida por la organización. Se desarrolla en modalidad 100 % remota.	- Incidentes reportados - Alertas del sistema - Solicitudes de usuario - Políticas internas de seguridad y respaldo	- Recepción y registro de incidentes - Diagnóstico y resolución de fallas - Aplicación de parches y actualizaciones - Gestión y verificación de respaldos	- Incidentes resueltos - Software disponible - Actualizaciones implementadas - Registros de soporte - Respaldos verificados
PROCESOS DE APOYO				
Gestión de Infraestructura Tecnológica	Proceso transversal comprende la administración, configuración y supervisión de los recursos tecnológicos que soportan la operación de la plataforma SaaS y demás servicios digitales de la organización.	- Requerimientos técnicos de desarrollo y soporte - Políticas de SI - Lineamientos de arquitectura tecnológica	- Administración de servidores - Configuración de entornos de desarrollo y producción - Gestión de accesos - Gestión de Backups - Monitoreo de disponibilidad y rendimiento	- Infraestructura operativa y disponible - Entornos configurados - Accesos habilitados - Registros técnicos de administración

Gestión de Recursos Humanos	Proceso responsable de la selección, contratación, capacitación y seguimiento del personal, así como de la gestión del desempeño y cumplimiento de obligaciones laborales.	- Información de personal - Requerimientos de contratación	- Selección de personal - Gestión de contratos - Pago de planillas	- Personal contratado - Registros laborales
Gestión Administrativa y Contable	Proceso encargado de la facturación, gestión tributaria, control financiero y cumplimiento de obligaciones económicas de la organización.	- Facturación - Pagos - Comprobantes	- Contabilidad - Gestión tributaria	- Estados financieros - Declaraciones
Gestión de Marketing	Proceso orientado a la promoción de los servicios de la empresa, posicionamiento de marca y generación de oportunidades comerciales.	- Información del mercado - Estrategias comerciales	- Campañas - Publicidad digital	- Leads - Posicionamiento

Nota. Elaborado por los investigadores.

- **Actividad 4: Definir el alcance del SGSI**

  Con base en los procesos identificados en la actividad anterior, se realizó el análisis de criticidad de los procesos de Iteprengo definidos en la propuesta metodológica de la Actividad 4. En la Tabla 29, se exponen los resultados.

Tabla 29.

Cálculo de la criticidad de los procesos de la organización

PROCESO	CRITERIO SENSIBILIDAD DE LA INFORMACIÓN		CRITERIO DEPENDENCIA TECNOLÓGICA		CRITERIO GENERACIÓN DE INGRESOS		CRITICIDAD	
	NIVEL	VALOR	NIVEL	VALOR	NIVEL	VALOR	VALOR	NIVEL
Gestión estratégica y Dirección	Sensible	3	Media	2	Indirecta	2	7	Media
Sistema de Gestión de la Calidad	Sensible	3	Media	2	Indirecta	2	7	Media
Gestión comercial	Sensible	3	Alta	3	Indirecta	2	8	Media
Capacitaciones en SST	Sensible	3	Media	2	Directa	3	8	Media
Consultorías en SST	Sensible	3	Media	2	Directa	3	8	Media
Monitoreos Ocupacionales	Sensible	3	Baja	1	Directa	3	7	Media
Desarrollo de Software SaaS	Critica	4	Muy alta	4	Directa	3	11	Alta
Soporte y Mantenimiento de Software SaaS	Critica	4	Muy alta	4	Directa	3	11	Alta
Gestión de Infraestructura Tecnológica	Critica	4	Muy alta	4	Indirecta	2	10	Alta
Gestión de Recursos Humanos	Sensible	3	Media	2	Indirecta	2	7	Media
Gestión Administrativa y Contable	Sensible	3	Media	2	Indirecta	2	7	Media
Gestión de Marketing	Media	2	Media	2	Indirecta	2	6	Media

Nota. Elaborado por los investigadores

Como resultado del análisis, se identificaron tres procesos con criticidad alta:

- Los procesos de Desarrollo de Software SaaS y Soporte y Mantenimiento de Software SaaS, los cuales constituyen el núcleo operativo de Iteprevengo, cualquier afectación en la seguridad de información impactaría directamente en la prestación del servicio a los clientes.
- El proceso de gestión de infraestructura tecnológica, si bien su influencia en la generación de ingresos es indirecta, este proceso constituye el soporte tecnológico esencial que habilita la operación de los procesos de desarrollo y soporte, garantizando la disponibilidad de los entornos productivos, repositorios de código, bases de datos y mecanismos de respaldo.

En consecuencia, el alcance del SGSI comprenderá los procesos de Desarrollo de Software SaaS y Soporte y Mantenimiento de Software SaaS, incorporando de manera complementaria la Gestión de Infraestructura Tecnológica como proceso habilitador indispensable para la operación segura del modelo SaaS.

- **Actividad 5: Definir los Roles y Responsabilidades**

Para identificar y documentar los roles y responsabilidades necesarios para la implementación, mantenimiento y mejora del SGSI, se tomó como base la estructura organizacional de Iteprevengo, presentada anteriormente en la Figura 17.

A partir de dicha estructura se definió la conformación del Comité de Seguridad de la Información (CSI), instancia responsable de la dirección, supervisión y seguimiento del SGSI dentro de la organización.

En la Tabla 30, se presenta la estructura interna del SGSI, en la que se detalla la composición del CSI. Sobre la base de esta estructura se establecen los roles y responsabilidades específicos asociados a la gestión del sistema.

Tabla 30.

Estructura interna del SGSI

CARGO	ROL DENTRO DEL SGSI	RESPONSABILIDADES PRINCIPALES
Gerente General	Presidente del Comité de Seguridad de la Información	Representar la alta dirección; aprobar políticas, recursos y resultados; liderar las reuniones del CSI; asegurar el compromiso de la dirección con la seguridad de la información.
Jefe de TI	Coordinador del Comité de Seguridad de la Información	Dirigir la implementación técnica y documental del SGSI; coordinar actividades, plazos y entregables; reportar avances al CSI.
Representante del área de desarrollo	Miembro del CSI	Aportar información técnica y operativa sobre los procesos dentro del alcance; colaborar en la identificación de activos, amenazas y riesgos.
Representante del área de RRHH	Miembro del CSI	Coordinar actividades de capacitación, concientización y comunicación interna sobre seguridad de la información.
Consultor externo	Consultor Externo	Brindar acompañamiento metodológico y asesoramiento especializado en la implementación del SGSI; conforme con la NTP ISO/IEC 27001.

Nota. Elaborado por los investigadores

El entregable completo de esta actividad "Roles y Responsabilidades", consúltese en el Anexo 3.

- **Actividad 6: Definir la Política de la Seguridad de la Información**

  En esta actividad se elaboró la Política de Seguridad de la Información, de acuerdo a los requisitos establecidos en la ISO/IEC 27001, cláusula 5.2; así como en el contexto organizacional de Iteprevengo.

El entregable de esta actividad “Política de la Seguridad de la Información”, consúltese en el Anexo 4.

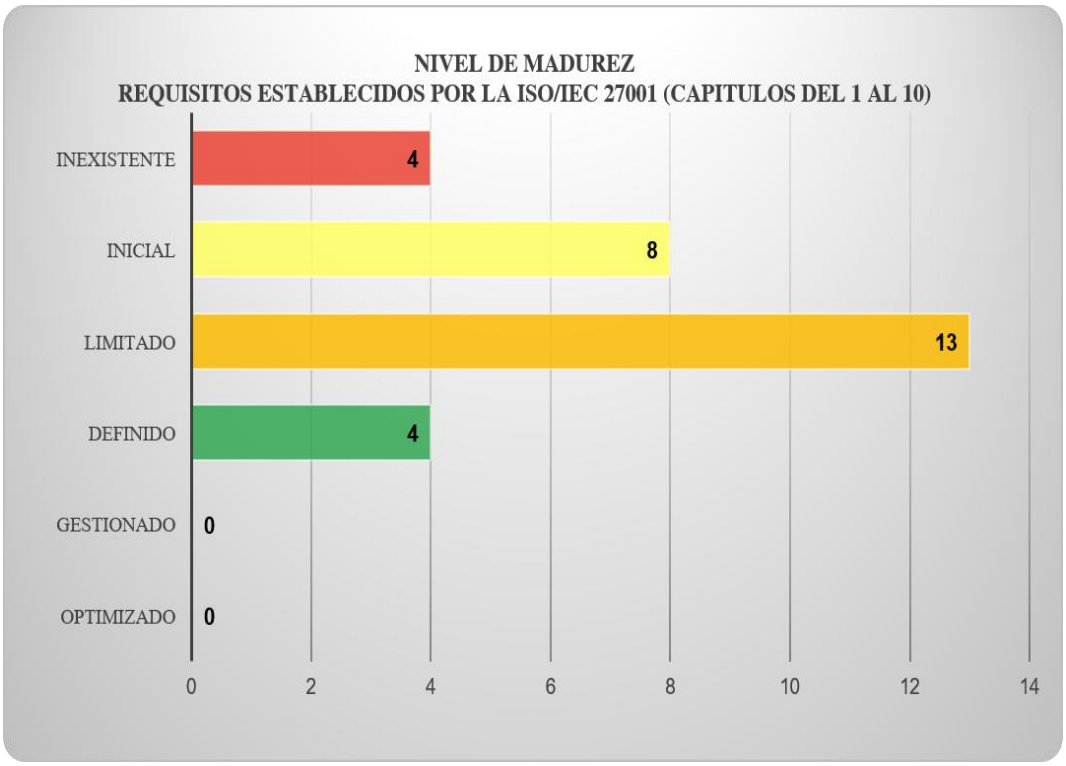
Fase III: Análisis de los Requisitos de Seguridad de Información

- **Actividad 7: Realizar un análisis de brechas**

El análisis de brechas se realizó por medio de la aplicación de una entrevista semiestructurada, la cual arrojó los siguientes resultados:

Figura 19.

Resultados del Check List – Requisitos de la ISO/IEC 27001



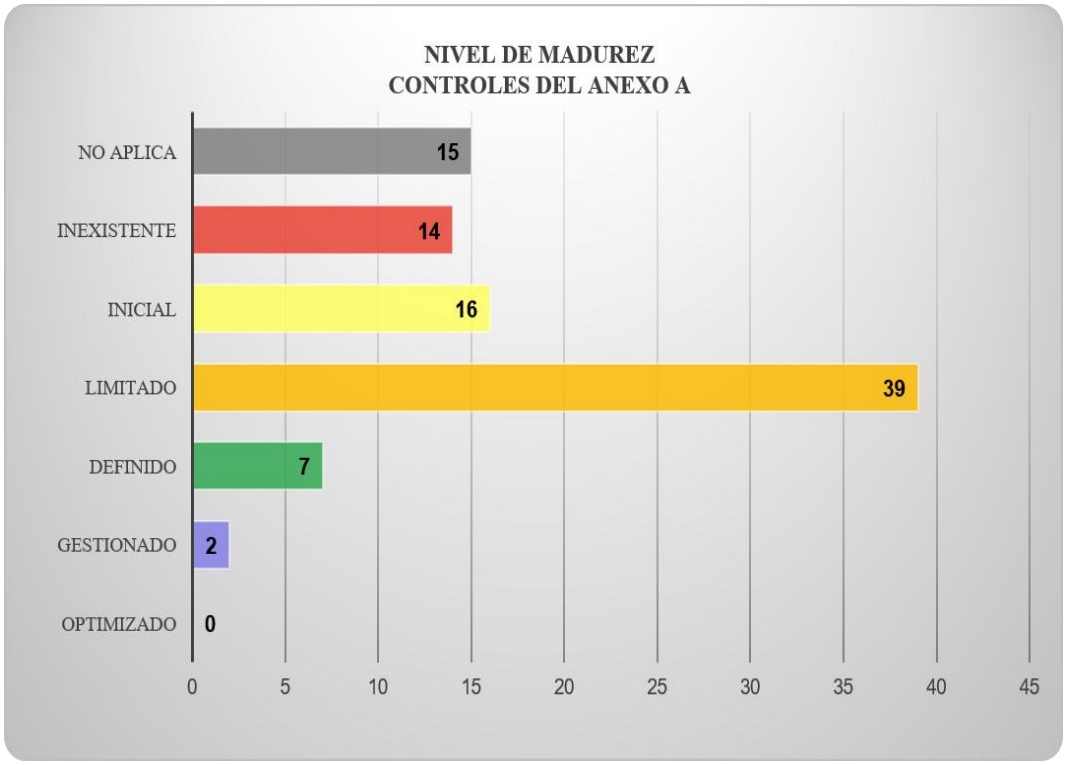
Nota. Elaborado por los investigadores.

En la Figura 19, se expone el panorama general del nivel de madurez de los requisitos de la NTP ISO/IEC 27001. Se puede evidenciar que la empresa no cuenta con un SGSI formal, ya que existen cuatro requisitos en nivel “inexistente”. Si bien hay esfuerzos

por parte de la alta dirección, reflejado en los requisitos que se encuentran en niveles "inicial" y "limitado", estos son aislados, informales y no se basan en un modelo de gestión estructurado.

Figura 20.

Resultados del Check List– Controles del Anexo A



Nota. Elaborado por los investigadores.

En la Figura 20, se expone el panorama general del nivel de madurez respecto a los controles del Anexo A de la NTP ISO/IEC 27001. Se puede evidenciar un nivel de madurez muy bajo en cuanto a implementación de medidas de seguridad dentro de la empresa. El 89 % de controles están en niveles básicos, reflejando una implementación débil o parcial.

Los resultados detallados de las entrevistas respecto al nivel de madurez de los requisitos y controles de la NTP ISO/IEC 27001:2022 no se adjuntan al informe por

razones de confidencialidad; solo se muestran las conclusiones obtenidas a partir de su análisis.

El entregable completo de esta actividad “Informe de Análisis de Brechas”, consúltese en el Anexo 5.

- **Actividad 8: Identificar los Activos de Información**

  En esta actividad, se procedió a identificar los activos de información comprendidos dentro del alcance del SGSI, es decir, aquellos vinculados a los procesos de soporte, desarrollo de software SaaS y gestión de infraestructura tecnológica. En la Tabla 31 se presentan los activos de información identificados:

Tabla 31.

Catalogación de activos de información

ID	NOMBRE DEL ACTIVO DE INFORMACIÓN	DESCRIPCIÓN DEL ACTIVO	RESPONSABLE	CATEGORÍA	TIPO
ACT 1	SERVIDOR DIGITAL OCEAN (VPS)	Servidor para alojamiento del software	Jefe de ti	Soporte	Software servicio
ACT 2	FIREWALL APACHE WAF	Cortafuegos de aplicaciones web basado en Apache que analiza y filtra el tráfico HTTP	Jefe de ti	Soporte	Red
ACT 3	BD (MARIA DB)	Base de datos	Jefe de ti	Primario	Información
ACT 4	AWS API GATEWAY	Servicio de Amazon Web Services para la creación y gestión de API	Jefe de ti	Soporte	Software servicio
ACT 5	AWS S3 (File server)	Servicio de almacenamiento en la nube proporcionado por Amazon Web Services (AWS)	Jefe de ti	Soporte	Software servicio
ACT 6	SERVICIO DE ENVÍO DE CORREOS CON AWS SES	Software de envío de correos electrónicos que usa el servicio de Amazon Web Services (AWS)	Jefe de ti	Soporte	Software servicio
ACT 7	AWS SNS	Servicio de mensajería en la nube proporcionado por Amazon Web Services (AWS)	Jefe de ti	Soporte	Software servicio
ACT 8	BITBUCKET	Plataforma de alojamiento de código fuente basada en la nube	Jefe de ti	Primario	Información

ACT 9	CERTIFICADO SSL	Protocolo de seguridad que crea un enlace cifrado entre un servidor web y un navegador web.	Jefe de ti	Soporte	Red
ACT 10	GODADDY	Servicio de gestión de dominios y de registros DNS.	Jefe de ti	Soporte	Software servicio
ACT 11	BACKUPS DE BD	Copias de seguridad de la data de las aplicaciones.	Jefe de ti	Primario	Información
ACT 12	FIREWALL DIGITAL OCEAN	Cortafuegos en la nube que permite controlar el tráfico de red hacia y desde los recursos de DigitalOcean	Jefe de ti	Soporte	Red
ACT 13	EQUIPOS INFORMÁTICOS	Computadoras portátiles o de escritorio utilizadas por los desarrolladores para el trabajo diario.	Desarrolladores	Soporte	Hardware
ACT 14	EQUIPO DE DESARROLLO	Desarrolladores web y mobile	Jefe de ti	Soporte	Personal
ACT 15	JEFE DE TI	Encargado del área de TI	Gerencia	Soporte	Personal

Nota. Elaborado por los investigadores.

- **Actividad 9: Definir criticidad de los activos de información**

  Tras la identificación de los activos de información, se procedió a valorar su importancia, el propósito de esta valoración es priorizar aquellos activos cuya afectación podría generar un mayor impacto en la organización.

  La criticidad de cada activo fue calculada aplicando la Fórmula 1, y clasificada según los criterios establecidos en la Tabla 20. Los resultados se presentan en la Tabla 32.

Tabla 32.

Criticidad de los activos de información

ID	NOMBRE DEL ACTIVO DE INFORMACIÓN	EVALUACIÓN DEL ACTIVO			NIVEL DE CRITICIDAD	
		C	I	D		
ACT 1	SERVIDOR DIGITAL OCEAN (VPS)	3	3	3	3	ALTO
ACT 2	FIREWALL APACHE WAF	3	3	3	3	ALTO
ACT 3	BD (MARIA DB)	3	3	3	3	ALTO
ACT 4	AWS API GATEWAY	2	2	1	2	MEDIO
ACT 5	AWS S3 (File server)	2	2	3	2	MEDIO
ACT 6	SERVICIO DE ENVÍO DE CORREOS CON AWS SES	2	1	2	2	MEDIO
ACT 7	AWS SNS	2	2	1	2	MEDIO
ACT 8	BITBUCKET (CODIGO FUENTE)	3	3	3	3	ALTO
ACT 9	CERTIFICADO SSL	3	3	3	3	ALTO
ACT 10	GODADDY (DOMINIO)	3	3	3	3	ALTO
ACT 11	BACKUPS DE BD	3	3	2	3	ALTO
ACT 12	FIREWALL DIGITAL OCEAN	3	3	3	3	ALTO
ACT 13	EQUIPOS INFORMÁTICOS	3	3	3	3	ALTO
ACT 14	EQUIPO DE DESARROLLO	3	3	3	3	ALTO
ACT 15	JEFE DE TI	3	3	3	3	ALTO

Nota. Elaborado por los investigadores.

Fase IV: Evaluación y Tratamiento de Riesgos

- **Actividad 10: Identificar amenazas y vulnerabilidades**

  En esta actividad se identificaron las amenazas y vulnerabilidades asociadas a cada activo de información, con el propósito de reconocer los posibles escenarios de riesgo (riesgos intrínsecos). En la Tabla 33 se exponen los resultados obtenidos:

Tabla 33.

Escenarios de riesgo

N°	ACTIVO	AMENAZA	VULNERABILIDAD
ACT 1	SERVIDOR DIGITAL OCEAN (VPS)	Ataques DDOS	Servidor sin protecciones adecuadas contra el tráfico no deseado
		Acceso no autorizado	Autenticación inadecuada
		Pérdida de datos	Falta de copias de seguridad regulares
		Malware y ransomware	Software desactualizado
			Falta de antivirus
		Acceso desde ubicación geográficas no seguras	Falta de restricciones por geolocalización/IP
		Intercepción de datos en tránsito	Transmisión no cifrada
		Ingeniería social	Personal no capacitado en seguridad
		Exposición de datos sensibles	Datos almacenados sin cifrado
		Ataques internos	Falta de control de acceso interno
		Fallas de configuración	Servicios y puertos innecesarios activos
		Ataques de fuerza bruta	Falta de limitaciones en intentos de acceso
ACT 2	FIREWALL APACHE WAF	Ataques externos	Falta de parches o actualizaciones
			Falta de redundancia
		Usuarios maliciosos internos	Configuración inadecuada
			Falta de seguimiento de cambios
		Ataques DDOS	Capacidad limitada de WAF
		Ingeniería social	Engaño a administradores
		Ataques de fuerza bruta	Ataques repetidos a autenticaciones
ACT 3	MARIA DB (BASE DE DATOS)	Usuarios maliciosos internos	Mala configuración de accesos
		Ataques de inyección SQL	Falta de validación de entradas

		Ingeniería social	Engaño a administradores
		Insuficiente espacio de almacenamiento	Incremento de transacciones o movimientos.
			No tener definido un procedimiento para el mantenimiento de base de datos
		Divulgación de información	Copias de la base de datos sin autorización o permiso.
		Malware y ransomware	Falta de controles de seguridad
		Ataques externos	BD expuesta a internet
			Falta de encriptación
ACT 4	**AWS API GATEWAY**	Atacantes externos	Configuración por defecto
			Falta de autenticación / autorización
		Ataques DDOS	API expuesta al publico
		Ingeniería social	Engaño a administradores
		Ataques de inyección	Falta de validación de entradas
		Manipulación o exfiltración de datos	Logs sin filtrar datos sensibles
		Personal interno malintencionado	Permisos excesivos en AWS
		Fallos de configuración	Uso incorrecto de dominios y certificados
ACT 5	**AWS S3 (FILE SERVER)**	Ataques DDOS	Servidor sin protecciones adecuadas contra el tráfico no deseado
		Acceso no autorizado	Autenticación inadecuada
		Pérdida de datos	Falta de copias de seguridad regulares
		Malware y ransomware	Software desactualizado
			Falta de antivirus
		Personal interno malintencionado	Acceso excesivo o inadecuado a colaboradores
		Ingeniería social	Personal no capacitado en seguridad
		Exposición de datos sensibles	Datos almacenados sin cifrado
		Ataques internos	Falta de control de acceso interno
		Fallos de configuración	Servicios y puertos innecesarios activos
		Acceso desde ubicación geográficas no seguras	Falta de restricción por ubicación
		Ataques de fuerza bruta	Falta de limitaciones en intentos de acceso

ACT 6	**SERVICIO DE ENVÍO DE CORREOS CON AWS SES**	Phishing y correos electrónicos maliciosos	No validación del contenido, falta de control de acceso, SPF/DKIM/DMARC incorrectos
		Suplantación de identidad (spoofing)	Configuraciones incorrectas de spf, dkim y dmarc
		Ataques DDOS	Falta de protección contra tráfico malicioso
		Acceso no autorizado	API sin autenticación o mal configurada, credenciales débiles o reutilizadas (IAM sin el principio de mínimo privilegio)
		Pérdida de disponibilidad del servicio	Dependencia exclusiva del servicio sin planes de contingencia
		Malware en archivos adjuntos	Falta de escaneo de archivos adjuntos
		intercepción de correos electrónicos en tránsito	transmisión no cifrada
		Ataques de fuerza bruta	Falta de limitaciones en intentos de acceso
		Sobrecarga del sistema	No hay rate limiting en API o control de uso en SES
		Errores de configuración	Claves mal gestionadas, endpoint mal expuesto, configuraciones incorrectas
		Enlaces maliciosos en correos electrónicos	Falta de concientización de los usuarios
ACT 7	**AWS SNS**	Intercepción de notificaciones en tránsito	Transmisión no cifrada
		Acceso no autorizado a la consola SNS	Credenciales débiles o comprometidas
		Ataques DDOS	Falta de protección contra tráfico malicioso
		Exposición de datos sensibles en notificaciones	Falta de controles de contenido
		Limitaciones de tasa excedida	Falta de monitorización de cuotas SNS
		Fallos en la entrega de notificaciones	Falta de mecanismos de reintentos
		Código malicioso en notificaciones	Falta de validación de contenido mensajes
		Personal interno malintencionado	Acceso excesivo o inadecuado a colaboradores

ACT 8	**BITBUCKET (CÓDIGO FUENTE)**	Ataques externos	Falta de autenticación de dos factores
		Personal interno malintencionado	Permisos excesivos en el repositorio
			Falta de autoría y seguimiento
		Ingeniería social	Engaño a desarrolladores
		Fallos en infraestructura cloud	Fallos de redundancia en bitbucket
		Código malicioso o malware	Dependencias vulnerables en el Código, no se usan escaneos
		Filtración pública (repos abiertos)	Configuración de visibilidad del repositorio en "público" por error
		Vulnerabilidades en dependencias	Ausencia de gestión de parches, no usar scanners (Snyk, Dependabot, etc.)
		Modificación no autorizada (maliciosa)	Falta de pull-requests revisados, sin firmas de commit ni protección de ramas
		Fugas de información sensible (tokens, claves)	Almacenamiento de secretos en el código o en .env dentro del repo
		Complejidad elevada / deuda técnica	Código sin mantenimiento ni estándares
		Acceso de ex empleados	Accesos no revocados
ACT 9	**CERTIFICADO SSL**	Compromiso de clave privada	Almacenamiento inseguro de la clave
		Caducidad del certificado	Falta de gestión de vida útil
		Ataque mitm	Certificado autofirmado
		Vulnerabilidades criptográficas	Uso de algoritmos inseguros
		Robo de identidad	Certificado emitido a nombre incorrecto
		Revocación no detectada	Falta de monitoreo de lista de revocación
ACT 10	**GODADDY (DOMINIO)**	Redirección de DNS maliciosa	Configuración insegura de DNS
		Renovación de dominio fallida	Falta de seguimiento de fechas de expiración
		Accesos no autorizados por colaboradores malintencionados	Permisos excesivos otorgados a usuarios
		Registro erróneo o malicioso de subdominios	Falta de control sobre creación de subdominios

ACT 11	**BACKUPS DE BD**	Usuarios maliciosos internos	Mala configuración de accesos
		Pérdida del Backup	No replicación, Backups locales únicamente.
		Ingeniería social	Engaño a administradores
		Malware y ransomware	Falta de controles de seguridad
		Ataques externos	Bd expuesta a internet
ACT 12	**FIREWALL DIGITAL OCEAN**	Acceso indebido	Reglas de firewall sin revisión, puertos innecesarios abiertos.
		Pérdida de disponibilidad	Reglas incorrectas que bloquean el tráfico legítimo.
ACT 13	**EQUIPOS INFORMÁTICOS**	Robo de equipo	Sin cifrado de disco ni rastreo.
		Malware y ransomware	Falta de controles de seguridad
		Acceso indebido	Contraseñas que no cumplen los estándares mínimos.
ACT 14	**EQUIPO DE DESARROLLO**	Error humano	Sin revisiones de código
		Acción maliciosa	Permisos no establecidos correctamente, falta de auditorías internas, incorrecta separación de roles.
		Mal desarrollo de los requerimientos	Personal nuevo de desarrollo con poco conocimiento de los procesos de la empresa
		Incumplimiento de tiempos de desarrollo	Sobrecarga de requerimientos a desarrollar por poco personal.
		Ingeniería social	Personal no capacitado en seguridad
ACT 15	**JEFE DE TI**	Abuso de privilegios	Sin segregación de funciones.
		Error de decisión	Falta de procedimientos estandarizados.
		Ingeniería social	Personal no capacitado en seguridad

Nota. Elaborado por los investigadores.

- **Actividad 11: Analizar el riesgo**

  Identificados los riesgos intrínsecos, se procedió a calcular su exposición al riesgo para cada uno de ellos, a partir de la estimación de su impacto y probabilidad. En la Tabla 34 se presentan los resultados obtenidos de esta actividad.

Tabla 34.

Tabla de análisis de riesgos

N°	ACT	AMENAZA	VULNERABILIDAD	RIESGO IDENTIFICADO		IMPACTO					PROBABILIDAD		NIVEL DE RIESGO INTRÍNSECO	
				COD	DESCRIPCIÓN	CS	EC	SE	VALOR TOTAL	NIVEL	VALOR	NIVEL	VALOR	NIVEL
ACT 1	SERVIDOR DIGITAL OCEAN (VPS)	Ataques DDOS	Servidor sin protecciones adecuadas contra el tráfico no deseado	**R1**	Interrupción del servicio y tiempo de inactividad	4	3	4	**4**	ALTO	**3**	POSIBLE	**12**	ALTO
		Acceso no autorizado	Autenticación inadecuada	**R2**	Compromiso del sistema o fuga de datos sensibles	3	4	5	**4**	ALTO	**4**	PROBABLE	**16**	CRÍTICO
		Pérdida de datos	Falta de copias de seguridad regulares	**R3**	Pérdida irreversible de datos críticos	5	5	4	**5**	MUY ALTO	**3**	POSIBLE	**15**	ALTO
		Malware y ransomware	Software desactualizado	**R4**	Compromiso del sistema	3	3	5	**4**	ALTO	**4**	PROBABLE	**16**	CRÍTICO
			Falta de antivirus	**R5**	Pérdida o cifrado de datos	4	4	5	**4**	ALTO	**3**	POSIBLE	**12**	ALTO
		Acceso desde ubicación geográficas no seguras	Falta de restricciones por geolocalización/ip	**R6**	Acceso no autorizado desde regiones inseguras	2	2	4	**3**	MEDIO	**4**	PROBABLE	**12**	ALTO
		Intercepción de datos en tránsito	Transmisión no cifrada	**R7**	Divulgación de información	2	3	4	**3**	MEDIO	**3**	POSIBLE	**9**	MEDIO
		Ingeniería social	Personal no capacitado en seguridad	**R8**	Divulgación de credenciales o información confidencial	3	4	5	**4**	ALTO	**3**	POSIBLE	**12**	ALTO

		Exposición de datos sensibles	Datos almacenados sin cifrado	**R9**	Acceso no autorizado a información confidencial	3	3	5	**4**	ALTO	**4**	PROBABLE	**16**	CRÍTICO
		Ataques internos	Falta de control de acceso interno	**R10**	Acceso o alteración malintencionada de archivos	4	4	4	**4**	ALTO	**3**	POSIBLE	**12**	ALTO
		Fallas de configuración	Servicios y puertos innecesarios activos	**R11**	Acceso no autorizado	3	3	4	**3**	MEDIO	**4**	PROBABLE	**12**	ALTO
				R12	Compromiso del sistema	3	3	5	**4**	ALTO	**4**	PROBABLE	**16**	CRÍTICO
		Ataques de fuerza bruta	Falta de limitaciones en intentos de acceso	**R13**	Acceso no autorizado	3	3	4	**3**	MEDIO	**3**	POSIBLE	**9**	MEDIO
ACT 2	**FIREWALL APACHE WAF**	Ataques externos	Falta de parches o actualizaciones	**R14**	Ataque de día cero	4	4	5	**4**	ALTO	**2**	IMPROBABLE	**8**	MEDIO
			Falta de redundancia	**R15**	Punto único de fallo	4	3	2	**3**	MEDIO	**4**	PROBABLE	**12**	ALTO
		Usuarios maliciosos internos	Configuración inadecuada	**R16**	Bypass del WAF	3	3	4	**3**	MEDIO	**3**	POSIBLE	**9**	MEDIO
			Falta de seguimiento de cambios	**R17**	Cambios no autorizados	4	4	4	**4**	ALTO	**4**	PROBABLE	**16**	CRÍTICO
		Ataques DDOS	Capacidad limitada de WAF	**R18**	Denegación de servicio	4	4	2	**3**	MEDIO	**4**	PROBABLE	**12**	ALTO
		Ingeniería social	Engaño a administradores	**R19**	Cambios malintencionados en configuraciones	3	3	4	**3**	MEDIO	**3**	POSIBLE	**9**	MEDIO
		Ataques de fuerza bruta	Ataques repetidos a autenticaciones	**R20**	Compromiso de cuentas	3	3	5	**4**	ALTO	**4**	PROBABLE	**16**	CRÍTICO
A C	**M A**	Usuarios maliciosos internos	Mala configuración de accesos	**R21**	Acceso no autorizado a datos	3	3	5	**4**	ALTO	**2**	IMPROBABLE	**8**	MEDIO

		Ataques de inyección SQL	Falta de validación de entradas	**R22**	Manipulación o exfiltración de datos	4	4	4	**4**	ALTO	**3**	POSIBLE	**12**	ALTO
		Ingeniería social	Engaño a administradores	**R23**	Acceso indebido a la BD	4	3	5	**4**	ALTO	**2**	IMPROBABLE	**8**	MEDIO
		Insuficiente espacio de almacenamiento	Incremento de transacciones o movimientos.	**R24**	Caída del sistema o lentitud crítica por sobrecarga de operaciones	4	3	2	**3**	MEDIO	**3**	POSIBLE	**9**	MEDIO
			No tener definido un procedimiento para el Mantenimiento de base de datos	**R25**	Pérdida de disponibilidad de la información, lo que podría generar interrupciones en los servicios y pérdida de confianza por parte de los usuarios.	4	3	2	**3**	MEDIO	**3**	POSIBLE	**9**	MEDIO
		Divulgación de información	Copias de la base de datos sin autorización o Permiso.	**R26**	Fuga de información sensible con impacto legal y reputacional	2	4	4	**3**	MEDIO	**4**	PROBABLE	**12**	ALTO
		Malware y ransomware	Falta de controles de seguridad	**R27**	Corrupción o encriptación de datos	5	4	5	**5**	ALTO	**3**	POSIBLE	**15**	ALTO
		Ataques externos	BD expuesta a internet	**R28**	Ataques remotos	4	4	5	**4**	ALTO	**2**	IMPROBABLE	**8**	MEDIO
			Falta de encriptación	**R29**	Acceso a datos en tránsito	4	3	5	**4**	ALTO	**2**	IMPROBABLE	**8**	MEDIO
ACT 4	**AWS API**	Atacantes externos	Configuración por defecto	**R30**	Acceso no autorizado a la API	3	3	4	**3**	MEDIO	**2**	IMPROBABLE	**6**	MEDIO
			Falta de autenticación / autorización	**R31**	Acceso indebido a recursos	3	3	4	**3**	MEDIO	**2**	IMPROBABLE	**6**	MEDIO

		Ataques DDOS	API expuesta al público	**R32**	Denegación de servicio	4	3	5	**4**	ALTO	**2**	IMPROBABLE	**8**	MEDIO
		Ingeniería social	Engaño a administradores	**R33**	Modificación no autorizada de configuración	3	3	5	**4**	ALTO	**1**	REMOTO	**4**	BAJO
		Ataques de inyección	Falta de validación de entradas	**R34**	Manipulación o exfiltración de datos	3	3	5	**4**	ALTO	**2**	IMPROBABLE	**8**	MEDIO
		Manipulación o exfiltración de datos	Logs sin filtrar datos sensibles	**R35**	Filtración de datos	3	3	4	**3**	MEDIO	**2**	IMPROBABLE	**6**	MEDIO
		Personal interno malintencionado	Permisos excesivos en AWS	**R36**	Acciones no autorizadas en el API Gateway	3	3	4	**3**	MEDIO	**2**	IMPROBABLE	**6**	MEDIO
		Fallos de configuración	Uso incorrecto de dominios y certificados	**R37**	Interrupciones o mitm	3	4	4	**4**	ALTO	**2**	IMPROBABLE	**8**	MEDIO
ACT 5	**AWS S3 (FILE SERVER)**	Ataques DDOS	Servidor sin protecciones adecuadas contra el tráfico no deseado	**R38**	Interrupción del servicio y tiempo de inactividad	5	4	5	**5**	MUY ALTO	**2**	IMPROBABLE	**10**	ALTO
		Acceso no autorizado	Autenticación inadecuada	**R39**	Extracción de archivos	3	3	5	**4**	ALTO	**2**	IMPROBABLE	**8**	MEDIO
				R40	Modificación de archivos	4	4	5	**4**	ALTO	**2**	IMPROBABLE	**8**	MEDIO
		Pérdida de datos	Falta de copias de seguridad regulares	**R41**	Pérdida irreversible de datos críticos	4	4	5	**4**	ALTO	**2**	IMPROBABLE	**8**	MEDIO
		Malware y ransomware	Software desactualizado	**R42**	Corrupción de archivos	4	4	4	**4**	ALTO	**2**	IMPROBABLE	**8**	MEDIO
			Falta de antivirus	**R43**	Cifrado de datos	4	4	4	**4**	ALTO	**2**	IMPROBABLE	**8**	MEDIO
		Personal interno malintencionado	Acceso excesivo o inadecuado a colaboradores	**R44**	Exposición de datos	4	4	5	**4**	ALTO	**2**	IMPROBABLE	**8**	MEDIO
		Ingeniería social	Personal no capacitado en seguridad	**R45**	Divulgación de credenciales o información confidencial	3	4	5	**4**	ALTO	**2**	IMPROBABLE	**8**	MEDIO

		Exposición de datos sensibles	Datos almacenados sin cifrado	**R46**	Acceso no autorizado a información confidencial	4	4	5	**4**	ALTO	**2**	IMPROBABLE	**8**	MEDIO
		Ataques internos	Falta de control de acceso interno	**R47**	Acceso o alteración malintencionada de archivos	4	4	5	**4**	ALTO	**2**	IMPROBABLE	**8**	MEDIO
		Fallos de configuración	Servicios y puertos innecesarios activos	**R48**	Acceso no autorizado	4	2	4	**3**	MEDIO	**1**	REMOTO	**3**	BAJO
				R49	Compromiso del sistema	4	3	4	**4**	ALTO	**1**	REMOTO	**4**	BAJO
		Acceso desde ubicación geográficas no seguras	Falta de restricción por ubicación	**R50**	Compromiso de datos	4	3	4	**4**	ALTO	**1**	REMOTO	**4**	BAJO
		Ataques de fuerza bruta	Falta de limitaciones en intentos de acceso	**R51**	Acceso no autorizado	4	3	4	**4**	ALTO	**1**	REMOTO	**4**	BAJO
ACT 6	**SERVICIO DE ENVIO DE CORREOS CON AWS SES**	Phishing y correos electrónicos maliciosos	No validación del contenido, falta de control de acceso, SPF/DKIM/DMARC incorrectos	**R52**	Compromiso de información	2	3	3	**3**	MEDIO	**2**	IMPROBABLE	**6**	MEDIO
		Suplantación de identidad (spoofing)	Configuraciones incorrectas de spf, dkim y dmarc	**R53**	Confianza en correos electrónicos falsificados	2	3	3	**3**	MEDIO	**2**	IMPROBABLE	**6**	MEDIO
		Ataques DDOS	Falta de protección contra tráfico malicioso	**R54**	Inaccesibilidad del servicio de correos y denegación del servicio legítimo.	3	2	3	**3**	MEDIO	**2**	IMPROBABLE	**6**	MEDIO
		Acceso no autorizado	API sin autenticación o mal configurada, credenciales débiles o reutilizadas (IAM sin el principio de mínimo privilegio)	**R55**	Envío de correos masivos maliciosos por actores externos, sobrecarga y bloqueo de servicio	3	3	4	**3**	MEDIO	**3**	POSIBLE	**9**	MEDIO

		Pérdida de disponibilidad del servicio	Dependencia exclusiva del servicio sin planes de contingencia	**R56**	No se pueden enviar correos en procesos críticos (ej. autenticación, alertas), afectando funcionalidades clave de los software	3	2	3	**3**	MEDIO	**2**	IMPROBABLE	**6**	MEDIO
		Malware en archivos adjuntos	Falta de escaneo de archivos adjuntos	**R57**	Infección y compromiso de sistemas	2	3	3	**3**	MEDIO	**2**	IMPROBABLE	**6**	MEDIO
		Intercepción de correos electrónicos en tránsito	Transmisión no cifrada	**R58**	Divulgación en tránsito sensible	2	3	3	**3**	MEDIO	**2**	IMPROBABLE	**6**	MEDIO
		Ataques de fuerza bruta	Falta de limitaciones en intentos de acceso	**R59**	Acceso no autorizado	2	2	3	**2**	BAJO	**2**	IMPROBABLE	**4**	BAJO
		Sobrecarga del sistema	No hay rate limiting en API o control de uso en SES	**R60**	Agotamiento de recursos o suspensión del servicio por exceder límites de AWS SES	2	2	3	**2**	BAJO	**2**	IMPROBABLE	**4**	BAJO
		Errores de configuración	Claves mal gestionadas, endpoint mal expuesto, configuraciones incorrectas	**R61**	Fallos funcionales, exposición de información, vulnerabilidad a ataques	2	3	3	**3**	MEDIO	**2**	IMPROBABLE	**6**	MEDIO
		Enlaces maliciosos en correos electrónicos	Falta de concientización de los usuarios	**R62**	Robo de información	2	3	4	**3**	MEDIO	**2**	IMPROBABLE	**6**	MEDIO
ACT 7	**AWS SNS**	Intercepción de notificaciones en tránsito	Transmisión no cifrada	**R63**	Acceso no autorizado	1	2	3	**2**	BAJO	**1**	REMOTO	**2**	BAJO
		Acceso no autorizado a la consola sns	Credenciales débiles o comprometidas	**R64**	Extracción de información confidencial	1	3	3	**2**	BAJO	**2**	IMPROBABLE	**4**	BAJO
		Ataques DDOS	Falta de protección contra tráfico malicioso	**R65**	Interrupción del servicio de notificaciones	1	2	3	**2**	BAJO	**2**	IMPROBABLE	**4**	BAJO

		Exposición de datos sensibles en notificaciones	Falta de controles de contenido	**R66**	Divulgación de información	2	2	3	**2**	BAJO	**2**	IMPROBABLE	**4**	BAJO
		Limitaciones de tasa excedida	Falta de monitorización de cuotas SNS	**R67**	Interrupción del servicio	2	2	2	**2**	BAJO	**3**	POSIBLE	**6**	MEDIO
		Fallos en la entrega de notificaciones	Falta de mecanismos de reintentos	**R68**	Notificación no recibida	2	2	2	**2**	BAJO	**2**	IMPROBABLE	**4**	BAJO
		Código malicioso en notificaciones	Falta de validación de contenido mensajes	**R69**	Infección y compromiso de sistemas	2	3	3	**3**	MEDIO	**1**	REMOTO	**3**	BAJO
		Personal interno malintencionado	Acceso excesivo o inadecuado a colaboradores	**R70**	Exposición de datos	2	2	3	**2**	BAJO	**1**	REMOTO	**2**	BAJO
ACT 8	**BITBUCKET (CODIGO FUENTE)**	Ataques externos	Falta de autenticación de dos factores	**R71**	Acceso no autorizado al repositorio	4	3	5	**4**	ALTO	**3**	POSIBLE	**12**	ALTO
		Personal interno malintencionado	Permisos excesivos en el repositorio	**R72**	Modificaciones maliciosas del código	4	3	4	**4**	ALTO	**3**	POSIBLE	**12**	ALTO
			Falta de autoría y seguimiento	**R73**	Cambios no registrados	4	3	4	**4**	ALTO	**3**	POSIBLE	**12**	ALTO
		Ingeniería social	Engaño a desarrolladores	**R74**	Filtración de acceso o código	4	3	4	**4**	ALTO	**2**	IMPROBABLE	**8**	MEDIO
		Fallos en infraestructura cloud	Fallos de redundancia en bitbucket	**R75**	Pérdida temporal de acceso al código	4	4	5	**4**	ALTO	**2**	IMPROBABLE	**8**	MEDIO
		Código malicioso o malware	Dependencias vulnerables en el código, no se usan escaneos	**R76**	Integración de malware en la aplicación	4	3	5	**4**	ALTO	**3**	POSIBLE	**12**	ALTO

		Filtración pública (repos abiertos)	Configuración de visibilidad del repositorio en “público” por error	**R77**	Divulgación de código propietario y secretos empresariales, facilitando la identificación de vulnerabilidades por atacantes externos.	4	3	5	**4**	ALTO	**2**	IMPROBABLE	**8**	MEDIO
		Vulnerabilidades en dependencias	Ausencia de gestión de parches, no usar scanner (Snyk, Dependabot, etc.)	**R78**	Explotación de fallos en librerías de terceros que puede permitir ejecución de código arbitrario o escalada de privilegios en la aplicación.	4	3	4	**4**	ALTO	**3**	POSIBLE	**12**	ALTO
		Modificación no autorizada (maliciosa)	Falta de pull-requests revisados, sin firmas de commit ni protección de ramas	**R79**	Introducción de vulnerabilidades o lógica maliciosa en producción, poniendo en riesgo la confidencialidad e integridad del software.	4	3	4	**4**	ALTO	**4**	PROBABLE	**16**	CRÍTICO
		Fugas de información sensible (tokens, claves)	Almacenamiento de secretos en el código o en .env dentro del repo	**R80**	Exposición de claves que permite ataques a otros sistemas, escalada de privilegios y posibles brechas de datos.	3	3	5	**4**	ALTO	**3**	POSIBLE	**12**	ALTO
		Complejidad elevada / deuda técnica	Código sin mantenimiento ni estándares	**R81**	Retrasos en desarrollo y acumulación de errores.	3	4	3	**3**	MEDIO	**4**	PROBABLE	**12**	ALTO
		Acceso de ex empleados	Accesos no revocados	**R82**	Uso malintencionado del código	4	3	5	**4**	ALTO	**2**	IMPROBABLE	**8**	MEDIO

ACT 9	**CERTIFICADO SSL**	Compromiso de clave privada	Almacenamiento inseguro de la clave	**R83**	Descifrado de tráfico cifrado	4	4	5	**4**	ALTO	**3**	POSIBLE	**12**	ALTO
		Caducidad del certificado	Falta de gestión de vida útil	**R84**	Interrupciones del servicio web	5	3	4	**4**	ALTO	**3**	POSIBLE	**12**	ALTO
		Ataque mitm	Certificado auto firmado	**R85**	Intercepción y manipulación de datos	4	3	5	**4**	ALTO	**3**	POSIBLE	**12**	ALTO
		Vulnerabilidades criptográficas	Uso de algoritmos inseguros	**R86**	Compromiso de la integridad y confidencialidad	3	3	5	**4**	ALTO	**2**	IMPROBABLE	**8**	MEDIO
		Robo de identidad	Certificado emitido a nombre incorrecto	**R87**	Suplantación de identidad	3	3	5	**4**	ALTO	**2**	IMPROBABLE	**8**	MEDIO
		Revocación no detectada	Falta de monitoreo de lista de revocación	**R88**	Uso de certificado revocado	2	2	4	**3**	MEDIO	**2**	IMPROBABLE	**6**	MEDIO
ACT 10	**GODADDY (DOMINIO)**	Redirección de DNS maliciosa	Configuración insegura de DNS	**R89**	Desvío de tráfico a sitios web maliciosos	4	4	5	**4**	ALTO	**3**	POSIBLE	**12**	ALTO
		Renovación de dominio fallida	Falta de seguimiento de fechas de expiración	**R90**	Pérdida del dominio y posible cybersquatting	4	4	5	**4**	ALTO	**2**	IMPROBABLE	**8**	MEDIO
		Accesos no autorizados por colaboradores malintencionados	Permisos excesivos otorgados a usuarios	**R91**	Manipulación o eliminación de dominios	4	3	4	**4**	ALTO	**2**	IMPROBABLE	**8**	MEDIO
		Registro erróneo o malicioso de subdominios	Falta de control sobre creación de subdominios	**R92**	Abuso del dominio para actividades maliciosas	3	3	5	**4**	ALTO	**2**	IMPROBABLE	**8**	MEDIO
ACT 11	**BACKUPS DE BD**	Usuarios maliciosos internos	Mala configuración de accesos	**R93**	Acceso no autorizado a datos	3	4	5	**4**	ALTO	**2**	IMPROBABLE	**8**	MEDIO
		Pérdida del backup	No replicación, backups locales únicamente.	**R94**	Pérdida de datos críticos, incapacidad de recuperación ante fallos.	4	4	5	**4**	ALTO	**3**	POSIBLE	**12**	ALTO

		Ingeniería social	Engaño a administradores	**R95**	Acceso indebido a la BD	3	3	5	**4**	ALTO	**2**	IMPROBABLE	**8**	MEDIO
		Malware y ransomware	Falta de controles de seguridad	**R96**	Corrupción o encriptación de datos	4	3	5	**4**	ALTO	**2**	IMPROBABLE	**8**	MEDIO
		Ataques externos	BD expuesta a internet	**R97**	Ataques remotos	4	3	5	**4**	ALTO	**2**	IMPROBABLE	**8**	MEDIO
ACT 12	**FIREWALL DIGITAL**	Acceso indebido	Reglas de firewall sin revisión, puertos innecesarios abiertos.	**R98**	Acceso no autorizado	4	4	4	**4**	ALTO	**3**	POSIBLE	**12**	ALTO
		Pérdida de disponibilidad	Reglas incorrectas que bloquean el tráfico legítimo.	**R99**	Caída del servicio	4	4	4	**4**	ALTO	**3**	POSIBLE	**12**	ALTO
ACT 13	**EQUIPOS INFORMÁTICOS (COMPUTADORAS)**	Robo de equipo	Sin cifrado de disco ni rastreo.	**R100**	Pérdida de datos y robo de información confidencial.	3	3	5	**4**	ALTO	**3**	POSIBLE	**12**	ALTO
		Malware y ransomware	Falta de controles de seguridad	**R101**	Infección de equipos, pérdida de productividad, propagación de virus.	3	3	4	**3**	MEDIO	**3**	POSIBLE	**9**	MEDIO
		Acceso indebido	Contraseñas que no cumplen los estándares mínimos.	**R102**	Acceso no autorizado a datos	3	3	4	**3**	MEDIO	**3**	POSIBLE	**9**	MEDIO
ACT 14	**EQUIPO DE DESARROLLO**	Error humano	Sin revisiones de código	**R103**	Introducción de bugs, vulnerabilidades no detectadas a tiempo.	4	3	3	**3**	MEDIO	**4**	PROBABLE	**12**	ALTO
		Acción maliciosa	Permisos mal configurados, ausencia de auditorías internas y separación inadecuada de roles.	**R104**	Pérdida de código, sabotaje o espionaje industrial.	4	4	5	**4**	ALTO	**2**	IMPROBABLE	**8**	MEDIO

		Mal desarrollo de los requerimientos	Personal nuevo con poco conocimiento de los procesos.	**R105**	Desarrollo deficiente de nuevas funcionalidades del software.	4	3	4	**4**	ALTO	**3**	POSIBLE	**12**	ALTO
		Incumplimiento de tiempos de desarrollo	Sobrecarga de requerimientos a desarrollar por Poco personal.	**R106**	Pérdida de reputación por lo clientes al incumplir los requerimientos pactados	3	3	3	**3**	MEDIO	**3**	POSIBLE	**9**	MEDIO
		Ingeniería social	Personal no capacitado en seguridad	**R107**	Divulgación de información sensible.	4	4	4	**4**	ALTO	**3**	POSIBLE	**12**	ALTO
ACT 15	**JEFE DE TI**	Abuso de privilegios	Sin segregación de funciones.	**R108**	Modificación indebida de configuraciones, comprometiendo la seguridad de la información.	4	3	5	**4**	ALTO	**3**	POSIBLE	**12**	ALTO
		Error de decisión	Falta de procedimientos estandarizados.	**R109**	Caída de servicios	4	3	5	**4**	ALTO	**3**	POSIBLE	**12**	ALTO
		Ingeniería social	Personal no capacitado en seguridad	**R110**	Divulgación de información sensible.	4	4	4	**4**	ALTO	**3**	POSIBLE	**12**	ALTO

Nota. Elaborado por los investigadores.

- **Actividad 12: Valorar el riesgo**

  En esta actividad, se comparó el NER de cada riesgo intrínseco con los criterios de aceptación de riesgo establecidos. Todos los riesgos que superaron el umbral de tolerancia, es decir con un valor de NER superior a 9, fueron incluidos en el Plan de Tratamiento de Riesgo (PTR). En la Tabla 35 se exponen los resultados obtenidos:

Tabla 35.

Valoración del riesgo

N°	ACTIVO	RIESGOS		EVALUACIÓN DEL RIESGO		¿EL RIESGO SERÁ INCLUIDO EN EL PTR?
		COD	DESCRIPCIÓN	VALOR	NIVEL	
ACT 1	SERVIDOR DIGITAL OCEAN (VPS)	R1	Interrupción del servicio y tiempo de inactividad	12	ALTO	SI
		R2	Compromiso del sistema o fuga de datos sensibles	16	CRÍTICO	SI
		R3	Pérdida irreversible de datos críticos	15	ALTO	SI
		R4	Compromiso del sistema	16	CRÍTICO	SI
		R5	Pérdida o cifrado de datos	12	ALTO	SI
		R6	Acceso no autorizado desde regiones inseguras	12	ALTO	SI
		R7	Divulgación de información	9	MEDIO	NO
		R8	Divulgación de credenciales o información confidencial	12	ALTO	SI
		R9	Acceso no autorizado	16	CRÍTICO	SI
		R10	Acceso o alteración malintencionada de archivos	12	ALTO	SI
		R11	Acceso no autorizado	12	ALTO	SI
		R12	Compromiso del sistema	16	CRÍTICO	SI
		R13	Acceso no autorizado	9	MEDIO	NO
ACT 2	FIREWALL APACHE WAF	R14	Ataque de día cero	8	MEDIO	NO
		R15	Punto único de fallo	12	ALTO	SI
		R16	Bypass del WAF	9	MEDIO	NO
		R17	Cambios no autorizados	16	CRÍTICO	SI
		R18	Denegación de servicio	12	ALTO	SI

		R19	Cambios malintencionados en configuraciones	9	MEDIO	NO
		R20	Compromiso de cuentas	16	CRÍTICO	SI
ACT 3	**MARIA DB (BASE DE DATOS)**	**R21**	Acceso no autorizado a datos	8	MEDIO	NO
		R22	Manipulación o exfiltración de datos	12	ALTO	SI
		R23	Acceso indebido a la BD	8	MEDIO	NO
		R24	Caída del sistema o lentitud crítica por sobrecarga de operaciones	9	MEDIO	NO
		R25	Pérdida de disponibilidad de la información, y pérdida de confianza por parte de los usuarios.	9	MEDIO	NO
		R26	Fuga de información sensible con impacto legal y reputacional	12	ALTO	SI
		R27	Corrupción o encriptación de datos	15	ALTO	SI
		R28	Ataques remotos	8	MEDIO	NO
		R29	Acceso a datos en tránsito	8	MEDIO	NO
ACT 4	**AWS API GATEWAY**	**R30**	Acceso no autorizado a la API	6	MEDIO	NO
		R31	Acceso indebido a recursos	6	MEDIO	NO
		R32	Denegación de servicio	8	MEDIO	NO
		R33	Modificación no autorizada de configuración	4	BAJO	NO
		R34	Manipulación o exfiltración de datos	8	MEDIO	NO
		R35	Filtración de datos	6	MEDIO	NO
		R36	Acciones no autorizadas en el API gateway	6	MEDIO	NO
		R37	Interrupciones o mitm	8	MEDIO	NO
ACT 5	**AWS S3**	**R38**	Interrupción del servicio y tiempo de inactividad	10	ALTO	SI
		R39	Extracción de archivos	8	MEDIO	NO
		R40	Modificación de archivos	8	MEDIO	NO
		R41	Pérdida irreversible de datos críticos	8	MEDIO	NO
		R42	Corrupción de archivos	8	MEDIO	NO
		R43	Cifrado de datos	8	MEDIO	NO
		R44	Exposición de datos	8	MEDIO	NO
		R45	Divulgación de credenciales o información confidencial	8	MEDIO	NO
		R46	Acceso no autorizado a información confidencial	8	MEDIO	NO

		R47	Acceso o alteración malintencionada de archivos	8	MEDIO	NO
		R48	Acceso no autorizado	3	BAJO	NO
		R49	Compromiso del sistema	4	BAJO	NO
		R50	Compromiso de datos	4	BAJO	NO
		R51	Acceso no autorizado	4	BAJO	NO
ACT 6	**SERVICIO DE ENVIO DE CORREOS CON AWS SES**	**R52**	Compromiso de información	6	MEDIO	NO
		R53	Confianza en correos electrónicos falsificados	6	MEDIO	NO
		R54	Inaccesibilidad del servicio de correos y denegación del servicio legítimo.	6	MEDIO	NO
		R55	Envío de correos masivos maliciosos por actores externos	9	MEDIO	NO
		R56	No se pueden enviar correos en procesos críticos (ej. autenticación, alertas), afectando funcionalidades clave de los software	6	MEDIO	NO
		R57	Infección y compromiso de sistemas	6	MEDIO	NO
		R58	Divulgación en tránsito sensible	6	MEDIO	NO
		R59	Acceso no autorizado	4	BAJO	NO
		R60	Agotamiento de recursos o suspensión del servicio por exceder límites de AWS SES	4	BAJO	NO
		R61	Fallos funcionales, exposición de información, vulnerabilidad a ataques	6	MEDIO	NO
		R62	Robo de información	6	MEDIO	NO
ACT 7	**AWS SNS**	**R63**	Acceso no autorizado	2	BAJO	NO
		R64	Extracción de información confidencial	4	BAJO	NO
		R65	Interrupción del servicio de notificaciones	4	BAJO	NO
		R66	Divulgación de información	4	BAJO	NO
		R67	Interrupción del servicio	6	MEDIO	NO
		R68	Notificación no recibida	4	BAJO	NO
		R69	Infección y compromiso de sistemas	3	BAJO	NO
		R70	Exposición de datos	2	BAJO	NO
ACT 8	**BITBUCKET (CODIGO FUENTE)**	**R71**	Acceso no autorizado al repositorio	12	ALTO	SI
		R72	Modificaciones maliciosas del código	12	ALTO	SI
		R73	Cambios no registrados	12	ALTO	SI

		R74	Filtración de acceso o código	8	MEDIO	NO
		R75	Pérdida temporal de acceso al código	8	MEDIO	NO
		R76	Integración de malware en la aplicación	12	ALTO	SI
		R77	Divulgación de código propietario y secretos empresariales	8	MEDIO	NO
		R78	Explotación de fallos en librerías de terceros que puede permitir ejecución de código arbitrario o escalada de privilegios en la aplicación.	12	ALTO	SI
		R79	Introducción de vulnerabilidades o lógica maliciosa en producción	16	CRÍTICO	SI
		R80	Exposición de claves que permite ataques a otros sistemas, escalada de privilegios y posibles brechas de datos.	12	ALTO	SI
		R81	Retrasos en desarrollo y acumulación de errores.	12	ALTO	SI
		R82	Uso malintencionado del código	8	MEDIO	NO
ACT 9	**CERTIFICADO SSL**	**R83**	Descifrado de tráfico cifrado	12	ALTO	SI
		R84	Interrupciones del servicio web	12	ALTO	SI
		R85	Intercepción y manipulación de datos	12	ALTO	SI
		R86	Compromiso de la integridad y confidencialidad	8	MEDIO	NO
		R87	Suplantación de identidad	8	MEDIO	NO
		R88	Uso de certificado revocado	6	MEDIO	NO
ACT 10	**GODADDY (DOMINIO)**	**R89**	Desvío de tráfico a sitios web maliciosos	12	ALTO	SI
		R90	Pérdida del dominio y posible cybersquatting	8	MEDIO	NO
		R91	Manipulación o eliminación de dominios	8	MEDIO	NO
		R92	Abuso del dominio para actividades maliciosas	8	MEDIO	NO
ACT 11	**BACKUPS DE BD**	**R93**	Acceso no autorizado a datos	8	MEDIO	NO
		R94	Pérdida de datos críticos, incapacidad de recuperación ante fallos.	12	ALTO	SI
		R95	Acceso indebido a la BD	8	MEDIO	NO
		R96	Corrupción o encriptación de datos	8	MEDIO	NO
		R97	Ataques remotos	8	MEDIO	NO

ACT 12	**FIREWALL DIGITAL OCEAN**	**R98**	Acceso no autorizado	12	ALTO	SI
		R99	Caída del servicio	12	ALTO	SI
ACT 13	**EQUIPOS INFORMÁTICOS (COMPUTADORAS)**	**R100**	Pérdida de datos y robo de información confidencial.	12	ALTO	SI
		R101	Infección de equipos, pérdida de productividad, propagación de virus.	9	MEDIO	NO
		R102	Acceso no autorizado a datos	9	MEDIO	NO
ACT 14	**EQUIPO DE DESARROLLO**	**R103**	Introducción de bugs, vulnerabilidades no detectadas a tiempo.	12	ALTO	SI
		R104	Pérdida de código, sabotaje o espionaje industrial.	8	MEDIO	NO
		R105	Desarrollo deficiente de nuevas funcionalidades del software.	12	ALTO	SI
		R106	Pérdida de reputación ante los clientes por incumplimiento de requerimientos acordados.	9	MEDIO	NO
		R107	Divulgación de credenciales o información confidencial	12	ALTO	SI
ACT 15	**JEFE DE TI**	**R108**	Modificación indebida de configuraciones, comprometiendo la seguridad de la información.	12	ALTO	SI
		R109	Caída de servicios	12	ALTO	SI
		R110	Divulgación de credenciales o información confidencial	12	ALTO	SI

Nota. Elaborado por los investigadores.

- **Actividad 13: Definir el Plan de Tratamiento del Riesgo**

  En esta actividad, se analizó cada riesgo incluido en el PTR y se determinó la estrategia de gestión de riesgo más adecuada, las acciones necesarias para cumplir el objetivo así como las salvaguardas (controles) relacionados a cada acción especificada.

  A continuación, en la Tabla 36 se exponen los resultados obtenidos:

Tabla 36.

Plan de Tratamiento del Riesgo: Selección de salvaguardas

N°	ACTIVO	RIESGOS		ESTRATEGIA DE TRATAMIENTO	ACCIÓN POR IMPLEMENTAR	CONTROL RELACIONADO
		COD	DESCRIPCIÓN			
ACT 1	SERVIDOR DIGITAL OCEAN (VPS)	R1	Interrupción del servicio y tiempo de inactividad	MITIGAR	Implementar sistemas de protección contra DDoS (ej. servicios como Cloudflare)	A.5.23 - Seguridad de la información para el uso de servicios en la nube
					Configurar firewalls correctamente, usar limitación de tasas y monitorear tráfico	A.8.20 - Seguridad de redes
		R2	Compromiso del sistema o fuga de datos sensibles	MITIGAR	Implementar MFA	A.8.5 - Autenticación segura
					Implementar configuración y políticas de contraseñas fuertes	A.5.17 - Información de autenticación
		R3	Pérdida irreversible de datos críticos	MITIGAR	Implementar rutinas de respaldo y recuperación	A.8.13 - Copias de seguridad

		R4	Compromiso del sistema	MITIGAR	Mantener SO actualizado	A.8.8 - Gestión de vulnerabilidades técnicas
		R5	Pérdida o cifrado de datos	MITIGAR	Implementar antivirus y antimalware	A.8.7 - Protección contra malware
		R6	Acceso no autorizado desde regiones inseguras	MITIGAR	Configurar VPN	A.8.20 - Seguridad de redes
					Restringir IP's por geolocalización	A.5.23 - Seguridad de la información para el uso de servicios en la nube
		R8	Divulgación de credenciales o información confidencial	MITIGAR	Capacitaciones regulares en conciencia de seguridad	A.6.3 - Concienciación, educación y formación en seguridad de la información
		R9	Acceso no autorizado a información confidencial	MITIGAR	Configurar cifrado en reposo para datos sensible	A.8.24 - Uso de criptografía
		R10	Acceso o alteración malintencionada de archivos	MITIGAR	Implementar registro de auditoría	A.8.15 – Logueo
						A.8.16 - Actividades de monitoreo
					Aplicar políticas de privilegio mínimo	A.5.15 - Control de acceso
					Revocar permisos de manera adecuada al cese del contrato	A.6.5 - Responsabilidades tras la terminación o cambio de empleo
		R11	Acceso no autorizado	MITIGAR	Realizar hardening regularmente	A.8.9 - Gestión de la configuración
		R12	Compromiso del sistema	MITIGAR	Implementar una herramienta de escaneo de seguridad	A.8.9 - Gestión de la configuración
ACT 2	**FIREWAL L APACHE WAF**	**R15**	Punto único de fallo	MITIGAR	Implementar un sistema de gestión de parches para actualizar regularmente el WAF y software relacionado	A.8.9 - Gestión de la configuración
		R17	Cambios no autorizados	MITIGAR		A.5.15 - Control de acceso

					Implementar controles de acceso estrictos para los cambios de configuración, asegurando que solo el personal autorizado pueda modificar los ajustes del WAF. Configurar registro detallado y monitoreo de todos los cambios	A.8.15 – Logueo
						A.8.16 - Actividades de monitoreo
		R18	Denegación de servicio	MITIGAR	Implementar soluciones DDOS	A.5.23 - Seguridad de la información para el uso de servicios en la nube
						A.8.20 - Seguridad de redes
		R20	Compromiso de cuentas	MITIGAR	Implementar bloqueo tras intentos fallidos	A.8.5 - Autenticación segura
ACT 3	**MARIA DB (BASE DE DATOS)**	**R22**	Manipulación o exfiltración de datos	MITIGAR	Implementar prácticas de codificación segura y sanitización de datos	A.8.28 - Pruebas de seguridad en el desarrollo
		R26	Fuga de información sensible con impacto legal y reputacional	MITIGAR	Restringir copias a personal autorizado, implementar auditoría y logging, cifrar datos	A.5.15 - Control de acceso
						A.8.15 – Logueo
						A.8.24 - Uso de criptografía
		R27	Corrupción o encriptación de datos	MITIGAR	Realizar backups con regularidad, probar restauraciones, implementar IPS/IDS, mantener actualizado los parches de seguridad	A.8.11 - Enmascaramiento de datos
						A.8.7 - Protección contra malware
						A.8.9 - Gestión de la configuración

ACT 5	**AWS S3 (FILE SERVER)**	**R38**	Interrupción del servicio y tiempo de inactividad	MITIGAR	Habilitar AWS WAF para buckets S3, usar Amazon CloudFront con protección contra DDoS, monitorear tráfico con Amazon CloudWatch y S3 Access Logs, revisar privacidad del bucket	A.5.23 - Seguridad de la información para el uso de servicios en la nube
						A.8.20 - Seguridad de redes
ACT 8	**BITBUCKET (CÓDIGO FUENTE)**	**R71**	Acceso no autorizado al repositorio	MITIGAR	Habilitar autenticación multifactor e implementar contraseñas robustas a través de políticas y procedimientos adecuados	A.8.5 - Autenticación segura
						A.5.15 - Control de acceso
						A.5.16 - Gestión de identidad
		R72	Modificaciones maliciosas del código	MITIGAR	Revisar y ajustar permisos aplicando RBAC. Aplicar principio de privilegio mínimo	A.5.15 - Control de acceso
		R73	Cambios no registrados	MITIGAR	Habilitar logs de auditoría en Bitbucket, revisar logs con regularidad para detectar cualquier actividad sospechosa	A.8.15 – Logueo
		R76	Integración de malware en la aplicación	MITIGAR	Usar herramientas como Snyk o Dependabot para escanear dependencias, actualizarlas regularmente	A.8.7 - Protección contra malware
						A.8.9 - Gestión de la configuración
		R78	Explotación de fallos en librerías de terceros que puede permitir ejecución de código arbitrario o escalada de privilegios en la aplicación	MITIGAR	Implementar una gestión de parches de seguridad	A.8.9 - Gestión de la configuración

		R79	Introducción de vulnerabilidades o lógica maliciosa en producción, poniendo en riesgo la confidencialidad e integridad del software	MITIGAR	Implementar ramas protegidas que exijan revisiones de Pull Request (por otros miembros del equipo) y el paso de pruebas automatizadas de CI/CD antes de cualquier fusión. Además, aplica una gestión de permisos asegurando que solo roles autorizados puedan aprobar y fusionar	A.8.15 – Logueo
						A.5.15 - Control de acceso
		R80	Exposición de claves que permite ataques a otros sistemas, escalada de privilegios y posibles brechas de datos	MITIGAR	Configurar herramientas como HashiCorp Vault o AWS Secrets Manager	A.8.24 - Uso de criptografía
		R81	Retrasos en desarrollo y acumulación de errores.	MITIGAR	Establecer estándares de desarrollo, realizar revisiones y refactorización, usar herramientas de análisis estático	A.8.9 - Gestión de la configuración
						A.6.3 - Concienciación, educación y formación en seguridad de la información
ACT 9	**CERTIFICADO SSL**	**R83**	Descifrado de tráfico cifrado	MITIGAR	Implementar un almacenamiento seguro como HSM o almacenes de claves protegidos	A.8.9 - Gestión de la configuración
						A.8.24 - Uso de criptografía
		R84	Interrupciones del servicio web	MITIGAR	Implementar un proceso de gestión de ciclo de vida del certificado con renovaciones programadas de manera automática	A.8.9 - Gestión de la configuración
		R85	Intercepción y manipulación de datos	MITIGAR	Usar certificados de una CA(Autoridad de Certificación) reconocida y de confianza	A.8.24 - Uso de criptografía

ACT 10	**GODADDY (DOMINIO)**	**R89**	Desvío de tráfico a sitios web maliciosos	MITIGAR	Revisar regularmente los registros dns y uso de dnssec	A.8.20 - Seguridad de redes
						A.8.21 - Seguridad de servicios de red
						A.8.9 - Gestión de la configuración
ACT 11	**BACKUPS DE BD**	**R94**	Pérdida de datos críticos, incapacidad de recuperación ante fallos	MITIGAR	Implementar una estrategia de backup que incluya replicación a ubicaciones offsite o en la nube, como AWS S3, Google Cloud Storage o Azure Blob Storage	A.8.13 - Copias de seguridad
ACT 12	**FIREWALL DIGITAL OCEAN**	**R98**	Acceso no autorizado	MITIGAR	Implementar gestión de configuraciones para documentar y aprobar cambios en el firewall	A.8.9 - Gestión de la configuración
					Monitorear continuamente las actividades de red para detectar accesos no autorizados	A.8.16 - Actividades de monitoreo
		R99	Caída del servicio	MITIGAR	Gestionar configuraciones para asegurar que los cambios no afecten la disponibilidad	A.8.9 - Gestión de la configuración
					Monitorear continuamente para detectar y responder a caídas de servicio	A.8.16 - Actividades de monitoreo
ACT 13	**EQUIPOS INFORMÁTICOS**	**R100**	Pérdida de datos y robo de información confidencial.	MITIGAR	Implementar cifrado de disco completo a los equipos	A.8.24 - Uso de criptografía

ACT 14	**EQUIPO DE DESARROLLO**	**R103**	Introducción de bugs, vulnerabilidades no detectadas a tiempo.	MITIGAR	Implementar un pipeline de CI/CD robusto que incluya pruebas automatizadas y herramientas de análisis estático y dinámico de seguridad (SAST/DAST). Implementar un proceso obligatorio de revisión de código (Pull Requests).	A.8.27 - Política de desarrollo seguro de sistemas
		R105	Desarrollo defectuoso de las nuevas funcionalidades del software	MITIGAR	Implementar un proceso de gestión de requisitos claro, involucrar a partes interesadas	A.8.27 - Política de desarrollo seguro de sistemas
						A.6.3 - Concienciación, educación y formación en seguridad de la información
		R107	Divulgación de credenciales o información confidencial	MITIGAR	Capacitación al personal e implementación de seguridad en los accesos como MFA	A.6.3 - Concienciación, educación y formación en seguridad de la información
						A.5.16 - Gestión de identidad
ACT 15	**JEFE DE TI**	**R108**	Modificación indebida de configuraciones, comprometiendo la seguridad de la información	MITIGAR	Implementar segregación de funciones, limitar privilegios, revisar regularmente configuraciones	A.5.15 - Control de acceso
						A.5.3 - Segregación de funciones
						A.5.1 - Políticas de seguridad de la información
		R109	Caída de servicios	MITIGAR	Establecer procedimientos estandarizados para decisiones críticas, documentar y revisar procesos	A.8.9 - Gestión de la configuración
						A.5.1 - Políticas de seguridad de la información
		R110	Divulgación de credenciales o información confidencial	MITIGAR	Capacitar al jefe de TI en reconocimiento de ingeniería social, implementar MFA para cuentas críticas	A.6.3 - Concienciación, educación y formación en seguridad de la información
						A.5.16 - Gestión de identidad

Nota. Elaborado por los investigadores.

El entregable de esta actividad “Declaración de Aplicabilidad”, consúltese en el Anexo 6.

Fase V: Diseño del Sistema de Gestión de la seguridad de la Información

- **Actividad 14: Definir estructura documental del SGSI**

  En esta actividad se definió la estructura documental del SGSI, considerando los requisitos establecidos en la ISO/IEC 27001:2022 y el alcance de la presente investigación.

  A continuación en la Tabla 37 se define la documentación aplicable de acuerdo al alcance de la investigación:

Tabla 37.

Documentos obligatorios de la ISO/IEC 27001

CLÁUSULA	NOMBRE DEL DOCUMENTO	DESCRIPCIÓN
4.3	Alcance del SGSI	Consultar Anexo 2
5.2	Política de seguridad de la información	Consultar Anexo 4
6.1.2 y 6.1.3	Proceso de evaluación y tratamiento de riesgos de seguridad de la información	Modelo de gestión de riesgos desarrollada en la investigación
6.1.3 d	Declaración de Aplicabilidad	Consultar Anexo 6
6.2	Objetivos de seguridad de la información	Consultar Anexo 7
7.2	Evidencia de la competencia	No aplica por el alcance de la investigación.
8.2	Resultados de la evaluación de riesgos	No aplica por el alcance de la investigación.
8.3	Plan de tratamiento de riesgos	Revisar Actividad 13
9.1	Evidencia de monitoreo, medición, análisis y evaluación	No aplica por el alcance de la investigación.
9.2	Programa de auditoría interna y resultados	No aplica por el alcance de la investigación.
9.3	Resultados de revisiones por la dirección	No aplica por el alcance de la investigación.
10.2	Evidencia de no conformidades y acciones correctivas.	No aplica por el alcance de la investigación.

Nota. Elaborado por los investigadores.

- **Actividad 15: Plan de Concientización de Seguridad de la Información**

  En esta actividad se establece un Plan de Concientización de Seguridad de la Información, alineado con la norma ISO/IEC 27001:2022, con el fin de fortalecer la cultura de seguridad y reducir los riesgos derivados de errores humanos.

  El entregable de esta actividad "Plan de Concientización y Sensibilización en Seguridad de la Información", consúltese en el Anexo 8.

- **Actividad 16: Definir Indicadores de Desempeño del SGSI**

  Las métricas e indicadores del SGSI fueron definidos en concordancia con la cláusula 9.1 de la ISO/IEC 27001:2022, utilizando como guía metodológica la ISO/IEC 27004 para su estructuración.

  En función del alcance del SGSI, de los objetivos definidos para el sistema y del análisis realizado, se establecieron las siguientes dimensiones de mediciones: Gobierno del SGSI, Gestión de riesgos, Seguridad en el Desarrollo de Software, Gestión de Accesos, Gestión de Incidentes, Protección de Datos y Respaldo, Concientización y Competencias , Disponibilidad y Continuidad del Servicio y Seguridad de Proveedores Cloud.

  A partir de dichas dimensiones se definieron nueve indicadores de desempeño, los cuales permiten evaluar el cumplimiento de los objetivos del SGSI y el nivel de eficacia de los controles establecidos.

  En las siguientes tablas se presentan los indicadores definidos, incluyendo su objetivo, tipo de indicador (KPI o KRI), métrica asociada, fórmula de cálculo, fuente de datos, frecuencia de medición, meta y responsable de seguimiento:

Tabla 38.

Indicador de la dimensión gobierno del SGSI

Objetivo SGSI	Indicador	Tipo	Métrica	Fórmula	Fuente	Frecuencia	Meta	Responsable	Requisito ISO
Evaluar el SGSI	Cumplimiento del plan del SGSI	KPI	% de actividades implementadas	(Acciones Implementadas / Acciones Planificadas) × 100	Plan SGSI	Trimestral	≥ 90%	Jefe de TI (Coordinador del CSI)	6.2, 9
Verificar controles	Controles operativos del SGSI	KPI	% controles efectivos	(Controles conformes / Total controles SoA) × 100	Auditoría interna	Semestral	≥ 85%	Responsable SGSI	9.2

Nota. Elaborado por los investigadores tomando como referencia la ISO/ IEC 27004.

Tabla 39.

Indicador de la dimensión gestión de riesgos

Objetivo SGSI	Indicador	Tipo	Métrica	Fórmula	Fuente	Frecuencia	Meta	Responsable	Requisito ISO
Tratar riesgos	Riesgos con tratamiento	KRI	% riesgos tratados	(Tratados / Totales) × 100	Matriz riesgos	Semestral	≥ 95%	Jefe de TI	6.1

Controlar riesgo residual	Riesgos residuales altos	KRI	Nº riesgos altos	Conteo	Matriz riesgos	Trimestral	≤ 2	Comité de Seguridad de la Información (CSI)	6.1

Nota. Elaborado por los investigadores tomando como referencia la ISO/ IEC 27004.

Tabla 40.

Indicador de la dimensión seguridad en el desarrollo de software

Objetivo SGSI	Indicador	Tipo	Métrica	Fórmula	Fuente	Frecuencia	Meta	Responsable	Requisito ISO
Desarrollo seguro	Proyectos con prácticas seguras (SDL)	KPI	% proyectos con SDL aplicados	(Con prácticas / Total) × 100	Checklists SDLC	Trimestral	≥ 100%	Representante del área de Desarrollo	A.8.25
Reducir vulnerabilidades	Vulnerabilidades críticas y/o /altas sin remediar antes de producción	KPI	Nº vulnerabilidades críticas y/o altas pendientes al momento del reléase	Conteo por release (SAST/DAST)	Issue tracker / reporte SAST-DAST	Por release	0	Representante del área de Desarrollo	A.8.8

Nota. Elaborado por los investigadores tomando como referencia la ISO/ IEC 27004.

Tabla 41.

Indicador de la dimensión gestión de accesos

Objetivo SGSI	Indicador	Tipo	Métrica	Fórmula	Fuente	Frecuencia	Meta	Responsable	Requisito ISO
Controlar accesos	Accesos revisados	KPI	% accesos revisados	(Revisados / Totales) × 100	Listado accesos	Trimestral	100%	Jefe de TI	A.8.2
Reducir riesgo	Cuentas inactivas	KRI	Nº cuentas	Conteo	IAM	Mensual	0	Jefe de TI	A.5.15
Controlar privilegios	Cuentas con privilegios no autorizados	KRI	N° de cuentas con privilegios sin justificación documentada	Conteo de cuentas privilegiadas sin aprobación en registro IAM	IAM/ Registro de accesos	Mensual	0	Jefe de TI	A.8.2 A.5.15

Nota. Elaborado por los investigadores tomando como referencia la ISO/ IEC 27004.

Tabla 42.

Indicador de la dimensión gestión de incidentes

Objetivo SGSI	Indicador	Tipo	Métrica	Fórmula	Fuente	Frecuencia	Meta	Responsable	Requisito ISO
Responder incidentes	Tiempo de contención inicial	KPI	Tiempo promedio	Σ tiempos / Nº	Registro incidentes	Mensual	≤ 4h	Jefe de TI	A.5.26

Responder incidentes	Tiempo de resolución completa	KPI	Tiempo promedio	Σ tiempos / Nº	Registro incidentes	Mensual	≤ 24h	Jefe de TI	A.5.26
Resolver incidentes	Incidentes resueltos	KPI	% resueltos	(Resueltos / Totales) × 100	Registro incidentes	Mensual	≥ 95%	Comité de Seguridad de la Información (CSI)	A.5.27

Nota. Elaborado por los investigadores tomando como referencia la ISO/ IEC 27004.

Tabla 43.

Indicador de la dimensión protección de datos y respaldo

Objetivo SGSI	Indicador	Tipo	Métrica	Fórmula	Fuente	Frecuencia	Meta	Responsable	Requisito ISO
Disponibilidad	Backups exitosos	KPI	% backups	(Exitosos / Planificados) × 100	Logs backup	Mensual	≥ 98%	Jefe de TI	A.8.13
Recuperación	Tasa de restauración exitosa	KPI	% de pruebas de restauración exitosas	(Pruebas exitosas / Total realizadas) × 100	Actas de prueba	Semestral	≥ 95%	Jefe de TI	A.8.13

Nota. Elaborado por los investigadores tomando como referencia la ISO/ IEC 27004.

Tabla 44.

Indicador de la dimensión concientización y competencias

Objetivo SGSI	Indicador	Tipo	Métrica	Fórmula	Fuente	Frecuencia	Meta	Responsable	Requisito ISO
Concientización	Personal capacitado con aprobación (nota ≥ 70%)	KPI	% capacitado con nota aprobatoria	(Capacitado aprobado / Total de colaboradores) × 100	RRHH	Anual	100%	Representante del área de RR.HH	A.6.3
Reducir error humano	Incidentes atribuibles a error humano	KRI	% incidentes por error humano	(Incidentes por error humano / Total incidentes) × 100	Registro de incidentes	Trimestral	≤ 20% con tendencia decreciente	Comité de Seguridad de la Información (CSI)	A.6.3

Nota. Elaborado por los investigadores tomando como referencia la ISO/ IEC 27004.

Tabla 45.

Indicadores de la dimensión de disponibilidad y continuidad del servicio

Objetivo SGSI	Indicador	Tipo	Métrica	Fórmula	Fuente	Frecuencia	Meta	Responsable	Requisito ISO

Garantizar disponibilidad	Uptime del servicio SaaS	KPI	% disponibilidad	(Horas disponible / Horas totales) × 100	Monitor cloud	Mensual	≥ 99.5%	Jefe de TI	A.8.14
Reducir tiempo de caída	Tiempo de recuperación real (MTTR)	KPI	Tiempo promedio de recuperación	Σ tiempos recuperación / Nº interrupciones	Registro de interrupciones	Mensual	≤ 4h	Jefe de TI	A.8.14
Validar continuidad	Efectividad de pruebas de continuidad	KPI	% escenarios con resultado satisfactorio	(Escenarios exitosos / Total escenarios probados) × 100	Actas de prueba	Semestral	≥ 90%	Jefe de TI	A.8.14
Asegurar desempeño del SaaS	Tiempo de respuesta de la aplicación	KPI	Tiempo promedio de respuesta (ms)	Σ tiempos respuesta / Nº solicitudes medidas	APM / Monitor cloud	Mensual	≤ 2,000 ms	Jefe de TI	A.8.14
Garantizar resiliencia del servicio	Cumplimiento del RTO en incidentes reales	KPI	% incidentes recuperados dentro del RTO	(Recuperados dentro del RTO / Total incidentes) × 100	Registro de incidentes	Mensual	≥ 90%	Jefe de TI	A.8.14

Nota. Elaborado por los investigadores tomando como referencia la ISO/ IEC 27004.

Tabla 46.

Indicadores de la dimensión de seguridad de proveedores cloud

Objetivo SGSI	Indicador	Tipo	Métrica	Fórmula	Fuente	Frecuencia	Meta	Responsable	Requisito ISO
Evaluar proveedores	Proveedores cloud con certificación verificada	KPI	% proveedores certificados	(Proveedores con ISO 27001 o SOC 2 / Total proveedores críticos) × 100	Contratos / Certificados	Anual	100%	Jefe de TI	A.5.19
Controlar acceso de proveedores	Proveedores con acuerdo de protección de datos documentado	KPI	% acuerdo documentado	Proveedores con DPA o ToS registrado / Total proveedores con acceso) × 100	Registro contratos y acuerdos	Semestral	100%	Jefe de TI	A.5.20
Controlar riesgo de terceros	Proveedores críticos sin revisión anual	KRI	Nº proveedores	Conteo	Registro proveedores	Anual	0	Jefe de TI	A.5.19

Nota. Elaborado por los investigadores tomando como referencia la ISO/ IEC 27004.

VALIDACIÓN DE RESULTADOS

Enfoque de validación del diseño

La presente investigación de tipo descriptiva aplicada no experimental, tiene como propósito diseñar un Sistema de Gestión de la Seguridad de la Información (SGSI) para los procesos de soporte y desarrollo de Software SaaS de la empresa Iteprevengo, conforme a los lineamientos de la NTP ISO/IEC 27001:2022.

Dado que el alcance de la investigación no contempla la implementación del SGSI, la validación del diseño propuesto se realizó mediante el método Delphi. Al respecto Ramirez (2024) refiere que es un instrumento de investigación que recoge y contrasta diversas opiniones de expertos, con el propósito de lograr consenso sobre un tema específico.

El juicio de expertos estuvo conformado por tres profesionales, seleccionados en función de los siguientes criterios:

- Experiencia profesional en Sistemas de Gestión de la Seguridad de la Información y/o Gestión de Riesgos.
- Conocimiento y/o experiencia en la norma NTP ISO/IEC 27001:2022.
- Independencia respecto al diseño del SGSI propuesto.

El procedimiento para la validación del diseño del SGSI propuesto fue el siguiente:

1. Definición de criterios de evaluación y elaboración del instrumento.
2. Presentación del diseño del SGSI a cada experto.
3. Aplicación individual del instrumento de evaluación.
4. Recopilación, sistematización y análisis de resultados.

Instrumento de evaluación

El instrumento fue estructurado en torno a doce (12) componentes del diseño del SGSI, evaluados en función de cinco criterios: pertinencia, claridad, coherencia, suficiencia y alineación normativa.

La valoración de cada criterio se realizó mediante una escala ordinal de cuatro niveles: Deficiente (1), Regular (2), Adecuado (3) y Excelente (4). Se optó por una escala sin punto medio con el fin de evitar respuestas neutrales o indecisas, promoviendo así una valoración más definida por parte de los expertos y una mayor claridad en la interpretación de los resultados.

El instrumento incluyó, además, una pregunta de validación global vinculada a la pregunta de investigación, orientada a determinar si el diseño del SGSI garantiza los principios de confidencialidad, integridad y disponibilidad de la información en el contexto organizacional.

Los formatos aplicados a cada experto se presentan en la sección de anexos.

Interpretación de resultados

Con el propósito de estandarizar la interpretación de los valores promedio obtenidos, se definieron rangos de clasificación que permiten agruparlos en niveles comparables, tal como se muestra en la Tabla 47.

La escala utilizada se definió en base al umbral de aceptación de 2,5, valor que corresponde al punto medio teórico de una escala ordinal de 1 a 4; lo que permite diferenciar valoraciones favorables de no favorables. A partir de este umbral, los intervalos se distribuyeron de forma simétrica entre los valores superiores e inferiores, asignando menor amplitud a los extremos para incrementar el nivel de exigencia en dichas categorías y mejorar la precisión en la interpretación de los resultados.

Tabla 47.

Tabla de interpretación de resultados

RANGO DE PROMEDIO	NIVEL DE VALORACIÓN	INTERPRETACIÓN
3.50 – 4.00	Excelente	El componente cumple plenamente con los criterios evaluados, evidenciando alta calidad, consistencia y alineación normativa. No requiere mejoras significativas.
2.50 – 3.49	Adecuado	El componente cumple en buen nivel con los criterios, pero presenta oportunidades de mejora que no afectan su validez general.
1.50 – 2.49	Regular	El componente cumple parcialmente, evidenciando deficiencias que requieren ajustes importantes para asegurar su adecuación.
1.00 – 1.49	Deficiente	El componente no cumple con los criterios establecidos, requiriendo rediseño o reformulación completa.

Nota. Elaborado por los investigadores.

Resultados

A partir de la aplicación individual del instrumento, se procedió a la consolidación de las puntuaciones asignadas por cada experto a los 12 componentes evaluados. La Tabla 48 presenta la matriz consolidada, en la cual se incluyen promedios obtenidos por cada criterio de evaluación, así como el promedio general por componente.

Tabla 48.

Matriz de resultados

	COMPONENTE/ CRITERIOS	PUNTUACIONES															PROMEDIO POR CRITERIO DE EVALUACIÓN					PROMEDIO GENERAL POR COMPONENTE
		EXPERTO 1					EXPERTO 2					EXPERTO 3										
		PERTINENCIA	CLARIDAD	COHERENCIA	SUFICIENCIA	ALINEACION NORMATIVA	PERTINENCIA	CLARIDAD	COHERENCIA	SUFICIENCIA	ALINEACION NORMATIVA	PERTINENCIA	CLARIDAD	COHERENCIA	SUFICIENCIA	ALINEACION NORMATIVA	PERTINENCIA	CLARIDAD	COHERENCIA	SUFICIENCIA	ALINEACION NORMATIVA	
1	Contexto de la organización	4	4	4	3	4	4	4	4	4	4	4	4	4	4	4	4.0	4.0	4.0	3.7	4.0	**3.9**
2	Alcance del SGSI	4	4	4	3	4	4	4	4	4	4	4	4	4	4	4	4.0	4.0	4.0	3.7	4.0	**3.9**
3	Política de la Seguridad de la Información	4	4	4	4	4	4	4	4	3	4	4	4	4	4	4	4.0	4.0	4.0	3.7	4.0	**3.9**
4	Objetivos de la Seguridad de la Información	4	4	4	3	4	4	4	4	3	4	4	4	3	3	4	4.0	4.0	3.7	3.0	4.0	**3.7**
5	Roles y responsabilidades	4	4	4	3	4	4	4	4	3	4	4	3	2	3	2	4.0	3.7	3.3	3.0	3.3	**3.5**
6	Modelo de Gestión de Riesgos	4	4	4	4	4	4	4	4	4	4	4	4	4	3	4	4.0	4.0	4.0	3.7	4.0	**3.9**
7	Plan de Tratamiento de Riesgos	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4.0	4.0	4.0	4.0	4.0	**4.0**
8	SOA	4	4	4	4	4	4	3	4	4	4	4	4	4	4	4	4.0	3.7	4.0	4.0	4.0	**3.9**
9	Implementación de controles	4	4	4	3	4	4	3	4	3	4	4	4	4	4	4	4.0	3.7	4.0	3.3	4.0	**3.8**
10	Plan de concientización	4	4	4	3	4	4	4	4	4	4	4	4	4	4	4	4.0	4.0	4.0	3.7	4.0	**3.9**
11	Documentación del SGSI	4	4	4	4	4	4	4	4	3	4	4	4	4	4	4	4.0	4.0	4.0	3.7	4.0	**3.9**
12	Métricas e indicadores	4	4	4	3	4	4	4	4	4	4	4	4	3	3	4	4.0	4.0	3.7	3.3	4.0	**3.8**
	PROMEDIO POR CRITERIO DE EVALUACIÓN																**4.0**	**3.9**	**3.9**	**3.6**	**3.9**	**3.8**

Nota. Elaborado por los investigadores. El resaltado amarillo indica el criterio de evaluación con menor promedio (suficiencia = 3.6); el rojo, el componente con menor promedio (Roles y responsabilidades = 3.5); y el verde, el componente con mayor promedio (Plan de Tratamiento de Riesgos = 4.0).; y el azul corresponde al promedio general del SGSI.

Análisis de resultados

Los resultados evidencian que la totalidad de los doce componentes evaluados se ubica en el rango de 3.50 a 4.00, correspondiente al nivel de valoración Excelente, con un promedio general de 3.8 sobre 4.0.

A nivel de criterio, la pertinencia obtuvo la puntuación máxima (4.0), evidenciando que todos los componentes son considerados plenamente relevantes para los objetivos del SGSI y la realidad organizacional de Iteprevengo. La claridad, coherencia y alineación normativa alcanzaron un promedio de 3.9, reflejando que los componentes están formulados con precisión, guardan consistencia lógica entre sí y se alinean correctamente con los requisitos de la NTP ISO/IEC 27001:2022. La suficiencia fue el criterio de menor valor (3.6), manteniéndose dentro del nivel Excelente, e indica que algunos componentes podrán ampliar su nivel de detalle progresivamente durante la fase de implementación.

A nivel de componente, el Plan de Tratamiento de Riesgos alcanzó la puntuación máxima de 4.0 con valoración unánime de los tres expertos. Roles y responsabilidades obtuvo el promedio más bajo del conjunto (3.5), con puntuaciones menores en coherencia y alineación normativa asociadas a las limitaciones en la segregación de funciones. Esta situación responde a la naturaleza de Iteprevengo como microempresa, cuya estructura de personal restringe la implementación plena del Control 5.3 de la norma. La ISO/IEC 27001:2022 reconoce que los controles deben ser proporcionales al tamaño y contexto de la organización, por lo que esta valoración no compromete la validez general del diseño.

CONCLUSIONES

1. El análisis de brechas realizado respecto a los requisitos de la NTP ISO/IEC 27001:2022 y al Anexo A de dicha norma evidenció que en los procesos de soporte y desarrollo de software SaaS de Iteprevengo no se cuenta con un SGSI formalmente establecido, esto se ve evidenciado por los niveles de madurez iniciales en la mayoría de requisitos y controles definidos por la norma.
2. La gestión de riesgos realizada bajo los lineamientos de la NTP ISO/IEC 27005:2022 permitió identificar y analizar las principales vulnerabilidades y amenazas a las que se encuentra expuesta la información de Iteprevengo, así como estimar los niveles de riesgo críticos asociados al uso de dispositivos personales, trabajo remoto y servicios en la nube, confirmando la necesidad de adoptar una metodología estructurada para su gestión.
3. El diseño del SGSI propuesto, basado en la NTP ISO/IEC 27001:2022, permitió establecer un enfoque estructurado alineado a los procesos de soporte y desarrollo de software SaaS de Iteprevengo, el cual incluye políticas, procedimientos, roles y controles. El presente diseño contempla la gestión de riesgos, la protección de la información y la continuidad del negocio, constituyendo una base sólida para fortalecer la seguridad de la información dentro de la organización.
4. Los resultados del juicio de expertos permiten concluir que el diseño propuesto es válido y técnicamente viable para ser considerado como punto de partida para la implementación del SGSI en la empresa Iteprevengo, contribuyendo a la protección de los principios de confidencialidad, integridad y disponibilidad de la información.

RECOMENDACIONES

1. Se recomienda desarrollar una investigación aplicada orientada a la implementación progresiva del SGSI propuesto en los procesos de soporte y desarrollo de software SaaS de Iteprevengo. Esta aplicación deberá ser evaluada mediante los indicadores de desempeño definidos, así a través de la medición periódica del nivel de madurez del sistema, con el fin de validar su efectividad en un entorno real.
2. Se recomienda que futuras investigaciones incorporen el análisis de dependencias entre los activos de información, con el propósito de obtener una evaluación más precisa de su criticidad. Esto permitirá identificar posibles variaciones en los niveles de riesgo y optimizar las decisiones relacionadas con el tratamiento de dichos riesgos.
3. Se recomienda realizar un análisis de brechas respecto a los controles del Anexo A de la NTP ISO/IEC 27001:2022, clasificándolos según sus dominios (Gobernanza y Ecosistema, Protección, Defensa y Resiliencia), con el fin de obtener una visión integral y complementaria del estado de la seguridad de la información. Aunque el presente estudio permitió identificar riesgos de naturaleza física, humana, organizacional y tecnológica, una clasificación basada en dominios podría contribuir a una reinterpretación de dichos riesgos, así como a la identificación de nuevos escenarios de riesgo no evidenciados en el análisis inicial.

REFERENCIAS BIBLIOGRÁFICAS

Arias Odón, F. G. (2012). *El Proyecto de Investigación: Introducción a la metodología científica* (6.ª ed.). Editorial Episteme.

Accenture. (2023). *State of Cybersecurity Resilience 2023*. Recuperado de: https://www.accenture.com/content/dam/accenture/final/accenture-com/document/Accenture-State-Cybersecurity.pdf

Burgos Gordon, C. A. (2020). *Plan de contingencia informático para el área de TI en base a la norma de calidad ISO 27001:2013 para la fundación cultural y educativa Ambato - Unidad Educativa Atenas*. Universidad Técnica de Ambato.

Costas Santos J. (2014). *Seguridad y Alta Disponibilidad. Editorial RA-MA*

CrowdStrike. (2024). *Informe Global de Amenazas 2024*. https://www.crowdstrike.com/wp-content/uploads/2024/02/gtr-2024-infographic_es-LA.pdf

Davila Puicon, S. M. (2022). *Modelo de Gestión de Riesgos de TI que dan soporte a los procesos de evaluación, financiamiento y cobranza de la empresa CHANCAFE NORTE S.A.C. basada en la metodología MAGERIT*. Universidad Nacional Pedro Ruiz Gallo.

Edelman. (2022). Impacto del COVID-19 en las PYMES: aceleración digital y un cambio de paradigmas. https://news.microsoft.com/es-xl/aceleracion-digital-mas-del-94-de-las-pymes-peruanas-invirtio-en-tecnologia-en-el-ultimo-ano/

Espinoza Montes, C. (2014). *Metodología de investigación tecnológica. Pensando en sistemas* (2.ª ed.). Soluciones Gráficas S.A.C.

García Porras, J.C., Huamani Pastor, S.C., & Lomparte Alvarado, R.F.(2018). *Modelo de gestión de riesgos de seguridad de la información para PYMES peruanas. Revista*

Peruana de Computación y Sistemas, 1(1), 47-56. https://doi.org/10.15381/rpcs.v1i1.14856

Garre Gui, S., Segovia Henares, A. J., & Tortajada Gallego, A. (2020). Introducción a la seguridad de la información (3era ed.). Fundació Universitat Oberta de Catalunya (FUOC).

Gatell Sánchez, C., & Pardo Álvarez, J. M. (2014). *Éxito de un sistema integrado*. Editorial AENOR.

Guano Zapata, M. J., & Jaramillo Vinueza, M. N. (2020). *Diseño de un SGSI bajo norma ISO/IEC 27001:2013 aplicado a un caso de estudio*. Escuela Politécnica Nacional.

Hernandez Sampieri, R., Fernandez Collado, C., & Baptista Lucio, M. del P. (2014). *Metodología de la investigación* (6.ª ed.). McGRAW-HILL / Interamericana Editores, S.A. DE C.V.

Huaman Fernández, J. R. (2021). *Impacto económico y social de la COVID-19 en el Perú*. Debates en CAEN, 2(1), 31–42.

Instituto de Auditores Internos de España. (s.f.). *Definición e implantación de apetito de riesgo*. La Fábrica de Pensamiento.

Instituto Nacional de Calidad. (2018). *Tecnología de la información. Técnicas de seguridad. Gestión de la seguridad de la información. Seguimiento, medición, análisis y evaluación* (NTP ISO/IEC 27004; 2.a ed.).

Instituto Nacional de Calidad. (2019). *Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Orientación* (NTP ISO/IEC 27003; 2.a ed.).

Instituto Nacional de Calidad. (2022a). *Seguridad de la información, ciberseguridad y protección de la privacidad. Controles de seguridad de la información* (NTP ISO/IEC 27002; 2.a ed.).

Instituto Nacional de Calidad. (2022b). *Seguridad de la información, ciberseguridad y protección de la privacidad. Orientación sobre la gestión de los riesgos de seguridad de la información* (NTP ISO/IEC 27005; 3.a ed.).

Instituto Nacional de Calidad. (2022c). *NTP-ISO/IEC 27001:2022. Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de seguridad de la información. Requisitos* (NTP ISO/IEC 27001; 3.a ed.).

ISACA. (2023). *State of Cybersecurity 2023: Global Update on Workforce Efforts, Resources and Cyberoperations*.

International Organization for Standardization. (2018). *Tecnologías de la información Técnicas de seguridad – Sistemas de gestión de la seguridad de la información – Visión general y vocabulario.* (No. ISO/IEC 27000).

Johansen Bertoglio, O. (1982). *Introducción a la teoría general de sistemas*. Limusa.

Katz, Daniel y Khan, Robert L. (1966): Psicología social de las organizaciones. México: Trillas, 1977.

Magerit - Libro 1. (2012). MAGERIT – *versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* Madrid: Ministerio de Hacienda y Administraciones Públicas.

Navarro Cid, J. L. (2001). *Las organizaciones como sistemas abiertos alejados del equilibrio.* Universidad de Barcelona.

Ñaupas Paitán, H., Valdivia Dueñas, M. R., Palacios Vilela, J. J., & Romero Delgado, H. E. (2018). *Metodología de la investigación cuantitativa-cualitativa y redacción de la tesis* (5.ª ed.). Ediciones de la U.

Prislan, K., Lobrikar, B. y Bernik, I. (2017). *Information security management practices: expectations and reality.* En I. Bernik, B. Markelj y S. Vhorvec (eds.), Advances in cibersecurity 2017 (pp. 5-22). Máribor: University of Maribor Press.

Ramírez Chávez, M. A., & Ramírez Torres, T. Z. (2024). El método DELPHI como herramienta de investigación. Una revisión. LATAM Revista Latinoamericana de Ciencias Sociales y Humanidades 5 (1), 3368 – 3383. https://doi.org/10.56712/latam.v5i1.1842

Silva Guerrero, A. R. (2022). *Implementación de un Sistema de Gestión de Seguridad de la Información para mejorar la Seguridad de la Información en una empresa MYPE - 2021*. Universidad Tecnológica del Perú.

Tapia Carrillo, J. M., & Vidal Castillo, J. L. (2020). La seguridad de la información y su relación con la gestión de los riesgos de negocio en las empresas agroindustriales azucareras. Universidad Nacional Pedro Ruiz Gallo.

Valencia Duque, F. J. y Orozco Alzate, M. (2017). *Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas iso/iec 27000.* Revista Ibérica de Sistemas y Tecnologías de Información, 22, 73-88. doi: http://dx.doi.org/10.17013/risti.22.73-88

Valencia Duque, F. J. (2021). *Sistema de gestión de seguridad de la información basad en la familia de normas iso/iec 27000.* Editorial Universidad Nacional de Colombia.

Valles-Coral, M. A. (2023). *La información como activo estratégico y de valor para las organizaciones.* Revista Científica de Sistemas e Informática, 3(1), e496.

Villadeza Romero, K. L., & Condor Simon, R. D. (2022). Diseño de un sistema de gestión de seguridad de la información basado en la norma técnica peruana -ISO/IEC 27001:2014 para la municipalidad distrital de Huácar 2022. Universidad Nacional Hermiliovaldizán.

Zapata Gómez, A. (2015). *Ciclo de la Calidad PHVA* (1era ed.). Editorial Universidad Nacional de Colombia. https://studylib.es/doc/9354502/ciclo-de-la-calidad-phva?p=15

ANEXOS

ANEXO 1

PLAN DEL PROYECTO

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

1. **Finalidad y usuarios**

   El presente documento tiene como propósito definir claramente el objetivo del proyecto de diseño del Sistema de Gestión de Seguridad de la Información en Iteprevengo, establecer la estructura organizacional, los entregables, los plazos, los roles y responsabilidades en el proyecto.

   Los usuarios de este documento son el Gerente General, el Jefe de TI y los miembros del equipo del proyecto.

2. **Justificación del proyecto**

   Iteprevengo es una microempresa dedicada al desarrollo de software especializado en Seguridad y Salud en el Trabajo (SST). Dada la naturaleza de sus operaciones, el manejo de información sensible y el modelo de trabajo remoto adoptado, la organización se encuentra altamente expuesta a incidentes que podrían comprometer la confidencialidad, integridad y disponibilidad de los datos. En este contexto, un Sistema de Gestión de la Seguridad de la Información (SGSI), basado en la NTP ISO/IEC 27001, no es sólo una medida de cumplimiento, sino una necesidad estratégica para la organización. Este sistema proveerá de un marco metodológico para identificar, evaluar y mitigar los riesgos asociados a la SI fortaleciendo la protección de los activos de la empresa y asegurando la continuidad del negocio frente a potenciales incidentes.

3. **Objetivo general del proyecto**

   Diseñar el Sistema de Gestión de Seguridad de la Información de acuerdo con la NTP ISO/IEC 27001 antes de julio del año 2026 a más tardar.

4. **Objetivos específicos del proyecto**

   Se definen como objetivos específicos:

   - Proteger la información sensible de la empresa y de los clientes, asegurando la confidencialidad, integridad y disponibilidad de los datos manejados en los procesos críticos de la organización.
   - Establecer políticas y procedimientos para la seguridad de la información que sean efectivos, medibles y aplicables a todas las áreas críticas de la empresa.
   - Identificar y gestionar riesgos de seguridad asociados a los activos de información.

- Garantizar la mejora continua del SGSI, adaptándolo a los cambios tecnológicos y de negocio, asegurando que las medidas de seguridad evolucionen junto con la empresa.
- Fomentar una cultura de seguridad dentro de la organización.
- Mejorar la confianza de clientes y socios comerciales, demostrando el compromiso de Iteprevengo con la seguridad de la información .

5. Alcance preliminar del proyecto

Se determina como alcance preliminar del proyecto los procesos de soporte y desarrollo de Software SaaS de la empresa Iteprevengo.

6. Organización del proyecto

Se establece la siguiente estructura organizacional

Tabla 1

Estructura organizacional del proyecto

CARGO	ROL DENTRO DEL SGSI	NOMBRE	RESPONSABILIDADES PRINCIPALES
Gerente General	Presidente del Comité de Seguridad de la Información	Herbert Parimango Rodríguez	Representar la alta dirección; aprobar políticas, recursos y resultados; liderar las reuniones del CSI; asegurar el compromiso de la dirección con la seguridad de la información.
Jefe de TI	Coordinador del Comité de Seguridad de la Información	Kevin Alberca Cubas	Dirigir la implementación técnica y documental del SGSI; coordinar actividades, plazos y entregables; reportar avances al CSI.
Representante del área de desarrollo	Miembro del CSI	Erick Rodriguez	Aportar información técnica y operativa sobre los procesos dentro del alcance; colaborar en la identificación de activos, amenazas y riesgos.
Representante del área de RRHH	Miembro del CSI	Marco Parimango Rodríguez	Coordinar actividades de capacitación, concientización y comunicación interna sobre seguridad de la información.
Consultor externo	Consultor Externo	Joel Cesar Fernandez Segura	Brindar acompañamiento metodológico y asesoramiento especializado en la implementación del SGSI; conforme con la NTP ISO/IEC 27001.

Nota. Elaborado por los investigadores.

7. Descripción general del proyecto

El proyecto de implementación del SGSI se estructurará en cinco fases, las cuales se presentan a continuación:

Tabla 2

Fases del proyecto

FASE	ACTIVIDADES PRINCIPALES
Fase I Contexto organizacional y compromiso de la alta dirección.	- Analizar y comprender el contexto organizacional. - Obtener la aprobación de la alta dirección para inicio del proyecto, por medio del plan de proyecto.
Fase II Definir el alcance y la política del SGSI	- Describir los procesos de la organización e identificar el proceso crítico. - Determinar el alcance del SGSI. - Definir roles y responsabilidades - Definir la política de la seguridad de la información.
Fase III Análisis de los requisitos de la seguridad de la información	- Realizar un análisis de brechas. - Identificar activos de información. - Definir criticidad de los activos de información.
Fase IV Evaluación y Tratamiento de riesgos	- Identificar amenazas y vulnerabilidades - Análisis del riesgo (probabilidad, impacto y nivel de exposición al riesgo). - Definir el Plan de Tratamiento del Riesgo
Fase V Diseño del SGSI	- Determinar estructura documental - Diseñar el Plan de Concientización y Sensibilización de Seguridad de Información - Definir indicadores de desempeño del SGSI

Nota. Elaborado por los investigadores.

Fecha: 15 de diciembre del 2024

Aprobado por:
Ing. Herbert Parimango
Gerente General

ANEXO 2

ALCANCE DEL SGSI

SISTEMA DE GESTIÓN DE LA SEGURIDAD DE INFORMACIÓN

Código:	SGSI-001
Versión:	1.0
Fecha de versión:	05/11/2025
Nivel de confidencialidad:	Medio
Elaborado por:	Alberca Cubas Kevin y Guerrero Diaz Lalita
Revisado por:	Joel Cesar Fernandez Segura (Consultor Externo)
Aprobado por:	Herbert Parimango Rodríguez (Gerente General)

1. **Objetivo, alcance y usuarios**

   El objetivo de este documento es definir claramente los límites del Sistema de Gestión de la Seguridad de la Información (SGSI) en Iteprevengo.

   Su aplicación abarca toda la documentación, procedimientos, registros y actividades comprendidas dentro del SGSI.

   Este documento está dirigido a la Alta Dirección, miembros del Comité de Seguridad de la Información y los responsables de los procesos incluidos en el alcance.

2. **Documentación de referencia**

   - Norma ISO/IEC 27001:2022, cláusula 4.3
   - Documento Contexto de la Organización
   - Acta de constitución del proyecto del SGSI.

3. **Definición del alcance**

   La organización necesita definir los límites del SGSI para determinar qué información se desea proteger. Dicha información deberá resguardarse adecuadamente, sin importar si es almacenada, procesada o transferida dentro o fuera del alcance del SGSI. En caso de que cierta información se gestione fuera del alcance, esto no la excluye de las medidas de seguridad; sino que transfiere la responsabilidad de su aplicación a un tercero encargado de su administración.

   Considerando los requisitos legales, normativos, contractuales y de otra índole, el alcance del SGSI se define de acuerdo a los siguientes aspectos:

   a. **Procesos y servicios**

      El alcance del SGSI incluye los siguientes procesos y servicios de ITEPREVENGO:

      - Desarrollo de software SaaS para la gestión de Seguridad y Salud en el Trabajo (SST).
      - Soporte técnico a clientes de software.
      - Gestión de infraestructura en la nube.
      - Gestión de cuentas de usuario y accesos.
      - Gestión de copias de seguridad y recuperación ante incidentes.
      - Gestión de recursos humanos (en lo que respecta a la seguridad de la información).

b. Unidades organizativas

El alcance abarca las siguientes unidades:

- Gerencia General, encargada de la toma de decisiones estratégicas y aprobación de políticas.
- Área de Tecnología, responsable del desarrollo de software, mantenimiento de servidores, control de accesos y seguridad técnica.
- Área de Soporte al Cliente, encargada de la atención y gestión de incidencias relacionadas con el uso del software.

c. Ubicaciones

El SGSI aplica a:

- Entornos virtuales y plataformas en la nube utilizadas para el desarrollo, despliegue y respaldo de software.
- Espacios de trabajo remoto del personal técnico autorizado.

d. Redes e infraestructura de TI

El SGSI cubre la infraestructura tecnológica utilizada para el desarrollo, despliegue y mantenimiento de los sistemas SaaS, incluyendo:

- Servidores virtuales en la nube (plataformas PaaS/IaaS).
- Repositorios de código fuente.
- Herramientas colaborativas y de control de versiones (como GitHub o GitLab).
- Redes internas seguras con autenticación y control de acceso.

e. Exclusiones del alcance

No se incluyen en el alcance del SGSI:

- Actividades comerciales, de marketing y contabilidad, salvo aquellas que utilicen información gestionada dentro del SGSI.
- Dispositivos personales no administrados por la organización.
- Servicios de terceros fuera del control contractual de ITEPREVENGO.

4. Validez y gestión del documento

Este documento entra en vigor a partir de su aprobación por la Dirección de Iteprevengo y será revisado anualmente o ante cualquier cambio relevante en los procesos, servicios o estructura organizacional.

ANEXO 3

ROLES Y RESPONSABILIDADES DEL SGSI

SISTEMA DE GESTIÓN DE LA SEGURIDAD DE INFORMACIÓN

Código	SGSI-002
Versión	1.0
Fecha de versión	05/11/2025
Nivel de confidencia	Uso interno
Elaborado por:	Alberca Cubas Kevin y Guerrero Diaz Lalita
Revisado por:	Joel Cesar Fernandez Segura (Consultor Externo)
Aprobado por:	Herbert Parimango Rodríguez (Gerente General)

1. **Objetivo y alcance**

   El objetivo de este documento es establecer de manera clara y formar los roles, funciones y responsabilidades de los actores involucrados en la dirección, coordinación, supervisión y operación del Sistema de Gestión de la Seguridad de la Información (SGSI).

   Este documento aplica a todo el personal que forma parte de la organización, y, en especial, a los miembros del Comité de Seguridad de Información (CSI), así como aquellos colaboradores que, por sus funciones tengan acceso al uso, administración o custodia de activos dentro del alcance del SGSI.

2. **Documentación de referencia**

   - Norma ISO/IEC 27001:2022, cláusula 5.3
   - Política de la Seguridad de Información de Iteprevengo

3. **Estructura organizacional**

   Para gestionar la Seguridad de la Información, Iteprevengo ha establecido el Comité de Seguridad de la Información (CSI), el cual se encuentra conformado por:

Tabla 1

Estructura organizacional del proyecto

CARGO	ROL DENTRO DEL SGSI
Gerente General	Presidente del Comité de Seguridad de la Información
Jefe de TI	Coordinador del Comité de Seguridad de la Información
Representante del área de Desarrollo	Miembro del CSI
Representante del área de RR.HH	Miembro del CSI
Consultor Externo	Consultor Externo en Seguridad de Información

Nota. Elaborado por los investigadores.

4. **Roles y responsabilidades**

   a. **Comité de Seguridad de la Información**

Órgano responsable de la dirección estratégica, supervisión y toma de decisiones relacionadas con el Sistema de Gestión de Seguridad de la Información (SGSI). Sus responsabilidades incluyen:

- Revisar y proponer actualizaciones a la Política de Seguridad de la Información y demás documentación del SGSI.
- Revisar y aprobar la metodología de gestión de riesgos de seguridad de la información.
- Evaluar los resultados de la identificación, análisis y tratamiento de riesgos. Recomendar la aceptación del riesgo residual.
- Supervisar la implementación del Plan de Tratamiento de Riesgos.
- Revisar periódicamente indicadores, auditorías, incidentes y acciones correctivas. Proponer mejoras.
- Impulsar iniciativas de mejora continua del SGSI.
- Aprobar el plan técnico anual de capacitación y sensibilización en seguridad de la información.

b. Gerente General (Presidente del CSI)

Es el responsable de liderar y respaldar el Sistema de Gestión de la Seguridad de la Información. Sus responsabilidades incluyen:

- Aprobar formalmente la Política de Seguridad de la Información y asegurar su alineación con los objetivos estratégicos del negocio.
- Garantizar la disponibilidad de recursos financieros, humanos y tecnológicos necesarios para la implementación, operación y mejora del SGSI.
- Definir y aprobar los criterios de aceptación del riesgo.
- Aprobar el plan de tratamiento de riesgos y aceptar formalmente el riesgo residual.
- Autorizar recursos y presupuesto para su ejecución del plan de concientización y sensibilización en seguridad de información.
- Promover la cultura de la Seguridad de la Información en toda la organización.

c. Jefe de TI (Coordinador del CSI)

Es el responsable de coordinar operativamente las actividades del SGSI. Sus responsabilidades incluyen:

- Participar en las reuniones del CSI.

- Coordinar las reuniones del CSI y realizar el seguimiento de los acuerdos adoptados.
- Consolidar reportes técnicos para su presentación al CSI y a la Alta Dirección.
- Coordinar la ejecución del proceso de identificación, análisis y evaluación de riesgos.
- Supervisar la implementación de los controles definidos en el plan de tratamiento de riesgos.
- Coordinar la atención de incidentes de seguridad de la información.
- Coordinar con las áreas involucradas la ejecución de actividades de gestión de riesgos.
- Monitorear indicadores de seguridad del SGSI.
- Coordinar auditorías internas del SGSI.
- Coordinar la ejecución del plan de capacitación en seguridad de la información.
- Mantener actualizada la documentación del SGSI dentro del alcance definido.

d. Representante del área de desarrollo y soporte (Miembro del CSI)

Es responsable de representar al área de desarrollo dentro del SGSI. Sus funciones incluyen:

- Participar en las reuniones del Comité de Seguridad de la Información (CSI).
- Aportar información técnica y operativa sobre los procesos de desarrollo dentro del alcance del SGSI.
- Colaborar con el desarrollo del proceso de gestión de riesgos (análisis, evaluación y tratamiento).
- Apoyar la implementación de controles de seguridad definidos para el proceso de desarrollo.
- Identificar y reportar riesgos de seguridad asociados a los sistemas y aplicaciones desarrolladas.
- Cumplir y promover el cumplimiento de las políticas y procedimientos de seguridad de la información en su área.

e. Representante del área de RR. HH (Miembro del CSI)

Es responsable de integrar la seguridad de la información en los procesos de gestión del personal. Sus funciones son:

- Participar en el Comité de Seguridad de la Información.

- Apoyar la difusión de políticas, normas y buenas prácticas de seguridad de la información al personal.
- Asegurar que los procesos de ingreso, permanencia y salida del personal consideren controles de seguridad de la información.
- Coordinar y apoyar la ejecución del plan anual de concientización en seguridad de la información.

f. Consultor Externo

Es el responsable de brindar asesoría especializada en materia de seguridad de la información. Sus responsabilidades incluyen:

- Asesorar en la implementación y mejora del Sistema de Gestión de Seguridad de la Información.
- Apoyar en la identificación, análisis y tratamiento de riesgos de seguridad de la información.
- Brindar recomendaciones técnicas y normativas alineadas a la ISO/IEC 27001:2022.
- Apoyar en actividades de evaluación, auditoría interna o revisión del SGSI, cuando corresponda.

g. Colaboradores

Todo el personal de la organización es responsable de:

- Cumplir con la Política de Seguridad de la Información y los procedimientos establecidos.
- Proteger la confidencialidad, integridad y disponibilidad de la información a la que tenga acceso.
- Reportar oportunamente cualquier incidente o debilidad de seguridad de la información.
- Participar en las actividades de capacitación y concientización en seguridad de la información**.**

5. Validez y gestión del documento

Este documento entra en vigor a partir de su aprobación por la Dirección de Iteprevengo y será revisado anualmente o ante cualquier cambio relevante en los procesos, servicios o estructura organizacional.

ANEXO 4

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

SISTEMA DE GESTIÓN DE LA SEGURIDAD DE INFORMACIÓN

Código	SGSI-003
Versión	1.0
Fecha de versión	05/11/2025
Nivel de confidencia	Uso interno
Elaborado por:	Alberca Cubas Kevin y Guerrero Diaz Lalita
Revisado por:	Joel Cesar Fernandez Segura (Consultor Externo)
Aprobado por:	Herbert Parimango Rodríguez (Gerente General)

1. **Objetivo, alcance y usuarios**

   El objetivo de esta política de alto nivel es definir el propósito, la dirección, los principios y las reglas básicas para la gestión de la seguridad de la información en Iteprevengo en conformidad con la NTP ISO/IEC 27001:2022.

   La presente Política de Seguridad de la Información se aplica a todos los procesos, activos, sistemas, personas y servicios comprendidos dentro del alcance del Sistema de Gestión de Seguridad de la Información (SGSI) de Iteprevengo.

   El alcance específico del SGSI, se encuentra definido en el documento "Alcance del SGSI", el cual deberá ser consultado para mayor detalle.

2. **Documentación de referencia**

   - Norma ISO/IEC 27001, cláusulas 5.2,5.3,6.2,7.4 y A.6.3
   - ISO/IEC 27005 – Gestión de Riesgos.
   - Ley N° 29733 – Ley de Protección de Datos Personales.
   - Documento de alcance del SGSI
   - Metodología de evaluación y tratamiento de riesgos
   - Declaración de aplicabilidad (SoA)
   - Registro de requisitos legales, contractuales y otros

3. **Glosario**

   - **Activo de información:** Todo aquello que tiene valor para Iteprevengo, como información digital o física, software, hardware, red de datos, personas, servicios entre otros.
   - **Confidencialidad:** Propiedad de la información de ser accesible sólo a personas o sistemas autorizados.
   - **Disponibilidad:** Propiedad de la información de ser accesible y utilizable cuando se necesita.
   - **Frecuencia:** Intervalo con el que se mide, revisa o ejecuta una actividad de forma periódica.
   - **Impacto:** Consecuencia o efecto que tendría un incidente de seguridad sobre la organización.
   - **Incidente:** Evento único o conjunto de eventos no deseados que comprometen o pueden comprometer la seguridad de la información.
   - **Integridad:** Propiedad de la información de ser completa, precisa y sin modificaciones deliberadas o accidentales.

- **Mejora continua:** Actividad recurrente destinada a mejorar el desempeño en relación con la gestión de actividades, procesos, servicios, sistemas u organizaciones.
- **Política:** Declaración formal que establece lineamientos obligatorios para guiar acciones o comportamientos dentro de la organización.
- **Riesgo:** Posibilidad de que una amenaza explote una vulnerabilidad de un activo de información y cause daño a la organización.
- **Seguridad de la Información:** Es la preservación de la confidencialidad, integridad y disponibilidad de la información en cualquier formato.

4. Compromiso de la Alta Dirección

La Alta Dirección demuestra su liderazgo y compromiso mediante:

- La integración del SGSI en los procesos organizacionales.
- Proteger los activos de información frente a amenazas internas y externas.
- Implementar un proceso sistemático de gestión de riesgos de seguridad.
- El cumplimiento de requisitos legales, regulatorios y contractuales.
- Asignar responsabilidades en materia de seguridad de la información.
- Proporcionar recursos razonables para la operación del SGSI.
- La promoción de una cultura organizacional orientada a la seguridad.
- La revisión periódica del desempeño del SGSI.

5. Gestión de Riesgos

La organización establecerá, implementará y mantendrá un proceso sistemático de identificación, análisis, evaluación y tratamiento de riesgos de seguridad de la información, conforme a la metodología definida en el documento "Metodología de Evaluación y Tratamiento de Riesgos".

El resultado del tratamiento de riesgos se verá reflejado en la Declaración de Aplicabilidad, donde se justificarán los controles seleccionados del Anexo A de la NTP ISO/IEC 27001:2022.

6. Lineamientos Generales de Seguridad

En este apartado se presentan los lineamientos generales de seguridad de la información que orientan la gestión y protección de los activos de información de la organización. Dichos lineamientos se estructuran tomando como referencia los catorce dominios establecidos en la NTP ISO/IEC 27001:2013, los cuales permiten organizar y abordar

de manera integral los distintos aspectos relacionados con la seguridad de la información dentro del SGSI. Estos son:

a. Políticas de la Seguridad de Información

- La política de Seguridad de Información será aprobada por la Gerencia General y comunicada a todo el personal.
- Será revisada anualmente o ante cambios importantes en la organización o en el entorno tecnológico.
- Todos los documentos del SGSI derivarán de esta política como marco principal.

b. Organización de la Seguridad de la Información

- Se definirán roles y responsabilidades en materia de seguridad de la información dentro de la organización.
- Existirá un responsable del SGSI designado formalmente por la Gerencia.
- La seguridad será considerada en todo el ciclo de vida del software.
- El acceso a sistemas corporativos deberá realizarse mediante mecanismos de autenticación segura.
- Los dispositivos utilizados para el acceso a información corporativa deberán contar con medidas básicas de protección (actualizaciones, antivirus y configuración adecuada).
- Se prohíbe el uso de redes públicas no seguras sin mecanismos de protección adecuados.
- El acceso remoto será mediante VPN.
- La información confidencial no deberá almacenarse en dispositivos personales sin autorización.
- El personal es responsable de garantizar que terceros no autorizados no accedan visual o físicamente a información sensible.

c. Seguridad del Personal

- Verificación básica de antecedentes en contratación según el cargo.
- Revocación inmediata de accesos al finalizar contrato.
- Devolución de activos asignados al termino de relación laboral.
- Todo el personal firmará acuerdos de confidencialidad al inicio de la relación laboral.

- Las responsabilidades en seguridad de la información serán incluidas en los términos y condiciones de cada contrato.
- Se aplicarán medidas disciplinarias formales ante incumplimientos de la política de seguridad.
- Las actividades formativas serán planificadas, ejecutadas y evaluadas conforme a los objetivos del SGSI.
- Capacitación anual obligatoria en seguridad de la información para todo el personal.
- Simulación de phishing como mecanismo de evaluación y concientización.

d. Gestión de activos

- Se realizará inventario de activos de información y tecnológicos.
- La información se clasificará como: pública, interna, confidencial y sensible.
- Los activos serán clasificados conforme a su clasificación.
- Se asignará un responsable a cada activo de información, denominado "propietario del activo".
- Se definirán procedimientos para el uso aceptable, devolución y eliminación segura de activos.
- Los activos tecnológicos se usarán exclusivamente para fines laborales autorizados.
- Queda prohibida la instalación o uso de software no autorizado en equipos de la empresa.

e. Control de acceso

- El acceso a sistemas será otorgado bajo el principio de mínimo privilegio.
- Se usará autenticación segura y MFA cuando sea posible, y de preferencia para accesos de administrador.
- Las altas, bajas y modificaciones de accesos serán gestionadas y supervisadas de manera controlada.
- Los accesos serán revisados cada tres meses por el jefe de TI.

f. Criptografía

- Se definirá una política de uso de criptografía para la protección de información sensible en tránsito y en reposo.
- Se utilizarán algoritmos y protocolos de cifrado reconocidos y actualizados (TLS 1.5 o superior, AES-256 y SHA 256).
- La gestión de claves criptográficas será controlada y documentada, incluyendo su generación, distribución, almacenamiento y revocación.

g. Seguridad física y del entorno

- Al no contar con infraestructura física propia, la seguridad del entorno físico de los servidores recae en el proveedor cloud contratado, cuyo nivel de seguridad será documentado.
- Los colaboradores en trabajo remoto deberán asegurar que su entorno de trabajo cumpla condiciones mínimas: pantalla no visible a terceros, escritorio limpio y bloqueo de pantalla automático.
- Los equipos de trabajo no deberán ser compartidos con personas ajenas a la empresa.
- El traslado de equipos con acceso a información corporativa deberá realizar con precaución.

h. Seguridad en las operaciones

- Registro de accesos, cambios y eventos críticos.
- Retención de logs según criticidad.
- Monitoreo de anomalías e intentos de intrusión.
- Los servicios cloud serán configuración bajo principal de seguridad por diseño y mínima exposición.
- Se habilitarán los servicios de logging y monitoreo nativos del proveedor cloud.
- Se definirán alertas automáticas ante eventos críticos en el entorno cloud.
- Se realizarán backups semanales almacenados en ubicaciones separadas dentro del entorno cloud.

i. Seguridad en las comunicaciones

- Cifrado en transición de información sensible.

- Restricción de acceso por roles e IP.
- Se prohibirá el uso de herramientas de comunicación no autorizadas para el intercambio de información corporativa sensible.
- Las APIs respuestas en el entorno cloud deberán contar con autenticación y cifrado obligatorio.

j. Adquisición, desarrollo y mantenimiento de sistemas

- Se adoptarán principios de desarrollo seguro en todo el SDLC.
- Se aplicarán buenas prácticas de codificación segura.
- Separación de entornos: desarrollo, pruebas y producción.
- Se realizarán pruebas de seguridad antes de despliegues en producción.
- Se gestionarán versiones y cambios mediante repositorios controlados con roles y permisos definidos para cada desarrollador.
- Protección de repositorios y CI/CD.

k. Relaciones con proveedores

- Evaluación de seguridad de proveedores cloud y software.
- Contratos con cláusulas de confidencialidad.
- Revisión anual de proveedores críticos.
- Se documentarán los proveedores cloud críticos con su nivel de acceso a la información de la empresa.
- Se verificará que los proveedores cloud cuenten con certificaciones de seguridad reconocidas (ISO 27001, SOC 2 o equivalente).
- Se definirá un plan de contingencia ante la interrupción del servicio de un proveedor cloud crítico.

l. Gestión de incidentes de seguridad

- Se establecerán procedimientos para reportar y gestionar incidentes.
- Se documentarán los eventos relevantes para su análisis.
- Se adoptarán acciones correctivas cuando corresponda.

m. Continuidad del negocio

- Se mantendrán copias de seguridad periódicas.
- Se elaborarán procedimientos de restauración segura de la información a partir de backups.

- Se definirán medidas para garantizar la disponibilidad del servicio SaaS ante interrupciones.
- Los planes de continuidad serán probados y actualizados periódicamente

n. Cumplimiento

- Se cumplirá con los requisitos legales, regulatorios y contractuales aplicables, incluyendo la Ley N° 29733 (Protección de Datos Personales) y la Ley N° 30096 (Delitos Informáticos).
- Se realizarán revisiones periódicas del cumplimiento de esta política y los controles del SGSI.
- Las auditorías internas del SGSI se planificarán y ejecutarán conforme a lo establecido en la norma ISO/IEC 27001:2022.
- Los indicadores de seguridad serán revisados periódicamente por la dirección en el marco de la revisión por la dirección del SGSI.
- Se aplicarán acciones correctivas ante no conformidades o desviaciones identificadas en el SGSI.

7. Responsabilidades

Las responsabilidades del CSI son las siguientes:

- El Gerente General es responsable de garantizar que el SGSI se implemente y mantenga de acuerdo con esta política, y de asegurar que todos los recursos necesarios estén disponibles.
- El Jefe de TI es responsable de la coordinación operativa del SGSI, así como informar sobre el desempeño del mismo.
- El Comité de Seguridad Información (CSI) debe revisar el SGSI al menos una vez al año o cada vez que se produzca un cambio significativo. El propósito de la revisión por la dirección es establecer la idoneidad, adecuación y eficacia del SGSI.
- El Representante de RRHH en coordinación con el Jefe de TI son encargados de implementar programas de capacitación y concientización sobre la seguridad de la información para los empleados.
- La protección de la integridad, disponibilidad y confidencialidad de los activos es responsabilidad del propietario de cada activo.
- Todos los incidentes o debilidades deben ser reportados al Jefe de TI.

- El Jefe de TI definirá qué información relacionada con la SI se comunicará a qué partes interesadas (tanto internas como externas), por quien y cuando.

8. Comunicación de políticas

El Jefe de TI debe asegurarse de que todos los colaboradores de Iteprevengo, así como las partes externas correspondientes, estén familiarizados con esta política, mediante:

- Publicación en el repositorio del SGSI en Google Drive.
- Sesiones de inducción y capacitación sobre seguridad de la información.
- Comunicación directa del Comité a todos los responsables de los procesos.

9. Apoyo a la implementación del SGSI

El Gerente General declara por la presente que la implementación del SGSI y la mejora continua serán apoyadas con los recursos adecuados para alcanzar todos los objetivos establecidos en esta política, así como para satisfacer todos los requisitos identificados.

10. Validez y gestión del documento

Este documento entra en vigor a partir de su aprobación por la Dirección de Iteprevengo.

El titular de este documento es el Jefe de TI, quien deberá revisarlo y, en su caso, actualizarlo anualmente.

ANEXO 5

INFORME DE ANÁLISIS DE BRECHAS

SISTEMA DE GESTIÓN DE LA SEGURIDAD DE INFORMACIÓN

1. Objetivo, alcance y usuarios

El objetivo del presente análisis es determinar el grado de cumplimiento de Iteprevengo frente a los requisitos de la NTP ISO/IEC 27001 y sus controles asociados, identificando brechas que permitan orientar acciones de mejora para el diseño y futura implementación del SGSI.

El análisis de brechas abarca los procesos definidos en el alcance del SGSI.

Los usuarios de este documento son la Alta Dirección, miembros del Comité de Seguridad de la Información y los responsables de los procesos incluidos en el alcance, estos últimos con acceso restringido según la necesidad.

2. Documentos de referencia

- Norma NTP ISO/IEC 27001:2022
- Norma NTP ISO/IEC 27002:2022

3. Metodología aplicada

a. Técnicas de recopilación de información

Para obtener una perspectiva transversal de las prácticas actuales en la organización, se realizaron sesiones de focus group. Las sesiones se realizaron en 2 dos reuniones con la participación del Gerente General, el Jefe de TI, programadores y el personal de Recursos Humanos.

b. Instrumentos aplicados

Se utilizaron dos guías de entrevista, diseñadas para evaluar la existencia, formalidad, implementación, mejora y medición de los requerimientos de la NTP ISO/IEC 27001:

- *Guía de entrevista basada en los requisitos de la NTP ISO/IEC 27001*
  Preguntas respecto a los capítulos del 4 al 10 de la norma relacionadas con el contexto, liderazgo, planificación, apoyo, operación, evaluación del desempeño y mejora de un SGSI.

- *Guía de entrevista basada en los controles del Anexo A*
  Preguntas respecto a los 93 controles (organizativos, personas, tecnológicos y físicos) referidos por la NTP ISO/IEC 27001.

c. Escala de evaluación

Para determinar el nivel de cumplimiento, se empleó una versión adaptada del modelo de madurez de procesos de COBIT 5 (Obsérvese Tabla 1).

Tabla 1

Modelo de madurez adaptado de COBIT 5

NIVEL DE MADUREZ	DESCRIPCIÓN
NO APLICA	El control no es relevante para la organización debido a su contexto, modelo de negocio o estructura.
INEXISTENTE	No hay evidencia de que el control se aplique en la organización. Puede o no haber conocimiento sobre él.
INICIAL	Se reconoce la importancia del control, se aplican algunas buenas prácticas de manera reactiva e informal, pero sin estructura ni documentación.
LIMITADO	El control se aplica de un modo totalmente informal. Existen documentos preliminares (políticas, procedimientos, configuraciones), pero sin estandarización, ni aprobación.
DEFINIDO	El control está formalmente establecido (documentado, aprobado y comunicado) y se aplica en base a estos. Puede tratarse de un procedimiento, una política o una configuración técnica.
GESTIONADO	Se aplica y se mide la efectividad del control mediante auditorías, métricas o revisiones periódicas. Se aplican mejoras basadas en datos.
OPTIMIZADO	El control está en mejora continua, se ajusta según resultados y nuevas amenazas o regulaciones.

Nota. Elaborado por los investigadores.

d. Método de análisis

El análisis de brechas se desarrolló en tres etapas:

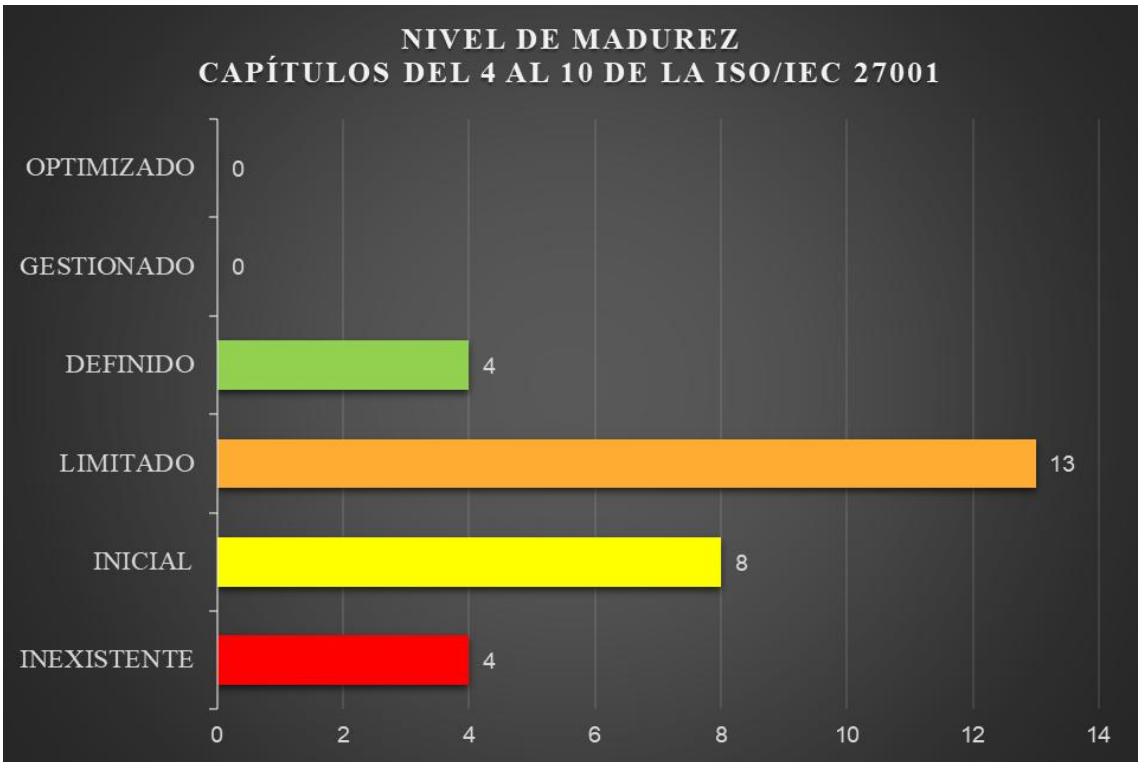
1. Recolección de la información, se aplicaron entrevistas semiestructuradas en modalidad focus group, utilizando los instrumentos del punto 3.2.
2. Evaluación del cumplimiento, con base en la evidencia aportada durante las entrevistas, se determinó el nivel de cumplimiento de cada requisito y control según la escala establecida en el punto 3.3.
3. Identificación de brechas, se analizaron los niveles de cumplimiento obtenidos y se identificaron las brechas significativas actuales de la organización.

4. Resultados e interpretación de los capítulos del 4 al 10 de la NTP ISO/IEC 27001

En la Figura 1 se presenta el nivel de madurez de las cláusulas de 4 al 10 establecidos por la NTP ISO/IEC 27001.

Figura 1

Nivel de madurez - Capítulos del 4 al 10



Nota. Elaborado por los investigadores.

Se evidencia que la organización presenta un nivel de madurez bajo, con una concentración significativa de requisitos en etapas tempranas de implementación, lo que indica la necesidad de priorizar acciones orientadas al fortalecimiento del SGSI.

5. Resultados e interpretación de los controles del Anexo A

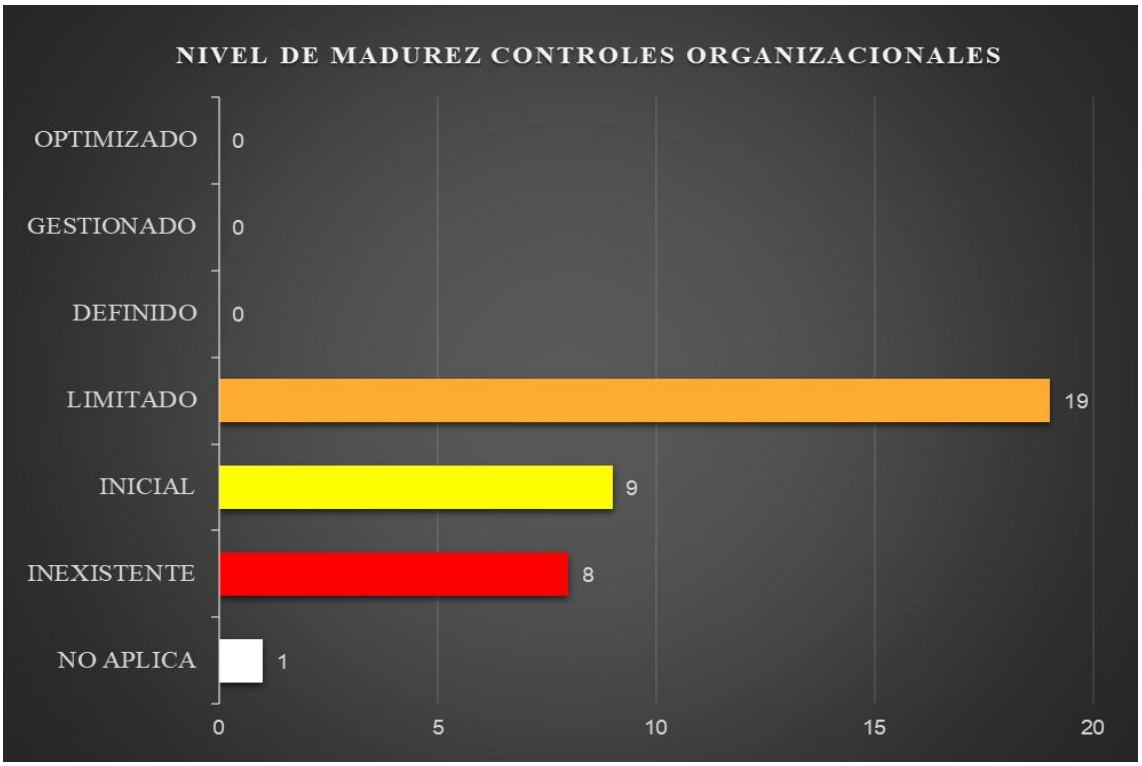
- **Controles organizacionales**

  Del total de 37 controles organizacionales, uno fue considerado no aplicable. En la Figura 2 se presenta el análisis conjunto de los 36 controles aplicables, desde donde se puede evidenciar lo siguiente:

  - Más del 97% de los controles evaluados están en niveles básicos o sin implementación formal (inexistente, inicial o limitado).
  - No se evidencia ningún control que esté completamente definido o gestionado, lo cual refleja la ausencia de políticas, procedimientos documentados, asignación formal de responsabilidades, o seguimiento sistemático.

Figura 2

Nivel de madurez - Controles organizacionales



Nota. Elaborado por los investigadores.

- **Controles físicos**

  Dado que la organización trabaja de manera remota, no cuenta con oficinas físicas ni infraestructura tecnológica local, 12 de los 14 controles físicos fueron considerados no aplicables.

  Sin embargo, los dos controles aplicables sí reflejan aspectos críticos en un entorno remoto:

  - *7.9 Seguridad de los activos fuera de las instalaciones* se encuentra en nivel inicial, lo que sugiere que no existen directrices formales ni controles efectivos para proteger los dispositivos y medios utilizados por los trabajadores remotos, como laptops o teléfonos móviles.
  - *7.10 Medios de almacenamiento* presenta un nivel definido, lo que indica que existen procedimientos básicos para la protección y disposición de los medios de almacenamiento, aunque aún podrían reforzarse.

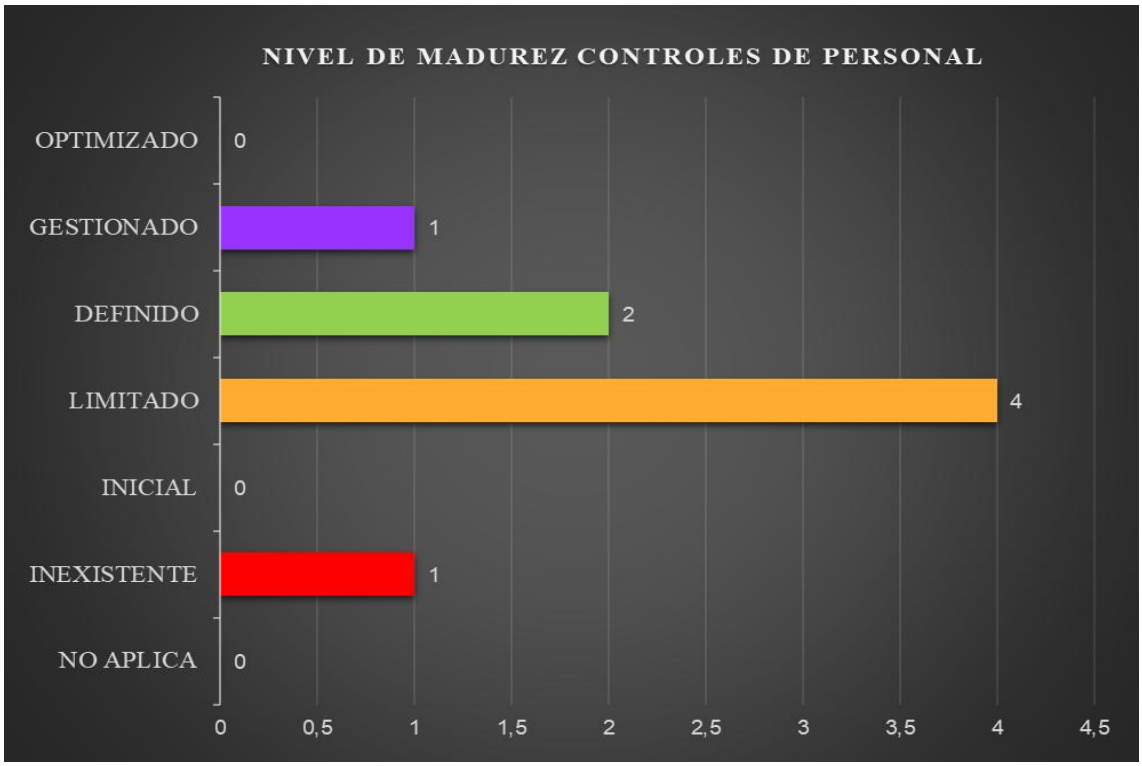
- **Controles de personal**

  En la Figura 3 se muestran los resultados de la evaluación de los controles relacionados con el personal, se identifican controles con avances significativos y otros que requieren atención prioritaria. Los principales resultados fueron los siguientes:

  - Casi la mitad de los controles se encuentran en un nivel limitado, lo que sugiere que existen prácticas informales o parcialmente implementadas, pero sin una documentación adecuada ni seguimiento sistemático.
  - Se identificó un control en estado inexistente: "6.8 Reporte de eventos de seguridad de la información", lo cual representa una brecha crítica, ya que afecta directamente la capacidad de la organización para responder ante incidentes.

Figura 3

Nivel de madurez - Controles de personal



Nota. Elaborado por los investigadores.

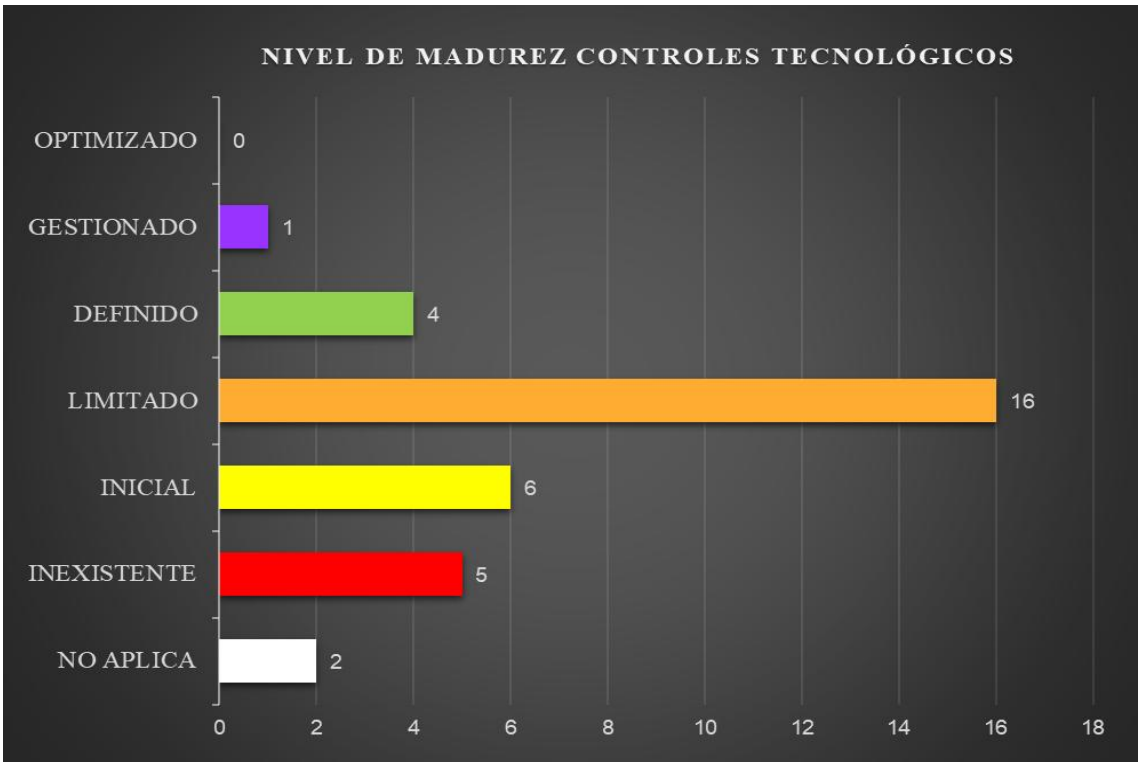
- **Controles tecnológicos**

  En la Figura 4 se puede evidenciar que, si bien existen algunos avances en controles tecnológicos, el nivel general de madurez aún es bajo. Los principales resultados fueron los siguientes:

  - Casi la mitad de los controles se encuentran en nivel limitado, lo que implica que las medidas técnicas están parcialmente implementadas, sin una estandarización o documentación robusta.
  - Solo 5 controles están en niveles superiores (definido o gestionado), lo cual es insuficiente para un entorno que depende significativamente de plataformas digitales.
  - Los 5 controles clasificados como inexistentes representan brechas críticas por tratarse de una organización de servicios tecnológicos.

Figura 3

Nivel de madurez - Controles de personal



Nota. Elaborado por los investigadores.

6. Conclusiones

A partir del análisis realizado, se llegó a los siguientes conclusiones:

- Se evidencia que la empresa trabaja en base a buenas prácticas, sin una visión integral, ni procesos definidos o controlados.
- La organización requiere una intervención estructural y prioritaria, empezando por los procesos operativos del SGSI, para que los demás elementos del sistema (liderazgo, planificación, soporte, evaluación y mejora) tengan un soporte real.
- El hecho de que las brechas más críticas estén en el corazón operativo del SGSI debe considerarse una alerta prioritaria, sobre todo considerando que la organización maneja servicios SaaS, donde la operación segura es vital.

ANEXO 6

DECLARACIÓN DE APLICABILIDAD

SISTEMA DE GESTIÓN DE LA SEGURIDAD DE INFORMACIÓN

Código	SGSI-005
Versión	1.0
Fecha de versión	05/11/2025
Nivel de confidencia	Uso interno
Elaborado por:	Kevin Alberca Cubas y Lalita Guerrero Diaz
Revisado por:	Joel Cesar Fernandez Segura (Asesor de TI)
Aprobado por:	Herbert Parimango Rodríguez (Gerente General)

1. Objetivo, alcance y usuarios

El objetivo de esta Declaración de aplicabilidad (SoA) es documentar y justificar la selección de controles del Anexo A de la NTP ISO/IEC 27001:2022, basados en el análisis de riesgos realizado para el modelo de SGSI y en las buenas prácticas que se debe seguir para cumplir con los objetivos del negocio a mediano y largo plazo.

El SoA cubre la evaluación de los 93 controles del Anexo A considerando la naturaleza de la empresa y los riesgos asociados, se excluyen por ejemplo la mayoría de controles físicos debido al sistema de trabajo remoto y basado en la nube con el que se cuenta.

Los usuarios de este documento son la alta dirección y el jefe de TI de Iteprevengo, así como las partes externas relevantes (clientes, proveedores, consultores y terceros con acceso a la información de la organización).

2. Documentación de referencia

- NPT ISO/IEC 27001:2022
- Documento de alcance del SGSI
- Metodología de evaluación y tratamiento de riesgos
- Registro de requisitos legales, contractuales y otros

3. Tabla de Controles del Anexo A

En la Tabla 1 se presentan los controles establecidos en el Anexo A de la NTP ISO/IEC 27001:2022, junto con la justificación correspondiente basada en los riesgos identificados y el contexto de la empresa, así como la documentación que respalda su implementación cuando corresponde.

Tabla 1

Justificación de la aplicación de controles

ÍTEM	CONTROLES NTP IS0 27001:2022	APLICABILIDAD	JUSTIFICACIÓN	DOCUMENTACIÓN
CONTROLES ORGANIZACIONALES				

5.1	Políticas para la seguridad de la información	SI	Base para el diseño del SGSI y la concienciación del personal y la alta dirección.	Política de seguridad de la información
5.2	Roles y responsabilidades en seguridad de la información	SI	Es necesario definir la estructura de seguridad.	Política de roles y responsabilidades, Organigrama institucional y Matriz RACI.
5.3	Segregación de funciones	SI	Para minimizar el riesgo de fraude o error al separar responsabilidades.	Procedimiento de separación de funciones
5.4	Responsabilidades de la gerencia	SI	Asegurar la aprobación y apoyo de la alta dirección al SGSI.	Acta de Reunión del Comité de Seguridad
5.5	Contacto de autoridades	SI	Obligatorio para notificar incidentes que involucren datos sensibles de clientes debido al riesgo legal.	Política de Gestión de Incidentes
5.6	Contacto con grupos especiales de interés	SI	Mantener relación con entidades de ciberseguridad para estar al tanto de nuevas amenazas.	Participación en foros de la industria
5.7	Inteligencia de amenazas	SI	Esencial para un servicio SaaS, identificando proactivamente vulnerabilidades y ataques.	Procedimiento de Gestión de Amenazas
5.8	Seguridad de la información en gestión de proyectos	SI	Importante integrar la seguridad en el ciclo de vida del desarrollo de software.	Procedimiento SDLC seguro
5.9	Inventario de información y otros activos asociados	SI	Necesario para gestión de riesgos y clasificación.	Inventario de activos de información
5.10	Uso aceptable de la información y otros activos asociados	SI	Establecer las reglas para el uso de equipos y datos por parte del personal remoto.	Política de uso aceptable
5.11	Devolución de activos	SI	Proceso formal para la devolución de equipos y acceso cuando finaliza la relación laboral.	Procedimiento de Fin de Relación Laboral
5.12	Clasificación de la información	SI	Necesario para identificar el nivel de sensibilidad de los datos.	Política de Clasificación de la Información

5.13	Etiquetado de la información	SI	Aplicable a los datos gestionados para su identificación y manejo correcto.	Procedimiento de Etiquetado de Información
5.14	Transferencia de la información	SI	Necesario controlar el intercambio de datos entre sistemas, terceros y desarrolladores.	Procedimiento de Transferencia de Información
5.15	Control de acceso	SI	Restringir el acceso a los sistemas y datos de la plataforma SaaS y la infraestructura de nube según el rol dentro del equipo de TI.	Política de Control de Acceso
5.16	Gestión de identidades	SI	Importante implementar un sistema robusto para la gestión de identidades y accesos del personal o externos.	Procedimiento de Gestión de Identidad
5.17	Información de autenticación	SI	Se debe aplicar procesos de gestión de la información de autenticación y capacitaciones a los colaboradores sobre el uso adecuado de esta.	Política de Control de Acceso
5.18	Derechos de acceso	SI	Se deben implementar políticas y procedimientos válidos por la alta dirección controlando el acceso correcto a los activos de la información.	Política de Control de Acceso
5.19	Seguridad de la información en las relaciones con los proveedores	SI	Se debe gestionar la información que brindamos a los proveedores.	Inventario de proveedores, Política de seguridad de proveedores
5.20	Abordar la seguridad de la información dentro de los acuerdos con proveedores	SI	Necesario gestionar para determinar el nivel de responsabilidad de ambas partes en cuanto a la seguridad de la información.	Contratos y acuerdos de nivel de servicio (SLA) con el proveedor , Política de seguridad de proveedores
5.21	Gestión de la seguridad de la información en la cadena de suministro de las tecnologías de la información y comunicación (tic)	SI	Se utilizan servicios cloud donde no existen contratos personalizados, pero si se deben revisar sus políticas, certificaciones ISO 27001/SOC 2 y modelo de responsabilidad compartida.	Contratos y acuerdos de nivel de servicio (SLA) con el proveedor, Política de seguridad de proveedores

5.22	Seguimiento, revisión y gestión de cambios en servicios de proveedores	SI	Para mantener el nivel de seguridad de la información se deben realizar revisiones periódicas de los servicios brindados principalmente por los proveedores en la nube ya que estos pueden sufrir alteraciones o modificar sus políticas sin previo aviso.	Contratos y acuerdos de nivel de servicio (SLA) con el proveedor, Política de seguridad de proveedores
5.23	Seguridad de la información en el uso de servicios en la nube	SI	Debido a las vulnerabilidades encontradas en la configuración de servidores en la nube de la empresa es vital gestionar e implementar acciones preventivas para resguardar la información alojada.	Contratos y acuerdos de nivel de servicio (SLA) con el proveedor , Inventario de servicios cloud, Política de seguridad de proveedores.
5.24	Planificación y preparación de la gestión de incidentes de seguridad de la información	SI	Este control es crítico, al manejar datos sensibles de los colaboradores de los clientes, cualquier incidente no controlado de manera eficaz puede poner en riesgo esta información y causar graves consecuencias legales, financieras y de reputación.	Plan de Gestión de Incidentes de Seguridad, Procedimiento de registro de incidentes
5.25	Evaluación y decisión sobre eventos de seguridad de la información	SI	Es crucial contar con un proceso formal para evaluar la severidad y el impacto potencial de estos eventos, distinguiendo entre uno menor y una amenaza real que requiere una respuesta inmediata.	Procedimiento de Evaluación y Clasificación de Eventos de Seguridad
5.26	Respuesta a incidentes de seguridad de la información	SI	La respuesta a incidentes, es decir, la ejecución del plan de gestión de incidentes debe ser rápida, eficaz y coordinada para contener, mitigar y recuperarse de cualquier evento de seguridad que pueda alterar la disponibilidad, integridad o confidencialidad de la información.	Plan de Gestión de Incidentes de Seguridad
5.27	Aprendizaje de los incidentes de seguridad de la información	SI	Control esencial para el ciclo de mejora continua de la seguridad del SGSI. Es crucial analizar las causas raíz, identificar las debilidades en los controles existentes y aplicar los cambios necesarios para evitar la recurrencia.	Plan de Gestión de Incidentes de Seguridad

5.28	Recolección de evidencia	SI	La empresa puede enfrentar incidentes de seguridad o auditorías que requieran preservar evidencia digital (logs de sistema, registros de acceso, etc.), para un análisis posterior o que permita protegerla en conflictos legales.	Plan de Gestión de Incidentes de Seguridad
5.29	Seguridad de la información durante una interrupción	SI	La organización depende de servicios cloud (Digital Ocean, AWS, S3, SES) y bases de datos críticas para su operación SaaS. Es necesario proteger la información durante interrupciones o procesos de restauración, asegurar que, incluso en un estado de crisis o recuperación, los controles de seguridad se mantengan , los datos sensibles permanezcan protegidos y solo el personal autorizado tenga acceso a los sistemas para la recuperación.	Planes de Continuidad del Negocio (BCP) y Recuperación ante Desastres (DRP)
5.30	Preparación de las tic para la continuidad del negocio	SI	Es necesario asegurar que la infraestructura tecnológica pueda recuperarse y estar operativa en el tiempo tras una interrupción. Sin la preparación adecuada de las TIC, el servicio SaaS no podría reanudarse, lo que resultaría en incumplimiento contractual, pérdida de ingresos y hasta un gran daño reputacional.	Plan de Recuperación ante Desastres (DRP)
5.31	Requisitos legales, estatutarios, regulatorios y contractuales	SI	Fundamental y de máxima prioridad debido a la naturaleza del negocio. Al tener un software SaaS que gestiona datos sensibles de Seguridad y Salud en el Trabajo (SST), están sujetos a una estricta regulación de protección de datos. Además, los contratos con los clientes imponen requisitos específicos de seguridad. El cumplimiento de estas obligaciones es obligatorio y crucial para evitar sanciones legales, multas y la pérdida de la confianza del cliente.	Registro de requisitos legales y contractuales

5.32	Derechos de propiedad intelectual	SI	La empresa debe proteger uno de sus activos más valiosos, el software SST, por eso es importante implementar este control, para cuidar la propiedad intelectual, prevenir el uso no autorizado o robo de parte de sus propios colaboradores o terceros. Actualmente los contratos de los desarrolladores los inhabilitan de participar en desarrollo de productos similares o de usar alguna de las funcionalidades hechas en la empresa.	Registros de propiedad intelectual
5.33	Protección de registros	SI	Es fundamental para la trazabilidad, la responsabilidad y el cumplimiento normativo. La empresa genera y gestiona numerosos registros críticos (logs de actividad, auditorías, acuerdos contractuales, informes de incidentes, registros de SST, etc.). Es vital asegurar la protección de estos registros contra pérdida, destrucción, falsificación, acceso no autorizado y divulgación indebida. Esto es especialmente importante para cumplir con los requisitos legales y para demostrar la evidencia antes posibles auditorías.	Procedimiento de gestión de registros
5.34	Privacidad y protección de la información de identificación personal (iip)	SI	Al contar con datos muy sensibles como datos personales y de salud de los colaboradores de los clientes, la empresa debe alinearse a leyes como la Ley N° 29733 en Perú (protección de datos personales) y a requisitos contractuales para salvaguardar esta información y prevenir el daño reputacional.	Política de Privacidad y Protección de Datos Personales
5.35	Revisión independiente de la seguridad de la información	SI	Importante para garantizar la objetividad y eficacia del SGSI y poder evaluar oportunidades de mejora.	Plan de auditoría interna, certificaciones externas, registro de no conformidades

5.36	Cumplimiento con políticas, reglas y normas de seguridad de la información	SI	Este control es esencial para la gobernanza y la eficacia del SGSI. Asegura que el personal y los procesos de la organización se adhieran consistentemente a las políticas, procedimientos, reglas y estándares internos de seguridad establecidos.	Política de seguridad de la información, Plan de auditoría interna
5.37	Procedimientos operativos documentados	SI	Es importante que los colaboradores tengan acceso a procedimientos actualizados que les permita ejercer sus actividades de manera correcta y siguiendo los lineamientos de la seguridad de la información.	Política de desarrollo seguro y Procedimiento de seguridad para TI
CONTROLES DE PERSONAL				
6.1	Selección	SI	Se debe realizar un buen proceso selección de personal para garantizar el buen manejo de los activos de la información.	Procedimiento de selección de personal
6.2	Términos y condiciones de empleo	SI	Dada las condiciones de trabajo remoto y lo sensible de la información manejada es necesario establecer correctamente las bases contractuales con los colaboradores al inicio del servicio de estos.	Contrato laboral con cláusulas de confidencialidad
6.3	Toma de conciencia, educación y entrenamiento sobre la seguridad de la información	SI	Es necesario mantener concientizadas a las parte interesadas, sobre todo tener un buen nivel de capacitación para el equipo de TI que dado a la naturaleza del trabajo remoto pueden estar más expuestos a riesgos.	Plan de Concienciación y Capacitación en Seguridad de la Información
6.4	Proceso disciplinario	SI	Es importante que se establezcan procedimientos justos para abordar las faltas a la seguridad de la información y que los colaboradores las conozcan, todo esto con el fin de mantener los altos estándares.	Procedimiento disciplinarios por violaciones de seguridad de la información

6.5	Responsabilidades después del cese o cambio de empleo	SI	Es crucial un proceso de "offboarding" riguroso para revocar accesos de inmediato, recuperar equipos y asegurar el cumplimiento continuo de la confidencialidad. Mitiga el riesgo de acceso no autorizado, robo de datos o propiedad intelectual.	Procedimiento de offboarding y revocación de accesos
6.6	Acuerdos de confidencialidad o no divulgación	SI	Se deben establecer acuerdos contractuales de confidencialidad que contemplen los activos cruciales, con el fin de garantizar el uso indebido de la información.	Contrato laboral con cláusulas de confidencialidad , acuerdos de confidencialidad con proveedores y con externos
6.7	Trabajo remoto	SI	Con todo el equipo de TI trabajando remotamente es crucial definir un marco de seguridad robusto que garantice el cumplimiento de los lineamientos de seguridad de la información establecidos por la empresa.	Política de trabajo remoto
6.8	Reporte de eventos de seguridad de la información	SI	Es importante implementar este control mediante procedimientos que permitan a los colaboradores reportar de forma óptima cualquier sospecha de incidente, esto permitirá que el equipo de TI pueda minimizar el impacto.	Plan de Gestión de Incidentes de Seguridad
CONTROLES FÍSICOS				
7.1	Perímetros de seguridad física	NO	Se maneja un entorno cloud y la modalidad de trabajo es remoto	
7.2	Ingreso físico	NO	Se maneja un entorno cloud y la modalidad de trabajo es remoto	
7.3	Asegurar oficinas, salas e instalaciones	NO	Se maneja un entorno cloud y la modalidad de trabajo es remoto	
7.4	Supervisión de la seguridad física	NO	Se maneja un entorno cloud y la modalidad de trabajo es remoto	
7.5	Protección contra amenazas físicas y ambientales	NO	Se maneja un entorno cloud y la modalidad de trabajo es remoto	
7.6	Trabajo de áreas seguras	NO	Se maneja un entorno cloud y la modalidad de trabajo es remoto	
7.7	Escritorio y pantallas limpios	NO	Se maneja un entorno cloud y la modalidad de trabajo es remoto	

7.8	Ubicación y protección de los equipos	NO	Se maneja un entorno cloud y la modalidad de trabajo es remoto	
7.9	Seguridad de los activos fuera de las instalaciones	SI	Importante control para proteger los dispositivos que usa el equipo de TI de manera remota.	Política de trabajo remoto, Política de seguridad informática
7.10	Medios de almacenamiento	SI	Necesario gestionar la información que puedan extraer los colaboradores con el fin de evitar robo de información.	Política de trabajo remoto, Política de seguridad informática
7.11	Servicios de suministro de apoyo	NO	Se maneja un entorno cloud y la modalidad de trabajo es remoto	
7.12	Seguridad del cableado	NO	Se maneja un entorno cloud y la modalidad de trabajo es remoto	
7.13	Mantenimiento de equipo	NO	Se maneja un entorno cloud y la modalidad de trabajo es remoto	
7.14	Eliminación segura o reutilización de equipos	NO	Se maneja un entorno cloud y la modalidad de trabajo es remoto	
CONTROLES TECNOLÓGICOS				
8.1	Dispositivos terminales del usuario	SI	Asegurar la seguridad de los dispositivos usados por el equipo de TI en el desarrollo es crucial para mitigar riesgos de acceso no autorizado, malware, pérdida de datos y garantizar un entorno de trabajo seguro fuera de las instalaciones tradicionales como lo es en este caso.	Política de trabajo remoto, Política de seguridad informática
8.2	Derechos de acceso privilegiados	SI	Es crucial implementar controles estrictos sobre estos derechos de acceso al entorno cloud(servidores, BD,etc.) para prevenir el abuso, el error humano, el acceso no autorizado y las amenazas internas.	Política de control de acceso
8.3	Restricción de acceso a la información	SI	La implementación de restricciones de acceso es crucial para garantizar que los colaboradores (incluso aquellos con acceso privilegiado, control 8.2) solo puedan acceder a la información que es estrictamente necesaria para realizar sus tareas.	Política de control de acceso, Modelo de Control de Acceso basado en Roles (RBAC)

8.4	Acceso al código fuente	SI	Este control es fundamental y de máxima prioridad, ya que protege la propiedad intelectual más valiosa de la empresa. Su acceso no autorizado podría llevar al robo, la divulgación de vulnerabilidades o la introducción de código malicioso.	Política de control de acceso, Modelo de Control de Acceso basado en Roles (RBAC)
8.5	Autenticación segura	SI	En un entorno donde la seguridad física no es posible, este control es muy importante para validar la identidad de los usuarios. Se debe garantizar el acceso a la infraestructura cloud, código fuente, entre otros activos con autenticaciones robustas que eviten ataques de fuerza bruta, phishing y el uso indebido de credenciales.	Política de control de acceso, Política de contraseñas robustas
8.6	Gestión de capacidad	SI	Importante para garantizar la disponibilidad y rendimiento del servicio y evitar incumplir con los Acuerdos de Nivel de Servicio (SLA) con los clientes.	Procedimiento de seguridad para TI
8.7	Protección contra programas maliciosos	SI	Es crucial contar con medidas que garanticen la protección de los datos contra software malicioso que pueden llevar a incumplimiento de contrato lo que causaría problemas legales, de reputación y económicos.	Política de seguridad informática, Procedimiento de seguridad para TI
8.8	Gestión de vulnerabilidades técnicas	SI	Importante para garantizar la integridad y confidencialidad de los activos de la información. Una gestión deficiente de vulnerabilidades podría permitir a los atacantes explotar debilidades, resultando en interrupciones del servicio, ataques de ransomware o acceso no autorizado. Este control es clave para la resiliencia operativa de la empresa y la seguridad.	Política de seguridad informática, Procedimiento de seguridad para TI

8.9	Gestión de la configuración	SI	Se debe contar con una buena configuración de los servicios en la nube y de dispositivos usados por el equipo de TI para poder garantizar la disponibilidad del software SaaS a los clientes y evitar errores provenientes de una configuración defectuosa.	Procedimiento de seguridad para TI
8.10	Eliminación de información	SI	Dado los datos sensibles que se maneja de los clientes la empresa tiene la obligación legal y contractual de eliminar la información al finalizar el servicio, por la tanto debe implementar procedimientos que garanticen se haga esto de una forma segura e irreversible.	Procedimiento de borrado seguro de la información
8.11	Enmascaramiento de datos	SI	Para evitar la exposición de datos sensibles como los datos de salida que maneja la empresa en ambientes no productivos o ante personal no autorizado, se requiere aplicar técnicas de enmascaramiento y anonimización.	Política de desarrollo seguro
8.12	Prevención de fuga de datos	SI	Al tener implementado una metodología de trabajo remoto es complicado llevar un control de donde se descargan o almacenan los datos, por tanto es crucial contar con medidas robustas que prevengan la filtración o divulgación no autorizada y así evitar incumplimientos legales.	Política de seguridad informática, Procedimiento de seguridad para TI
8.13	Copia de seguridad de la información	SI	La implementación de un sistema de backups robusto es importante para garantizar la continuidad de las operaciones.	Política y procedimientos de backups
8.14	Redundancia de las instalaciones de procesamiento de información	SI	Control esencial para garantizar la disponibilidad de la información y cumplir con los Acuerdos de Nivel de Servicio(SLA)	Plan de recuperación antes desastres, SLA con proveedor
8.15	Registro	SI	Es necesario mantener registros detallados para auditar accesos, detectar anomalías y responder de manera oportuna ante incidentes de seguridad.	Procedimiento de seguridad para TI

8.16	Actividades de monitoreo	SI	Necesario implementar monitoreo continuo para detectar accesos indebidos, caídas de servicios o anomalías operativas. Permite también identificar tempranamente incumplimientos en las políticas de seguridad.	Procedimiento de seguridad para TI
8.17	Sincronización de reloj	SI	Es esencial para la trazabilidad de eventos de seguridad, cumplimiento de auditorías y correlación de incidentes.	Procedimiento de seguridad para TI
8.18	Uso de programas de utilidad privilegiados	SI	En el entorno cloud y de desarrollo remoto, existen utilidades administrativas (paneles de control cloud, clientes MySQL, Docker CLI y herramientas de gestión de logs) que pueden alterar configuraciones críticas o acceder a información sensible. Es necesario restringir y monitorear su uso para evitar el abuso de privilegios y garantizar la trazabilidad de la información.	Procedimiento de seguridad para TI
8.19	Información de software en sistemas operativos	SI	Control necesario para evitar vulnerabilidades derivadas de versiones desactualizadas o configuraciones inseguras.	Procedimiento de seguridad para TI
8.20	Seguridad de redes	SI	La organización utiliza servidores cloud y conexiones remotas para acceso administrativo por tanto es necesario este control para proteger la red y los datos contra accesos no autorizados y ataques externos.	Procedimiento de seguridad para TI
8.21	Seguridad de servicios de red	SI	La empresa depende de servicios de red proporcionados por terceros (VPS, DNS, balanceadores, y WAF), es necesario asegurar que estos servicios estén protegidos y gestionados conforme a las políticas de seguridad de la información establecidas.	Procedimiento de seguridad para TI
8.22	Segregación de redes	SI	Los entornos cloud de la organización (producción, desarrollo y pruebas) requieren separación lógica y controlada por eso es importante este control para	Procedimiento de seguridad para TI

			evitar accesos cruzados y minimizar riesgos de ataque o fuga de datos.	
8.23	Filtrado de la web	SI	Este control es importante en un equipo de trabajo remoto que se conecta a redes domésticas para mitigar los riesgos de malware, phishing, acceso a contenido inapropiado y la exposición accidental de datos.	Política de seguridad informática, Procedimiento de seguridad para TI
8.24	Uso de criptografía	SI	Al manejar datos de salud de los colaboradores de los clientes, el uso de cifrado es un requisito legal y regulatorio clave (leyes de protección de datos Ley N° 29733). Es crucial implementar la criptografía para proteger los datos en reposo (almacenados en la nube, bases de datos, equipos remotos) y en tránsito (comunicaciones entre el cliente y el SaaS).	Política de uso de criptografía
8.25	Ciclo de vida de desarrollo seguro	SI	Al ser el principal eje de la empresa el software SaaS, la empresa debe garantizar que se apliquen las mejores prácticas en todo el SDLC, minimizando las vulnerabilidades desde el inicio y cuidando la integridad de la información que se almacenará en este.	Política de desarrollo seguro
8.26	Requisitos de seguridad de la aplicación	SI	Este control asegura que los requisitos funcionales de la aplicación estén alineados con los requisitos de seguridad de la información, necesarios. Es crucial para el cumplimiento normativo y para garantizar que el software sea seguro y confiable, mitigando los riesgos de fallos de seguridad causados por la falta de requisitos claros desde el inicio del desarrollo.	Política de desarrollo seguro

8.27	Arquitectura de sistemas seguros y principios de ingeniería	SI	Este control es fundamental para la seguridad a largo plazo y la continuidad del negocio, asegura que el diseño y la evolución de la arquitectura de la plataforma (aplicación, bases de datos, infraestructura en la nube) se basen en principios de seguridad sólidos.	Política de desarrollo seguro
8.28	Codificación segura	SI	Es esencial y de máxima prioridad, ya que el código mal escrito es la causa de muchas vulnerabilidades de seguridad.	Política de desarrollo seguro
8.29	Pruebas de seguridad en desarrollo y aceptación.	SI	Este control es fundamental para verificar la eficacia de los controles de seguridad anteriormente mencionados implementados durante el desarrollo del software SaaS. Asegura que las vulnerabilidades se identifiquen y corrijan antes de que el software llegue a producción y por tanto evitar problemas de disponibilidad e integridad de la información.	Política de desarrollo seguro
8.30	Desarrollo subcontratado	NO	La empresa desarrolla sus propios productos.	
8.31	Separación de los entornos de desarrollo, prueba y producción	SI	Este control asegura que las actividades en los entornos de desarrollo y pruebas no puedan afectar la operación del entorno de producción. La segregación es crucial para prevenir la introducción accidental de errores, vulnerabilidades o código malicioso en producción, y para proteger los datos reales de los clientes del acceso en entornos menos controlados.	Política de desarrollo seguro, Procedimiento de seguridad para TI
8.32	Gestión de cambios	SI	La empresa debe asegurar que todos los cambios en los sistemas (código, BD, configuraciones en la nube, etc.) se gestionan de forma controlada, minimizando el riesgo de interrupciones del servicio, fallos de seguridad o errores de configuración. Es crucial para	Política de desarrollo seguro, Procedimiento de seguridad para TI

			mantener la confianza del cliente y cumplir con los SLA.	
8.33	Información en las pruebas	SI	El control garantiza que los entornos de pruebas no utilicen datos reales de producción sin controles adecuados. Importante para el cumplimiento de las regulaciones de protección de datos y para mitigar los riesgos de exposición de IIP (información de identificación personal) en entornos menos seguros que la producción.	Política de desarrollo seguro
8.34	Protección de los sistemas de información durante las pruebas de auditoría	SI	El control permite asegurar que las pruebas no causen interrupciones del servicio, corrupción de datos o incidentes de seguridad. Al realizar auditorías tanto internas como externas, o por ejemplo pruebas de penetración en la plataforma SaaS en producción, es vital gestionar los riesgos asociados con estas actividades.	Plan de auditoría interna

Nota. Elaborado por los autores en base a NTP ISO/IEC 27002

4. Validez y gestión del documento

Este documento entra en vigor a partir de su aprobación por la Dirección de Iteprevengo.

El titular de este documento es el Jefe de TI, quien deberá revisarlo y, en su caso, actualizarlo anualmente.

ANEXO 7

OBJETIVOS DE SEGURIDAD DE INFORMACIÒN

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Código	SGSI-004
Versión	1.0
Fecha de versión	05/11/2025
Nivel de confidencia	Uso interno
Elaborado por:	Alberca Cubas Kevin y Guerrero Diaz Lalita
Revisado por:	Joel Cesar Fernandez Segura (Consultor Externo)
Aprobado por:	Herbert Parimango Rodríguez (Gerente General)

1. Objetivo, alcance y usuarios

El objetivo del presente documento es definir los objetivos generales y específicos de la Seguridad de la Información, así como los responsables, recursos, plazos de ejecución y mecanismos de evaluación, garantizando la mejora continua del SGSI.

Este documento aplica a todos los procesos incluidos dentro del alcance del SGSI.

Los usuarios de este documento son la Alta Dirección, el Comité de Seguridad de la Información, así como a los colaboradores, proveedores y terceros que tengan acceso a los activos de información definidos por la organización.

2. Documentación de referencia

- NTP ISO/IEC 27001, cláusula 6.2
- Documento de alcance del SGSI
- Metodología de evaluación y tratamiento de riesgos
- Declaración de aplicabilidad (SoA)
- Registro de requisitos legales, contractuales y otros

3. Objetivos de Seguridad de la Información

Iteprevengo establece los siguientes objetivos generales:

OG 1: Proteger la confidencialidad, integridad y disponibilidad de la información crítica.

OG 2: Reducir la probabilidad e impacto de incidentes de seguridad de la información.

OG 3: Cumplir con requisitos legales, normativos y contractuales aplicables

OG 4: Fortalecer la cultura organizacional de seguridad de la información.

4. Objetivos específicos, responsables, planificación y métricas

Tabla 1

Métricas e indicadores de objetivos

OBJETIVO GENERAL	OBJETIVO ESPECÍFICO (SMART)	RECURSOS REQUERIDOS	RESPONSABLE	FECHA DE CUMPLIMIENTO	INDICADOR	META	FRECUENCIA
OG1. Proteger la confidencialidad, integridad y disponibilidad de la información crítica.	OE 1.1 Identificar y clasificar el 100% de los activos de información de los procesos de soporte y desarrollo SaaS, según la metodología MAGERIT, antes del 30 de junio de 2026.	Plantilla Excel o software de inventario; tiempo del Jefe TI.	Jefe de TI	30/06/2026	% de activos identificados y clasificados	100 %	Trimestral
	OE 1.2 Garantizar la ejecución exitosa del 100% de los respaldos automáticos diarios y verificar su integridad semanalmente, a partir del 1er trimestre de 2026.	Servicio cloud; scripts de backup; recursos del área TI.	Jefe de TI	31/12/2026	% de respaldos exitosos verificados	100 %	Semanal

OG2. Reducir la probabilidad e impacto de incidentes de seguridad de la información.	OE 2.1 Capacitar al 100% de los colaboradores en seguridad de la información, con evaluación aprobatoria (≥ 70%), completando al menos dos sesiones por colaborador antes del 31 de octubre de 2026.	Plan de concientización y sensibilización; recursos de RRHH.	Jefe de TI / Representante de RRHH	31/10/2026	% de colaboradores capacitados con evaluación aprobatoria (≥ 70%)	100 %	Anual
	OE 2.2 Reducir en un 30% el número de clics en campañas de phishing simulado respecto al resultado de la primera medición del año, mediante simulacros trimestrales durante 2026.	Plataforma de simulación; analistas TI.	Jefe de TI	31/12/2026	% de clics en simulacros de phishing	-30 % respecto al año previo	Trimestral
OG3. Cumplir con requisitos legales, normativos y contractuales aplicables.	OE 3.1 Mantener un nivel de cumplimiento igual o superior al 90% en las auditorías trimestrales de políticas del SGSI, considerando la Ley N° 29783 y la NTP ISO/IEC 27001:2022 como marcos de referencia, durante todo el año 2026.	Auditor interno; listas de verificación.	Jefe de TI	Trimestral	% de cumplimiento por política auditada	≥ 90 %	Trimestral

OG4. Fortalecer la cultura organizacional de seguridad de la información.	OE 4.1 Revisar, actualizar y comunicar el 100% de las políticas de seguridad de la información vigentes antes del 31 de marzo de cada año, tomando como línea base la versión aprobada en el año anterior.	Equipo de TI; comunicaciones internas.	Jefe de TI / Representante de RRHH	31/03/2026	% de políticas revisadas y comunicadas formalmente	100 %	Anual

Nota. Elaborado por los investigadores.

5. Validez y gestión del documento

Este documento entra en vigor a partir de su aprobación por la Dirección de Iteprevengo.

El titular de este documento es el Jefe de TI, quien deberá revisarlo y, en su caso, actualizarlo anualmente.

ANEXO 8

PLAN DE CONCIENTIZACIÓN Y SENSIBILIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN

SISTEMA DE GESTIÓN DE LA SEGURIDAD DE INFORMACIÓN

1. Introducción

Iteprevengo es una microempresa que brinda servicios de desarrollo de software SaaS para la gestión integral de la Seguridad y Salud en el trabajo. La organización opera bajo un modelo 100% remoto y almacena su información en entornos cloud. Bajo esta realidad, la concientización y sensibilización en Seguridad de la Información resulta un pilar fundamental para garantizar el éxito del Sistema de Gestión de la Seguridad de la Información (SGSI).

El presente plan forma parte del diseño del SGSI y tiene como propósito asegurar que todo el personal de la organización comprenda su rol en la protección de la información. El plan sigue los principios de la NTP ISO/IEC 27001 y las buenas prácticas en entornos cloud y de trabajo remoto.

2. Documentos de referencia

- NTP ISO/IEC 27001:2022
- Política de la Seguridad de la Información de Iteprevengo.

3. Objetivo General

Definir los canales y mecanismos de comunicación necesarios para informar, motivar e involucrar al personal de Iteprevengo, respecto de la importancia de trabajar bajo los lineamientos del SGSI, asegurando que los interesados conozcan, comprendan y pongan en práctica las políticas, controles y buenas prácticas establecidas con el fin de garantizar la seguridad de la información.

4. Objetivos Específicos

- Difundir entre los colaboradores de Iteprevengo los principios y lineamientos del SGSI, asegurando su conocimiento y comprensión.
- Fortalecer la cultura de la seguridad de la información en el personal involucrado en los procesos de soporte y desarrollo de software SaaS.
- Sensibilizar a los colaboradores de Iteprevengo sobre los riesgos asociados al uso de tecnologías de la información, el trabajo remoto y el almacenamiento de información en la nube.
- Promover la correcta aplicación de las políticas, procedimientos y controles de Seguridad de la Información establecidos en el SGSI.
- Implementar simulacros periódicos de ingeniería social para evaluar y fortalecer la capacidad de respuesta real del personal ante ataques controlados.

- Establecer un programa periódico de capacitación y evaluación que permita medir, monitorear y mejorar continuamente el nivel de concientización a lo largo del año.

5. Alcance

El presente plan aplica exclusivamente al personal interno de Iteprevengo que participa en los procesos de desarrollo y soporte del software SaaS, de acuerdo con el alcance definido para el Sistema de Gestión de Seguridad de la Información (SGSI).

6. Responsables

Los roles y responsabilidades para la implementación del presente plan se detallan a continuación:

a. **Presidente y Comité de Seguridad de la Información (CSI)**

Responsable de la aprobación, supervisión y seguimiento del plan. Sus responsabilidades incluyen:

- Aprobar el Plan de Concientización y Sensibilización.
- Garantizar la asignación de los recursos necesarios para la ejecución del plan (Presidente).
- Supervisar la correcta implementación del plan.
- Evaluar la efectividad del plan y proponer acciones de mejora continua.
- Asegurar la alineación del plan con el SGSI y los objetivos de la organización.
- Autorizar la realización de simulacros de ingeniería social.

b. Jefe de TI

Responsable de la planificación, coordinación y ejecución operativa del plan. Sus responsabilidades incluyen:

- Identificar las necesidades del personal de la empresa en materia de concientización y sensibilización en Seguridad de la Información.
- Definir el contenido técnico de las capacitaciones.
- Diseñar, planificar y ejecutar las actividades del plan, incluyendo simulacros.
- Supervisar el cumplimiento del cronograma y los ciclos de evaluación.
- Monitorear los indicadores de desempeño del plan y resultados de simulacros.
- Reportar al CSI los avances, resultados y métricas del plan.

- Configurar y operar las herramientas de simulación de ataques de ingeniería social.

c. Área de Recursos Humanos

Responsable de la gestión, difusión y seguimiento de las actividades desde el enfoque del factor humano. Sus responsabilidades incluyen:

- Participar en el diseño, planificación y ejecución de las actividades del plan.
- Incorporar la concientización en Seguridad de la Información en el proceso de inducción de nuevos colaboradores.
- Coordinar la programación de capacitaciones, campañas y evaluaciones periódicas.
- Difundir las comunicaciones relacionadas con el SGSI a todo el personal.
- Mantener los registros de asistencia, participación y resultados de evaluaciones.
- Apoyar en la evaluación del nivel de concientización del personal.

d. Colaboradores

Usuarios finales y actores clave en la protección de la información de la organización. Tienen como responsabilidades:

- Participar activamente en las actividades de concientización, capacitación y evaluación.
- Cumplir las políticas, procedimientos y controles del SGSI.
- Aplicar las buenas prácticas de Seguridad de la Información en su trabajo diario.
- Proteger la información de la organización y de los clientes.

7. Descripción general del plan

a. Instrumentos de capacitación y sensibilización:

Los instrumentos son los materiales y herramientas concretas utilizadas para transmitir el contenido de cada actividad:

- Presentaciones digitales y diapositivas.
- Videos cortos explicativos.
- Guías y materiales de lectura digital.
- Infografías y banners.
- Boletines digitales.
- Encuestas y formularios de evaluación (diagnóstica, de cierre y periódica).

- Casos prácticos y escenarios simulados.
- Plataformas de simulación de phishing e ingeniería social (ej. GoPhish o equivalente).
- Reportes de resultados de simulacros (insumo para las sesiones de retroalimentación).

b. Modalidades de capacitación y sensibilización:

Las modalidades definen el canal y formato mediante el cual se entrega cada actividad:

- Sesión virtual sincrónica: exposición en tiempo real orientada a la presentación de conceptos generales y lineamientos del SGSI.
- Capacitación técnica virtual: actividad estructurada para reforzar conocimientos específicos según el rol del colaborador.
- Taller virtual participativo: sesión orientada al análisis de casos prácticos y escenarios reales de seguridad.
- Video + guía (asincrónico): material de refuerzo que el colaborador puede revisar a su propio ritmo.
- Campaña digital por correo electrónico: difusión periódica de mensajes de concientización a través de medios digitales internos.
- Actividad virtual lúdica (concursos / trivias): formato gamificado para reforzar conocimientos y medir el nivel de concientización.
- Simulación práctica no anunciada: ejercicio controlado de ingeniería social ejecutado sin previo aviso, seguido de una sesión de retroalimentación virtual.
- Formulario digital en línea: modalidad asincrónica utilizada para la aplicación de encuestas diagnósticas y evaluaciones periódicas.

8. Programa periódico de capacitación y evaluación

Con el fin de garantizar la mejora continua del nivel de concientización del personal, el plan se organiza en cuatro ciclos trimestrales a lo largo del año. Cada ciclo combina actividades de capacitación, campañas de sensibilización, simulacros de ingeniería social y evaluaciones de conocimiento, permitiendo medir la evolución del personal y ajustar las acciones según los resultados obtenidos.

El siguiente cuadro resume el programa anual de actividades por ciclo:

Tabla 1
Cronograma anual de actividades

Ciclo	Mes	Actividad Principal	Evaluación	Meta
Ciclo 1	Mes 1-2	Diagnóstico + Capacitación base SGSI	Encuesta diagnóstica inicial	100% participación
	Mes 3	Campaña amenazas + Simulacro phishing #1	Tasa de detección simulacro	≥ 50% detección
Ciclo 2	Mes 4-5	Capacitación técnica (roles específicos)	Evaluación técnica escrita	≥ 85% aprobación
	Mes 6	Simulacro ingeniería social #2 + Taller	Tasa de detección + reporte	≥ 65% detección
Ciclo 3	Mes 7-8	Campaña avanzada + Trivia/Concurso	Concurso de conocimientos	≥ 80% aprobación
	Mes 9	Simulacro combinado #3 + Retroalimentación	Informe comparativo ciclos	Mejora progresiva
Ciclo 4	Mes 10-11	Capacitación roles + Actualización temas	Evaluación final anual	≥ 90% aprobación
	Mes 12	Simulacro #4 + Revisión anual del plan	Encuesta diagnóstica final	Mejora vs. inicio

Nota. Elaborado por los investigadores

9. Plan de actividades

A continuación, se detalla el plan de actividades mediante las tablas presentadas a continuación :

Tabla 2
Planificación de la actividad N°1

ACTIVIDAD N°1 : Aplicación de encuesta de conocimientos al personal involucrado en el alcance del SGSI	
Objetivo	Medir el nivel de conocimiento de los colaboradores respecto al SGSI, con el fin de identificar brechas y definir acciones de capacitación y sensibilización.

Descripción de la actividad	Diseñar y aplicar una encuesta virtual de conocimientos básicos en Seguridad de la Información al inicio y al cierre de cada año, permitiendo comparar la evolución del nivel de concientización.
Instrumentos	Encuesta digital (formularios en línea — Google Forms o equivalente).
Modalidad	Formulario digital en línea (asincrónico).
Periodicidad	Al inicio del año (diagnóstico), al cierre del año (evaluación final) y al ingreso de nuevos colaboradores.
Recursos	Jefe de TI, RR. HH y Formulario Drive
Indicador	Porcentaje de colaboradores que completan la encuesta y variación del puntaje promedio entre diagnóstico inicial y evaluación final.
Meta	100% de participación. Mejora de al menos 20% en el puntaje promedio respecto al diagnóstico inicial.
Resultados	Información que permita determinar el nivel de conocimiento del personal sobre Seguridad de la Información, priorizar temas a reforzar y medir la efectividad del plan a lo largo del tiempo.

Nota. Elaborado por los investigadores.

Tabla 3

Planificación de la actividad N°2

ACTIVIDAD N°2 : Capacitación base en Seguridad de Información y SGSI	
Objetivo	Proporcionar a los colaboradores los conocimientos básicos sobre Seguridad de Información y el SGSI de Iteprevengo.
Descripción de la actividad	Planificar y ejecutar capacitaciones introductorias mediante sesiones interactivas. Cada sesión incluirá preguntas, dinámicas de interacción (juegos, trivias) y una encuesta de cierre. Las actividades se realizarán dentro del horario laboral.
Instrumentos	Presentaciones digitales, guías breves, videos cortos, registros de participación y encuesta digital.
Modalidad	Sesiones virtuales de (60 minutos por sesión).
Periodicidad	Anual (inicio de año) y al ingreso de nuevos colaboradores.
Duración	Una semana
Recursos	Jefe de TI, RR. HH, Plataforma Meet

Indicador	Porcentaje de colaboradores que participan en las sesiones de capacitación.
Meta	100% de participación de los colaboradores
Resultados	Colaboradores sensibilizados y con conocimientos básicos fortalecidos en Seguridad de la Información y en el SGSI de Iteprevengo.
Temas	- Conceptos básicos de Seguridad de la Información. - Principios de confidencialidad, integridad y disponibilidad. - ¿Qué es el SGSI y por qué es importante para Iteprevengo? - Alcance del SGSI (desarrollo y soporte del software SaaS). - Roles y responsabilidades en Seguridad de la Información. - Riesgos del trabajo remoto. - Uso seguro de servicios en la nube. - Gestión y reporte de incidentes de Seguridad de la Información.

Nota. Elaborado por los investigadores.

Tabla 4

Planificación de la actividad N°3

ACTIVIDAD N°3 : Campaña de sensibilización sobre amenazas informáticas	
Objetivo	Sensibilizar a los colaboradores sobre las principales amenazas informáticas, fortaleciendo la identificación de riesgos y la adopción de buenas prácticas en un entorno remoto y cloud
Descripción de la actividad	Diseñar y difundir campañas de sensibilización mediante correo electrónico con infografías, banners y boletines sobre amenazas informáticas actuales.
Instrumentos	Infografías, banners y boletines digitales.
Modalidad	Campaña digital
Periodicidad	Como mínimo 4 veces al mes, con mayor frecuencia previa a los simulacros de ingeniería social.
Recursos	Jefe de TI, RR. HH y, correo corporativo.
Indicador	Número de campañas de sensibilización realizadas.
Meta	>= 8 campañas de sensibilización al año
Resultados	Colaboradores informados y sensibilizados sobre las principales amenazas informáticas, con mayor capacidad para identificar situaciones de riesgo y aplicar buenas prácticas.
Temas	- Phishing y correos electrónicos maliciosos.

	- Spear phishing. - Malware: virus, gusanos, troyanos, ransomware y keyloggers. - Ataques de denegación de servicio. - Ingeniería social en entornos remotos. - Riesgos asociados al uso de dispositivos personales (BYOD). - Seguridad en redes Wi-Fi domésticas y públicas. - Uso seguro de contraseñas y autenticación multifactor (MFA).

Nota. Elaborado por los investigadores.

Tabla 5

Planificación de la actividad N°4

ACTIVIDAD N° 4 : Capacitación y simulacros sobre amenazas informáticas	
Objetivo	Fortalecer las capacidades de los colaboradores para identificar, comprender, prevenir y responder ante amenazas informáticas, profundizando los conceptos abordados en las campañas de sensibilización y conectándolos con los resultados de los simulacros.
Descripción de la actividad	Planificar y ejecutar capacitaciones y talleres virtuales orientados a la gestión de riesgos informáticos. Cada sesión incluirá análisis de casos reales, dinámicas de interacción y una encuesta de cierre. Se aprovecharán los resultados de los simulacros de ingeniería social para contextualizar los temas y reforzar los comportamientos correctos.
Instrumentos	Presentaciones digitales, casos prácticos y encuestas de retroalimentación.
Modalidad	Capacitación técnica virtual / Taller virtual participativo
Periodicidad	Mensual (capacitación). Sesiones de retroalimentación de simulacros: trimestral.
Duración	Todo el año
Recursos	Jefe de TI, RR. HH., plataforma Meet
Indicador	- Porcentaje de participación en capacitaciones. - Puntaje promedio en evaluaciones de cierre de sesión.
Meta	- 100% de participación del personal. - ≥ 80% de aprobación en evaluaciones de cierre. -
Resultados	Colaboradores con mayor capacidad para identificar riesgos informáticos y aplicar buenas prácticas de seguridad en sus actividades diarias, con mejora medible en cada ciclo del programa periódico.
Temas	- Phishing y correos electrónicos maliciosos. - Spear phishing.

	- Malware: virus, gusanos, troyanos, ransomware y keyloggers. - Ataques de denegación de servicio. - Ingeniería social en entornos remotos. - Riesgos asociados al uso de dispositivos personales (BYOD). - Seguridad en redes Wi-Fi domésticas y públicas.

Nota. Elaborado por los investigadores.

Tabla 6

Planificación de la actividad N°5

ACTIVIDAD N°5 : Sesiones de capacitación técnica en Seguridad de la Información	
Objetivo	Fortalecer los conocimientos y competencias del personal de Iteprevengo en temas específicos de Seguridad de la Información, de acuerdo con sus roles y responsabilidades dentro de los procesos de desarrollo y soporte del software SaaS.
Descripción de la actividad	Planificar y ejecutar sesiones de capacitación técnica, con énfasis en los riesgos y controles aplicables a sus funciones. Los contenidos estarán enfocados en riesgos reales aplicables a las actividades diarias y en la forma correcta de prevenirlos o reportarlos, reforzando los lineamientos del SGSI.
Instrumentos	Presentaciones digitales, casos prácticos y encuestas de retroalimentación.
Modalidad	Capacitación técnica virtual / Taller virtual participativo.
Audiencia	Personal técnico (desarrollo y soporte del software SaaS).
Periodicidad	Una vez al mes o según necesidad identificada en las evaluaciones del programa periódico.
Recursos	Jefe de TI, RR. HH y plataforma Meet
Indicador	Porcentaje de colaboradores técnicos capacitados y puntaje de evaluación técnica por ciclo.
Meta	100% de participación del personal técnico. ≥ 85% de aprobación en evaluaciones técnicas.
Resultados	Personal técnico con conocimientos fortalecidos en Seguridad de la Información, aplicables a sus funciones dentro del desarrollo y soporte del software SaaS.
Temas	- Metodología de gestión de riesgos del SGSI - Identificación y tratamiento de riesgos en entornos SaaS - Gestión de accesos y control de privilegios - Principio de mínimo privilegio - Gestión segura de credenciales y secretos

	- Autenticación multifactor (MFA) y controles de acceso - Uso seguro de repositorios de código - Protección de información sensible en el desarrollo - Buenas prácticas básicas de desarrollo seguro - Gestión de cambios y control de versiones - Uso seguro de servicios en la nube - Configuración segura de entornos cloud - Gestión de vulnerabilidades técnicas - Manejo seguro de logs y monitoreo - Gestión técnica de incidentes de Seguridad de la Información - Respaldo y recuperación de información (backups) - Continuidad del servicio en entornos SaaS

Nota. Elaborado por los investigadores.

Tabla 7

Planificación de la actividad N°6

ACTIVIDAD N° 6 : Simulacros de Ingeniería Social	
Objetivo	Evaluar el comportamiento real de los colaboradores ante ataques controlados de ingeniería social, identificando brechas de comportamiento y fortaleciendo la capacidad de detección y respuesta ante amenazas reales.
Descripción de la actividad	Implementar simulacros periódicos y no anunciados de ingeniería social, tales como: campañas controladas de phishing, envío de correos electrónicos simulados, mensajes fraudulentos (smishing/vishing) y escenarios de suplantación de identidad. Los resultados de cada simulacro serán analizados por el Jefe de TI y comunicados al equipo con fines formativos, no punitivos. Cada simulacro incluirá una sesión de retroalimentación posterior donde se explique qué señales debieron identificarse.
Instrumentos	Plataformas de simulación de phishing (GoPhish u equivalente), herramientas de análisis de resultados y reportes de métricas.
Modalidad	Simulación práctica (no anunciada) + Sesión de retroalimentación virtual.
Periodicidad	Trimestral (4 simulacros al año, uno por ciclo del programa periódico).
Duración	Todo el año
Recursos	Jefe de TI, RR. HH., herramientas de simulación de ataques de ingeniería social, plataforma Meet para retroalimentación
Indicador	- Tasa de usuarios que hacen clic en el enlace de phishing simulado (click rate).

	- Tasa de usuarios que reportan el correo simulado como sospechoso (report rate). - Tasa de usuarios que ingresan credenciales en el sitio simulado (credential submission rate). - Evolución de indicadores entre simulacros (mejora progresiva).
Meta	- Reducción progresiva de la tasa de clics en simulacros: de ≤ 50% en el simulacro #1 a ≤ 10% en el simulacro #4. - Incremento de la tasa de reporte de correos sospechosos: de ≥ 20% en el #1 a ≥ 70% en el #4. - 100% de participación en las sesiones de retroalimentación.
Resultados	Colaboradores con mayor capacidad para identificar y reportar intentos de ingeniería social, comportamiento de seguridad mejorado y métricas comparables entre ciclos que demuestren la efectividad del plan.
Temas	- Simulacro #1 (Mes 3): Phishing básico — correo genérico de suplantación. - Simulacro #2 (Mes 6): Spear phishing — correo dirigido con datos contextuales. - Simulacro #3 (Mes 9): Escenario combinado (phishing + suplantación de identidad interna). - Simulacro #4 (Mes 12): Simulacro avanzado con múltiples vectores.

Nota. Elaborado por los investigadores.

10. Validez y gestión documental

El presente documento es válido a partir de su aprobación por la Dirección de Iteprvengo.

El titular de este documento es el Jefe de TI, quien deberá revisarlo y, en su caso, actualizarlo anualmente.

ANEXO 9

SOLICITUD DE AUTORIZACIÓN PARA APLICACIÓN DE LA INVESTIGACIÓN

"Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho"

SOLICITUD: SOLICITUD DE AUTORIZACIÓN PARA APLICACIÓN DE INVESTIGACIÓN ACADÉMICA

Ing. Herbert Parimango
Gerente General de Iteprevengo

Presente.

De nuestra consideración:

Alberca Cubas Kevin, identificado con **DNI N° 73036252** y **Guerrero Diaz Lalita**, identificada con **DNI N° 75532935,** nos dirigimos a usted para saludarlo cordialmente y, a la vez, solicitar respetuosamente su autorización formal para aplicar una investigación académica en la empresa ItePrevengo, en el marco de nuestro trabajo titulado:

"Sistema de Gestión de la Seguridad de la Información para los procesos de soporte y desarrollo de software SaaS de la empresa ItePrevengo".

La presente investigación tiene como finalidad diseñar un Sistema de Gestión de la Seguridad de la Información (SGSI), alineado a las NTP ISO/IEC 27001:2022, enfocado en los procesos de soporte y desarrollo de software, con el propósito de fortalecer la protección de la información, mejorar la gestión de riesgos y contribuir a la mejora continua de los procesos organizacionales.

Para el desarrollo del estudio, se requiere recopilar información mediante la aplicación de instrumentos de evaluación, entrevistas y análisis documental, los cuales serán utilizados únicamente con fines académicos. Es importante señalar que toda la información obtenida será tratada con estricta confidencialidad, respetando los principios éticos de la investigación, y no se divulgarán datos sensibles ni estratégicos de la organización.

Agradecemos de antemano la atención brindada a la presente solicitud y quedamos a su disposición para ampliar cualquier información que considere necesaria.

Sin otro particular, nos despedimos reiterándole nuestro agradecimiento.

Atentamente,

Chiclayo, 10 de julio del 2024

Alberca Cubas Kevin
DNI N° 73036252
kevinalbercacubas@gmail.com
Cel: 970324811

Guerrero Díaz Lalita
DNI N° 75532935
guerrerodiazlalita@gmail.com
Cel: 998813025

ANEXO 10

CARTA DE AUTORIZACIÓN PARA INICIO DE LA INVESTIGACIÓN

CARTA DE AUTORIZACIÓN

Trujillo, 30 de julio de 2024

Señores:
Alberca Cubas Kevin y Guerrero Díaz Lalita
Presente.-

ASUNTO: AUTORIZACIÓN PARA APLICACIÓN DE INVESTIGACIÓN ACADÉMICA

De nuestra consideración:
En atención a la solicitud presentada con fecha 10 de julio de 2024, respecto a la autorización para desarrollar la investigación titulada:
"Sistema de Gestión de la Seguridad de la Información para los procesos de soporte y desarrollo de software SaaS de la empresa Iteprevengo",
nos es grato comunicarles que Iteprevengo autoriza la aplicación de la investigación académica en nuestra organización, en el marco del desarrollo de su trabajo.

La presente autorización comprende el acceso a información necesaria para la ejecución del estudio, así como la aplicación de entrevistas, instrumentos de evaluación y análisis documental, siempre que se respeten los principios de confidencialidad, uso exclusivo con fines académicos y protección de la información sensible de la empresa.

Asimismo, se deja constancia de que cualquier información estratégica, datos personales o información clasificada deberá ser tratada conforme a los lineamientos internos de la organización y no podrá ser divulgada sin autorización expresa.

Sin otro particular, reiteramos nuestra disposición para colaborar con el desarrollo del estudio.

Atentamente,

Ing. Herbert Parimango Rodríguez
GERENTE GENERAL

ANEXO 11

GUIAS DE ENTREVISTA UTILIZADAS

Tabla 1

Guía de entrevista basada en los requisitos de la NTP ISO/IEC 27001

REQUISITOS DE LA NORMA ISO 27001:2022		CRITERIOS	PREGUNTA RELACIONADA
CONTEXTO DE LA ORGANIZACIÓN			
4.1) Contexto organizacional: Determinar las cuestiones externas e internas que son pertinentes para su propósito y que afectan su capacidad de lograr el resultado(s) previstos de su SGSI		Existencia	¿Se ha identificado y documentado aspectos internos y externos relevantes (por ejemplo: sector, misión, visión, procesos principales, modelo de negocio, entorno tecnológico, proveedores, regulaciones aplicables)?
		Formalidad	¿Existe un documento formal y aprobado (acta, formato, informe) que describa el análisis del contexto organizacional?
		Implementación	¿Se utiliza el análisis del contexto para tomar decisiones respecto del SGSI (riesgos, alcance, objetivos)?
		Medición / Mejora	¿Cada cuánto se revisa y actualiza el análisis del contexto?
4.2) Partes interesadas	4.2 a) Las partes interesadas pertinentes al SGSI	Existencia	¿La organización ha identificado quiénes son las partes interesadas relevantes para la seguridad de la información?
		Formalidad	¿Existe un registro documentado con la lista de partes interesadas?
		Implementación	¿Se consultan o consideran estas partes interesadas para definir riesgos, controles, procesos o servicios del SGSI?
		Medición / Mejora	¿Se revisa o actualiza la lista de partes interesadas cuando cambian los servicios, los contratos o el modelo de trabajo?

	4.2 b) Los requisitos pertinentes de estas partes interesadas	Existencia	¿Se han identificado los requisitos (legales, contractuales, regulatorios, SLA, expectativas) de cada parte interesada?
		Formalidad	¿Existe un registro documentado y aprobado donde se describen estos requisitos?
		Implementación	¿La organización gestiona y cumple estos requisitos en procesos y controles?
		Medición / Mejora	¿Se revisan estos requisitos ante cambios regulatorios, nuevas leyes, modificaciones de contratos o incorporación de nuevos clientes?
	4.2 c) Cuáles de estos requisitos se abordarán mediante el SGSI	Existencia	¿Se ha definido explícitamente qué requisitos de partes interesadas serán cubiertos por el SGSI?
		Formalidad	¿Los criterios de inclusión/exclusión están documentados y justificados formalmente?
		Implementación	¿El alcance y los controles del SGSI reflejan fielmente los requisitos seleccionados?
		Medición / Mejora	¿El listado se actualiza cuando cambian procesos, servicios o requisitos contractuales?
4.3 Determinar el alcance del SGSI		Existencia	¿La organización cuenta con un alcance formalmente definido para el SGSI?
		Formalidad	¿Está documentado, describe límites, procesos, ubicaciones, servicios y exclusiones justificadas?
		Implementación	¿Las actividades y procesos operan de acuerdo con lo definido en el alcance?
		Medición / Mejora	¿Se revisa y actualiza el alcance ante cambios organizacionales o tecnológicos?
4.4 SGSI: La organización debe establecer, implementar, mantener y mejorar continuamente un SGSI, en		Existencia	¿Se han establecido los elementos fundamentales del SGSI (políticas, procesos, roles, controles)?
		Formalidad	¿Existe documentación oficial, aprobada y controlada del SGSI (manual, políticas, procedimientos, roles)?

conformidad con los requisitos de esta Norma Técnica Peruana	Implementación	¿Los procesos y controles del SGSI se aplican realmente en la operación diaria?
	Medición / Mejora	¿Se realizan auditorías, revisiones, mediciones e iniciativas de mejora continua sobre el SGSI?
LIDERAZGO		
5.1) Liderazgo y compromiso	Existencia	¿La dirección manifiesta su compromiso con la seguridad de la información de manera visible (comunicaciones, participación, iniciativas, decisiones)?
	Formalidad	¿Existe evidencia documentada del compromiso de la dirección (reuniones, comunicaciones, asignación de recursos)?
	Implementación	¿La dirección participa realmente en decisiones del SGSI, asignación de presupuesto, resolución de brechas, aprobación de políticas o revisión de riesgos?
	Medición / Mejora	¿La dirección revisa periódicamente el desempeño del SGSI y toma acciones de mejora (revisión por la dirección, seguimiento de indicadores, acciones correctivas)?
5.2) Política	Existencia	¿La organización cuenta con una política de seguridad de la información formalmente redactada?
	Formalidad	¿La política está aprobada por la alta dirección, versionada, actualizada y comunicada a los colaboradores y partes interesadas pertinentes?
	Implementación	¿El personal conoce y aplica la política de seguridad?
	Medición / Mejora	¿Se revisa periódicamente la política o ante cambios organizacionales, regulatorios o tecnológicos?
5.3) Roles, responsabilidades y autoridades en la organización.	Existencia	¿Se han definido roles y responsabilidades relacionadas con la seguridad, ya sea por puesto, función o actividad?
	Formalidad	¿Los roles están documentados en organigramas, descripciones de puesto, políticas o procedimientos del SGSI?

		Implementación	¿El personal conoce sus responsabilidades y las aplica en la práctica?
		Medición / Mejora	¿Se revisan y actualizan los roles ante cambios organizacionales o tecnológicos?
PLANIFICACIÓN			
6.1)Acciones para tratar con los riesgos y oportunidades	6.1.1) Diseñar/ planificar el SGSI para satisfacer los requisitos, tratando con los riesgos y oportunidades.	Existencia	¿Se han identificado riesgos y oportunidades relacionados con la seguridad?
		Formalidad	¿Existe una metodología o lineamiento documentado que integre el análisis del contexto, las partes interesadas y el alcance dentro de la planificación del SGSI?
		Implementación	¿Las acciones del SGSI se basan efectivamente en el contexto, requisitos y alcance?
		Medición / Mejora	¿Se revisa esta integración ante cambios organizacionales?
	6.1.2) Definir y aplicar un proceso de apreciación de riesgos de seguridad de información.	Existencia	¿La organización cuenta con una metodología definida para identificar, analizar y evaluar riesgos de seguridad de la información?
		Formalidad	¿La metodología está documentada, aprobada y contiene criterios de impacto, probabilidad, evaluación del nivel de riesgo y criterios de aceptación?
		Implementación	¿La organización aplica esta metodología para evaluar riesgos ?
		Medición / Mejora	¿La metodología se revisa y mejora periódicamente, o ante incidentes o cambios significativos?
	6.1.3) Documentar y aplicar un proceso de tratamiento de riesgos de seguridad de la información	Existencia	¿Se han definido opciones de tratamiento para cada riesgo identificado (evitar, mitigar, transferir o aceptar)?
		Formalidad	¿Existe un plan de tratamiento documentado con controles seleccionados y justificados (incluyendo el Anexo A)?
		Implementación	¿Las acciones y controles del plan de tratamiento se ejecutan realmente?

		Medición / Mejora	¿Se revisa el riesgo residual y la eficacia de los controles implementados?
6,2) Objetivos y planes de seguridad de información: Establecer y documentar los objetivos y planes de la seguridad de la información.		Existencia	¿Se han definido objetivos de seguridad de la información?
		Formalidad	¿Los objetivos están documentados, aprobados, alineados al SGSI y son medibles mediante indicadores?
		Implementación	¿Se están ejecutando acciones o planes para alcanzar estos objetivos?
		Medición / Mejora	¿Se realiza seguimiento mediante indicadores, revisión de desempeño o informes?
6,3) Planificación de cambios: Los cambios sustanciales al SGSI deben ser llevados de manera planificada.		Existencia	¿Se han identificado cambios que pueden afectar el SGSI (nuevas funciones SaaS, cambios en servidores cloud, personal, proveedores)?
		Formalidad	¿Existe un proceso documentado para planificar, aprobar, evaluar riesgos y comunicar los cambios?
		Implementación	¿El proceso se aplica efectivamente cuando ocurren cambios reales en sistemas, tecnología o procesos?
		Medición / Mejora	¿Se revisa la eficacia del proceso de gestión de cambios y se actualiza cuando es necesario?
SOPORTE			
7,1) Recursos: Determinar y proporcionar los recursos necesarios para el SGSI.		Existencia	¿Se han identificado los recursos necesarios para implementar y mantener el SGSI?
		Formalidad	¿Existe documentación o planificación que describa los recursos asignados (humanos, tecnológicos, financieros, etc)?
		Implementación	¿Los recursos identificados se están proporcionando realmente a las áreas responsables del SGSI?
		Medición / Mejora	¿La asignación de recursos se revisa y ajusta periódicamente según prioridades, incidentes o nuevas necesidades?

7,2) Competencias: Determinar, documentar y poner a disposición las competencias necesarias.		Existencia	¿Se han identificado las competencias necesarias para roles vinculados a la seguridad de la información (TI, desarrolladores, responsables de SGSI, soporte)?
		Formalidad	¿Existe evidencia de evaluación de competencias, perfiles de puesto o planes de capacitación técnica y de seguridad?
		Implementación	¿El personal recibe capacitaciones y entrenamientos adecuados según sus responsabilidades?
		Medición / Mejora	¿Las competencias se evalúan periódicamente y se actualizan según cambios tecnológicos o normativos?
7,3) Concientización: Establecer un programa de concientización de seguridad.		Existencia	¿Existe un programa o acciones de concientización en seguridad de la información?
		Formalidad	¿Están documentadas las actividades de concientización (temas, frecuencia, responsables)?
		Implementación	¿El personal recibe regularmente información, recordatorios o formación sobre seguridad?
		Medición / Mejora	¿Se evalúa la efectividad de las campañas (test, métricas, incidentes, simulaciones)?
7,4) Comunicación: Determinar la necesidad para las comunicaciones internas y externas relevantes al SGSI.		Existencia	¿Se han identificado necesidades de comunicación interna y externa relacionadas con la seguridad de la información?
		Formalidad	¿Existe un plan o procedimiento que describa cómo se difunden políticas, incidentes, roles, requisitos legales o cambios?
		Implementación	¿Se comunican efectivamente políticas, cambios, incidentes, requisitos y roles?
		Medición / Mejora	¿Se revisa la efectividad de los canales y métodos de comunicación utilizados (emails, reuniones, plataforma interna)?
7,5	7.5.1) Proveer la documentación requerida por la norma	Existencia	¿Existe claridad respecto a qué documentación es obligatoria para el SGSI?
		Formalidad	¿Se han definido una estructura documental y un procedimiento para su control?

Información documentada	así como la requerida por la organización.	Implementación	¿Los documentos se elaboran, mantienen y almacenan conforme a las reglas establecidas?
		Medición / Mejora	¿Se revisan periódicamente los documentos para asegurar pertinencia y completitud?
	7.5.2) Proveer títulos, autores, etc, para la documentación, adecuar el formato consistentemente, revisarlo y aprobarlos.	Existencia	¿La creación o actualización de documentos sigue un proceso formal?
		Formalidad	¿Los documentos incluyen atributos como versión, autor, fecha, aprobador y control de cambios?
		Implementación	¿Los responsables crean y actualizan documentos usando el proceso definido?
		Medición / Mejora	¿Se verifica periódicamente si la documentación está actualizada?
	7.5.3) Controlar la documentación adecuadamente.	Existencia	¿Existe un proceso formal para controlar, proteger y asegurar los documentos del SGSI?
		Formalidad	¿Se han definido métodos de almacenamiento, acceso, permisos, distribución, recuperación y retención?
		Implementación	¿Los documentos se almacenan correctamente (por ejemplo, en repositorios cloud con permisos)?
		Medición / Mejora	¿Se revisa la eficacia del control documental y se mejora si es necesario?
OPERACIÓN			
8,1 Planificación y control operacional: Planificar, implementar, controlar y documentar el proceso de SGSI para gestionar los riesgos.		Existencia	¿Se han identificado los procesos operativos necesarios para cumplir con los requisitos del SGSI?
		Formalidad	¿Estos procesos están documentados mediante políticas, procedimientos, instructivos, flujogramas o matrices de roles?
		Implementación	¿Los procesos se ejecutan tal como están definidos?

	Medición / Mejora	¿Se monitorea la eficacia de los procesos y se actualizan cuando es necesario?
8,2 Evaluación de riesgos de seguridad de la información: RE-hacer la apreciación y documentación de los riesgos de seguridad de la información en forma regular y ante cambios o modificaciones.	Existencia	¿Se realizan reevaluaciones de riesgos cuando se implementan cambios operativos relevantes?
	Formalidad	¿Existe un procedimiento que establezca cuándo debe reevaluarse el riesgo?
	Implementación	¿Se evalúa realmente los riesgos antes de implementar cambios o mejoras importantes?
	Medición / Mejora	¿¿Se revisa la calidad de las reevaluaciones y ajusta el proceso cuando se detectan debilidades?
8,3 Tratamiento de riesgo de seguridad de la información: Implementar el plan de tratamiento de riesgo y documentar los resultados.	Existencia	¿Se han definido acciones específicas para tratar los riesgos que afectan a la operación del negocio y los servicios SaaS?
	Formalidad	¿Existe un plan de tratamiento vigente que incluya controles seleccionados del Anexo A, responsables y plazos?
	Implementación	Las acciones, controles y medidas definidas en el plan de tratamiento se ejecutan realmente en la operación diaria?
	Medición / Mejora	¿Se revisa regularmente el riesgo residual y verifica la efectividad de los controles implementados?
EVALUACIÓN DEL DESEMPEÑO		
9,1 Seguimiento, medición, análisis y evaluación : Hacer seguimiento, medir, analizar y evaluar el SGSI y los controles.	Existencia	¿Se ha identificado qué elementos del SGSI deben medirse o monitorearse (controles, incidentes, cumplimiento, disponibilidad, desempeño operativo, etc.)?
	Formalidad	¿Existen métricas, indicadores o métodos documentados para medir el desempeño del SGSI?
	Implementación	¿Se recopilan datos reales periódicamente y se realizan actividades de seguimiento y medición?

	Medición / Mejora	¿Los resultados se analizan y se toman decisiones o acciones de mejora basadas en ellos?
9,2 Auditoría interna : Planificar y llevar a cabo auditorías internas del SGSI.	Existencia	¿La organización reconoce la necesidad de realizar auditorías internas del SGSI?
	Formalidad	¿Existe un programa o plan de auditoría interna documentado?
	Implementación	¿Se han realizado auditorías internas siguiendo los criterios definidos?
	Medición / Mejora	¿Los resultados de las auditorías internas se analizan y se ejecutan acciones correctivas y de mejora cuando corresponda?
9,3 Revisión por la dirección: Emprender revisiones por la dirección del SGSI regularmente.	Existencia	¿La dirección realiza revisiones del SGSI?
	Formalidad	¿Existe agenda, actas o informes asociados a la revisión por la dirección?
	Implementación	¿La revisión se realiza realmente y se analizan los aspectos clave: incidentes, desempeño, recursos, riesgos,cu mplimiento, etc.?
	Medición / Mejora	¿Se generan decisiones, acuerdos o acciones de mejora que quedan documentadas y se les da seguimiento?
MEJORA		
10,1 Mejora Continua: La organización debe mejorar continuamente la idoneidad, adecuación y eficacia del SGSI.	Existencia	¿La organización reconoce la necesidad de mejorar el SGSI de manera continua?
	Formalidad	¿Existe un mecanismo documentado (revisiones, auditorías, métricas) que impulse la mejora del SGSI?
	Implementación	¿Las mejoras identificadas en revisiones, auditorías o análisis de desempeño se implementan realmente en procesos, controles, políticas o documentación?
	Medición / Mejora	¿Se evalúa si las mejoras realizadas han sido eficaces y contribuyen realmente al fortalecimiento del SGSI?

10,2 No conformidad con acciones correctivas: Identificar, corregir y llevar a cabo acciones para prevenir la recurrencia de no conformidades, documentación de las acciones.	Existencia	¿Se identifica y registra las no conformidades relacionadas con el SGSI?
	Formalidad	Existe un procedimiento documentado para gestionar no conformidades y acciones correctivas?
	Implementación	¿Se aplican acciones correctivas cuando ocurre un incidente, fallo de control o incumplimiento?
	Medición / Mejora	¿La organización revisa la eficacia de las acciones correctivas implementadas?

Nota. Elaborado por los investigadores.

Tabla 2

Guía de entrevista basada en los controles del Anexo A de la NTP ISO/IEC 27001

CONTROLES DEL ANEXO A	CRITERIOS	PREGUNTA RELACIONADA
CONTROLES ORGANIZACIONALES		
5.1 Políticas para la seguridad de la información	Existencia	¿Existe una política o conjunto de políticas de seguridad?
	Formalidad	¿La política está aprobada por la dirección, versionada y publicada?
	Implementación	¿El personal conoce y aplica la política?
	Medición / Mejora	¿Se revisa periódicamente la política y se actualiza según cambios?
5.2 Roles y responsabilidades en seguridad de la información	Existencia	¿Se han definido roles y responsabilidades específicas de seguridad?
	Formalidad	¿Están documentadas en perfiles de puesto, organigramas, procedimientos o matrices RACI?
	Implementación	¿El personal conoce y cumple las funciones asignadas?

	Medición / Mejora	¿Se revisan y ajustan los roles ante cambios organizacionales?
5.3 Segregación de funciones	Existencia	¿La organización reconoce funciones que deben estar separadas para evitar conflictos o errores? ¿Se ha identificado si existen actividades que necesitan segregación de funciones?
	Formalidad	¿Existe documentación que establezca segregación (ej. desarrollo vs. despliegue)? ¿Hay reglas documentadas para separar funciones críticas?
	Implementación	¿La segregación realmente se cumple en la práctica?
	Medición / Mejora	¿Se revisa la segregación para evitar conflictos de intereses?
5.4 Responsabilidades de la gerencia	Existencia	¿La gerencia asume responsabilidades explícitas sobre la seguridad?
	Formalidad	¿Existen evidencias documentadas de su rol en el SGSI?
	Implementación	¿La gerencia apoya y supervisa la seguridad en la operación?
	Medición / Mejora	¿La gerencia revisa y mejora sus responsabilidades?
5.5 Contacto de autoridades	Existencia	¿Se han identificado las autoridades relevantes (policía, fiscalía, reguladores)?
	Formalidad	¿Existe un procedimiento para contactar autoridades ante incidentes?
	Implementación	¿El personal sabe cuándo y cómo activar este contacto?
	Medición / Mejora	¿Se revisa periódicamente si la información de contacto está actualizada?
5.6 Contacto con grupos especiales de interés	Existencia	¿La organización identifica grupos relevantes (CERTs, comunidades de seguridad, asociaciones)?
	Formalidad	¿Hay un registro documentado de estos grupos?
	Implementación	¿Se mantienen relaciones activas o intercambio de información?

	Medición / Mejora	¿Se actualiza la lista de grupos según necesidades?
5.7 Inteligencia de amenazas	Existencia	¿La empresa recopila información sobre amenazas relevantes?
	Formalidad	¿Existe un mecanismo o fuente definida (feeds, boletines, proveedores)? I
	Implementación	¿Se analizan estas amenazas y se aplican ajustes?
	Medición / Mejora	¿Se revisa la utilidad y vigencia de las fuentes de información?
5.8 Seguridad de la información en gestión de proyectos	Existencia	¿Los proyectos consideran requisitos de seguridad desde el inicio?
	Formalidad	¿Existe un procedimiento para incluir seguridad en la gestión de proyectos?
	Implementación	¿Los proyectos SaaS integran revisiones de seguridad (código, arquitectura, acceso)?
	Medición / Mejora	¿Se revisa y mejora la integración de seguridad en proyectos?
5.9 Inventario de información y otros activos asociados	Existencia	¿Existe un inventario de activos de información?
	Formalidad	¿Está documentado y actualizado (propietario, clasificación, ubicación)?
	Implementación	¿El inventario se usa realmente para riesgos y controles?
	Medición / Mejora	¿Se revisa y actualiza periódicamente?
5.10 Uso aceptable de la información y otros activos asociados	Existencia	¿Existe una política o lineamientos sobre el uso aceptable de activos?
	Formalidad	¿Está documentada, aprobada y comunicada?
	Implementación	¿El personal conoce y cumple las reglas (equipos, correo, nube)?

	Medición / Mejora	¿Se revisa y actualiza según riesgos o incidentes?
5.11 Devolución de activos	Existencia	¿Se exige la devolución de activos cuando una persona deja de trabajar o cambia de puesto?
	Formalidad	¿Existe un procedimiento o checklist formal para devolución de activos?
	Implementación	¿Se ejecuta este proceso en cada baja o cambio?
	Medición / Mejora	¿Se verifica el estado y la integridad de los activos devueltos?
5.12 Clasificación de la información	Existencia	¿Se han definido categorías de clasificación de la información basadas en su sensibilidad (p. ej., pública, interna, confidencial)?
	Formalidad	¿Estas categorías están documentadas en una política formal o lineamiento?
	Implementación	¿El personal aplica consistentemente la clasificación al crear, almacenar o compartir información?
	Medición / Mejora	¿Se evalúa periódicamente si la clasificación sigue siendo adecuada o si requiere ajustes?
5.13 Etiquetado de la información	Existencia	¿Hay directrices para etiquetar información según su clasificación?
	Formalidad	¿Existe alguna directiva documentada que establezca cómo se debe etiquetar la información física y digital?
	Implementación	¿Los usuarios aplican etiquetas o marcas (ej., “Confidencial”) en documentos, repositorios, carpetas o correos según corresponda?
	Medición / Mejora	¿Se verifica la correcta aplicación de etiquetas?
5.14 Transferencia de la información	Existencia	¿La organización identifica los tipos de información que se transfieren dentro y fuera de la empresa?

	Formalidad	¿Existe un procedimiento documentado que defina los mecanismos seguros de transferencia (cifrado, canales autorizados, responsable de envío)?
	Implementación	¿Los colaboradores usan exclusivamente los canales autorizados para transferir información sensible?
	Medición / Mejora	¿Se monitorea o audita la calidad y seguridad de esas transferencias?
5.15 Control de acceso	Existencia	¿Se han definido criterios claros para otorgar y revocar accesos a sistemas, aplicaciones y datos?
	Formalidad	¿Existe una política o procedimiento documentado de control de acceso alineado al principio de privilegio mínimo?
	Implementación	¿Se gestionan los accesos mediante solicitudes formales, revisiones periódicas y segregación por roles?
	Medición / Mejora	¿Se revisan los accesos periódicamente? ¿Se revisan logs, se realizan auditorías y se ajustan los accesos ante desviaciones detectadas?
5.16 Gestión de identidades	Existencia	¿Se ha definido cómo se crean, mantienen y eliminan identidades digitales de usuarios?
	Formalidad	¿Existe un proceso documentado describiendo el ciclo de vida de identidades (creación, modificación, desactivación)?
	Implementación	¿Se aplica el principio de menor privilegio al otorgar accesos? ¿Está implementada la autenticación multifactor en el trabajo remoto?
	Medición / Mejora	¿Se realizan auditorías internas o se revisan periódicamente las identidades para detectar cuentas obsoletas y privilegios excesivos?
5.17 Información de autenticación	Existencia	¿Se utiliza algún mecanismo formal para gestionar credenciales y demás información de autenticación (contraseñas, tokens, llaves, etc.)?

	Formalidad	¿Existe un documento formal (política o procedimiento) que establezca cómo se deben crear, proteger, almacenar y renovar las credenciales?
	Implementación	¿El personal cumple los requisitos definidos para la protección de credenciales (por ejemplo, uso de gestores de contraseñas, MFA, prohibición de compartir claves, almacenamiento seguro de API keys, etc.)?
	Medición / Mejora	¿Se realizan revisiones periódicas o monitoreo para detectar credenciales débiles, filtradas, expiradas o expuestas?
5.18 Derechos de acceso	Existencia	¿Existen definiciones claras respecto a los tipos de derechos (lectura, escritura, administración)?
	Formalidad	¿Hay procedimientos documentados para asignar, modificar y revocar derechos?
	Implementación	¿Se aplican matrices de acceso basadas en roles (RBAC) o perfiles?
	Medición / Mejora	¿Se realizan revisiones de accesos periódicas para detectar permisos inadecuados?
5.19 Seguridad de la información en las relaciones con los proveedores	Existencia	¿Se han identificado los proveedores críticos y los riesgos asociados?
	Formalidad	¿Los contratos incluyen cláusulas de seguridad, confidencialidad y protección de datos?
	Implementación	¿Se supervisa el cumplimiento de los requisitos de seguridad por parte del proveedor?
	Medición / Mejora	¿Se revisan y actualizan los contratos y evaluaciones según cambios en los servicios?
5.20 Abordar la seguridad de la información dentro de los acuerdos con proveedores	Existencia	¿La organización cuenta con acuerdos o contratos que incluyan aspectos de seguridad con sus proveedores?
	Formalidad	¿Existe un documento o cláusula estándar que establezca los requisitos de seguridad que deben incluirse en los acuerdos con proveedores?

	Implementación	¿Se ha incorporado y aplicado estos requisitos de seguridad cada vez que contrata, renueva o modifica un servicio proveedor?
	Medición / Mejora	¿Se revisan los acuerdos para actualizar o reforzar controles ante cambios de riesgo, normativas o servicios?
5.21 Gestión de la seguridad de la información en la cadena de suministro de las tecnologías de la información y comunicación (tic).	Existencia	¿Se ha identificado a los proveedores TIC y a los subproveedores que forman parte de su cadena de suministro?
	Formalidad	¿Existe un documento formal que establezca cómo se deben gestionar los riesgos de seguridad asociados a la cadena de suministro TIC?
	Implementación	Se evalúan los riesgos de los proveedores y se consideran los controles de seguridad que ofrecen antes de contratarlos o renovar el servicio?
	Medición / Mejora	¿Se revisa periódicamente la seguridad de los proveedores TIC y su cadena de suministros?
5.22 Seguimiento, revisión y gestión de cambios en servicios de proveedores	Existencia	¿Se realizan seguimientos a los cambios que los proveedores realizan en sus servicios, equipos, personal o procesos?
	Formalidad	¿Existe un procedimiento documentado que defina cómo se evalúan y gestionan estos cambios?
	Implementación	¿Se revisan los comunicados o avisos de cambios para evaluar su impacto?
	Medición / Mejora	¿Se realiza revisión periódica para evaluar si los cambios han generado incidentes o riesgos?
5.23 Seguridad de la información en el uso de servicios en la nube	Existencia	¿Se han identificado los servicios cloud que utilizan y los riesgos asociados a cada uno?
	Formalidad	¿Existe una política o procedimiento formal que regule el uso seguro de servicios cloud?

	Implementación	¿Se aplican controles de seguridad (cifrado, gestión de acceso, revisiones de configuración, monitoreo, backups) en los servicios cloud actualmente en uso?
	Medición / Mejora	¿Se evalúa periódicamente el nivel de cumplimiento y seguridad del proveedor cloud y de las configuraciones internas?
5.24 Planificación y preparación de la gestión de incidentes de seguridad de la información	Existencia	¿Tienen identificados qué tipos de incidentes pueden afectarles (pérdida de datos, accesos no autorizados, fallas técnicas)?
	Formalidad	¿Existe un procedimiento formal que describa cómo reportar, registrar, escalar y resolver incidentes? ¿Se han definido roles responsables para la gestión de incidentes?
	Implementación	¿El personal sabe a quién avisar y qué pasos seguir si ocurre un incidente?
	Medición / Mejora	¿Se revisan los incidentes para identificar tendencias y oportunidades de mejora? ¿Se realizan simulacros?
5.25 Evaluación y decisión sobre eventos de seguridad de la información	Existencia	¿Se cuenta con un procedimiento que indique cómo evaluar eventos y decidir si califican como incidentes?
	Formalidad	¿Se diferencia entre eventos e incidentes?
	Implementación	¿El personal registra los eventos detectados en algún canal o sistema?
	Medición / Mejora	¿Se revisan las decisiones pasadas para identificar inconsistencias?
5.26 Respuesta a incidentes de seguridad de la información	Existencia	¿Saben qué pasos seguir cuando ocurre un incidente real?
	Formalidad	¿Tienen un procedimiento que indique acciones, responsables y tiempos?
	Implementación	¿La organización ha respondido previamente a incidentes y queda evidencia de cómo actuó?
	Medición / Mejora	¿Se elaboran informes post-incidente?

5.27 Aprendizaje de los incidentes de seguridad de la información	Existencia	¿Se cuenta con un proceso para analizar incidentes después de su resolución?
	Formalidad	Existe un formato o método para documentar las causas y mejoras?
	Implementación	¿Aplican mejoras reales después de incidentes?
	Medición / Mejora	¿Se hace seguimiento a la implementación de las mejoras?
5.28 Recolección de evidencia	Existencia	¿Saben qué información podría servir como evidencia si ocurre un incidente?
	Formalidad	¿Tienen un procedimiento para recopilar y guardar evidencia sin alterarla?
	Implementación	¿El personal sabe cómo preservar logs, correos, archivos o capturas?
	Medición / Mejora	¿Evalúan si el proceso de recolección fue adecuado tras un incidente?
5.29 Seguridad de la información durante una interrupción	Existencia	¿Saben qué debe mantenerse protegido durante una caída de servicio o falla?
	Formalidad	¿Existe un documento que indique cómo se debe gestionar la seguridad durante interrupciones?
	Implementación	¿El personal conoce cómo operar de forma segura cuando los sistemas principales están caídos?
	Medición / Mejora	¿Se realizan simulacros o pruebas de continuidad?¿Revisan si la seguridad se mantuvo correctamente ante interrupciones reales?
5.30 Preparación de las tic para la continuidad del negocio	Existencia	¿Existen identificados los sistemas TI críticos para la continuidad del negocio?
	Formalidad	¿Tienen un plan documentado de continuidad o recuperación TI?

	Implementación	¿Se realizan respaldos, pruebas o simulacros?
	Medición / Mejora	¿Analizan si los tiempos de recuperación fueron adecuados?
5.31 Requisitos legales, estatutarios, regulatorios y contractuales	Existencia	¿La organización sabe qué leyes y obligaciones debe cumplir (por ejemplo: protección de datos, propiedad intelectual, contratos con clientes)?
	Formalidad	¿Tienen una lista documentada de todos estos requisitos y responsables de cumplirlos?
	Implementación	¿Aplican estos requisitos en la práctica (por ejemplo: consentimiento, derechos ARCO, confidencialidad contractual)?
	Medición / Mejora	¿El cumplimiento se revisa periódicamente?
5.32 Derechos de propiedad intelectual	Existencia	¿Se reconoce la importancia de la propiedad intelectual propia y de terceros? ¿Saben qué información, software o contenido está protegido por derechos de PI?
	Formalidad	¿Existen políticas, lineamientos o cláusulas que establezcan cómo se deben usar los materiales protegidos por PI?
	Implementación	¿El personal respeta licencias y evita usar material sin autorización?
	Medición / Mejora	¿Se revisa periódicamente el uso de software, licencias o contenidos para asegurar cumplimiento y detectar riesgos?
5.33 Protección de registros	Existencia	¿Se generan y guardan registros necesarios (logs, auditorías, inventarios, evidencias)?
	Formalidad	¿Existe documentación que defina cómo se crean, almacenan, protegen, retienen y eliminan los registros?
	Implementación	¿El equipo mantiene estos registros accesibles, completos y protegidos?

	Medición / Mejora	¿Se revisa periódicamente la actualización, exactitud y seguridad de los registros documentados?
5.34 Privacidad y protección de la información de identificación personal (iip)	Existencia	¿La organización reconoce que trata datos personales de clientes, trabajadores, aliados o proveedores y que debe protegerlos?
	Formalidad	¿Existen controles específicos para su tratamiento?
	Implementación	¿Se aplican medidas como consentimiento, minimización, derechos ARCO, protección técnica?
	Medición / Mejora	¿Se revisan prácticas de privacidad ante nuevos proyectos o servicios?
5.35 Revisión independiente de la seguridad de la información	Existencia	¿Se realizan auditorías internas de seguridad o de SGSI?
	Formalidad	¿Existe documentación (procedimientos, plan de auditoría, cronograma, definiciones de roles) que establezca cómo se realizan las revisiones independientes?
	Implementación	¿Se han realizado revisiones o auditorías independientes en la práctica? ¿Se aplican criterios imparciales y basados en evidencia?
	Medición / Mejora	¿Se realiza seguimiento a los hallazgos y se incorporan mejoras en función de los resultados de estas revisiones?
5.36 Cumplimiento con políticas, reglas y normas de seguridad de la información	Existencia	¿Se reconoce la importancia de que el personal cumpla con las políticas, lineamientos y normas internas de seguridad de la información?
	Formalidad	¿Existen políticas, reglas y procedimientos formalmente aprobados y comunicados, así como mecanismos que describen cómo se controla su cumplimiento?
	Implementación	¿El personal aplica las políticas en la práctica?

	Medición / Mejora	¿Se revisa periódicamente el grado de cumplimiento mediante supervisión, auditorías, revisiones o monitoreo?
5.37 Procedimientos operativos documentados	Existencia	¿Se reconoce la necesidad de procedimientos documentados para las operaciones críticas relacionadas con la seguridad de la información?
	Formalidad	¿Existen procedimientos operativos aprobados y disponibles para el personal correspondiente?
	Implementación	¿El personal sigue los procedimientos documentados en sus actividades diarias?
	Medición / Mejora	¿Se revisan periódicamente los procedimientos para asegurar que se mantienen actualizados y eficaces?
CONTROLES DE PERSONAL		
6.1 Selección	Existencia	¿Se verifica la información básica del candidato (identidad, antecedentes laborales, referencias) antes de contratar?
	Formalidad	¿Existe un proceso documentado de selección que incluya validación de antecedentes, verificación de información, evaluación de competencias y criterios de seguridad?
	Implementación	¿Se ejecutan verificaciones de antecedentes laborales, referencias o validación de información declarada antes del ingreso del personal?
	Medición / Mejora	¿Se revisa el proceso de selección periódicamente y se ajusta para reducir riesgos detectados o cumplir nuevos requisitos legales?
6.2 Terminos y condiciones de empleo	Existencia	¿Se reconoce la necesidad de incluir obligaciones de seguridad de la información en los términos de empleo del personal?
	Formalidad	¿¿Existen contratos, reglamentos o documentos formales que describan explícitamente las responsabilidades de seguridad para los trabajadores (confidencialidad, uso aceptable, sanciones)?

	Implementación	¿El personal firma y acepta estos términos antes de recibir accesos a sistemas o información?
	Medición / Mejora	¿Se revisa y actualiza periódicamente los términos de empleo para incorporar nuevas obligaciones, riesgos, normas o controles?
6.3 Toma de conciencia, educación y entrenamiento sobre la seguridad de la información	Existencia	¿La organización contempla actividades de concientización o capacitación en seguridad de la información?
	Formalidad	¿Existe un plan, programa o calendario formal de capacitación en seguridad de información?
	Implementación	¿El personal recibe capacitación al incorporarse?
	Medición / Mejora	¿Se evalúa la eficacia del entrenamiento (evaluaciones, métricas, incidentes)?
6.4 Proceso disciplinario	Existencia	¿Existe algún mecanismo para tratar incumplimientos de seguridad por parte del personal?
	Formalidad	¿Existe un procedimiento formal o política que defina las medidas disciplinarias ante incumplimientos?
	Implementación	¿El personal conoce las consecuencias de incumplir políticas de seguridad? ¿Se ha aplicado el proceso disciplinario en algún caso reciente?
	Medición / Mejora	¿Se revisa si el proceso sigue siendo proporcional y efectivo?
6.5 Responsabilidades después del cese o cambio de empleo	Existencia	¿La organización establece responsabilidades para los trabajadores después de su cese o cambio de puesto?
	Formalidad	¿Existe documentación formal (política, cláusula contractual, NDA) que indique que la confidencialidad continúa después de finalizada la relación laboral?
	Implementación	¿El personal recibe esta información durante la inducción y al momento del cese?

	Medición / Mejora	¿Se valida su efectividad mediante auditorías internas o casos pasados?
6.6 Acuerdos de confidencialidad o no divulgación	Existencia	¿Se exigen acuerdos de confidencialidad para el personal con acceso a información sensible?
	Formalidad	¿Existe un documento formal que establezca las obligaciones de confidencialidad?
	Implementación	¿Todo el personal firma estos acuerdos antes de iniciar labores (NDA)? ¿Se almacenan y gestionan adecuadamente los NDA firmados?
	Medición / Mejora	¿Se revisan y actualizan los acuerdos para alinearse con cambios normativos o internos?
6.7 Trabajo remoto	Existencia	¿Se han definido lineamientos o requisitos específicos para el trabajo remoto?
	Formalidad	¿Existe una política o procedimiento formal que regule la seguridad de la información cuando el personal trabaja desde casa u otros lugares?
	Implementación	¿El personal aplica prácticas seguras en el trabajo remoto, como evitar redes públicas, bloquear pantalla, no compartir equipos, etc.? ¿Se controla el acceso a la información sensible desde ubicaciones remotas?
	Medición / Mejora	¿Verifican si estas medidas tomadas se cumplen (auditorías, revisiones de acceso, monitoreo)?
6.8 Reporte de eventos de seguridad de la información	Existencia	¿Existe un procedimiento o política que indique qué es un evento y cómo se debe reportar?
	Formalidad	¿Existe un canal formal (correo, formulario, línea directa) para reportar eventos?
	Implementación	¿El personal reporta oportunamente eventos reales o sospechosos?

	Medición / Mejora	¿Revisan la eficacia del proceso de reporte (tiempos, calidad, respuesta)?
CONTROLES FÍSICOS		
7.1 Perímetros de seguridad física	No aplica	No aplica; trabajo remoto servidores en la nube
7.2 Ingreso físico	No aplica	No aplica; trabajo remoto servidores en la nube
7.3 Asegurar oficinas, salas e instalaciones	No aplica	No aplica; trabajo remoto servidores en la nube
7.4 Supervisión de la seguridad física	No aplica	No aplica; trabajo remoto servidores en la nube
7.5 Protección contra amenazas físicas y ambientales	No aplica	No aplica; trabajo remoto servidores en la nube
7.6 Trabajo de áreas seguras	No aplica	No aplica; trabajo remoto servidores en la nube
7.7 Escritorio y pantallas limpios	No aplica	No aplica; trabajo remoto servidores en la nube
7.8 Ubicación y protección de los equipos	No aplica	No aplica; trabajo remoto servidores en la nube
7.9 Seguridad de los activos fuera de las instalaciones	Existencia	¿La organización reconoce los riesgos de utilizar activos fuera de instalaciones?
	Formalidad	¿Existe una política o directriz que establezca cómo deben protegerse físicamente los activos durante el teletrabajo?

	Implementación	¿Los colaboradores aplican medidas como bloqueo de pantalla, almacenamiento seguro, no dejar el equipo en autos o lugares expuestos?
	Medición / Mejora	¿Las políticas se revisan periódicamente? ¿Se refinan las medidas tras incidentes o auditorías?
7.10 Medios de almacenamiento	Existencia	¿La organización reconoce los riesgos asociados al uso de medios de almacenamiento?
	Formalidad	¿Existe una política que regule el uso, transporte, almacenamiento y eliminación de medios? ¿Hay reglas sobre permitir/prohibir el uso de USBs y almacenamiento local?
	Implementación	¿El personal cumple con estas reglas? ¿El almacenamiento está limitado a plataformas autorizadas (Google Workspace)? ¿Se evita el uso de medios externos no cifrados?
	Medición / Mejora	¿Se revisan incidentes o malas prácticas relacionadas al uso de medios de almacenamiento?
7.11 Servicios de suministro de apoyo	No aplica	No aplica; trabajo remoto servidores en la nube
7.12 Seguridad del cableado	No aplica	No aplica; trabajo remoto servidores en la nube
7.13 Mantenimiento de equipo	No aplica	No aplica; trabajo remoto servidores en la nube
7.14 Eliminación segura o reutilización de equipos	No aplica	No aplica; trabajo remoto servidores en la nube
CONTROLES TECNOLÓGICOS		
8.1 Dispositivos terminales del usuario	Existencia	¿La empresa sabe qué dispositivos se usan para acceder a la información corporativa (equipos propios o entregados)?

	Formalidad	¿Tienen reglas documentadas sobre cómo se deben configurar y protegerse estos dispositivos?
	Implementación	¿Los colaboradores cumplen con estas medidas (cifrado, bloqueo automático, antivirus, actualizaciones) ?
	Medición / Mejora	¿Revisan periódicamente la seguridad de estos dispositivos (revisiones, alertas, auditorías técnicas)?
8.2 Derechos de acceso privilegiados	Existencia	¿Conocen qué cuentas tienen privilegios especiales en los sistemas?
	Formalidad	¿Existe un documento que indique cómo se asignan, usan y controlan estos privilegios?
	Implementación	¿El acceso privilegiado se otorga sólo con aprobación y se usa únicamente cuando es necesario?
	Medición / Mejora	¿Revisan periódicamente quién tiene privilegios y si siguen siendo necesarios?
8.3 Restricción de acceso a la información	Existencia	¿Identifican qué información es sensible o restringida?
	Formalidad	¿Existe un esquema documentado de control de accesos basado en roles?
	Implementación	¿Los accesos se otorgan según necesidad y se retiran cuando ya no se requieren?
	Medición / Mejora	¿Se revisan periódicamente los accesos para detectar excesos o errores?
8.4 Acceso al código fuente	Existencia	¿Existe algún mecanismo, aunque sea informal, que limite quién puede tener acceso completo o parcial al código fuente?
	Formalidad	¿Existen reglas documentadas para otorgar, revisar y revocar acceso al repositorio?
	Implementación	¿Se usan ramas protegidas, revisiones de código y MFA?

	Medición / Mejora	¿Se revisan periódicamente los accesos, logs de commits o actividades sospechosas para detectar permisos innecesarios o riesgos de seguridad?
8.5 Autenticación segura	Existencia	¿Utilizan algún método de autenticación para acceder a sistemas, aplicaciones o recursos críticos?
	Formalidad	¿Existe una política o procedimiento formal que defina cómo se deben generar, almacenar y renovar credenciales?
	Implementación	¿Los métodos de autenticación definidos (MFA, contraseñas seguras, tokens, etc.) están implementados realmente en todos los sistemas relevantes?
	Medición / Mejora	¿Se evalúa periódicamente la eficacia de los mecanismos de autenticación?
8.6 Gestión de capacidad	Existencia	¿La empresa monitorea el uso de recursos (almacenamiento, CPU, memoria, ancho de banda) en los servicios o infraestructura en la nube?
	Formalidad	¿Existe un procedimiento formal o documento que defina cómo se planifica, monitorea y gestiona la capacidad de los sistemas?
	Implementación	¿El equipo aplica el monitoreo de capacidad y toma acciones cuando se detectan límites cercanos o posibles saturaciones?
	Medición / Mejora	¿Se evalúan periódicamente tendencias de uso para anticipar necesidades futuras y ajustar la capacidad antes de que se convierta en un riesgo?
8.7 Protección contra programas maliciosos	Existencia	¿Se utiliza algún mecanismo (antivirus, antimalware, filtros en la nube, etc.) para proteger los dispositivos y servicios contra software malicioso?
	Formalidad	¿Existe una política o procedimiento formal que establezca los requisitos para prevenir, detectar y responder a amenazas de malware?
	Implementación	¿Los mecanismos anti malware están realmente instalados, configurados y actualizados en todos los dispositivos y sistemas relevantes?

	Medición / Mejora	¿Se revisan periódicamente los incidentes, alertas o tendencias para mejorar la protección contra nuevas variantes de malware?
8.8 Gestión de vulnerabilidades técnicas	Existencia	¿Se realiza alguna actividad para identificar vulnerabilidades técnicas en los sistemas (por ejemplo, escaneos, revisión de avisos de seguridad, parches)?
	Formalidad	¿Existe un procedimiento o política formal que defina cómo se identifican, evalúan, priorizan y corrigen las vulnerabilidades técnicas?
	Implementación	¿Las vulnerabilidades identificadas se gestionan realmente, se toman acciones al respecto?
	Medición / Mejora	¿Se revisa periódicamente la eficacia del proceso de gestión de vulnerabilidades para ajustar tiempos, herramientas o priorización?
8.9 Gestión de la configuración	Existencia	¿Se realiza algún tipo de control o registro sobre los cambios o configuraciones aplicadas en los sistemas, servicios o infraestructura?
	Formalidad	¿Existe un procedimiento documentado que defina cómo se debe gestionar, aprobar y registrar las configuraciones de los sistemas?
	Implementación	¿Los administradores aplican realmente las configuraciones siguiendo lo documentado, asegurando que solo se apliquen cambios autorizados?
	Medición / Mejora	¿Se revisa periódicamente el proceso de gestión de configuraciones para identificar oportunidades de mejora o evitar riesgos?
8.10 Eliminación de información	Existencia	¿Se realiza algún tipo de eliminación o depuración de información cuando deja de ser necesaria o cuando expira su tiempo de conservación?
	Formalidad	¿Existe una política o procedimiento formal que establezca cómo, cuándo y bajo qué métodos se debe eliminar la información de forma segura?
	Implementación	¿La eliminación de información se realiza realmente según lo establecido, asegurando que no pueda recuperarse o accederse posteriormente?

	Medición / Mejora	¿Se revisa periódicamente la eficacia del proceso de eliminación para ajustar métodos, tiempos de retención o controles aplicados?
8.11 Enmascaramiento de datos	Existencia	¿Se aplica algún tipo de enmascaramiento, anonimización o sustitución de datos sensibles en los sistemas o bases de datos utilizadas por la organización?
	Formalidad	¿Existe una política, estándar o procedimiento formal que establezca qué datos se deben enmascarar, en qué entornos y bajo qué técnicas?
	Implementación	¿El enmascaramiento de datos se realiza efectivamente en los entornos que lo requieren (por ejemplo, pruebas, desarrollo, soporte) y se verifica que los datos enmascarados no permiten la identificación real de la información?
	Medición / Mejora	¿Se revisa periódicamente la efectividad del enmascaramiento (por ejemplo, para evitar reidentificación o fuga de datos)?
8.12 Prevención de fuga de datos	Existencia	¿La organización realiza alguna acción o utiliza algún mecanismo para prevenir la fuga, filtración o divulgación no autorizada de información?
	Formalidad	¿Existe una política o lineamiento relacionado que establezca controles para prevenir fugas de información (restricciones sobre copia, transferencia, descarga o almacenamiento de datos sensibles)?
	Implementación	¿Se aplican realmente medidas para evitar la fuga de datos (restricciones en el uso de dispositivos externos, controles en plataformas cloud, bloqueo de descargas o supervisión del uso indebido de información)?
	Medición / Mejora	¿Se revisa periódicamente la efectividad de los controles para prevenir fugas de información y se ajustan según incidentes, auditorías o nuevas amenazas?
8.13 Copia de seguridad de la información	Existencia	¿Se realizan copias de seguridad periódicas de la información crítica?
	Formalidad	¿Existe una política o procedimiento formal que defina qué información se debe respaldar, con qué frecuencia y cómo se debe gestionar las copias de seguridad?

	Implementación	¿Las copias de seguridad se ejecutan realmente según lo establecido y se verifica periódicamente su integridad o capacidad de restauración?
	Medición / Mejora	¿Se revisa periódicamente la eficacia del proceso de copias de seguridad (frecuencia, cobertura, restauración) y se ajusta cuando cambian los sistemas o surgen nuevos riesgos?
8.14 Redundancia de las instalaciones de procesamiento de información	Existencia	¿La organización cuenta con algún tipo de redundancia o mecanismos alternos para asegurar la continuidad de los sistemas y servicios en caso de fallas en la infraestructura principal?
	Formalidad	¿Existe documentación formal (política, procedimiento o diseño técnico) que defina los requisitos de redundancia, disponibilidad y continuidad para los servicios críticos?
	Implementación	¿Los mecanismos de redundancia establecidos (por ejemplo, replicación en la nube, respaldos automáticos, entornos alternos) funcionan realmente y han sido probados en la práctica?
	Medición / Mejora	¿Se evalúa periódicamente la capacidad de la infraestructura redundante para garantizar disponibilidad?
8.15 Registro	Existencia	¿Se registran eventos o actividades relevantes en los sistemas, aplicaciones o servicios utilizados por la organización?
	Formalidad	¿Existe una política o procedimiento formal que establezca qué eventos se deben registrar, cómo se deben almacenar y quién puede acceder a dichos registros?
	Implementación	¿Los sistemas generan y conservan realmente los registros definidos, y se garantiza que no puedan ser alterados o eliminados sin autorización?
	Medición / Mejora	¿Se revisan periódicamente los registros o el proceso de registro para asegurar su completitud, utilidad y cumplimiento con los requisitos establecidos?
8.16 Actividades de monitoreo	Existencia	¿Se realiza algún tipo de monitoreo sobre el comportamiento de los sistemas, redes o servicios para detectar actividades inusuales o potencialmente maliciosas?

	Formalidad	¿Existe una política o procedimiento formal que defina qué actividades se deben monitorear, con qué frecuencia y qué herramientas se deben utilizar?
	Implementación	¿La organización ejecuta realmente las actividades de monitoreo definidas, revisando alertas, logs o paneles de seguridad de manera periódica?
	Medición / Mejora	¿Se evalúa periódicamente la efectividad del monitoreo (por ejemplo, cantidad de alertas relevantes, incidentes detectados)?
8.17 Sincronización de reloj	Existencia	¿Los sistemas y servicios utilizados por la organización están sincronizados con una fuente de tiempo confiable?
	Formalidad	¿Existe un procedimiento o lineamiento formal que establezca cómo se deben sincronizar los relojes del sistema y qué fuentes de tiempo deben utilizarse?
	Implementación	¿La sincronización del tiempo se aplica realmente en todos los sistemas relevantes? ¿Los servidores cloud, aplicaciones y bases de datos usan NTP u otro servicio de sincronización?
	Medición / Mejora	¿Se verifica periódicamente la precisión de la sincronización?
8.18 Uso de programas de utilidad privilegiados	Existencia	¿Se utilizan herramientas o utilitarios con privilegios elevados (por ejemplo, herramientas de administración, scripts con permisos, consolas avanzadas) dentro de la organización?
	Formalidad	¿Existe documentación formal que establezca qué programas privilegiados se pueden usar, por quién y bajo qué condiciones de seguridad?
	Implementación	¿El uso de utilitarios privilegiados se gestiona realmente según lo establecido, asegurando acceso restringido, registro de uso o autorizaciones previas?
	Medición / Mejora	¿Se revisa periódicamente el uso de estos programas para detectar accesos indebidos, eliminar herramientas innecesarias o fortalecer los controles aplicados?

8.19 Información de software en sistemas operativos	Existencia	¿Se lleva algún registro o control sobre el software instalado en los sistemas operativos utilizados en la organización?
	Formalidad	¿Existe una política o procedimiento formal que defina qué software se puede instalar, cómo se debe autorizar y cómo debe mantenerse actualizado?
	Implementación	¿Se aplica realmente el control sobre el software instalado, verificando que solo se utilicen aplicaciones autorizadas y seguras en los sistemas operativos?
	Medición / Mejora	¿Se revisa periódicamente el inventario o estado del software instalado para eliminar aplicaciones no autorizadas, identificar vulnerabilidades o mejorar el proceso de control?
8.20 Seguridad de redes	Existencia	¿Se aplican medidas para proteger las redes utilizadas (como firewalls, segmentación, VPN o reglas de acceso)?
	Formalidad	¿Existe una política o procedimiento formal que defina los requisitos de seguridad de red, incluyendo controles de acceso, uso de VPN, segmentación y protección perimetral?
	Implementación	¿Se aplican realmente las configuraciones de seguridad?
	Medición / Mejora	¿Se revisa periódicamente la seguridad de la red (configuraciones, alertas, vulnerabilidades) para identificar mejoras o ajustar controles según nuevos riesgos?
8.21 Seguridad de servicios de red	Existencia	¿Se aplican controles específicos para proteger los servicios de red (DNS, correo, VPN, servicios cloud, etc.)?
	Formalidad	¿Existe documentación formal que establezca los requisitos de seguridad para los servicios de red, incluyendo configuración segura, monitoreo y protección contra abuso?
	Implementación	¿Los servicios de red se gestionan realmente según lo establecido?
	Medición / Mejora	¿Se evalúa periódicamente la seguridad de los servicios de red para identificar vulnerabilidades, configuraciones débiles o mejoras necesarias?

8.22 Segregación de redes	Existencia	¿Se aplica algún tipo de separación o segmentación entre distintas partes de la red (por ejemplo, producción, desarrollo, administración, invitados)?
	Formalidad	¿Existe una política o procedimiento formal que defina cómo se debe segregar las redes y bajo qué criterios se deben separar los distintos entornos o niveles de acceso?
	Implementación	¿La segregación de redes se encuentra realmente aplicada en la práctica (separadas mediante firewalls, VLANs o grupos de seguridad en la nube) ?
	Medición / Mejora	¿Se revisa periódicamente la efectividad de la segregación de redes para identificar posibles brechas, configuraciones incorrectas o la necesidad de crear nuevos segmentos?
8.23 Filtrado de la web	Existencia	¿Se aplica algún mecanismo de filtrado o restricción para limitar el acceso a sitios web no autorizados o potencialmente riesgosos?
	Formalidad	¿Existe una política o procedimiento formal que establezca qué tipos de sitios web están permitidos, bloqueados o restringidos para los trabajadores?
	Implementación	¿El filtrado web se aplica realmente en los dispositivos o servicios utilizados por el personal?
	Medición / Mejora	¿Se revisa periódicamente la efectividad del filtrado web para ajustar categorías bloqueadas, responder a incidentes o mejorar la protección ante nuevas amenazas?
8.24 Uso de criptografía	Existencia	¿Se utiliza algún mecanismo criptográfico (cifrado, hash, firmas digitales, certificados) para proteger la información en tránsito o en reposo?
	Formalidad	¿Existe una política o procedimiento formal que defina cuándo y cómo se debe utilizar la criptografía, incluidos los algoritmos permitidos, la gestión de claves y los niveles de protección requeridos??
	Implementación	¿Se aplica cifrado en bases de datos, servidores cloud, comunicaciones, backups y claves?

	Medición / Mejora	¿Se revisa periódicamente vulnerabilidades o actualizan estándares criptográficos periódicamente?
8.25 Ciclo de vida de desarrollo seguro	Existencia	¿Se consideran prácticas de seguridad durante el desarrollo del software, como validación de requisitos, revisión de código o pruebas de seguridad?
	Formalidad	¿Existe un proceso o lineamiento formal que defina las actividades de seguridad que se deben incorporar en cada etapa del ciclo de desarrollo (requisitos, diseño, construcción, pruebas y despliegue)?
	Implementación	¿Las actividades de seguridad definidas se aplican realmente en los proyectos de desarrollo?
	Medición / Mejora	¿Se revisa periódicamente la efectividad del proceso de desarrollo seguro para identificar brechas, incorporar mejoras o actualizar prácticas ?
8.26 Requisitos de seguridad de la aplicación	Existencia	¿Se identifican o consideran requisitos de seguridad cuando se diseñan, desarrollan o adquieren aplicaciones?
	Formalidad	¿Existe documentación formal (política, estándar o procedimiento) que establezca cómo se debe definir, documentar y validar los requisitos de seguridad de las aplicaciones?
	Implementación	¿Los requisitos de seguridad definidos se aplican realmente durante el desarrollo, adquisición o integración de aplicaciones?
	Medición / Mejora	¿Se revisa periódicamente la adecuación de los requisitos de seguridad aplicados en las aplicaciones para incorporar mejoras, nuevos controles o cambios tecnológicos?
8.27 Arquitectura de sistemas seguros y principios de ingeniería	Existencia	¿Se aplican principios de diseño seguro o se considera la seguridad al definir la arquitectura de los sistemas que utiliza o desarrolla la organización?
	Formalidad	¿Existe documentación formal (estándares, guías, arquitectura de referencia) que establezca los principios de ingeniería y los controles de seguridad que se deben aplicar al diseñar o modificar sistemas?

	Implementación	¿Los proyectos realmente siguen los principios de arquitectura segura establecidos? (controles como separación de componentes, privilegios mínimos, validación de entradas o protección de interfaces)
	Medición / Mejora	¿Se revisa periódicamente la arquitectura de los sistemas para identificar debilidades, introducir mejoras o actualizar principios de diseño?
8.28 Codificación segura	Existencia	¿Se aplican prácticas de codificación segura durante el desarrollo del software (por ejemplo, validación de entradas, uso seguro de dependencias, etc.)?
	Formalidad	¿Existe una guía, estándar o procedimiento formal que establezca las prácticas de codificación segura que deben seguir los desarrolladores?
	Implementación	¿Se realizan revisiones de código, análisis SAST o controles de calidad para asegurar buenas prácticas?
	Medición / Mejora	¿Se revisan periódicamente las prácticas de codificación segura para incorporar nuevas recomendaciones, lecciones aprendidas o actualizaciones según vulnerabilidades recientes?
8.29 Pruebas de seguridad en desarrollo y aceptación.	Existencia	¿Se realizan pruebas de seguridad (como escaneos, pruebas estáticas, dinámicas o revisión de controles) antes de liberar o aceptar una aplicación o funcionalidad?
	Formalidad	¿Existe un procedimiento formal que establezca qué pruebas de seguridad se deben efectuar durante el desarrollo y antes de la aceptación de software?
	Implementación	¿Las pruebas de seguridad realmente se ejecutan en los proyectos?
	Medición / Mejora	¿Se revisa periódicamente la eficacia de las pruebas de seguridad realizadas?

8.30 Desarrollo subcontratado	Existencia	¿Se externaliza o a externalizado alguna actividad de desarrollo de software a terceros?
	Formalidad	¿Existe documentación formal (contratos, acuerdos o políticas) que establezca los requisitos de seguridad que deben cumplir los proveedores?
	Implementación	¿Se verifica que el proveedor aplique medidas de seguridad adecuadas (revisiones, informes, cumplimiento)?
	Medición / Mejora	¿Se evalúa y retroalimenta al proveedor cuando hay incumplimientos o incidentes?
8.31 Separación de los entornos de desarrollo, prueba y producción	Existencia	¿Se mantienen separados los entornos de desarrollo, pruebas y producción para evitar interferencias, accesos indebidos o riesgos de seguridad?
	Formalidad	¿Existe documentación formal que establezca cómo se debe segregar los entornos y qué restricciones de acceso y manipulación aplican en cada uno?
	Implementación	¿La separación de entornos se cumple realmente en la práctica?
	Medición / Mejora	¿Se revisa periódicamente la separación entre entornos para identificar brechas, accesos innecesarios o necesidades de reforzar la segregación?
8.32 Gestión de cambios	Existencia	¿Se realiza algún proceso para registrar, revisar o aprobar los cambios que se realizan en sistemas, aplicaciones o infraestructura?
	Formalidad	¿Existe una política o procedimiento formal que establezca cómo deben solicitar, evaluar, aprobar, implementar y documentar los cambios?
	Implementación	¿Los cambios realmente se gestionan siguiendo el proceso establecido, evitando modificaciones no autorizadas o sin evaluación de impacto?
	Medición / Mejora	¿Se revisa periódicamente la eficacia del proceso de gestión de cambios para identificar fallas, retrasos o la necesidad de mejorar controles o trazabilidad?

8.33 Información en las pruebas	Existencia	¿El área de desarrollo evita usar datos personales reales en ambientes de prueba?
	Formalidad	¿Existe un lineamiento que indique cómo se debe proteger, anonimizar o enmascarar los datos en pruebas?
	Implementación	¿Los ambientes de prueba usan datos ficticios o enmascarados?
	Medición / Mejora	¿Se revisa periódicamente la gestión de la información en pruebas para garantizar que se cumplan los estándares de seguridad?
8.34 Protección de los sistemas de información durante las pruebas de auditoría	Existencia	¿Se asegura que auditorías o pruebas de seguridad no afecten la operación del sistema?
	Formalidad	¿Existe un procedimiento formal que defina cómo se deben proteger los sistemas de información durante las pruebas de auditoría, incluyendo responsabilidades, métodos de control y limitaciones de acceso?
	Implementación	¿Se cumplen realmente las medidas de protección durante las pruebas de auditoría, garantizando que los sistemas y datos no se vean comprometidos?
	Medición / Mejora	¿Se revisa y evalúa periódicamente la eficacia de las medidas de protección aplicadas durante las auditorías y se implementan mejoras si se detectan vulnerabilidades o incidentes?

Nota. Elaborado por los investigadores.

ANEXO 12

FICHAS DE JUICIO DE EXPERTOS

- Ficha Experto N° 1

UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO
FACULTAD DE INGENIERÍA CIVIL, SISTEMAS Y ARQUITECTURA
ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

FICHA DE JUICIO DE EXPERTOS VALIDACIÓN DEL DISEÑO DEL SGSI BASADO EN LA NTP ISO/IEC 27001:2022 PARA LA EMPRESA ITEPREVENGO		
TRABAJO DE INVESTIGACIÓN	Sistema de Gestión de Seguridad de la Información para los procesos de soporte y desarrollo de software SaaS de la empresa Iteprevengo	
AUTORES	Alberca Cubas Kevin y Guerrero Diaz Lalita	
DATOS GENERALES DEL EXPERTO		
NOMBRE COMPLETO	Ernesto Karlo Celi Arévalo	
PROFESIÓN	Ingeniero de Computación y Sistemas	
ESPECIALIDAD	Auditoría de SI, Gestión de Seguridad de la Información y Gestión de Riesgos de TI	
GRADO ACADÉMICO	[ ] Bachiller [ ] Licenciado/Ingeniero [ ] Magíster [X] Doctor	
INSTITUCIÓN LABORAL	Universidad Nacional Pedro Ruiz Gallo	
EXPERIENCIA ESPECÍFICA (Certificaciones relacionadas (ISO 27001, CISA, CISM, etc.)		
CERTIFICACIÓN	INSTITUCIÓN	AÑO
Certified Lead Implementer ISOIEC 270012017	CertoProf	2022 2025
IT Audit Control Security	ISACA	2019
Especialización Auditoría en Tecnologías de la información y Seguridad Informática	USAT	2013
SCRUM Fundamental Certified	SCRUMstudy	2019
Especialización en data Science & Big Data	ILEN	2022
OBJETIVO DE LA EVALUACIÓN		
La presente ficha tiene como finalidad validar, mediante juicio de expertos, el diseño del Sistema de Gestión de Seguridad de la Información (SGSI) basado en la NTP ISO/IEC 27001:2022 propuesto para la empresa ITEPREVENGO, evaluando cada uno de sus componentes según los criterios establecidos.		
INSTRUCCIONES		
Estimado(a) experto(a): Se le solicita valorar cada uno de los componentes del SGSI conforme a los criterios establecidos, asignando la calificación que, de acuerdo con su juicio y experiencia profesional, considere pertinente en cada caso, utilizando la escala de evaluación proporcionada.		
CRITERIOS DE EVALUACIÓN		
Pertinencia	El componente es relevante y adecuado para la realidad y necesidades de la organización.	
Claridad	El contenido está redactado de forma comprensible, precisa y sin ambigüedades.	

Coherencia	Existe consistencia interna y alineación con los demás componentes del SGSI.
Suficiencia	El contenido es completo y aborda los elementos necesarios.
Alineación normativa	El componente se encuentra conforme con los requisitos de la norma ISO/IEC 27001 y directrices complementarias consideradas en la presente investigación.

ESCALA DE VALORACIÓN

NIVEL	SIGNIFICADO	VALOR
Excelente	Cumple totalmente el criterio	4
Adecuado	Cumple en alto grado, requiere mejoras menores	3
Regular	Cumple parcialmente, requiere ajustes importantes	2
Deficiente	No cumple el criterio	1

MATRIZ DE EVALUACIÓN

COMPONENTE	PERTINENCIA	CLARIDAD	COHERENCIA	SUFICIENCIA	ALINEACIÓN NORMATIVA	OBSERVACIONES
Contexto de la organización	4	4	4	3	4	El análisis del contexto organizacional describe adecuadamente la situación de la empresa, considerando su modelo SaaS y trabajo remoto. Se recomienda ampliar el análisis de factores externos (regulatorios y contractuales con clientes) y relacionarlos con riesgos de seguridad de la información.
Alcance del SGSI	4	4	4	3	4	El alcance está claramente definido para los procesos de soporte y desarrollo SaaS. Se sugiere especificar con mayor precisión los límites del SGSI respecto a infraestructura cloud y responsabilidades compartidas con proveedores.
Política de la Seguridad de la Información	4	4	4	4	4	La política está alineada con los principios de confidencialidad, integridad y disponibilidad. Se recomienda incluir referencia explícita al compromiso de mejora continua y cumplimiento normativo.
Objetivos de la Seguridad de la Información	4	4	4	3	4	Los objetivos se encuentran alineados con el SGSI; sin embargo, podrían expresarse mediante indicadores medibles (SMART) para facilitar el seguimiento y evaluación del desempeño.
Roles y responsabilidades	4	4	4	3	4	La asignación de roles es adecuada. Se sugiere detallar responsabilidades específicas relacionadas con la gestión de incidentes, gestión de accesos y administración de servicios cloud.
Modelo de Gestión de Riesgos	4	4	4	4	4	El modelo basado en MAGERIT e ISO 27005 presenta coherencia metodológica y permite identificar activos, amenazas y vulnerabilidades. La propuesta es sólida en relación al diseño del SGSI.
Plan de Tratamiento de Riesgos	4	4	4	4	4	El plan define adecuadamente las salvaguardas y controles seleccionados para reducir los riesgos identificados. Se recomienda incluir responsables y cronograma de implementación para fortalecer la gestión operativa.

SOA	4	4	4	4	4	La declaración de aplicabilidad evidencia la selección de controles conforme al Anexo A de ISO/IEC 27001:2022. Se sugiere documentar con mayor detalle la justificación de exclusión de controles.
Implementación de controles	4	3	4	3	4	Los controles propuestos son pertinentes para el entorno SaaS; sin embargo, algunos podrían detallarse con mayor precisión en cuanto a procedimientos operativos y responsables de implementación.
Plan de concientización	4	4	4	3	4	El plan contempla la formación del personal en seguridad de la información. Se recomienda incorporar un programa periódico de capacitación y evaluación del nivel de concientización.
Documentación del SGSI	4	4	4	4	4	La documentación propuesta cumple con los requisitos de la norma ISO/IEC 27001 en cuanto a políticas, procedimientos y registros necesarios para el funcionamiento del SGSI.
Métricas e indicadores	4	4	4	3	4	Los indicadores definidos permiten evaluar el desempeño del SGSI. Se recomienda establecer metas cuantitativas y periodicidad de medición para facilitar el monitoreo y la mejora continua.

VALORACIÓN GLOBAL DEL DISEÑO

De manera global, ¿considera usted que el Diseño del Sistema de Gestión de la Seguridad de la Información basado en el estándar ISO/IEC 27001:2022 propuesto garantiza la confidencialidad, integridad y disponibilidad de la información en los procesos de soporte y desarrollo de software SaaS en la empresa Iteprevengo?

SI [X] NO [ ]

DECLARACIÓN DEL EXPERTO

Declaro que la evaluación realizada se basa en mi experiencia profesional y criterio técnico, y que ha sido emitida de manera objetiva e independiente, con fines exclusivamente académicos.

FIRMA DEL EXPERTO: 

Chiclayo, 09 de marzo del 2026.

- Ficha Experto N° 2

UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO
FACULTAD DE INGENIERÍA CIVIL, SISTEMAS Y ARQUITECTURA
ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

FICHA DE JUICIO DE EXPERTOS VALIDACIÓN DEL DISEÑO DEL SGSI BASADO EN LA NTP ISO/IEC 27001:2022 PARA LA EMPRESA ITEPREVENGO	
TRABAJO DE INVESTIGACIÓN	Sistema de Gestión de Seguridad de la Información para los procesos de soporte y desarrollo de software SaaS de la empresa Iteprevengo
AUTORES	Alberca Cubas Kevin y Guerrero Diaz Lalita
DATOS GENERALES DEL EXPERTO	
NOMBRE COMPLETO	Jessie Leila Bravo Jaico
PROFESIÓN	Ing. Computación y Sistemas
ESPECIALIDAD	Transformación Digital y Analítica de datos
GRADO ACADÉMICO	[ ] Bachiller [ ] Licenciado/Ingeniero [ ] Magíster [x] Doctor
INSTITUCIÓN LABORAL	Universidad Nacional Pedro Ruiz Gallo

EXPERIENCIA ESPECÍFICA (Certificaciones relacionadas (ISO 27001, CISA, CISM, etc.)		
CERTIFICACIÓN	INSTITUCIÓN	AÑO
ISO 27001	BS GOUP	2019
ISO 27032	PMC	2020

OBJETIVO DE LA EVALUACIÓN
La presente ficha tiene como finalidad validar, mediante juicio de expertos, el diseño del Sistema de Gestión de Seguridad de la Información (SGSI) basado en la NTP ISO/IEC 27001:2022 propuesto para la empresa ITEPREVENGO, evaluando cada uno de sus componentes según los criterios establecidos.
INSTRUCCIONES
Estimado(a) experto(a): Se le solicita valorar cada uno de los componentes del SGSI conforme a los criterios establecidos, asignando la calificación que, de acuerdo con su juicio y experiencia profesional, considere pertinente en cada caso, utilizando la escala de evaluación proporcionada.

CRITERIOS DE EVALUACIÓN	
Pertinencia	El componente es relevante y adecuado para la realidad y necesidades de la organización.
Claridad	El contenido está redactado de forma comprensible, precisa y sin ambigüedades.
Coherencia	Existe consistencia interna y alineación con los demás componentes del SGSI.
Suficiencia	El contenido es completo y aborda los elementos necesarios.
Alineación normativa	El componente se encuentra conforme con los requisitos de la norma ISO/IEC 27001 y directrices complementarias consideradas en la presente investigación.

ESCALA DE VALORACIÓN		
NIVEL	SIGNIFICADO	VALOR
Excelente	Cumple totalmente el criterio	4
Adecuado	Cumple en alto grado, requiere mejoras menores	3
Regular	Cumple parcialmente, requiere ajustes importantes	2
Deficiente	No cumple el criterio	1

MATRIZ DE EVALUACIÓN

COMPONENTE	PERTINENCIA	CLARIDAD	COHERENCIA	SUFICIENCIA	ALINEACIÓN NORMATIVA	OBSERVACIONES
Contexto de la organización	4	4	4	4	4	
Alcance del SGSI	4	4	4	4	4	
Política de la Seguridad de la Información	4	4	4	3	4	
Objetivos de la Seguridad de la Información	4	4	4	3	4	
Roles y responsabilidades	4	4	4	3	4	
Modelo de Gestión de Riesgos	4	4	4	4	4	
Plan de Tratamiento de Riesgos	4	4	4	4	4	
SOA	4	3	4	4	4	
Implementación de controles	4	3	4	3	4	

Plan de concientización	4	4	4	4	4	
Documentación del SGSI	4	4	4	3	4	
Métricas e indicadores	4	4	4	4	4	

VALORACIÓN GLOBAL DEL DISEÑO

De manera global, ¿considera usted que el Diseño del Sistema de Gestión de la Seguridad de la Información basado en el estándar ISO/IEC 27001:2022 propuesto garantiza la confidencialidad, integridad y disponibilidad de la información en los procesos de soporte y desarrollo de software SaaS en la empresa Iteprevengo?

SI [X] NO [ ]

DECLARACIÓN DEL EXPERTO

Declaro que la evaluación realizada se basa en mi experiencia profesional y criterio técnico, y que ha sido emitida de manera objetiva e independiente, con fines exclusivamente académicos.

Observación general: La propuesta del Sistema de Gestión de Seguridad de la Información presenta consistencia técnica, pertinencia respecto al contexto organizacional y adecuada alineación con los lineamientos de la NTP ISO/IEC 27001:2022. Se valora favorablemente la definición del alcance, la gestión de riesgos, el plan de tratamiento, las métricas y el enfoque de concientización. No obstante, algunos componentes como la declaración de aplicabilidad, la formalización de responsabilidades, la documentación operativa y la implementación de controles requieren validación en un escenario de ejecución real para confirmar plenamente su suficiencia.

FIRMA DEL EXPERTO: 

Chiclayo, 17 de marzo del 2026.

- Ficha Experto N° 3

UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO
FACULTAD DE INGENIERÍA CIVIL, SISTEMAS Y ARQUITECTURA
ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

FICHA DE JUICIO DE EXPERTOS VALIDACIÓN DEL DISEÑO DEL SGSI BASADO EN LA NTP ISO/IEC 27001:2022 PARA LA EMPRESA ITEPREVENGO		
TRABAJO DE INVESTIGACIÓN	Sistema de Gestión de Seguridad de la Información para los procesos de soporte y desarrollo de software SaaS de la empresa Iteprevengo	
AUTORES	Alberca Cubas Kevin y Guerrero Diaz Lalita	
DATOS GENERALES DEL EXPERTO		
NOMBRE COMPLETO	Cristian Miguel Guevara Ramirez	
PROFESIÓN	Ingeniería de Sistemas	
ESPECIALIDAD	Ciberseguridad (Identity and Access Management)	
GRADO ACADÉMICO	[X] Bachiller [ ] Licenciado/Ingeniero [ ] Magíster [ ] Doctor	
INSTITUCIÓN LABORAL	Centria Servicios Administrativos SAC	
EXPERIENCIA ESPECÍFICA (Certificaciones relacionadas (ISO 27001, CISA, CISM, etc.)		
CERTIFICACIÓN	INSTITUCIÓN	AÑO
SC-900: Security, Compliance, and Identity Fundamentals	Microsoft	2026
Interpretación y Formación de Auditor Interno de ISO 27001:2023	AENOR	2024
Interpretación de la norma y formación Auditor Interno ISO 27001:2022	TUVRheinland	2023
OBJETIVO DE LA EVALUACIÓN		
La presente ficha tiene como finalidad validar, mediante juicio de expertos, el diseño del Sistema de Gestión de Seguridad de la Información (SGSI) basado en la NTP ISO/IEC 27001:2022 propuesto para la empresa ITEPREVENGO, evaluando cada uno de sus componentes según los criterios establecidos.		
INSTRUCCIONES		
Estimado(a) experto(a): Se le solicita valorar cada uno de los componentes del SGSI conforme a los criterios establecidos, asignando la calificación que, de acuerdo con su juicio y experiencia profesional, considere pertinente en cada caso, utilizando la escala de evaluación proporcionada.		
CRITERIOS DE EVALUACIÓN		
Pertinencia	El componente es relevante y adecuado para la realidad y necesidades de la organización.	
Claridad	El contenido está redactado de forma comprensible, precisa y sin ambigüedades.	
Coherencia	Existe consistencia interna y alineación con los demás componentes del SGSI.	
Suficiencia	El contenido es completo y aborda los elementos necesarios.	

Alineación normativa	El componente se encuentra conforme con los requisitos de la norma ISO/IEC 27001 y directrices complementarias consideradas en la presente investigación.

ESCALA DE VALORACIÓN

NIVEL	SIGNIFICADO	VALOR
Excelente	Cumple totalmente el criterio	4
Adecuado	Cumple en alto grado, requiere mejoras menores	3
Regular	Cumple parcialmente, requiere ajustes importantes	2
Deficiente	No cumple el criterio	1

MATRIZ DE EVALUACIÓN

COMPONENTE	PERTINENCIA	CLARIDAD	COHERENCIA	SUFICIENCIA	ALINEACIÓN NORMATIVA	OBSERVACIONES
Contexto de la organización	4	4	4	4	4	Observación subsanada. Se ha incorporado correctamente la Ley de Seguridad y Salud en el Trabajo (N° 29783) dentro del contexto de la organización. Esta inclusión asegura que el sistema de gestión de seguridad de la información considere los lineamientos normativos específicos del sector.
Alcance del SGSI	4	4	4	4	4	El alcance está correctamente acotado al ciclo de vida del software, lo cual protege el activo principal de la empresa.
Política de la Seguridad de la Información	4	4	4	4	4	Documento de alto nivel, conciso y alineado a la norma ISO/IEC 27001:2022.
Objetivos de la Seguridad de la Información	4	4	3	3	4	Se recomienda agregar objetivos específicos alineados a la seguridad en el ciclo de vida del software.
Roles y responsabilidades	4	3	2	3	2	No se garantiza la segregación de funciones (Control 5.3) al concentrar la operación (TI) y la coordinación (CSI) en el mismo responsable.
Modelo de Gestión de Riesgos	4	4	4	3	4	El modelo debe mapear el "Acceso no autorizado" como riesgo transversal en todos los activos de TI.
Plan de Tratamiento de Riesgos	4	4	4	4	4	Las acciones propuestas son coherentes para mitigar las brechas detectadas en el análisis.
SOA	4	4	4	4	4	Bueno uso de la nueva estructura de controles del estándar 2022.
Implementación de controles	4	4	4	4	4	Adecuados para proteger la infraestructura cloud.
Plan de concientización	4	4	4	4	4	Observación subsanada. Las pruebas de ingeniería social proporcionan un enfoque medible para la evaluación de la cultura de seguridad de la información.
Documentación del SGSI	4	4	4	4	4	La estructura documental diseñada es suficiente para garantizar la trazabilidad exigida.
Métricas e indicadores	4	4	4	4	4	Observación subsanada. Se han definido métricas técnicas claras que permiten evaluar el rendimiento del software y su capacidad de respuesta ante incidentes

VALORACIÓN GLOBAL DEL DISEÑO
De manera global, ¿considera usted que el Diseño del Sistema de Gestión de la Seguridad de la Información basado en el estándar ISO/IEC 27001:2022 propuesto garantiza la confidencialidad, integridad y disponibilidad de la información en los procesos de soporte y desarrollo de software SaaS en la empresa Iteprevengo? SI [X] NO [ ]
DECLARACIÓN DEL EXPERTO
Declaro que la evaluación realizada se basa en mi experiencia profesional y criterio técnico, y que ha sido emitida de manera objetiva e independiente, con fines exclusivamente académicos. FIRMA DEL EXPERTO:    Chiclayo, 03 de Abril del 2026.