UNIVERSIDAD NACIONAL DE SAN CRISTÓBAL DE HUAMANGA

FACULTAD DE INGENIERÍA DE MINAS, GEOLOGÍA Y CIVIL

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

TESIS:

Sistema de gestión de seguridad de la información según ISO/IEC 27001 para las pymes del Perú, 2024

Para optar el título profesional de:

INGENIERA DE SISTEMAS

PRESENTADO POR:

Bach. Lisset Karen LIMA LOAYZA

ASESOR:

Mg. Ing. Hubner JANAMPA PATILLA

AYACUCHO - PERÚ

2024

DEDICATORIA

Quiero dedicar mi tesis a Dios por guiarnos y cuidarnos, a mis padres por siempre inculcarme el deseo de superación brindándome su apoyo incondicional y a mis hermanos, por el amor que me ofrecen en todo momento.

AGRADECIMIENTO

Expreso un especial agradecimiento a mi asesor el Mg. Ing. Hubner Janampa Patilla, por el tiempo dedicado y su valiosa guía en la elaboración de este proyecto, a mis padres, que, con su apoyo constante en mi vida, me siento capaz de poder cumplir mis metas actuales y futuras. Además, quiero agradecer a la Universidad Nacional de San Cristóbal de Huamanga, en especial a la plana de docentes de la Escuela de Ingeniería de Sistemas, quienes con su enseñanza me guiaron a lo largo de mi formación profesional.

ÍNDICE

DEDICATORIA ii
AGRADECIMIENTO iii
ÍNDICE iv
RESUMEN 7
CAPÍTULO I 9
PLANTEAMIENTO DEL PROBLEMA 9
1.1. IDENTIFICACIÓN Y ENUNCIADO DEL PROBLEMA 9
1.2. FORMULACIÓN DEL PROBLEMA 10
1.2.1 PROBLEMA GENERAL 10
1.2.2 PROBLEMAS ESPECÍFICOS 10
1.3. OBJETIVO 10
1.3.1 OBJETIVO GENERAL 10
1.3.2 OBJETIVOS ESPECÍFICOS 10
1.4 HIPÓTESIS 11
CAPÍTULO II 12
MARCO TEÓRICO 12
2.1. ANTECEDENTES DE LA INVESTIGACIÓN 12
2.2. MARCO TEÓRICO 13
2.2.1. DEFINICIONES BÁSICAS 13
2.2.2. LA SEGURIDAD DE LA INFORMACIÓN Y LA SEGURIDAD INFORMÁTICA 15
2.2.3. PYMES EN EL PERÚ 16
2.2.4. IMPORTANCIA DE LA TI EN UNA PYME 16
2.2.5. ATAQUES INFORMÁTICOS 17
2.2.6. SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN 18
2.2.7. ISO/IEC 27001 18
2.2.8. COMPARACIÓN DE LAS DIFERENTES EDICIONES DE LA NORMA ISO/IEC. 19
2.2.9. SELECCIÓN DEL MODELO DE LA ISO 27001 20
2.2.10. DISPOSICIÓN DE LA NORMA ISO/IEC 27001:2013 20
2.2.11. ISO/IEC 27002 - TÉCNICAS DE SEGURIDAD 21
2.2.12. CICLO DE DEMING (PDCA O PHVA) 22
2.2.13. SELECCIÓN DE METODOLOGÍA DE GESTIÓN DE RIESGO 23

2.2.14. METODOLOGÍA MAGERIT 23
2.2.15. ACTIVOS 25
2.2.16. AMENAZAS DE LA INFORMACIÓN 27
2.2.17. RIESGOS DE LA INFORMACIÓN 28
2.2.18. SGSI EN LAS PYMES 29
CAPÍTULO III 30
MATERIALES Y MÉTODOS 30
3.1 TIPO DE INVESTIGACIÓN 30
3.2 NIVEL DE INVESTIGACIÓN 30
3.3 DISEÑO DE INVESTIGACIÓN 31
3.4 POBLACIÓN Y MUESTRA 31
3.4.1 POBLACIÓN 31
3.4.2 MUESTRA 31
3.5 VARIABLES Y DIMENSIONES 32
3.5.1 DEFINICIÓN CONCEPTUAL DE LAS VARIABLES 32
3.5.2 DEFINICIÓN CONCEPTUAL DE LAS VARIABLES 33
3.6 TÉCNICAS E INSTRUMENTOS 33
CAPÍTULO IV 34
IMPLEMENTACIÓN DEL SGSI SEGÚN ISO/IEC 27001 EN LA PYME EKONOPHARMA.SAC 34
4.1 Planificación del SGSI 34
4.1.1 CASO DE NEGOCIO 35
4.2 FASE 1: PLANEAR (PLAN) 40
4.2.1 ANÁLISIS DE BRECHA INICIAL 40
4.2.1.1 INFORME DE ANÁLISIS DE BRECHA DE REQUISITOS 40
4.2.1.2 INFORME DE ANÁLISIS DE BRECHA DE CONTROLES 42
4.2.2 COMPROMISO CON LA ALTA DIRECCIÓN 44
4.2.3 PROPUESTA COMERCIAL DEL PROYECTO 45
4.2.4 REVISIÓN DE LA ALTA DIRECCIÓN 46
4.2.5 CONTEXTO DE LA EMPRESA 48
4.2.6 REQUERIMIENTOS Y ANTICIPACIONES DE LAS PARTES INTERESADAS 50
4.2.7 ALCANCE DEL SGSI 52
4.2.8 POLÌTICAS DE SEGURIDAD DE LA INFORMACIÓN 54
4.2.9 ROLES Y RESPONSABILIDADES 59
4.2.10 FICHA DE PUESTOS PARA ROLES DE LA SI 60

4.2.11 PROCESO DE VERIFICACIÓN DE LA DOCUMENTACIÓN INFORMATIVA 61
4.2.12 GESTIÓN Y TRATAMIENTO DE INCIDENTES 61
4.2.13 DOCUMENTACIÓN DEL PROCEDIMIENTO DE GESTIÓN DE INCIDENCIAS 63
4.2.14 PROCEDIMIENTO DE AUDITORÍA INTERNA 63
4.2.15 GESTIÓN DE RIESGOS 64
4.2.16 INVENTARIO DE LOS ACTIVOS EKONOPHARMA 68
4.2.17 IDENTIFICACIÓN DE AMENAZAS 71
4.2.18 EVALUACIÓN DE RIESGOS 73
4.2.18.1 ESTIMACIÓN DEL RIESGO 74
4.2.19 TRATAMIENTO DEL RIESGO 78
4.2.20 CONTROLES PARA ASEGURAR LA INFORMACIÓN 81
4.2.21 PLAN DE TRATAMIENTO DE RIESGOS 81
4.2.22 DECLARACIÓN DE APLICABILIDAD 82
4.2.23 MATRIZ DE COMUNICACIÓN INTERNA Y EXTERNA 91
4.2.24 PLAN DE CONCIENTIZACIÓN Y CAPACITACIÓN 92
CAPÍTULO V 95
CONCLUSIONES Y RECOMENDACIONES 95
5.1 CONCLUSIONES 95
5.2 RECOMENDACIONES 96
BIBLIOGRAFÍA 97
ANEXOS 99
PRESUPUESTO 150

RESUMEN

En los últimos años ha aumentado la cantidad de Pymes en Perú. Según información del INEI, el 99,6% de las corporaciones del país son clasificadas como pequeñas y medianas. Este incremento es por el aumento de necesidades, particularmente durante la pandemia, la cual ha generado múltiples limitaciones. Frente a esta situación, los peruanos optaron por nuevas formas de generar ingresos, las cuales continúan aplicándose en la actualidad.
La tecnología desempeña un papel fundamental en las empresas al mejorar su cadena de valor.

Además, la falta de conciencia sobre la importancia de la ciberseguridad en las PYMES puede llevar a graves consecuencias, como el robo de información confidencial, el acceso no autorizado a sistemas y la interrupción de operaciones comerciales. Es fundamental que las PYMES en Perú tomen medidas para proteger sus activos de información y datos sensibles, implementando políticas de seguridad, realizando auditorías de seguridad de manera regular y capacitando a su personal en buenas prácticas de seguridad informática.

El propósito fundamental de este proyecto es establecer que el Sistema de Gestión de Seguridad de la Información conforme a la norma ISO/IEC 27001 para ser implementado como una política de seguridad de la información para las pequeñas y medianas empresas en Perú para el año 2024. Esta iniciativa busca demostrar que el Sistema de Gestión de Seguridad de la Información para PYMES sea esencial como política de seguridad de la información, con la meta futura de obtener la certificación ISO 27001.

En este estudio se llevará a cabo un análisis de las normas ISO/IEC 27001, ISO/IEC 27002 y de los requisitos indispensables para la implantación del Sistema de Gestión de Seguridad de la Información en los activos físicos, humanos e informáticos de las PYMES. El objetivo es simplificar los obstáculos durante la implementación del SGSI debido a los recursos limitados, como el presupuesto, el personal y el conocimiento.

Palabras clave: Seguridad Informática, Sistema de Gestión de Seguridad de la Información (SGSI), ISO 27001, ISO 27002, Pymes, Riesgos, Activos físicos, Activos humanos, Activos de Información, Amenazas.

INTRODUCCIÓN

Actualmente, la mayoría de las pequeñas y medianas organizaciones no tienen un Sistema de Gestión de la Seguridad de la Información (SGSI). Esto se debe a que no consideraban esta medida como una política de seguridad de la información esencial, ya sea por falta de recursos para su implementación o por desconocimiento de los beneficios que podría aportar. Solo algunas empresas grandes disponen de los recursos económicos, humanos y tecnológicos necesarios para contratar los servicios de una empresa consultora.

La ciberseguridad se ha vuelto un elemento clave para asegurar la estabilidad y continuidad de las empresas, independientemente de su tamaño, ya que existe una conexión constante entre los datos personales y empresariales en un entorno de información interconectado.

El propósito de este proyecto es informar sobre la importancia de implementar un Sistema de Gestión de la Seguridad de la Información (SGSI) en las pequeñas y medianas empresas, así como brindar apoyo y motivación a aquellas que no cuentan con este sistema. Además, se busca asistir a las empresas que no poseen conocimientos sobre los estándares y políticas de seguridad de la información, los cuales son esenciales para establecer, implementar y supervisar un entorno seguro que garantice la confidencialidad, integridad y disponibilidad de la información

Los objetivos específicos son: a) Implementar el Sistema de Gestión de Seguridad de la Información para los activos de información según ISO/IEC 27001 como política de seguridad de la información para las Pymes del Perú, 2024.b) Implementar el Sistema de Gestión de Seguridad de la Información para los activos físicos según ISO/IEC 27001 como política de seguridad de la información para las Pymes del Perú, 2024. c) Implementar el Sistema de Gestión de Seguridad de la Información para los activos humanos según ISO/IEC 27001 como política de seguridad de la información para las Pymes del Perú, 2024.

CAPÍTULO I
PLANTEAMIENTO DEL PROBLEMA

1.1. IDENTIFICACIÓN Y ENUNCIADO DEL PROBLEMA

Según la Encuesta Global de Seguridad de la Información (2022), Grupos de ransomware afectaron a múltiples entidades gubernamentales y compañías privadas en América Latina.

Según el ESET Security Report (2023), en América Latina, dos tercios de las empresas expresaron que el mayor temor en cuanto a ciberseguridad es la pérdida o robo de información, al mismo tiempo que la mayoría considera que el presupuesto destinado a este ámbito no es adecuado.

De acuerdo con la investigación llevada a cabo por Camero y Carbajal (2020), en Perú, el 80% de las pequeñas empresas tienen una supervivencia promedio de 3 años debido a la falta de atención a la seguridad de la información, lo cual pone en riesgo su supervivencia. Según estudios, el 90% de las microempresas en el país no están preparadas para identificar vulnerabilidades en seguridad de la información, y el 51% han sido afectadas por ello. Solo un 10% de estas empresas cuentan con medidas de gestión de riesgos para protegerse.

Según la Encuesta Mundial de riesgos (2022), el 75% de los directivos de las empresas desean aumentar el gasto en el análisis de datos, la automatización de procesos y en tecnologías para apoyar la detección y el seguimiento de los riesgos.

El incremento de amenazas informáticas resalta el riesgo al que se exponen los datos de cualquier empresa, ya que la pérdida o alteración de información crucial podría llevar a la desaparición de la empresa en el futuro.

El propósito es identificar las necesidades para establecer medidas de seguridad que resguarden los datos utilizando los recursos disponibles para la empresa, con el fin de alcanzar sus metas establecidas.

1.2. FORMULACIÓN DEL PROBLEMA

1.2.1 PROBLEMA GENERAL

¿Cómo el Sistema de Gestión de Seguridad de la Información según ISO/IEC 27001 es una política de seguridad de la información para las Pymes del Perú, 2024?

1.2.2 PROBLEMAS ESPECÍFICOS

a. ¿Cómo el Sistema de Gestión de Seguridad de la Información para los activos de información según ISO/IEC 27001 es una política de seguridad de la información para las Pymes del Perú, 2024?

b. ¿Cómo el Sistema de Gestión de Seguridad de la Información para los activos físicos según ISO/IEC 27001 es una política de seguridad de la información para las Pymes del Perú, 2024?

c. ¿Cómo el Sistema de Gestión de Seguridad de la Información para los activos humanos según ISO/IEC 27001 es una política de seguridad de la información para las Pymes del Perú, 2024?

1.3. OBJETIVO

1.3.1 OBJETIVO GENERAL

Determinar que el Sistema de Gestión de Seguridad de la Información según ISO/IEC 27001 es una política de seguridad de la información para las Pymes del Perú, 2024.

1.3.2 OBJETIVOS ESPECÍFICOS

a. Implementar el Sistema de Gestión de Seguridad de la Información para los activos de información según ISO/IEC 27001 como política de seguridad de la información para las Pymes del Perú, 2024.

b. Implementar el Sistema de Gestión de Seguridad de la Información para los activos físicos según ISO/IEC 27001 como política de seguridad de la información para las Pymes del Perú, 2024.

c. Implementar el Sistema de Gestión de Seguridad de la Información para los activos humanos según ISO/IEC 27001 como política de seguridad de la información para las Pymes del Perú, 2024.

1.4 HIPÓTESIS

"No en todas las investigaciones cuantitativas se planean hipótesis. El hecho de que formulemos o no hipótesis depende de un factor esencial: el alcance inicial del estudio. Las investigaciones cuantitativas que formulan hipótesis son aquellas cuyo planteamiento define que su alcance será correlacional o explicativo, o en las que tienen un alcance descriptivo, pero que intentan pronosticar una cifra o un hecho" (Hernández, Baptista y Collado, 2014, p. 104).

CAPÍTULO II
MARCO TEÓRICO

2.1. ANTECEDENTES DE LA INVESTIGACIÓN

Según César y Martín (2019) en su estudio sobre la elaboración de un sistema de gestión de la seguridad de la información en una empresa pequeña basado en la norma ISO/IEC 27001, sugieren que el modelo SMESEC podría ser una solución para abordar la ausencia de un Sistema de Gestión de Seguridad de la Información en las pequeñas y medianas empresas en Perú. Este enfoque podría facilitar la implementación de un sistema de gestión en las PYME con el propósito de mantener un entorno protegido para preservar la confidencialidad, integridad y disponibilidad de los datos.

El ciclo Deming es útil para vincular las actividades clave que una pequeña o mediana empresa debe llevar a cabo si desea instaurar un sistema de gestión de seguridad de la información basado en la norma ISO 27001.

Aunque hay diversas metodologías para implementar un SGSI en una pyme, todas persiguen el mismo propósito: evaluar el riesgo vinculado a los activos de la empresa y establecer medidas para mitigarlo.

En Perú, la ONGEI ha proporcionado orientación a través de su plataforma en línea y el Diario el Peruano sobre la protección de la información. Su objetivo es ayudar a las entidades a resguardar datos sensibles mediante un sistema de seguridad de la información.

Actualmente, resulta ventajoso para las empresas implantar un Sistema de Gestión de Seguridad de la Información y obtener una certificación que garantice la excelencia de sus servicios y mantenga seguro sus activos para un futuro.

2.2. MARCO TEÓRICO

2.2.1. DEFINICIONES BÁSICAS

Según Roa Buendía (2013), en su compendio "Seguridad de la información", establece las siguientes definiciones:

1. Activo: Son los recursos disponibles, como el hardware, software, etc.
2. Amenaza: Es un evento o acción que pueda causar algún tipo de perjuicio, ya sea tangible o intangible, a los diferentes componentes de un sistema.
3. Identificación: La identificación es el proceso que asegura la veracidad de la identidad de un individuo o equipo, previniendo el riesgo de ser suplantado por un impostor.
4. Autorización: Es la característica que permite a un usuario o máquina acceder a diferentes privilegios una vez que ha sido verificado.
5. Acción correctiva: Es tomar medidas para corregir la raíz de un problema y evitar su repetición en el futuro
6. Alta dirección: Individuo o conjunto de individuos que lideran y supervisan una entidad en el nivel más alto.
7. Auditoría: Proceso riguroso, imparcial y documentado para recolectar evidencia de auditoría y evaluar si se cumplen los estándares de auditoría.
8. Botnet: Es un grupo de robots informáticos o bots. El responsable de la botnet controlar a distancia todos los dispositivos infectados, para llevar diversas actividades delictivas.
9. Cifrado: Se trata de la característica que asegura que solo quienes pasen la verificación puedan acceder a la información y que esta no sea útil para otros.
10. Copias de Seguridad: Se refieren a todas las duplicaciones o respaldos de los datos guardados en dispositivos de almacenamiento magnético.
11. Confidencialidad: La confidencialidad es la cualidad que asegura que la información permanezca protegida y no sea divulgada de forma no autorizados.
12. Competencia: Habilidad para utilizar el saber y destreza en alcanzar los objetivos.
13. Conformidad: Satisfacción de una condición o necesidad.
14. Contingencia: Otra manera de llevar a cabo una tarea en caso de no poder hacerlo de la manera convencional.
15. Control: Acción que altera un peligro

16. Control de acceso: Formas de garantizar que las personas autorizadas puedan acceder a los activos, de acuerdo a sus necesidades y estándares de seguridad de la empresa.
17. Corrección: Proceso para erradicar una conformidad identificada.
18. Gestión del Riesgo: Gestión coordinada de actividades para supervisar y administrar una entidad en cuanto a su exposición al riesgo.
19. Disponibilidad: La capacidad de que la información esté accesible y sea aprovechable mediante la petición de una entidad autorizada.
20. Desastres: Un inconveniente inesperado o una situación imprevista que provoca la interrupción de las operaciones comerciales durante un cierto periodo de tiempo.
21. Gusano Informático (Worm): Es un software malicioso capaz de difundirse de forma autónoma entre diferentes computadoras, replicándose en el mismo equipo u otros.
22. Hacker: Individuo con dominio de la informática que se involucra en prácticas ilegales.
23. Integridad: Mantener la integridad y precisión de los activos.
24. Impacto: Efecto analizado de una interrupción.
25. Malware: Se refiere al software dañino, malicioso o con intenciones malintencionadas, que busca infiltrarse o causar daño sin autorización.
26. Mejora continua: Actividad periódica que contribuye a la mejora del rendimiento.
27. Nivel de riesgo: La medida de peligro o la acumulación de amenazas, representadas en función de la combinación de resultados.
28. No conformidad: No cumplir con una exigencia.
29. No Repudio: En una relación entre dos partes, se impide que una de ellas pueda negar su participación en dicha relación.
30. Objetivo de control: La declaración que explica los objetivos que se pretenden alcanzar con la aplicación de controles.
31. Plan de continuidad del Negocio: Conjunto de pautas, reglas de conducta y recursos de planificación para la restauración de las operaciones ante un imprevisto.
32. Phishing: La suplantación de identidad es un tipo de fraude informático.
33. Parte interesada: Individuo u entidad que puede ser influenciada, resultar afectada o sentirse involucrada en una determinada decisión o acción.
34. Probabilidad: Probabilidad de que algún evento ocurra.
35. Responsable del Riesgo: Individuo o entidad con la autoridad y habilidad para manejar una situación de riesgo
36. Riesgo Residual: Riesgo residual posterior a la gestión del riesgo.

37. Requisito: Una necesidad o expectativa de manera implícita u obligatoria.
38. Riesgo: Impacto de la falta de certeza en el logro de metas.
39. Sistema de Gestión de Seguridad de Información: Es un conjunto de medidas que son implementadas para proteger sus activos, incluyendo políticas, procesos, directrices, recursos y actividades.
40. Tratamiento del Riesgo: Proceso de identificación y aplicación de acciones para cambiar la probabilidad de un riesgo.
41. Troyano: Un software conocido como "caballo de Troya" que se hace pasar por un programa legítimo para obtener control remoto sobre el dispositivo infectándolo una vez que se ejecuta.
42. Vulnerabilidad: Se refiere a las cualidades y características del sistema, así como la habilidad de enfrentar amenazas que pueden resultar en daños.

2.2.2. LA SEGURIDAD DE LA INFORMACIÓN Y LA SEGURIDAD INFORMÁTICA

De acuerdo con Jeimy y González (2011), la Seguridad de la Información nos brinda información sobre los peligros, riesgos, evaluación de situaciones posibles, mejores prácticas y marcos normativos, que requieren niveles de protección de procesos y tecnologías para aumentar la confianza en todas las fases de la información, desde su creación hasta su eliminación.

La seguridad de la información se enfoca en medidas preventivas para proteger los activos de información y garantizar la confidencialidad, disponibilidad e integridad de los datos, a diferencia de la seguridad informática que se concentra en proteger las infraestructuras tecnológicas de la empresa. La norma ISO 27000 define la información como cualquier conjunto de datos organizados que una entidad considera valioso, sin importar su forma de almacenamiento o transmisión, origen o fecha de creación.

a. La confidencialidad asegura que la información no se comparta ni se divulgue con personas, organizaciones o sistemas no autorizados.
b. La integridad se refiere a mantener la precisión y la integridad de la información y los procesos de procesamiento.
c. La disponibilidad garantiza que organizaciones o procedimientos autorizados tengan acceso y puedan utilizar la información y los sistemas de gestión.

Figura 1

Information security vs Cybersecurity

Nota: Adaptado de *Implementing an Information Security Management System*, por Chopra, A., & Chaudhary M., 2020.

2.2.3. PYMES EN EL PERÚ

Las Pymes son empresas pequeñas y medianas que se caracterizan por su tamaño en términos de recursos humanos, activos, ganancias y pérdidas, entre otros aspectos. Operan de manera independiente y representan una parte significativa del mercado global.

La definición de Pymes puede variar de un país a otro. En Perú, las Pymes han experimentado un aumento significativo en los últimos años" y constituyen el 99% de todas las empresas en el mercado.

Según la SUNAT (2020), Las pequeñas y medianas empresas forman parte activa de la economía nacional al llevar a cabo una variedad de actividades económicas diferentes. Las áreas de Comercio y Servicios son las que cuentan con mayor presencia de Pymes, con un 49% y 33% respectivamente, mientras que la Manufactura representa el 11% del total de empresas formales. En menor medida, el sector Agropecuario y la Construcción cuentan con un 3% cada uno.

2.2.4. IMPORTANCIA DE LA TI EN UNA PYME

Las TIC han tenido un gran impacto en la sociedad, en especial en el uso de Internet. Este fenómeno ha alcanzado al sector empresarial, donde las compañías más grandes han venido invirtiendo en sistemas de gestión como los ERP desde hace años.

Como resultado, las empresas más pequeñas han seguido su ejemplo y también han incorporado estas tecnologías para poder competir en el mercado.

ERRORES DE LAS PYMES

a No reconocer la relevancia de la información y la infraestructura.
b La seguridad se limita a hardware o software, o simplemente tener un antivirus.
c No se realizaron inversiones en tecnología.
d Excluir la cláusula de seguridad de los acuerdos con empleados, clientes y proveedores.
e Depender exclusivamente de un antivirus y un Firewall.
f No existe un campo de la informática.
g Demasiada seguridad en los trabajadores y proveedores.

2.2.5. ATAQUES INFORMÁTICOS

Según Buendía (2013), Un ciberataque consiste en el intento de asumir el control, desestabilizar o dañar un sistema informático utilizando otro sistema informático.

Los ataques informáticos más frecuentes son:

1. Denegación de servicio: Un ataque dos, abreviatura de denegación de servicio, es una forma de ataque informático que tiene como objetivo hacer que un servicio o recurso de un sistema o red esté inaccesible para los usuarios autorizados.
2. Mitm (man in the middle): Se trata de una situación en la que un hacker monitorea una comunicación entre dos partes, generalmente utilizando un escáner de puertos, y manipula los mensajes.
3. Ataques de replay ó arp: Una técnica de ataque cibernético en la cual la información válida es repetida o retardada de forma maliciosa o fraudulenta.
4. Ataque de día cero: Un ataque informático que aprovecha vulnerabilidades o fallos de seguridad en un programa para comprometer un ordenador.
5. Ataque por fuerza bruta: No siempre se requiere usar métodos informáticos para llevar a cabo este procedimiento, aunque su implementación podría resultar en un ahorro de tiempo, energía y esfuerzo.
6. Ingeniería social: La técnica de engaño y persuasión utilizada para obtener información valiosa de una persona o entidad, ya sea a través de engañar a un usuario para revelar datos personales o contraseñas al abrir un archivo adjunto.

7. Las amenazas internas incluyen el robo de información que proviene de dentro de la organización.
8. La nube: Las pequeñas y medianas empresas están optando por simplificar sus sistemas de información, optando por administrarlos a través de la nube.
9. APT (amenazas Persistentes avanzadas): Es la aparición de ataques dirigidos hacia sistemas de información, como afectar las estaciones de trabajo y los sistemas informáticos.

2.2.6. SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Un SGSI es un sistema creado con el propósito de controlar la seguridad de la información. En términos en inglés, este sistema se conoce como ISMS, por sus siglas en inglés Information Security Management System.

El Sistema de Gestión de la Seguridad de la Información (SGSI) se puede describir como una herramienta de gestión que ayuda a comprender, manejar y reducir los riesgos que pueden poner en peligro la seguridad de la información en las organizaciones.

Beneficios del SGSI

a. Reduzca los riesgos de pérdidas, robos, corrupción o uso inadecuado de información en las empresas.
b. Demuestra a clientes y socios que la empresa se preocupa por la confidencialidad y seguridad de la información, brindando seguridad.
c. Permite a la empresa llevar a cabo su producción de manera fluida.
d. Ayuda a reducir costos y aumentar la eficiencia en las operaciones.
e. Ofrece seguridad y directrices claras para el personal de la empresa.
f. Cumple con la legislación vigente en cuanto a protección de datos personales, propiedad intelectual y otras normativas aplicables.
g. Permite la integración con otros sistemas administrativos.

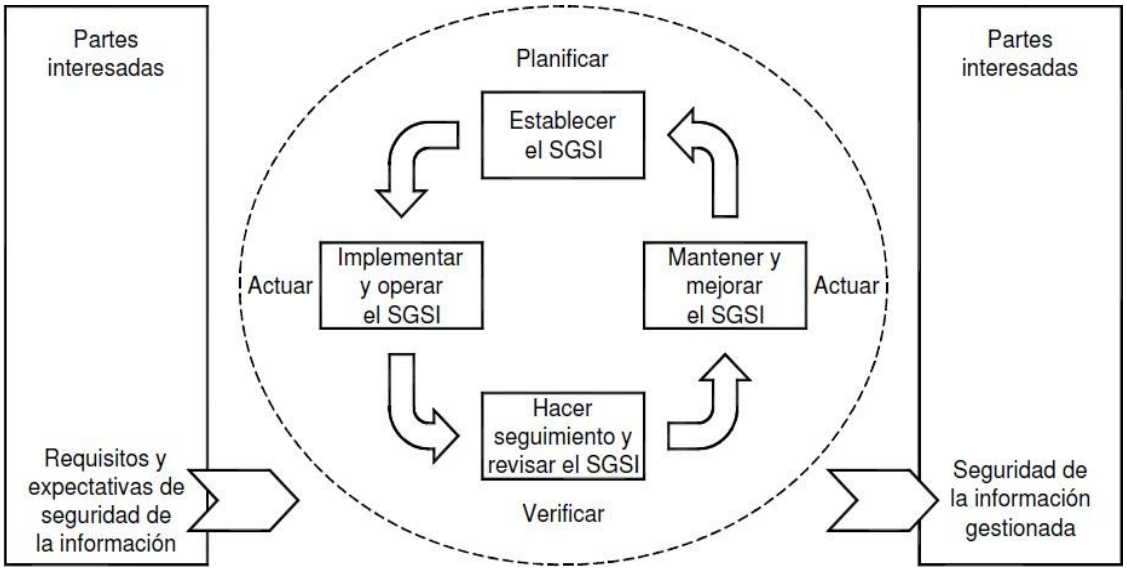
2.2.7. ISO/IEC 27001

Según lo expresado por Francisco (2016), la norma ISO/IEC 27001 establece los criterios necesarios para desarrollar, ejecutar, gestionar y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI) adaptado a las particularidades de cada entidad. Este estándar fomenta un enfoque centrado en procesos y en el ciclo de Mejora Continua, que

abarca las fases de "Planificar-Hacer-Verificar-Actuar", con el objetivo de alcanzar la excelencia en la protección de la información.

Figura 2

PDCA Model applied to ISMS processes - ISO 27001



Nota: Adaptado de *Sistema de gestión de la seguridad de la información (SGSI)*, por CONTEC, 2006, COMPENDIO (www.Icontec.org.com).

2.2.8. COMPARACIÓN DE LAS DIFERENTES EDICIONES DE LA NORMA ISO/IEC.

ISO/IEC 27001:2005: Diversas naciones habían incorporado la norma británica BS7799-2, a pesar de que era de origen británico. Para llevar a cabo su estandarización a nivel internacional, se lanzó el borrador final como la BS7799-2:2005 (ISO/IEC 27001:2005) en octubre de 2005 (Calder, 2013).

Esta norma fue adoptada en varios países y tardó 6 años en ser reconocida a nivel internacional.

ISO/IEC 27001:2013: De acuerdo con Rodríguez (2020), la normativa ISO/IEC 27001 proporcionó indicaciones para que una empresa pueda poner en marcha un Sistema de Gestión de Seguridad de la Información (SGSI), explicando detalladamente el procedimiento para su establecimiento y la forma de supervisar las medidas de protección de la información en la organización.

ISO/IEC 27001:2022: En la última versión publicada se realizaron modificaciones en las cláusulas 4.4, 8.1, 5.3, 7.4, 9.3, 10.1 y 10.2. Se creó un nuevo anexo A con solo 4 cláusulas, reduciendo las anteriores 14. Además, se añadieron 11 nuevos controles, sumando un total de 93. Los objetivos de control del Anexo A fueron revisados, actualizados, complementados y reorganizados con la inclusión de nuevos controles.

2.2.9. SELECCIÓN DEL MODELO DE LA ISO 27001

Basándose en las definiciones, se realizar una comparación con las normas reconocidas para la organización.

Tabla 1

Comparación de las normas ICEC27001

Características	**ISO-IEC27001:2014**	**ISO-IEC27001:2013**
El anexo ha sido rellenado con éxito.	Sí, pero poniendo especial atención en los segmentos del 1 al 4.	Sí, los 14 que forman parte del anexo A.
Riesgos de impactos positivos	No	Si
Alcances	GSI destaca especialmente las secciones que van desde el apartado 10 hasta el 4.	Gestión de seguridad de la información

Nota: Se implementa un cuadro para el análisis de las normas. (https://repository.unad.edu.co/bitstream/handle/10596/12028/52437232.pdf?sequence=1)

Por consiguiente, de acuerdo con los estándares mencionados, se decidió elegir la ISO-IEC27001:2013, debido a que aborda de manera detallada los aspectos del Anexo A.

2.2.10. DISPOSICIÓN DE LA NORMA ISO/IEC 27001:2013

Abad (2015) sostiene que la ISO/IEC: 2013 sigue una estructura organizada en cláusulas que se alinean con el Ciclo de Deming.

Figura 3

Structure of the ISO/IEC 27001:2013 Standard

Nota: Adaptado de *Structure of the ISO/IEC 27001:2013 Standard*, por AENOR, 2014.

2.2.11. ISO/IEC 27002 - TÉCNICAS DE SEGURIDAD

La norma ISO/IEC 27002 ofrece un conjunto de recomendaciones para asegurar la protección de la información en las organizaciones, adaptándose a sus requerimientos específicos.

En palabras de Miranda (2013), los objetivos de seguridad incluyen elementos fundamentales que deben evaluarse para asegurar un sistema seguro en todas sus facetas. En resumen, cada uno de estos objetivos tiene medidas de seguridad específicas detalladas en la norma ISO/IEC 27002.

La herramienta proporciona instrucciones detalladas para establecer medidas de seguridad de la información, que comprenden 14 áreas temáticas, 35 objetivos de control y 114 pasos para mitigar riesgos. También incluye 11 cláusulas de seguridad que cubren 39 categorías. Es responsabilidad de cada empresa determinar qué medidas son adecuadas para su implementación. Una característica importante es que la norma es compatible con diferentes tecnologías, lo que simplifica su adaptación a diferentes contextos.

Su estructura está conformada de la siguiente manera:

a. Descripción general de la seguridad de la información y el Sistema de Gestión de Seguridad de la Información.
b. Alcance: se detalla el propósito de la norma.

c. Definiciones: explicación breve de los términos más utilizados.
d. Estructura del estándar: explicación de la organización de la norma.
e. Evaluación y manejo del riesgo: pautas para evaluar y abordar los riesgos de seguridad de la información.
f. Política de seguridad: documento que establece la política de seguridad y su gestión.
g. Aspectos organizativos de la seguridad de la información: estructura interna y relación con terceros.
h. Gestión de activos: responsabilidades sobre los activos y clasificación de la información.
i. Seguridad relacionada con el personal: medidas antes, durante y después del empleo o cambio de posición.
j. Seguridad física y del entorno: áreas seguras y seguridad de los equipos.
k. Control de acceso: regulación de ingreso con base en necesidades empresariales.
l. Adquisición, desarrollo y mantenimiento de sistemas de información.
m. Gestión de incidentes de seguridad de la información: detalles sobre eventos, vulnerabilidades y medidas de mejora.
n. Gestión de la continuidad del negocio: elementos de protección de datos para garantizar la seguridad de la información en las operaciones continuas.
o. Cumplimiento: respeto a leyes, políticas y normativas relacionadas con la seguridad.

2.2.12. CICLO DE DEMING (PDCA O PHVA)

Esta estrategia se compone de cuatro fases PDCA: "Planificación", "Ejecución", "Evaluación" y "Acción", también llamado PHVA en castellano.

Se trata de un ciclo continuo en el que se identifican las actividades a mejorar y los objetivos a alcanzar en la primera fase. En la segunda fase se lleva a cabo lo que se ha planificado. Posteriormente, se prueba lo implementado durante un período de tiempo para verificar su correcto funcionamiento. En caso de no cumplir con lo esperado, se realizan ajustes necesarios para alcanzar los objetivos establecidos. Por último, en la etapa de Actuar se analizan los resultados obtenidos al finalizar el período de prueba y se comparan con la situación inicial de las actividades.

2.2.13. SELECCIÓN DE METODOLOGÍA DE GESTIÓN DE RIESGO

En este estudio se optará por el enfoque de MAGERIT como metodología para evaluar los riesgos, destacando su característica de no requerir automatización en la ejecución.

Tabla 2

Comparación de metodologías a implementar

Metodología	**ISO 25000**	**OCTAVE**	**MAGERIT**
Alcances	No se proporciona una descripción detallada de los activos de información.	No se especifican detalladamente de los activos de información.	Explica con precisión cada recurso de datos de manera detallada.
Implementación	Necesidad de obtener una licencia certificada para su uso.	Se necesita la licencia certificada para poder utilizarlo.	No es necesario automatizar su uso.

Nota: En la tabla se detalla la comparación de metodologías a implementar. (https://repository.unad.edu.co/bitstream/handle/10596/12028/52437232.pdf?sequence=1)

2.2.14. METODOLOGÍA MAGERIT

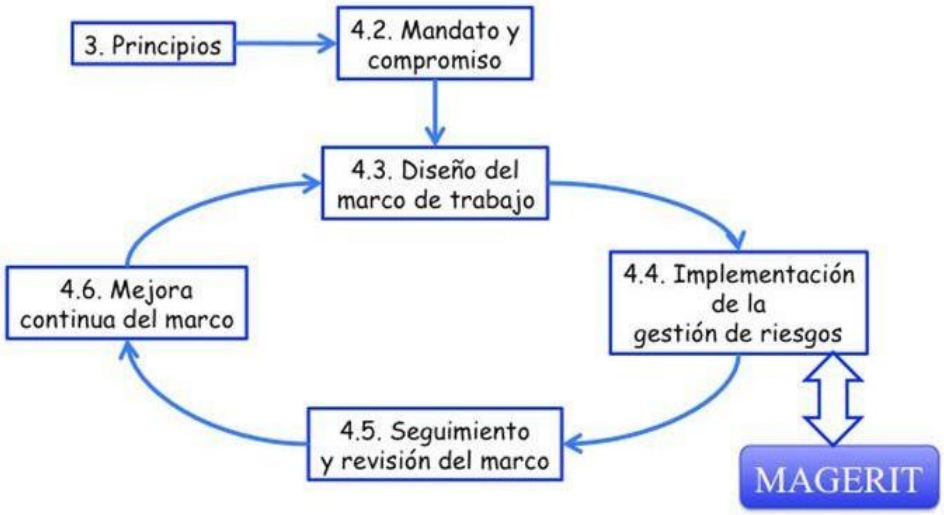
Es una metodología de acceso abierto que no necesita autorización previa para su uso, destinada a simplificar el manejo de riesgos en un ambiente laboral, permitiendo a los directivos tomar decisiones considerando los riesgos asociados con el uso de tecnologías de la información.

Para realizar un proyecto de evaluación y control de riesgos siguiendo el método MAGERIT, es necesario seguir tres etapas específicas:

a) Planificación del proyecto
b) Análisis de riesgos
c) Gestión de riesgos

Figura 4

Estructura para la administración de riesgos



Nota: Tomado de *MAGERIT-V3.0 Metodología para el Análisis y Gestión de Riesgos en Sistemas de Información* (https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html)

Esta forma de trabajo utiliza estrategias para gestionar riesgos con el objetivo de identificar vulnerabilidades a través de tecnologías informáticas, su implementación y comunicación, tomando medidas basadas en cada riesgo identificado.

Cuatro de sus objetivos incluyen:

a. Ayudar en el desarrollo de un proceso para realizar revisiones, certificaciones, auditorías o validaciones en la empresa.
b. Advertencias intimidatorias.
c. Describe estrategias adecuadas para enfrentar los exámenes de riesgos.
d. Comprender cada riesgo y tener la capacidad de abordarlos.

Según la metodología MAGERIT V3:

Un activo se describe como parte o elemento de un sistema de información que puede ser vulnerado de forma intencional o accidental, teniendo impacto en la organización. Esto abarca información, datos, servicios, programas, dispositivos, comunicaciones, recursos administrativos, físicos y humanos.

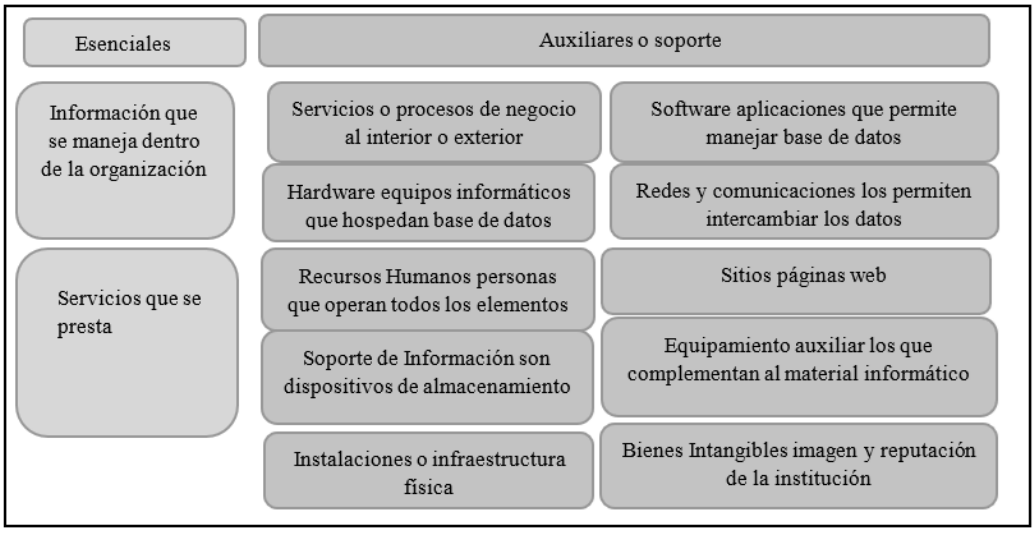
2.2.15. ACTIVOS

a) **Activos de información**

En la figura se muestra a manera de resumen los activos de información según la Metodología MAGERIT, donde clasifica de la siguiente manera: activos esenciales y activos auxiliares o de soporte.

Figura 5

Clasifican de activos de información



Nota: La imagen muestra la categorización de los recursos de información. (https://repositorio.unprg.edu.pe/handle/20.500.12893/8244)

b) Activos físicos

Un activo físico se refiere a un bien tangible que está en posesión de una persona, ya sea física o jurídica, como maquinaria, equipamiento, inmuebles, muebles, vehículos, materiales primos, productos en proceso, herramientas, entre otros.

c) Activos Humanos

Se refiere al aporte de valor económico que los trabajadores proporcionan a una empresa gracias a su pericia, destrezas y sabiduría. Este capital humano aumenta con el tiempo, sobre todo si se invierte en su crecimiento y formación.

A. Tipos de activos:

De acuerdo con el enfoque de MAGERIT, los activos se dividen en diferentes categorías como esenciales, información, servicios, programas informáticos, dispositivos, redes de comunicación, soporte de datos, equipo adicional, infraestructura y personal.

Tabla 3

Tipos de activos

Tipo de Activo	Explicación
[Esenciales] Activos Esenciales	Los activos críticos establecen las normas de seguridad que deben cumplir el resto de los elementos del sistema.
[D] Datos	Los datos son esenciales para el correcto desempeño de la entidad.
[S] Servicios	Estos son bienes que cumplen con las demandas de los usuarios, en términos de servicios proporcionados por el sistema.
[SW] Aplicaciones Informáticas (Software)	Se les conoce como programas, aplicaciones, desarrollos, entre otros. Tienen la función de automatizar, administrar y analizar datos.
[HW] Equipamiento Informático (Hardware)	Se refiere a los recursos tangibles utilizados para apoyar de manera directa o indirecta los servicios ofrecidos por la organización.
[COM] Redes de Comunicaciones	Estas instalaciones son utilizadas para contratar servicios de comunicaciones a proveedores externos.
[Media] Soporte de Información	Son aparatos tangibles que posibilitan la retención de datos de manera duradera.
[AUX]Equipamiento Auxiliar	Son aparatos que otorgan soporte a los sistemas de información, pero no están directamente conectados a la información.
[I] Instalaciones	Se refiere a lugares donde se ubican los equipos de tecnología y medios de comunicación.
[P] Personal	Las personas que tienen relación con los sistemas de información.

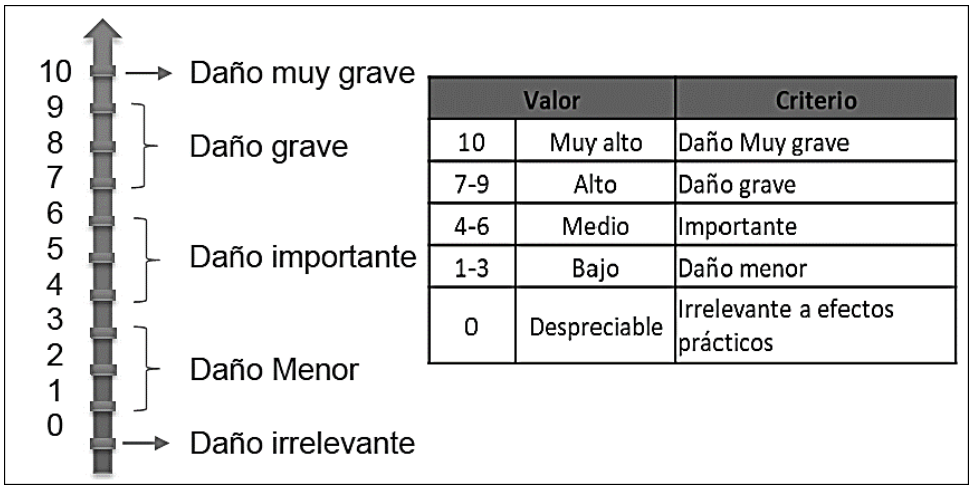
Nota: La figura representa la clasificación del tipo de activos. Tomado de *MAGERIT-V3.0 Metodología para el Análisis y Gestión de Riesgos en Sistemas de Información* (https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html)

B. Valoración de activos

En su segundo libro del catálogo de elementos, la metodología MAGERIT propone una escala unificada para la evaluación de riesgos, lo que facilita la comparación y la valoración de análisis de manera consistente.

Figura 6

Valores de los riesgos de información



Valor		Criterio
10	Muy alto	Daño Muy grave
7-9	Alto	Daño grave
4-6	Medio	Importante
1-3	Bajo	Daño menor
0	Despreciable	Irrelevante a efectos prácticos

Nota: La figura representa los valores de los riesgos. Tomado de *MAGERIT-V3.0 Metodología para el Análisis y Gestión de Riesgos en Sistemas de Información* (https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html)

2.2.16. AMENAZAS DE LA INFORMACIÓN

Una amenaza es la posibilidad de que ocurra un evento que pueda dañar un sistema de información o una organización Se refiere a la capacidad de aprovechar una debilidad para obtener, alterar o bloquear el acceso a un recurso o ponerlo en peligro. (Carpentier, 2016).

Tabla 4

Clasificación de amenazas

Tipo de Amenazas	Descripción
[N] Naturales	Estos eventos son acontecimientos que pueden tener lugar sin la influencia de los seres humanos, tales como terremotos, inundaciones, incendios, sismos, entre otros.
[IN] Origen Industrial	Pueden ser eventos que suceden de manera fortuita o causados por la actividad industrial humana, ya sea de forma accidental o intencionada.
[E] Errores y fallos no intencionados	Errores involuntarios originados por individuos que pueden suceder de forma no intencionada.

[A] Ataques intencionados	Errores intencionales causados por individuos, que buscan dañar o perjudicar a otros de manera deliberada.

Nota: La figura representa la clasificación de amenazas de los activos según la metodología MAGERIT. Tomado de *MAGERIT-V3.0 Metodología para el Análisis y Gestión de Riesgos en Sistemas de Información* (https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html)

Según Carpentier (2016), Las amenazas pueden ser categorizadas de acuerdo a su origen, tipo, motivación o acción.

Figura 7

División de las amenazas

Nota: Adaptado de *La seguridad informática en la PYME*, Carpentier (2016)

2.2.17. RIESGOS DE LA INFORMACIÓN

Un riesgo se refiere a la evaluación de la posibilidad de que una amenaza afecte a uno o varios activos de la empresa, causando daños o pérdidas. Los riesgos pueden ser categorizados de acuerdo a su origen, ya sea externo o interno. (Carpentier, 2016).

A Riesgos externos

Ataques enfocados pueden tomar la forma de infecciones de virus o ataques a gran escala a la red, como la denegación de servicio. Incidentes no focalizados. Las amenazas que pueden derivar en daños físicos (como robo o destrucción de equipos) o pérdidas de información debido a intrusiones de terceros.

B Riesgos internos

Son más fáciles de entender porque forman parte de los activos internos de la empresa.

2.2.18. SGSI EN LAS PYMES

Las grandes empresas tienen recursos, mientras que las pequeñas empresas requieren soluciones fáciles de usar y accesibles para afrontar los riesgos.

Por eso, la adopción de un SGSI puede ser una opción adecuada para que las PYMES establezcan una metodología y medidas de seguridad de forma continua, aunque no se pueda garantizar una seguridad al 100%.

Según INTECO, se observa una serie de beneficios:

i. Reducción de riesgos: Desde la evaluación de posibles peligros o amenazas requerido por la normativa, hasta la puesta en marcha de las medidas de control, todas las acciones tomadas disminuirán los riesgos a un nivel aceptable para las pequeñas y medianas empresas.
ii. Ahorro económico: Seguir la norma brinda la oportunidad de optimizar los recursos y disminuir los costos. al basar las decisiones en datos numéricos, no solo cualitativos, se facilita una gestión más eficiente del presupuesto en tecnología.
iii. La implementación del Sistema de Gestión de la Seguridad de la Información convierte la seguridad en un proceso gestionado, reemplazando acciones técnicas por un ciclo supervisado y sistematizado. Al involucrar a todos los miembros de la organización, se destaca la importancia de la calidad en la seguridad.
iv. Cumplimiento legal: Es fundamental seguir las leyes actuales. Todos los aspectos legales de la normativa deben cumplir con las leyes del país, y se verifica que se cumplan adecuadamente. Por tanto, la certificación asegura este cumplimiento y también establece una legislación que brindará protección a la empresa.
v. Competitividad en el mercado: La relevancia de esta norma es similar a la de ISO 9000 en la actualidad. Con el tiempo, las grandes empresas, clientes y socios comenzarán a exigir esta certificación para colaborar con las PYME. Esto es fundamental para asegurar un equilibrio en las medidas de seguridad entre todas las partes involucradas, convirtiéndola en un aspecto crucial para destacar frente a la competencia.

CAPÍTULO III

MATERIALES Y MÉTODOS

3.1 TIPO DE INVESTIGACIÓN

De acuerdo a Hernández, Fernández y Baptista (2014), “la Investigación aplicada se distingue por tener propósitos prácticos inmediatos definidos, es decir, se investiga para actuar, transformar, modificar o producir cambios en un determinado sector de la realidad. Para realizar investigaciones aplicadas es muy importante contar con el aporte de las teorías científicas, que son producidas por la investigación básica y sustantiva". Por esta consideración el tipo de **investigación es aplicada.**

3.2 NIVEL DE INVESTIGACIÓN

De acuerdo al autor Hernández Sampieri et. al (2014), las investigaciones descriptivas vienen a ser "los estudios descriptivos buscan especificar las propiedades, las características y los perfiles importantes de personas, grupos, comunidades o cualquier otro fenómeno que se someta a análisis." Una de las funciones principales de la investigación descriptiva es la capacidad para seleccionar las características fundamentales del objeto de estudio y su descripción detallada de las partes, categorías o clases de dicho objeto”; y agrega “La investigación descriptiva es uno de los tipos o procedimientos investigativos más populares y utilizados por los principiantes en la actividad investigativa. Los trabajos de grado, en los pregrados y en muchas maestrías, son estudios de carácter eminentemente descriptivo. En tales estudios se muestran, narran, reseñan o identifican hechos, situaciones, rasgos característicos de un objeto de estudio, o se diseñan productos, modelos, prototipos, guías, etcétera.

De acuerdo al autor Carrasco (2019), señala que, la investigación descriptiva se soporta principalmente en técnicas como la encuesta, la entrevista, la observación y revisión documental. Este tipo de investigación estudia, analiza, describe y especifica situaciones y propiedades de personas, grupos, comunidades o cualquier otro fenómeno u objeto que sea sometido al análisis. Por esta consideración el nivel de **investigación es descriptivo.**

3.3 DISEÑO DE INVESTIGACIÓN

De acuerdo con el autor Hernández Sampieri et. al. (2014), se puede definir la investigación no experimental, "como aquella investigación que se realiza sin manipular deliberadamente las variables, se trata de estudios donde no hacemos variar en forma intencional las variables independientes para ver su efecto sobre otras variables. Lo que hacemos en la investigación no experimental es observar fenómenos tal como se dan en su contexto natural, para posteriormente analizarlos" (p. 191).

Según Carrasco (2019), la investigación de diseño transversal descriptivo se utiliza para examinar y comprender las características, cualidades internas y externas, propiedades y rasgos esenciales de los hechos y fenómenos en un momento específico. Según Hernández et al. (2014), una investigación de diseño transversal implica la recopilación de datos en un solo momento o periodo de tiempo, con el fin de describir variables y analizar los hechos tal como se presentan. Los instrumentos de recolección de datos son utilizados de manera única durante el proceso.

En esta investigación se tiene que conocer procesos, características, estudiar rasgos y entender funcionalidades para encontrar datos necesarios para la construcción modelo operativo; por lo tanto, el diseño de investigación es **no experimental de tipo transversal descriptivo.**

3.4 POBLACIÓN Y MUESTRA

3.4.1 POBLACIÓN

Todos los clientes que recurren a los servicios de la empresa Ekonopharma. En este caso seria 20 clientes por día promedio, en cada establecimiento.

3.4.2 MUESTRA

Sistema de Seguridad de la Información ISO/IEC 27001 orientado a la muestra.

CALCULO DEL TAMAÑO DE MUESTRA EN EL MUESTREO SIMPLE ALEATORIO.

$$n = \frac{N \times S^2 \times Z(\propto/2)^2}{N \times d^2 + (s^2 \times Z(\propto/2)^2)}$$

$$n = \frac{20 \times 15^2 \times 1.96^2}{20 \times 2.5^2 + (15^2 \times (1.96)^2)}$$

$$n = 17$$

N=20, Z=1.96, s= 15 y d=15%.

Se tomo una muestra preliminar de 20 clientes con diferentes entradas diaria en ventas del negocio, resultando el tamaño de la muestra seria 17 clientes, contando con una precisión del 10%, y una varianza de 15.

3.5 VARIABLES Y DIMENSIONES

3.5.1 DEFINICIÓN CONCEPTUAL DE LAS VARIABLES

VARIABLE DE ESTUDIO 1

a. **Sistemas de Gestión de la Seguridad de la Información:** "Un sistema de gestión de la seguridad de la Información, es un enfoque gerencial para la seguridad. Se trata de un amplio proceso de gestión de riesgos sobre la seguridad. Como con todos los sistemas de gestión, en un sistema de gestión de la seguridad se prevé la fijación de objetivos, planificación y medición del desempeño. Un sistema de gestión de la seguridad es parte de una organización. Se convierte en parte de la cultura, y de la forma en que realizamos un trabajo". (Karina Miranda-Vázquez, 2013, p.4).

DIMENSIONES

a. **Activos de información:** Los activos de información son elementos clave en una política de seguridad, ya que permiten a la empresa identificar riesgos y tomar medidas para protegerlos. Estos activos incluyen documentación relevante, servidores, bases de datos y más.

b. **Activos físicos:** Son activos que poseen un valor intrínseco y están formados por máquinas, equipos, edificios y otros bienes de inversión de la empresa.

c. **Activos humanos:** Está formado por aquellas personas que gestionan la información. Las personas pueden generar acciones de control muy importantes dentro de una organización como: privilegios de acceso de usuarios, necesidad de aprobación de acciones por parte de determinados responsables, almacenamiento de información. Todo dependerá del riesgo de información al que este sujeto el activo persona.

VARIABLE DE ESTUDIO 2

i. **Política de seguridad de la información:** Se busca que este comité sea responsable de liderar y respaldar la administración de la seguridad de la información. La Alta Dirección debe establecer una política que refleje las directrices de la organización en cuanto a seguridad, aprobarla y comunicarla adecuadamente a todos los empleados. Este comité incluye controles tales como el documento de la Política de Seguridad de la Información y la revisión de la misma.

DIMENSIONES

i. Pymes**:** Las Pymes se refieren a las empresas de pequeño y mediano tamaño que operan de manera independiente, y constituyen una parte significativa del mercado global. Según la información proporcionada por el portal del empresario MYPE del ministerio de producción del Perú, se considera que una empresa es pequeña si cuenta con entre 1 y 100 empleados.

3.5.2 DEFINICIÓN CONCEPTUAL DE LAS VARIABLES

VARIABLE DE ESTUDIO 1

i. Sistemas de Gestión de la Seguridad de la Información

DIMENSIONES

ii. Activos de información
iii. Activos físicos
iv. Activos humanos

VARIABLE DE ESTUDIO 2

i. Política de seguridad de la información

DIMENSIONES

i. Pymes

3.6 TÉCNICAS E INSTRUMENTOS

a. TÉCNICAS

Análisis documental

b. INSTRUMENTOS

Fichas de Análisis Documental

CAPÍTULO IV

IMPLEMENTACIÓN DEL SGSI SEGÚN ISO/IEC 27001 EN LA PYME EKONOPHARMA.SAC

4.1 Planificación del SGSI

Se analizaron los componentes necesarios para diseñar la planificación del Sistema de Gestión de Seguridad de la Información, se creó un calendario en el Anexo A.

Según las últimas actualizaciones de la Norma ISO 27001, se centran en el enfoque de mejora continua mediante el ciclo PDCA (Plan-Do-Check-Act), contiene etapas para evaluar el nivel de progreso logrado por Ekonopharma. Se llegará a la fase1 Planear.

Tabla 5

Registro de documentos de ciclo de mejora continua PDCA. (fase planificar)

PLAN/ PLANEAR
1. Initial gap analysis report
2. High management commitment agreement
3. Organization context report
4. Stakeholder needs and expectations report
5. Information Security Management System (ISMS) scope statement
6. Information Security Policy
7. Job description for information security roles
8. ISMS objectives control dashboard
9. Procedure for controlling documented information
10. Risk assessment and treatment procedure
11. Internal audit procedure
12. Risk management report
13. Risk and opportunity treatment plan
14. Controls applicability statement
15. Internal and external communication matrix
16. Training and awareness plan

Nota: Se detalla en esta tabla la lista de entregables. Tomado de *La mejora continua: el ciclo pdca*, Héctor Santiago, 2001.

Tabla 6

Conexión Familiar ISO 27000

Metodología	**ISO 27001(requisitos del SGSI) – Sección**	**ISO 27002(código de buenas prácticas) – Sección**
Salida del proyecto	5.1 y 5.2.1	
P	4.2.1	
H	4.2.2 y 5.2.2	5 a 15
V	4.2.3.,6y7	
A	4.2.3 y 8	

Nota: Esta tabla que muestra la metodología y las normas que serán implementadas en la Empresa EKONOPHARMA.SAC.

Tabla 7

Equipo que participará en el proyecto

Nombre	**Unidad organizacional**	**Cargo**	**E-mail**
Lisset L.	Ekonopharma	CISO	lissetkarenlim@gmail.com
Pool C.	Ekonopharma	Gerente y QF	Poolchavez_qf_02_09@gmail.com
Rubén C. y Linda H.	Ekonopharma	Coordinadores QF	Ruben_qg_12@gmail.com lindaH_qf_9@gmail.com

Nota: La tabla representa la lista de participantes en el proyecto.

4.1.1 CASO DE NEGOCIO

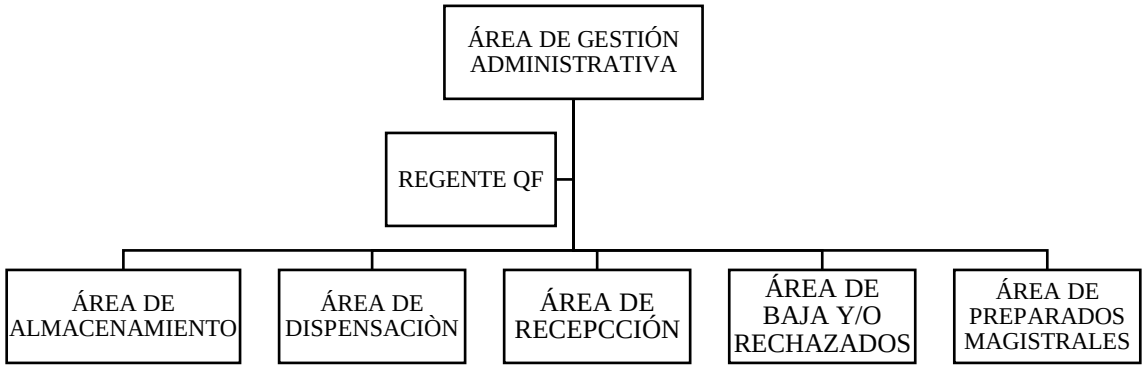
EKONOPHARMA SAC es una empresa farmacéutica, que opera por ahora con dos boticas en la actualidad, su sede principal está situada en Av. Ramón Castilla N °306, a cinco cuadras de la Plaza de Armas, en Huamanga, Ayacucho. Se especializa en la venta de productos de salud y busca proteger la información de sus clientes, proveedores, fórmulas magistrales y datos financieros para garantizar su confidencialidad y evitar su pérdida o robo. Actualmente, la empresa cuenta con siete empleados.

A. ESTRUCTURA ACTUAL DE LA EMPRESA EKONOPHARMA.SAC

La estructura de Ekonopharma está compuesta por 6 áreas fundamentales.

Figura 8

Organigrama EKONOPHARMA



Nota: La figura detalla las diferentes áreas del organigrama. Tomada de *Archivos Ekonopharma.*

La estructura de Ekonopharma se compone de la siguiente forma:

a) Área de gestión Administrativa: Responsable de manejar las cuestiones financieras de Ekonopharma, incluyendo la administración y control de los ingresos y egresos.

b) Área de almacenamiento: Responsable de gestionar la compra y almacenamiento de productos médicos, como materias primas y otros materiales, provenientes de distintos proveedores. Esta sección contará con:

1. Buenas condiciones de luz y ventilación
2. Ventilación apropiada (natural y artificial)
3. Espacio suficiente para realizar la limpieza diaria
4. Un termo higrómetro calibrado
5. Un extintor con carga vigente
6. Un botiquín de primeros auxilios
7. Una parihuela

c) Área de dispensación: responsable de administrar la comercialización de los medicamentos.

d) Área de Baja y/o Rechazados: En Ekonopharma, este departamento se encarga de verificar y seleccionar las fechas de caducidad o autenticidad de los medicamentos que deben ser descartados pronto.

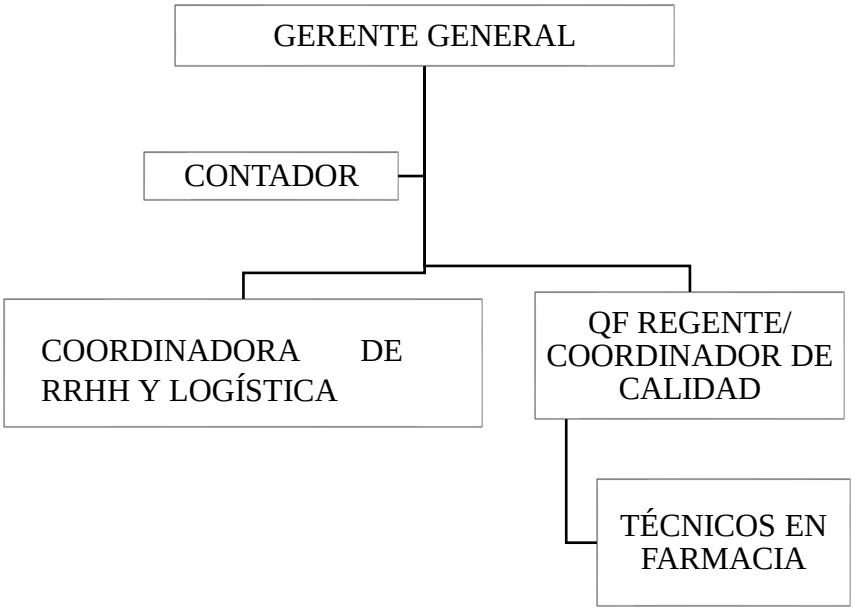
e) Área de preparados magistrales: En este lugar se ocupan de elaborar los medicamentos personalizados mediante la formulación, envasado e impresión de cada preparado magistral para el cliente.

En la actualidad, la Tecnología de la Información no se encuentra presente a pesar de su importancia en el control técnico requerido para aplicar políticas informáticas. En la empresa, no se brinda formación en seguridad de la información a los empleados. Ante estos desafíos identificados, es necesario buscar soluciones en este escenario.

a) Las políticas de seguridad de la información no están establecidas en Ekonopharma, lo cual es fundamental para proteger la información vital de la empresa y asegurar su continuidad.
b) La ausencia de un comité de seguridad de la información implica que las políticas se crean, revisan y modifican de manera reactiva, sin una planificación adecuada.
c) Los controles técnicos actuales no cumplen con su función de manera eficaz.
d) No se realiza un análisis completo de los riesgos para los activos de información más importantes.

Figura 9

Organigrama funcional de la empresa Ekonopharma



Nota. La figura representa el Organigrama funcional de la empresa EKONOPHARMA. Adaptada de *Archivos Ekonopharma.*

B. CARGOS Y FUNCIONES:

Tabla 8

Cargos y funciones de la empresa Ekonopharma

Gerente General:	• Garantizar que la botica funcione de manera adecuada • Proporcionar formación continua al personal de las Boticas junto con el Q.F. Regente • Contratar y dar de baja a los empleados • Asegurarse de que se cumplan los requisitos establecidos por las instituciones Coordinadores de salud.
QF Regente: /Coordinador De Calidad	• Comprobar y supervisar que las recetas se despachen de acuerdo con lo establecido. • Garantizar que el almacenamiento de los productos farmacéuticos y similares asegure su adecuada conservación, estabilidad y calidad. • Formar, capacitar y supervisar de manera constante al personal asistente y auxiliar para que realicen sus funciones correctamente. • Mostrar de forma visible una credencial con su nombre, profesión, número de colegiatura y cargo mientras realiza sus tareas.
Coordinadora de RRHH y Logística	• Coordinar el reclutamiento y selección de personal. • Administrar y mantener actualizada la información de los trabajadores registrados. • Supervisar el desarrollo profesional de los trabajadores. • Gestionar los recursos humanos y logísticos para la empresa. • Asegurar que se cumplan las políticas y los procedimientos.
Técnicos en Farmacia	• Supervisar y garantizar que las recetas se despachen de acuerdo a lo establecido. • Brindar orientación e información a los clientes sobre el uso adecuado de medicamentos y productos similares. • Presentar al cliente diferentes opciones de medicamentos. • Colaborar en el control de las fechas de caducidad al dispensar un producto farmacéutico.

Nota. La tabla representa las funciones por cargo de la empresa Ekonopharma. Adaptada de *Archivos Ekonopharma*.

C. PROCESOS DE EKONOPHARMA S.A.C.

PROCESO ESTRATÉGICO

a) Gestión Comercial: Durante este procedimiento se define la franquicia, se pone énfasis en la satisfacción del cliente, se elabora una estrategia de precios y marketing.

PROCESOS OPERATIVOS (Procesos Core de la empresa)

b) Recepción y almacenamiento de productos farmacéuticos, dispositivos médicos y productos sanitarios: Crear normas, procesos apropiados para recibir, revisar y almacenar, teniendo en cuenta las condiciones específicas de temperatura, luz y humedad indicadas por el fabricante, de acuerdo con el protocolo operativo establecido.

c) Dispensación y/o Expendio de productos farmacéuticos, dispositivos médicos y productos sanitarios: La correcta dispensación asegura que el paciente reciba los productos o dispositivos en la dosis y cantidad indicada, con instrucciones claras sobre su uso, seguridad y conservación.

d) Elaboración de Preparados Magistrales: Se trata del procedimiento encargado de crear y administrar fórmulas adaptadas a las necesidades individuales de cada paciente, específicamente destinadas a tratar cada enfermedad. Se asignan los recursos según la complejidad y extensión del tratamiento, y se lleva a cabo un seguimiento detallado de cada fórmula magistral desde su inicio hasta su conclusión.

e) Retiro y destrucción de medicamentos vencidos, deteriorado: Durante esta etapa, el responsable sigue las directrices proporcionadas por Digemid para la eliminación adecuada de medicamentos.

Procesos de Apoyo

a) Control de Calidad: En este momento se asegura que los productos y servicios cumplan con las normas de Digemid, garantizando su calidad, reduciendo posibles errores y mejorando la eficiencia en los costos de producción.

b) Gestión de recursos humanos y logística: Implica la supervisión adecuada de los empleados y los recursos logísticos de la empresa, garantizando que las actividades se desarrollen de forma eficiente y se cumplan los objetivos establecidos por la organización.

c) Gestión de contabilidad y finanzas: La contabilidad se encarga de la gestión de las finanzas y aspectos contables de la empresa. Se encarga de registrar los gastos y pagos a través de un registro de caja, mientras que las responsabilidades tributarias y laborales son manejadas por un contador externo.

4.2 FASE 1: PLANEAR (PLAN)

En el comienzo de esta fase, se busca implementar el Sistema de Gestión de Seguridad de la Información con el objetivo de examinar la situación inicial de la empresa en relación con los requisitos y controles establecidos en la norma ISO/IEC 27001:2013. Para lograrlo, se lleva a cabo una evaluación del entorno y posibles carencias (identificación de brechas en requisitos y controles). Estas evaluaciones tienen como finalidad definir y aclarar la situación actual de la compañía "EKONOPHARMA".

El Plan de proyecto se aplica a todos los procesos Core y a las que se relacionan entre ellas, y está dirigido a los miembros de la alta dirección y del equipo del proyecto. Para elaborar el Plan del Proyecto, se comenzará realizando varios tipos de análisis, como cuestionarios a los trabajadores y reuniones a los responsables de áreas, en el ANEXO B se detalla:

4.2.1 ANÁLISIS DE BRECHA INICIAL

Se recogieron las opiniones de los trabajadores de la compañía Ekonopharma mediante encuestas, cuyos resultados se presentan en el ANEXO C. Posteriormente, se realizaron dos análisis de discrepancias basados en los resultados de las encuestas y de la reunión con los directivos. Uno de los análisis evaluó el grado de cumplimiento de los requisitos iniciales, mientras que el otro examinó los controles establecidos.

4.2.1.1 INFORME DE ANÁLISIS DE BRECHA DE REQUISITOS

Para realizar esta evaluación de la discrepancia en el cumplimiento, se emplearon los criterios de la norma ISO/IEC 27001:2013 y se examinaron teniendo en cuenta los niveles de cumplimiento especificados en la tabla correspondiente.

Tabla 9

Grados de cumplimiento de requisitos

Descripción	Puntaje	Puntuación	Detalle
Completo	3	100%	Se ha cumplido al 100% con el requisito y se ha proporcionado la evidencia correspondiente.
Desarrollo	2	70%	En proceso de avance, se ha logrado un cumplimiento del requisito del 70%, mostrando evidencia de ello, aunque aún no se ha alcanzado el total del 100%.
Inicio	1	40%	Inicio, alrededor del 40% de ocurrencia. Se pueden observar señales de que se cumple con el requisito, aunque no hay pruebas concretas de ello.
No existe	0	0%	No existe, 0% de ocurrencia, no hay registros ni pruebas del cumplimiento.

Nota: La tabla muestra los diferentes niveles de cumplimiento de requisitos utilizados para evaluar la empresa Ekonopharma.

En el ANEXO C se detallan la evaluación detallada de cada control especifico, los resultados obtenidos son:

Figura 10

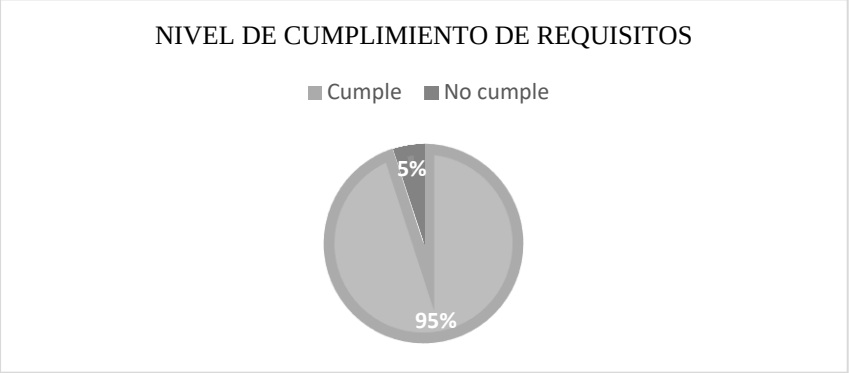
Resultados estadísticos

Nota: El gráfico representa los logros de la compañía Ekonopharma.

Luego de examinar cada requisito, el nivel promedio de cumplimiento es 5%. En nivel evaluado es muy bajo, sin embargo, el contexto y soporte son los más altos, siendo aún insuficiente para el resultado esperado de Ekonopharma.

Figura 11

Resultados de la evaluación los requisitos establecidos en la norma ISO/IEC 27001:2013.



Nota: El gráfico muestra los resultados en porcentaje de Ekonopharma.

4.2.1.2 INFORME DE ANÁLISIS DE BRECHA DE CONTROLES

Se llevó a cabo la evaluación de controles para obtener un panorama preciso de cuáles controles estaban ausentes y cuáles estaban presentes, así como para determinar su necesidad. Por lo tanto, se examinó y se detalla esta información en el ANEXO C.

Tabla 10

Niveles de cumplimiento de controles

Descripción	Puntaje	Puntuación	Detalle
Completo	3	100%	El control ha sido implementado, respaldado por la dirección ejecutiva y comunicado (según sea necesario).
Desarrollo	2	70%	Se está llevando a cabo la implementación del desarrollo de control.
Inicio	1	40%	Se ha comprendido la necesidad de implementar una supervisión. La supervisión apenas ha empezado.
No existe	0	0%	No existe supervisión, no se encuentra presente.

Nota: La tabla representa los niveles de cumplimiento de controles para evaluar la empresa Ekonopharma.

Estos resultados obtenidos para cada control se detallan en el ANEXO C

Tabla 11

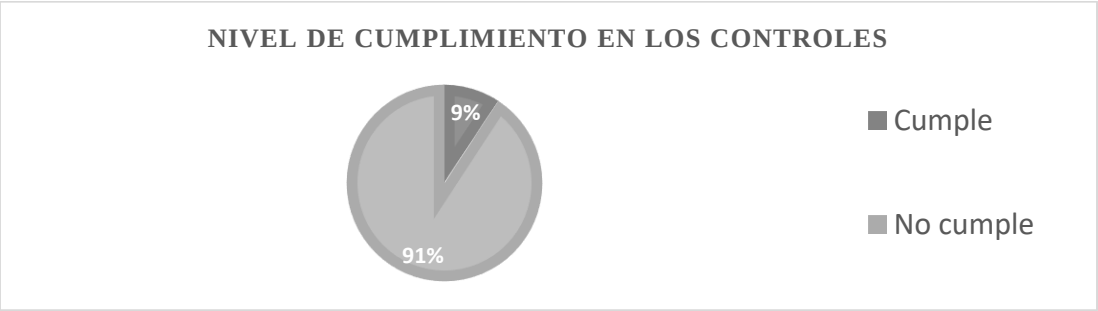
PORCENTAJES DE CUMPLIMIENTO POR CONTROL

N.º	DOMINIOS EVALUADOS SEGÚN ISO 27002	ANÁLISIS DE BRECHA INICIAL	
A.5	Políticas de seguridad de la información	5%	Inicio
A.6	Organización de la seguridad de la información	0%	No existe
A.7	Seguridad de los recursos humanos	5%	Inicio
A.8	Gestión de activos	5%	Inicio
A.9	Control de acceso	10%	Inicio
A.10	Criptografía	-	No aplica
A.11	Seguridad física y ambiental	10%	Inicio
A.12	Seguridad de las operaciones	10%	Inicio
A.13	Seguridad de las comunicaciones	10%	Inicio
A.14	Adquisición, desarrollo y mantenimiento de sistemas	-	No aplica
A.15	Relación con los proveedores	0%	No existe
A.16	Gestión de Incidentes de seguridad de la información	0%	No existe
A.17	Aspecto de seguridad de la información en la gestión de continuidad del negocio	5%	Inicio
A.18	Cumplimiento	5%	Inicio

Nota. La tabla representa los resultados totales del cumplimiento por control de la ISO/IEC.

Figura 12

Gráfico de Resultados del Análisis Inicial de Brechas



Nota. La tabla representa los resultados en porcentajes del nivel de cumplimiento de los controles.

Tabla 12

Niveles de cumplimiento

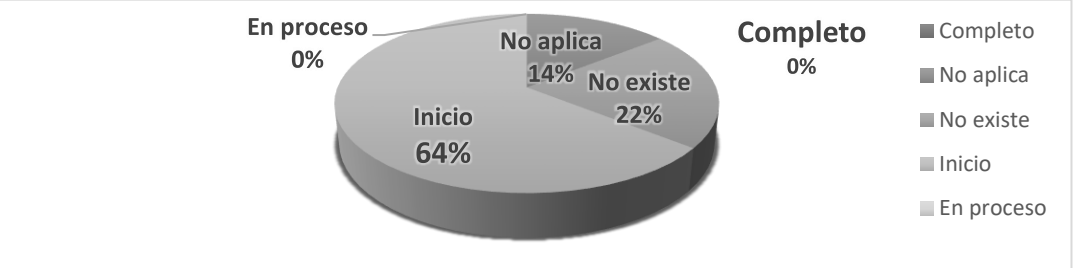
NIVELES DE MADUREZ	CUMPLIMIENTO
Completo	0%

En proceso	0%
Inicio	70.21%
No existe	17.67%
No aplica	12.12%

Nota. La tabla representa los porcentajes de cumplimiento de controles en Ekonopharma.

Figura 13

Diagrama circular que muestra el nivel de aplicación y cumplimiento.



Nota. La tabla muestra los resultados de la evaluación de qué tan cumplidos están los controles de la ISO/IEC.

La comparación de estudios nos ha proporcionado datos importantes sobre la empresa, permitiéndonos comprender su situación actual y estimar los recursos, tiempo y esfuerzo necesarios para iniciar la implementación de la primera etapa del Sistema de Gestión de Seguridad de la Información (SGSI).

4.2.2 COMPROMISO CON LA ALTA DIRECCIÓN

Se trató el tema de la protección de los datos en la compañía al exponer la "Propuesta Comercial" al gerente general, que comprendió una evaluación de la situación actual y las mejoras sugeridas, con actividades, recursos, plazos y alcance. Igualmente, se elaboró y consiguió la firma del "Acta de Compromiso" en el ANEXO D, en la que se describen los compromisos específicos para establecer, implementar, optimizar y conservar el Sistema de Gestión de Seguridad de la Información.

Después de recibir la aprobación de la propuesta, se procedió a detallar el contenido del compromiso en el acta a la cúpula directiva, la cual fue firmada por el Gerente General y el Coordinador de Calidad.

La dirección de Ekonopharma reafirmó su compromiso total con las políticas de seguridad vigentes, comprometiéndose a mantener las directrices establecidas en el documento y a proporcionar los recursos necesarios para su cumplimiento. Además, se acordó publicar y distribuir el documento a todos los empleados para que estén al tanto de los objetivos, políticas, principios y normas adoptadas por la dirección y su importancia para la seguridad de la organización.

4.2.3 PROPUESTA COMERCIAL DEL PROYECTO

Se propone la adopción del Sistema de Gestión de Seguridad de la información en la compañía Ekonopharma como una medida para resguardar los activos de información, tanto materiales como humanos, con el fin de garantizar su protección. Se pretende implementar este sistema siguiendo los lineamientos de la normativa ISO/IEC 27001:2013 en Ekonopharma.

A. PROPÓSITO DE LA PROPUESTA

El objetivo de la propuesta es establecer un protocolo de protección de datos en Ekonopharma de acuerdo con las pautas establecidas en la normativa ISO/IEC 27001:2013.

B. ALCANCE DEL PROYECTO

Dentro del marco del Sistema de Gestión de Seguridad de la Información (SGSI) se incluyen una variedad de procedimientos y enfoques establecidos.

Procesos Operativos (Core)

b) Recepción y Almacenamiento de productos farmacéuticos, dispositivos médicos y productos sanitarios.
c) Dispensación y/o Expendio de productos farmacéuticos, dispositivos médicos y productos sanitarios.
d) Elaboración de Preparados Magistrales
e) Retiro y destrucción de medicamentos vencidos o deteriorados.

Procesos de Apoyo

f) Control de Calidad
g) gestión de recursos humanos y Logística.

C. ALCANCE NO CONTEMPLADO

a) Gestión financiera (proceso externo)
b) Gestión Comercial (proceso externo)

No se abarcará el proceso de gestión financiera, ni comercial ya que se consideran procesos externos y no está tan relacionado con los procesos Core de la empresa Ekonopharma.

D. PROPUESTA DE SOLUCIÓN

Se aconseja utilizar el enfoque de mejora continua PDCA, basado en el ciclo de Deming, y seguir los lineamientos de la norma ISO 27001 para implementar un Sistema de Gestión de la Seguridad de la Información.

Los beneficios que se obtienen al implementar este sistema en una empresa son los siguientes:

a. Brindan a los clientes servicios y productos más seguros y confiables.
b. Se minimiza la posibilidad de que la información sea perdida o hurtada.
c. Se lleva a cabo una revisión constante de los riesgos y controles.
d. Se gana la confianza de clientes y socios estratégicos.
e. Puede ser utilizada en conjunto con otras metodologías de gestión como la ISO/IEC 9001, ISO/IEC 14001, entre otras.
f. Los colaboradores de la organización tendrán confianza y reglas bien definidas.
g. Aporta un beneficio adicional a la empresa, lo que contribuye a fortalecer su reputación.

4.2.4 REVISIÓN DE LA ALTA DIRECCIÓN

A. CONSEGUIR RESPALDO POR PARTE DE LA DIRECCIÓN

La Es fundamental contar con el respaldo de la Alta Dirección en la selección del consultor para la empresa Ekonopharma, por lo tanto, es importante evaluar las opciones disponibles:

1.-Implementar el estándar usando personal propio de la organización

2.-Implementar el estándar uno mismo (HUM).

3.-Seleccionar un consultor, este consultor debe tener:

a) Experiencia y habilidades
b) Reputación
c) Servicio personalizado

d) Lenguaje.

En EKONOPHARMA, estableceremos un estándar basado en el enfoque HUM (Hacerlo usted mismo), aprovechando el conocimiento externo. Vamos a colaborar con los empleados para que también adquieran el conocimiento, la documentación y el respaldo necesario de fuentes externas.

Cuando se emplea el estándar con un enfoque de "Hacerlo usted mismo" se logrará una mayor capacitación para los empleados, la recopilación de documentos confidenciales de la empresa sin tener que depender de personal externo, y se reducirán los costos de implementación para la empresa.

Se logrará una posición competitiva diferenciada, los consumidores confiarán en la seguridad de sus datos y en la calidad de los productos que compran, especialmente en cuanto a su distribución:

a. Se percibirá una disminución en los gastos de los temas vinculados a la ciberseguridad y confidencialidad que son de gran importancia los cuales suelen ser vistos como un costo. No obstante, existen beneficios financieros en la reducción de gastos ocasionados por incidentes, interrupciones en el servicio, filtraciones de datos o conflictos con empleados actuales o pasados.
b. La empresa podría estar expuesta a riesgos como incendios, robos, entre otros. Se concluye que estas amenazas pueden ser evitadas mediante la prevención, lo que sugiere una inversión mínima en medidas preventivas y la obtención de altas ganancias al eliminar estos riesgos que podrían representar un costo anual considerable para Ekonopharma.
c. En Ekonopharma se ha identificado dificultades en la toma de decisiones, la gestión de activos y el acceso a sistemas de información, lo que impacta en la eficacia de los procesos empresariales. Por lo tanto, implementar la norma ISO 27001 se presenta como la solución ideal, ya que clarifica funciones y responsabilidades, fortaleciendo la estructura interna de la compañía.

B. Acta de compromiso

La gerencia dio su aprobación y consenso a un documento, anexo D.

4.2.5 CONTEXTO DE LA EMPRESA

El contexto de Ekonopharma es un documento que se toma como base, el alcance, el análisis de brechas de controles y análisis de brechas de requisitos de la ISO-IEC27001 para identifica la situación actual.

Se describirán los elementos necesarios para entender el entorno de Ekonopharma, se examinaron la perspectiva y objetivos de la empresa, y se identificaron los factores que influyen tanto interna como externamente en la organización, a través de un análisis FODA.

Tabla 13

Foda de Ekonopharma

FACTORES INTERNOS	
FORTALEZAS	**DEBILIDADES**
a. Amplio dominio en el campo de la salud y la farmacología. b. Diversidad de servicios de atención médica y una amplia gama de productos de salud disponibles. c. Situado estratégicamente en una zona de alto tráfico. d. Personal comprometido y altamente capacitado para un servicio eficiente.	a. Restricciones en los horarios de servicio. b. Falta de un plan estratégico Coordinador. c. Escasa gestión de la información. d. Plan de formación y acreditación poco estructurado. e. Escasa disponibilidad de herramientas de gestión de proyectos. d. Ausencia de protección de la información para su continuidad en el mercado.
FACTORES EXTERNOS	
OPORTUNIDADES	**AMENAZAS**
a. Oportunidades de ampliar la oferta de servicios a través de convenios con empresas. b. Mantener la prestación de servicios a clientes existentes mediante la consolidación de la relación de confianza.	a. Mayor número de competidores cada cierto periodo. b. Cambio en las políticas de salud que podrían afectar la venta de determinados medicamentos. c. Robo de información secreta de la empresa.

Nota. La tabla representa los factores internos y externos de la empresa Ekonopharma.

A. ANÁLISIS DEL CONTEXTO DE EKONOPHARMA

"EKONOPHARMA SAC" es una empresa farmacéutica que comenzó sus operaciones en el año 2021. Cuenta con dos locales en el Distrito de Huamanga, en la Provincia del Ayacucho,

ambos ubicados a poca distancia de la Plaza de Armas. Su principal local está ubicado en Av. Ramón Castilla N °306 y el segundo en Jirón Callao N °324. Su proceso principal es la dispensación y/o expendio de productos farmacéuticos, dispositivos médicos y productos sanitarios al cliente, brindando atención personalizada de calidad.

Desde su establecimiento, las boticas de Ekonopharma son atendidas por personal del sector salud como a en farmacia y químicos farmacéuticos, con apoyo de enfermeros calificados y un médico general, para la atención a los clientes. La empresa se destaca por ofrecer servicios de alto valor, a precios económicos, con medicamentos y preparados magistrales para enfermedades de la piel, trabajando en colaboración con dermatólogos y un laboratorio especializado. Los servicios incluyen atención profesional, variedad de medicamentos, preparados personalizados, consultas gratuitas, atención eficiente y horarios extensos. A partir de 2022, Ekonopharma también brinda sus servicios a través de redes sociales para facilitar pedidos y consultas, en el año 2023 Ekonopharma optó por participar en licitaciones con instituciones estales y privadas. La empresa pertenece al sector de retail y se compromete a proteger la información de sus clientes, brindar promociones y emplear el SGSI con el objetivo de mejorar la credibilidad ante los clientes, obtener contratos y disminuir riesgos.

Misión es: “Seguir normas de calidad internacionales para ofrecer un servicio rápido y eficiente a nuestros clientes.”.

Visión es: “Ser la compañía líder en la industria farmacéutica en Ayacucho, ofreciendo los servicios de salud de la más alta calidad y facilitar un rápido acceso a los productos que precisen, primando los servicios profesionales y el máximo beneficio a sus medicamentos”.

B INFRAESTRUCTURA TECNÓLOGICA EXISTENTE

Tabla 14

Hardware de la empresa Ekonopharma

EQUIPOS	**Cantidad**
Case – Procesador	
Intel(R) Core (TM) i5-7400 CPU 3.00 GHz.	2
Monitores	
LG 27GP950	3

LG 32GP850	1
IMPRESORAS	
HP LASEJET P1002W	2
TICKETERAS	
BIXOLON SRP-270	2
CAMARAS DE SEGURIDAD	
HIKVISION FULL HD	6
DISCO 2TB	2

Nota. La tabla representa la parte del hardware con la que cuenta la empresa Ekonopharma.

Tabla 15

Software de la empresa Ekonopharma

NOMBRE	**VERSION**
MICROSOFT OFFICE	2019
MICROSOFT SQL SERVER	2008
TEAMVIEWER	12.0
SISTEMA DE VENTAS EKONOPHARMA	1.0
GOOGLE CHROME	60.0.3
ESET NOD 32 ANTIVIRUS	10.0
WINRAR	5.4

Nota. La tabla representa la parte del software con la que cuenta la empresa Ekonopharma.

4.2.6 REQUERIMIENTOS Y ANTICIPACIONES DE LAS PARTES INTERESADAS

En Ekonopharma, se ha establecido una estructura jerárquica para garantizar la correcta implementación de los procesos organizativos. Por tanto, es fundamental identificar el nivel de influencia e interés de los diferentes involucrados en el diseño del SGSI en Ekonopharma. Los datos importantes pueden ser vulnerables a manipulaciones por parte de terceros no autorizados y existe una falta de seguridad en las operaciones.

Tabla 16

Lista de partes interesados del desarrollo SGSI

Interesados	**Categoría de interesados**	**Nivel de interés**
Gerente General Q.F Pool Rudy	Patrocinador	Alto

Coordinadores	Trabajadores	Medio
Técnicos en Farmacia	Trabajadores	Bajos
Clientes	Clientes	Alto
Lisset	Miembro del proyecto	Alto

Nota. la tabla representa la lista de partes interesadas del desarrollo SGSI en Ekonopharma.

En relación al cuadro de las partes interesadas, llega a exhibirse la tabla especificando la toma de cada requerimiento relacionada a las partes interesadas

Tabla 17

Lista de partes interesados y requerimientos

Partes Interesadas	**Requerimientos**
Personal	Formación especializada, artículos de alta calidad y garantía en los servicios ofrecidos. Salvaguarda de los datos personales.
Propietario del negocio	Protección de la inversión y una rentabilidad satisfactoria
agencias/reguladores gubernamentales	Las entidades gubernamentales exigen el acatamiento de las leyes vigentes. Es necesario seguir las regulaciones relacionadas con la privacidad de los datos y los delitos informáticos.
clientes	Cumplimiento de las directrices establecidas en el Acuerdo de Seguridad de la información con el fin de asegurar la confidencialidad de la información personal.
Recursos Humanos	Cumplimiento de términos en el contrato del personal.
Comercial	Evitar filtraciones o extravíos de datos personales de los clientes

Nota. La tabla representa la lista de partes interesadas y requerimientos del desarrollo SGSI en Ekonopharma.

A ASPECTOS TÉCNICOS

En la actualidad, la empresa Ekonopharma cuenta con dos computadoras equipadas con un sistema antivirus que se actualiza automáticamente y están conectadas a Internet.

Tabla 18

Informe de necesidades y expectativa

Parte Interesada	**Interacción**		**Requerimiento**	
	contexto	Proceso	Necesidad	Expectativa
Todo el personal	Interno	• Gestión de RRHH y Logística • Recepción y Almacenamiento de PF, DM y PS	Contar con información disponible y mantener la SI.	Recibir formación y estímulos por cumplimiento de las políticas establecidas
Propietario del negocio	Externo	Gestión Comercial	Mantener la empresa y subir ganancias	Obtener fidelización de sus clientes
Agencias/ reguladoras Ministerio de Justicia	Externo	Control de Calidad	Seguir las regulaciones establecidas en la normativa.	Contar con organizaciones que compartan la visión de la empresa.
Clientes en general	Interno	• Dispensación y/o Expendio de PF, DM y PS • Elaboración de Preparados Magistrales	Calidad en medicamentos.	Recibir atención adecuada y resguardar su información.
Recursos Humanos Coordinadora de RR.HH. y Logística	Interno	Gestión de recursos humanos y Logística	Ejecución de las condiciones acordadas en el contrato.	Individuo que tiene conocimientos sobre la protección de la información.
Comercial Coordinador de calidad	Interno	• Gestión Comercial • Retiro y destrucción de medicamentos vencidos o deteriorados.	Prevenir fugas y pérdida de información	Datos completos y actualizados para la toma de decisiones.

Nota. La tabla representa las demandas y perspectivas de las partes en Ekonopharma.

4.2.7 ALCANCE DEL SGSI

Ekonopharma determinó la amplitud del SGSI considerando sus objetivos establecidos. Se acordó que el alcance del SGSI abarcará los procesos fundamentales de la

empresa, así como los procesos relacionados, siguiendo lo establecido por la normativa correspondiente.

Los procesos Core son los siguientes:

a) Recepción y almacenamiento de productos farmacéuticos, dispositivos médicos y productos sanitarios
b) Dispensación y/o Expendio de productos farmacéuticos, dispositivos médicos y productos sanitarios
c) Elaboración de Preparados Magistrales.
d) Retiro y/o destrucción de medicamentos vencidos y deteriorado.

Procesos que se relacionan con los procesos Core de Ekonopharma

e) Control de calidad
f) Gestión de Recursos Humanos y Logística

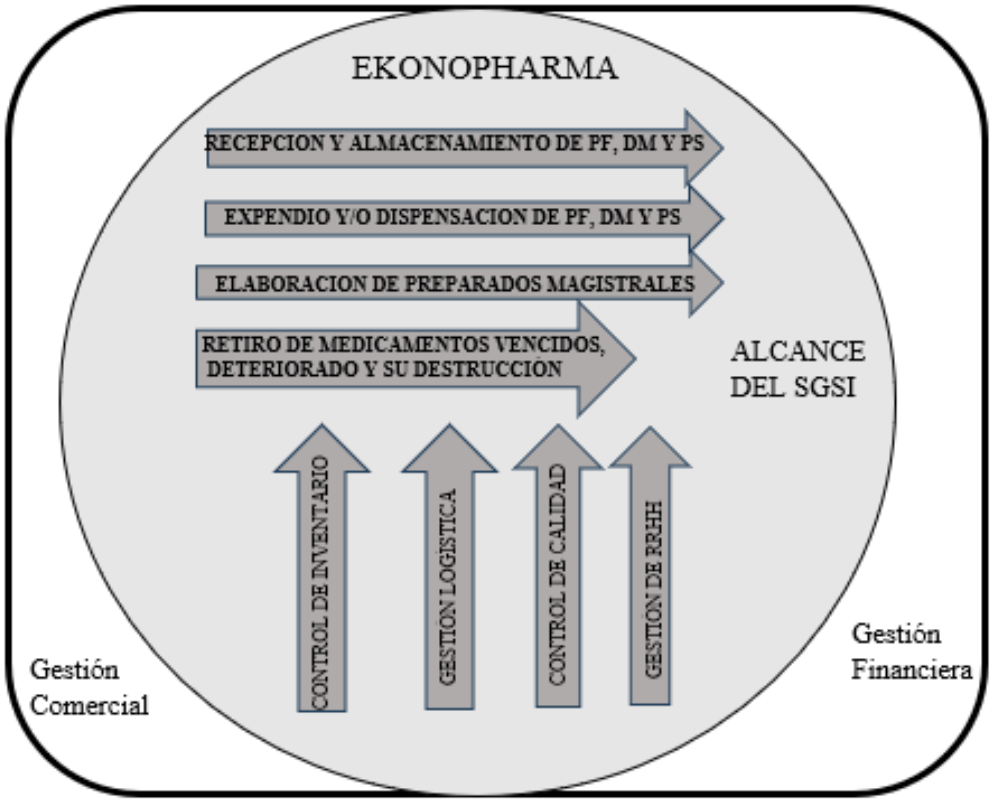
Los procedimientos que no están contemplados en la cobertura son:

a) gestión Comercial
b) Gestión financiera

La organización debe establecer los alcances del Sistema de Gestión de Seguridad de la Información (SGSI) para determinar qué datos desea proteger. La entidad comprende la importancia de asegurar la seguridad de la información, independientemente de su naturaleza, así como de cómo se maneja, procesa o transfiere, tanto interna como externamente al sistema.

Figura 14

Alcance de la implementación de la seguridad de la información de Ekonopharma



Nota: Alcance de la Implementación del Sistema de Gestión de Seguridad de la Información (SGSI) en Ekonopharma.

OBJETIVOS

a. Garantizar la confidencialidad de la información de los clientes en Ekonopharma.

b. Incrementar la disponibilidad y la calidad de los servicios brindados a los clientes.

c. Cumplir con la normativa vigente en materia de seguridad de la información en todas las actividades y proyectos de la empresa.

4.2.8 POLÌTICAS DE SEGURIDAD DE LA INFORMACIÓN

Se definen normas concretas que se adapten a los objetivos de control de acceso descritos en la Norma ISO 27001:2013 y que estén alineadas con la Política General de la empresa. Estas normas especificarán la forma en que se debe gestionar la información y qué medidas deben ser implementadas para cumplir con los objetivos de la política establecida.

A. POLÍTICAS DE SEGURIDAD PARA EKONOPHARMA S.A.C

Es esencial asegurar la protección de la información en EKONOPHARMA para garantizar la correcta prestación de servicios y la toma de decisiones seguras, manteniendo la confidencialidad, integridad y disponibilidad de los datos. Esto se logra a través del Sistema

de Gestión de Seguridad de la Información (SGSI), que guía a los empleados en la importancia de la información y servicios, así como en la identificación y corrección de posibles errores, fallos y vulnerabilidades.

a) **OBJETIVO:** La política de seguridad de Ekonopharma SAC tiene como meta mejorar la calidad de la información y ofrecer apoyo continuo en la prevención de incidentes, con el fin de lograr ciertos objetivos específicos.

b) **ALCANCE:** Esta política se aplica a todas las secciones más vulnerables de Ekonopharma, abarcando sus recursos y los procesos Core de la organización.

c) **COMITES: funciones y responsabilidades**: Ekonopharma designa un Comité de seguridad conformado por el Gerente, Coordinador de calidad, Coordinadora de recursos humanos y logística, pudiendo ser ampliado con consultores según sea necesario.

Funciones:

1. El equipo responsable de proteger la información trabaja en la creación de un plan para asegurar la seguridad de la información, estableciendo los procedimientos necesarios.
2. Cada miembro del Comité de Seguridad de la información debe designar a un representante de su departamento para tomar decisiones.
3. El Comité debe planificar encuentros regulares en caso de que surjan nuevas exigencias o cuestiones vinculadas con la protección de la información.
4. Después de cada encuentro, es necesario elaborar un documento que resuma lo discutido y sea ratificado con la firma de los participantes.

Funciones inherentes al cargo:

1. Organizar y validar los protocolos de seguridad de la información.
2. Fomentar la formación en el ámbito de la seguridad de la información.
3. Solucionar discrepancias y problemas habituales en la gestión de la seguridad.
4. Presentar y examinar nuevas políticas, normas y estándares para mejorar del SI.
5. Crear los planes de modificación en SI en aplicaciones o sistemas.

d) Control de Acceso.

1. Todas las personas que trabajan en Ekonopharma, solo puedan acceder a la información que necesaria para cumplir con sus responsabilidades laborales.
2. Aquellas personas ajenas a la organización que requieran acceso a información específica, deben demostrar la necesidad justificada de dicho acceso.
3. Toda petición para acceder a los servicios e información de la empresa por parte de empleados, socios o personas externas debe contar con la autorización del gerente.
4. El acceso a la información debe seguir las reglas y procedimientos establecidos.
5. El uso de los sistemas de información de la empresa debe limitarse al periodo en que el individuo preste sus servicios a la organización.
6. Es necesario que todos los empleados accedan a los sistemas informáticos a través de una identificación y contraseña exclusiva.
7. Ekonopharma necesita establecer un sistema de seguridad que incluya controles de acceso y alarmas para proteger sus instalaciones.

e) Seguridad de recursos humanos.

1. Todos los empleados de Ekonopharma deben conocer y seguir la Política de Seguridad de la Información de la empresa.
2. Antes de poder acceder a información importante de la empresa, los empleados de Ekonopharma deben comprometerse a mantener la confidencialidad firmando un acuerdo.
3. Es imprescindible establecer un plan de formación continua para todos los empleados de la empresa, centrándose especialmente en el personal nuevo.
4. En caso de violar la política de seguridad de la información, se aplicarán medidas disciplinarias correspondientes.
5. finalizar el contrato laboral de un empleado de Ekonopharma, se debe realizar la devolución de documentos, manuales, equipos y derechos de acceso.

f) Gestión de activos.

1. Es necesario identificar, clasificar y actualizar los activos de la empresa Ekonopharma según su valor, importancia, responsabilidad y ubicación, con el fin de protegerlos adecuadamente ante posibles riesgos.

2. La gestión de los activos, incluyendo la calidad y la seguridad, es responsabilidad de la gerencia. Asimismo, les corresponde proporcionar los recursos necesarios para alcanzar los objetivos establecidos.
3. Todos los activos utilizados en Ekonopharma deben ser asignados a un personal específico designado por el comité de seguridad. Esto garantiza que se clasifiquen correctamente y se restrinja el acceso de acuerdo con las políticas establecidas.

g) Protección de la integridad física.

1. Es necesario limitar el acceso a las zonas privadas de la empresa, y las personas que quieran entrar deben inscribirse con antelación y justificar el motivo de su visita.
2. Todos los empleados de la empresa deben llevar consigo su tarjeta de identificación de forma visible en todo momento.
3. Todos los dispositivos electrónicos como laptops, módems y celulares deben ser registrados al entrar y salir de la empresa.
4. Las computadoras, servidores y equipos de comunicaciones no deben ser movidos de su ubicación original a menos que se cuente con la aprobación correspondiente.
5. Es importante que las zonas vulnerables en la empresa tengan medidas de prevención y alerta ante incendios, inundaciones y otros riesgos.
6. Las redes de cableado se ven como áreas peligrosas y deben tener medidas de seguridad para regular el acceso.
7. Los colaboradores y terceros deben comprometerse a no utilizar la energía eléctrica para conectar dispositivos electrónicos que no pertenecen a Ekonopharma.

h) Acceso a Internet.

1. El uso indebido de recursos se produce cuando el personal accede a páginas como que no están relacionadas con las necesidades de Ekonopharma, lo que afecta la productividad debido al tiempo empleado en estas actividades en Internet.
2. Es importante que cualquier acceso a Internet sea utilizado exclusivamente con fines comerciales o laborales.

i) Medios extraíbles.

1. El personal de Ekonopharma solo puede utilizar los dispositivos de almacenamiento de la empresa, los cuales no deben conectarse ni utilizar en computadoras ajenas a la propiedad de la empresa.

2. Es necesario guardar la información confidencial en dispositivos de almacenamiento extraíbles, únicamente cuando sea necesario para cumplir con sus responsabilidades laborales o para compartir información con otras entidades. La información confidencial almacenada en estos dispositivos debe estar cifrada.

j) Administración de hardware y software.

1. Previo a realizar cualquier cambio en el hardware o software que pueda impactar en los recursos informáticos, es necesario contar con el consentimiento de los usuarios encargados de la información y del proceso.
2. El encargado de controlar los accesos tiene la facultad de revisar y decidir si acepta o rechaza la solicitud correspondiente.
3. No está permitido que el personal del área realice el reemplazo de hardware o software.
4. La administración del reemplazo de hardware o software debe realizarse siguiendo los procedimientos establecidos por la empresa Ekonopharma.
5. Todo cambio en los recursos tecnológicos debe ser documentado de manera formal desde su solicitud hasta su implementación, con el objetivo de facilitar el seguimiento y asegurar el cumplimiento de los procedimientos de calidad.

k) Software utilizado.

1. En Ekonopharma, es imprescindible que los programas empleados cumplan con las leyes actuales y se ajusten a los procedimientos y normativas internas de la empresa.
2. En Ekonopharma, es necesario proporcionar formación tecnológica al personal para garantizar que tengan habilidades en el uso de las computadoras de la empresa.

l) Email

1. Es fundamental que los correos electrónicos sean claros y estén alineados con las políticas de Ekonopharma, así como con las normas éticas y legales vigentes.
2. La cuenta de correo de Ekonopharma debe ser utilizada principalmente con propósitos relacionados con las operaciones de la empresa.
3. Los empleados no deben esperar que sus comunicaciones por correo electrónico sean privadas en ningún momento.

m) Establecimiento, uso y protección de claves de acceso.

1. Es recomendable modificar las contraseñas de forma regular.
2. Se establece que las contraseñas deben tener entre 6 y 14 caracteres de longitud.
3. Es importante evitar repetir contraseñas para garantizar la seguridad.

n) Relaciones con los proveedores.

1. La conexión entre los sistemas internos de una empresa y los de proveedores o terceros debe ser aprobada y certificada por el gerente.

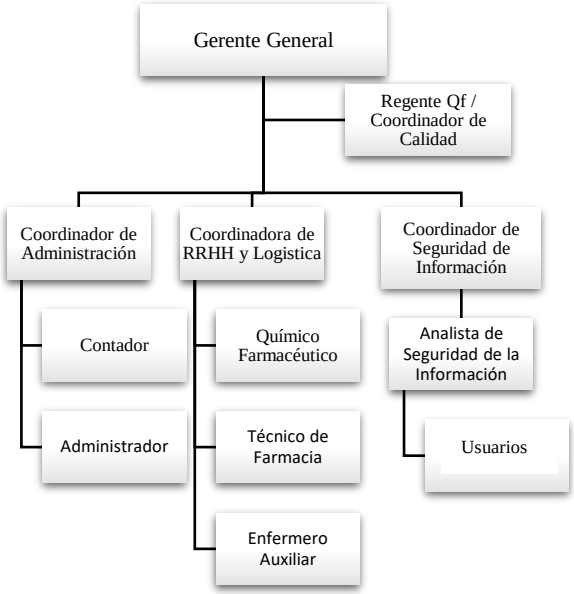
4.2.9 ROLES Y RESPONSABILIDADES

De acuerdo con las directrices de estándares internacionales o prácticas recomendadas, se aconseja crear un departamento dedicado exclusivamente a la independencia en el funcionamiento de la seguridad de la información.

En el contexto de esta pequeña empresa Ekonopharma, se designará a cada individuo una función particular, siendo factible otorgar diversas tareas a una misma persona.

Figura 15

Organigrama funcional



Nota. la figura representa el organigrama de Ekonopharma, agregadas los cargos que son necesarios para el SGSI.

Ya que todos los empleados de una empresa tienen la responsabilidad de proteger la información, es crucial definir y comunicar de manera clara las responsabilidades de cada persona en el Sistema de Gestión de Seguridad de la Información (SGSI) para garantizar su adecuada implementación y eficacia.

En la empresa Ekonopharma, que cuenta con un personal reducido, es posible que una única persona asuma múltiples roles si es necesario.

4.2.10 FICHA DE PUESTOS PARA ROLES DE LA SI

La descripción del cargo en la oficina de tecnología de la información está establecida en la "Ficha de Puesto", la cual especifica las tareas y obligaciones que deben ser comunicadas por la Coordinadora de Recursos Humanos y almacenadas en el repositorio de Ekonopharma. Antes de ser difundida tiene que ser aprobada por el Gerente.

Tabla 19

Ficha de puesto

Cargo	**Funciones**
Alta dirección/ Gerente General	• Dar el visto bueno al plan y la estrategia. • Involucrarse de forma activa en el programa de seguridad de la información. • Cumplir con la política establecida. • Contribuir en la creación de la política de seguridad de la información, los objetivos, el alcance y la estrategia.
Coordinador de Calidad/ Coordinador de la SI	• Colaborar en la elaboración de la política de seguridad de la información, definiendo metas, alcance y táctica. • Revisar y aprobar la documentación elaborada por el Departamento de Seguridad de la Información. • Comprometer a todas las áreas de la empresa en la seguridad de la información. • Detectar posibles riesgos que puedan perjudicar los sistemas de bases de datos y redes. • Evaluar los riesgos relacionados con las bases de datos de la compañía.
Analista de seguridad de la información/ Coordinadora de RRHH y Logística.	• Garantizar que el personal sea consciente de la importancia de salvaguardar la información. • Proporcionar los equipos tecnológicos necesarios al equipo de Seguridad de la Información.

	• Informar sobre posibles fallos de seguridad y sucesos de tecnología de la información, participar en la identificación y análisis de riesgos. • Implementar medidas de protección como contraseñas robustas, firewalls y controles de acceso físico en zonas críticas. • Establecer y mantener registros y métricas relacionadas con la seguridad de la información. • Desarrollar, actualizar y poner a prueba planes de emergencia para garantizar la disponibilidad de datos y la continuidad de las operaciones.
Usuarios del negocio/ Técnicos en Farmacia.	• Cumplir con las reglas y seguir los procedimientos de seguridad actuales, como la recomendación de mantener el área de trabajo organizada y usar contraseñas seguras.

Nota. La tabla representa la ficha de puestos necesarios en Ekonopharma.

4.2.11 PROCESO DE VERIFICACIÓN DE LA DOCUMENTACIÓN INFORMATIVA

Durante la etapa de ejecución, es necesario contar con documentación respaldada, por lo que se establece el "Procedimiento de Control de Información" descrito en el ANEXO F.

El propósito de la gestión de documentos es detallar las actividades necesarias para crear, registrar, supervisar y conservar la documentación del Sistema de Gestión de Seguridad de la Información, cumpliendo con las directrices de la normativa ISO/IEC 27001. Esta labor incluye todos los documentos vinculados a la seguridad de la información en la empresa, y la responsabilidad es compartida por todo el personal.

4.2.12 GESTIÓN Y TRATAMIENTO DE INCIDENTES

El manejo de problemas o debilidades comenzará por identificar las causas posibles. Se abordarán las incidencias y vulnerabilidades de forma correctiva y preventiva. La solución correctiva resolverá la situación originada por la incidencia, mientras que la preventiva establecerá medidas para evitar su repetición o reducir la vulnerabilidad.

Tabla 20

Registro de Incidencia

Identificador de la incidencia:
Fecha de notificación:
Tipo de incidencia/vulnerabilidad:

Información afectada:
Descripción detallada de la incidencia/vulnerabilidad:

Nota. La tabla representa la forma de registro de una incidencia en Ekonopharma.

El objetivo de este procedimiento es garantizar una correcta gestión de los incidentes comunicados, que implica identificarlos, evaluarlos y tomar medidas correctivas. Este proceso es aplicable a todos los empleados que participan en las actividades del Sistema de Gestión de Seguridad de la Información.

Tabla 21

Niveles de criticidad

Parámetro	**Descripción**	**Variables**
Impacto	La magnitud del impacto causado por el incidente puede variar dependiendo de los procedimientos y usuarios involucrados.	• Bajo: No afecta la operación del proceso principal, solo a los empleados involucrados directamente, y repercute en un máximo de dos colaboradores. • Medio: Perturba temporalmente los procesos vinculados con el proceso principal y afecta a entre tres y cinco colaboradores. • Alto: Interrumpe tanto el proceso principal como los procedimientos relacionados, impactando a más de cinco colaboradores.
Urgencia	El tiempo límite de espera permitido para resolver el incidente.	• Nivel mínimo de intensidad: 12 horas. • Nivel intermedio de intensidad: 10 horas. • Nivel máximo de intensidad: 4 horas.

Nota. La tabla representa *el nivel de criticidad de los incidentes* en Ekonopharma.

4.2.13 DOCUMENTACIÓN DEL PROCEDIMIENTO DE GESTIÓN DE INCIDENCIAS

En el registro de eventos se registrarán todas las anomalías que puedan comprometer la seguridad de los datos. También se informará al responsable de seguridad de cualquier vulnerabilidad o debilidad en el sistema que pueda poner en riesgo la información

Objetivo

Ekonopharma incorpora un sistema de gestión y alerta de incidentes de seguridad, con el objetivo de identificar a tiempo posibles vulnerabilidades en los sistemas de información y prevenir problemas de seguridad.

Alcance

Este proceso se aplica a todos los empleados internos y externos de Ekonopharma que necesiten acceder a los sistemas de información debido a sus responsabilidades laborales.

Responsabilidades

El encargado de seguridad tendrá la responsabilidad de garantizar que el procedimiento se cumpla de manera efectiva.

4.2.14 PROCEDIMIENTO DE AUDITORÍA INTERNA

Se ha establecido un procedimiento para realizar la inspección interna, que especifica las medidas de los criterios de la reglamentación ISO/IEC 27001. La autorización del gerente general, también fue requerida para este informe. Se describe el conjunto de tareas necesarias para una auditoría efectiva en el ANEXO H.

Objetivo, alcance y usuarios

Actividades para realizar las auditorías internas, con el propósito de comprobar si el Sistema de Gestión de Seguridad de la Información cumple con los requisitos de la norma ISO 27001 y si está operando de manera efectiva.

DEFINICIONES

a) Auditor: Persona competente que realiza auditorías.

b) Auditor líder: que dirige un equipo de auditores.

c) Auditoría interna: Proceso de evaluación interna estructurada e imparcial para verificar el cumplimiento de estándares de auditoría.

d) Equipo auditor: Grupo de auditores reunidos según el alcance y objetivos de la auditoría.

e) No conformidad: Falta de cumplimiento con los requisitos establecidos.

g) Hallazgo: Conclusión obtenida durante una auditoría en comparación con los criterios previamente establecidos.

Tabla 22

Requisitos para la calificación de auditores

Auditor Interno	**Auditor Externo**
Requisitos: • Observación activa en una auditoría interna. • Aprobación de curso de auditoría interna.	Requisitos: • • Se requiere haber completado satisfactoriamente un curso de auditor interno y contar con al menos una experiencia en auditoría en una compañía.

Nota. La tabla representa los requisitos que deben cumplir los auditores.

Tabla 23

Requisitos para la calificación de auditores

Auditor Líder Interno	**Auditor Líder Externo**
Requisitos: • Certificación como auditor interno completada. Experiencia previa incluye haber participado en una auditoría interna. • Debe tener al menos un año de antigüedad en la compañía.	Requisitos: • Se ha completado satisfactoriamente un curso de auditoría interna. • Se requiere un mínimo de 2 auditorías realizadas en empresas externas como experiencia.

Nota. La tabla representa los requisitos que deben cumplir los auditores.

4.2.15 GESTIÓN DE RIESGOS

La gestión de riesgos ha establecido un conjunto de protocolos con el fin de controlar los peligros relacionados con la seguridad de la información y disminuirlos a niveles aceptables. Se ha utilizado el enfoque Magerit, el cual incluye etapas para identificar activos, detectar amenazas, evaluar los riesgos, implementar medidas de seguridad y analizar el riesgo residual.

Se realizará una lista de los recursos de información utilizados en los procedimientos del Sistema de Gestión de Seguridad de la Información y se les asignará una clasificación de acuerdo a su impacto en la confidencialidad, integridad y disponibilidad.

a. Inventario de Activos

Se realiza un listado de los recursos de información empleados en las operaciones del Sistema de Gestión de Seguridad de la Información, los cuales se clasificarán según su impacto en la confidencialidad, integridad y disponibilidad.

Tabla 24

Inventario de activos de Ekonopharma

ÁMBITO	CATEGORÍA	ID	ACTIVO	DESCRIPCIÓN	PROCESO	UBICACIÓN
Datos	D] Datos	[D-001]	Base de Datos del personal	Datos personales	Gestión Recursos humanos	Ubicación Física
Datos	D] Datos	[D-004]	Base de Datos de Fórmulas magistrales	Datos acerca de las fórmulas personalizadas de los medicamentos preparados.	Elaboración de Preparados Magistrales	Ubicación Física
Datos	D] Datos	[D-005]	Datos de Inventariado de PF, DM Y PS	Información de los inventarios semanales de los PF, DM Y PS	Control de Calidad	Ubicación Física
Datos	D] Datos	[D-006]	Control de salarios	Información de los contratos del personal como la lista de salario	Gestión Recursos humanos	Ubicación Física
Datos	D] Datos	[D-007]	Formatos de entrevista	Información acerca de los postulantes que quieren trabajar en la empresa	Gestión Recursos humanos	Ubicación Física
Datos	D] Datos	[D-008]	Listas de asistencia	Información de las asistencias, permisos, y descuentos, para el control de seguimiento.	Gestión Recursos humanos	Ubicación Física
Datos	D] Datos	[D-009]	Listas de medicamentos vencidos y deteriorados	Información acerca de los medicamentos vencidos y deteriorados	Retiro y destrucción de medicamentos vencidos o deteriorados	Ubicación Física
Datos	D] Datos	[D-010]	Control de políticas	Información de todas las políticas internas de la empresa	Gestión Recursos humanos	Ubicación Física
Datos	D] Datos	[D-011]	Control de procesos	Información de los procesos	Gestión Recursos humanos y Logística	Ubicación Física
Servicios	[S] Servicios	[S-001]	Correo Electrónico	Correo con dominio institucional	Gestión Recursos humanos	Servidor
Servicios	[S] Servicios	[S-002]	Pago a servicios de terceros	Información de proveedores	Gestión de logística	Servidor

Servicios	[S] Servicios	[S-003]	Internet	Servicio contratado al proveedor MOVISTAR	Todos los procesos	-
Servicios	[S] Servicios	[S-004]	Boletas de ventas y compras emitidas	Información acerca de las facturas de nuestros clientes y proveedores	Dispensación y/o Expendio de PF, DM Y PS. /Recepción y Almacenamiento de PF, DM Y PS	Servidor Nube / Ubicación Física
Software	[SW] Software	[SW-001]	Sistema de ventas Ekonopharma	Antivirus ESET NOD32 3 unidades	Gestión Logística	Servidor Nube / Ubicación Física
Software	[SW] Software	[SW-002]	Antivirus	Antivirus ESET NOD32 3 unidades	Gestión Logística	Servidor Nube / Ubicación Física
Software	[SW] Software	[SW-003]	Licencias Office 365	Microsoft Office, Excel, 3 unidades	Gestión Logística	Plataforma de Office 365
Hardware	[HW] Hardware	[HW-001]	Monitores	2 unidades	Gestión Logística	Ubicación Física
Hardware	[HW] Hardware	[HW-002]	Computadoras	2 unidades	Gestión Logística	Ubicación Física
Equipamiento auxiliar	[AUX] Equipamiento auxiliar	[AUX-001]	Impresora	Impresora EPSON L375 2 unidad	Gestión Logística	Ubicación Física
Equipamiento auxiliar	[AUX] Equipamiento auxiliar	[AUX-002]	Equipamiento de cámaras	Sistema de cámaras, vigilancia, UPS.	Gestión Logística	Ubicación Física
Equipamiento auxiliar	[AUX] Equipamiento auxiliar	[AUX-003]	Discos externos	Dispositivo para guardar información	Todos los procesos	Ubicación Física
Redes de comunicación	[COM] Redes de comunicaciones	[COM-001]	Sistema de Red	Comunicaciones de Ekonopharma (cableado, switches, router, etc.)	Todos los procesos	Oficinas Ekonopharma
Redes de comunicación	[COM] Redes de comunicaciones	[COM-002]	Red Inalámbrica	Wifi para las boticas	Todos los procesos	Ubicación Física
Instalación	[I] Instalaciones	[I-001]	Oficinas Botica Ekonopharma	Oficinas de atención, Laboratorio	Todos los procesos	Ubicación Física
Personal	[P] Personal	[P-001]	Regente QF, Técnicos en Farmacia Coordinadora QF	Oficinas de atención, Laboratorio	Retiro y destrucción de medicamentos vencidos o deteriorados / Dispensación y/o Expendio de PF, DM Y PS/ Recepción y Almacenamiento de PF, DM Y PS / Elaboración de Preparados Magistrales /Elaboración de preparados magistrales.	Ubicación Física

Nota. La tabla muestra los activos de Ekonopharma.

b. Valoración de activos.

En la revisión de los recursos, se emplea la metodología MAGERIT para detectar los recursos, riesgos y debilidades. Se realizará una evaluación de los recursos en una escala de calificación que va desde 0 hasta 3 (puntuación máxima).

El valor de los activos se determina mediante la evaluación del promedio del impacto de la pérdida de Confidencialidad, Integridad y Disponibilidad, de acuerdo con una fórmula detallada. Una vez que se han identificado todos los activos, se calcula su valor total al promediar los impactos de la pérdida de estos elementos.

$$Valor\ del\ activo = (Confidencialidad + Integridad + Disponibilidad)\ /3$$

Se examinarán los activos teniendo en cuenta los distintos aspectos de seguridad que propone la metodología MAGERIT, como son la disponibilidad, la integridad de los datos y la confidencialidad de la información.

[D] Disponibilidad
[I] Integridad de datos
[C]Confidencialidad de la información

Esta escala se emplea para evaluar la repercusión de la pérdida de cada una de las tres categorías de valoración del activo.

Tabla 25

Valorización de criterios de seguridad

Rango	Valor	Confidencialidad	Integridad	Disponibilidad
7-10	Alto	Solamente el jefe tiene autorización para ver la información del activo, ya que su divulgación podría resultar en consecuencias graves.	El activo no puede soportar pérdidas del 5% de sus componentes, ya que esto afectaría a la empresa.	Es necesario que el activo no esté accesible durante al menos una hora, ya tendría un impacto negativo.
4-6	Medio	La información del activo es reservada y solo un selecto grupo de empleados tienen permiso para acceder a ella, su divulgación podría afectar a la empresa.	La información del activo solo puede ser consultada por el gerente, ya que su revelación podría tener consecuencias negativas.	Se estima que la falta de disponibilidad del activo durante un día como máximo podría tener un gran impacto en la empresa
1-3	Bajo	La información relacionada con el activo es confidencial y solo está disponible para ciertas áreas específicas, lo que implica que no es de acceso público y su divulgación tendría un impacto limitado.	Líderes responsables, ya que la revelación de esta información tendría un impacto negativo en la compañía.	Se estima que el activo no puede estar sin disponibilidad por más de un día, ya que su ausencia tendría un impacto significativo.

Nota. La tabla representa la valorización de criterios de seguridad en Ekonopharma.

Determinar la magnitud del impacto del activo se consigue al situar el valor del activo dentro de uno de los rangos de la tabla de valores suministrada.

Tabla 20

Matriz de Impacto

ID	RANGO	VALOR	CRITERIO	ID
3	Alto	4 a 6	A	Valor alto
2	Bajo	1 a 3	M	Valor medio
1	Medio	4 a 6	B	Valor bajo

Nota. La tabla representa el matriz de impacto en Ekonopharma.

Siguiendo los estándares de evaluación de impacto de activos, únicamente se consideran los riesgos de los activos de información que tengan un nivel de impacto clasificado como "ALTO" (Valoración de Activos).

4.2.16 INVENTARIO DE LOS ACTIVOS EKONOPHARMA

Se realizó una evaluación de los diversos sistemas de información y se clasificaron según su nivel de disponibilidad, confidencialidad e integridad. Después de establecer la metodología de riesgos, se llevó a cabo un recuento de los activos de información. Inicialmente, la empresa no tenía esta lista, por lo que se realizó una encuesta a todo el personal para identificar los activos y agregarlos a la lista.

Luego, se analizaron todos los activos, centrándose especialmente en los que tenían un gran impacto, así como en dos activos con un impacto medio.

Tabla 26

Valoración de Activos de información

IDENTIFICACIÓN Y VALORACIÓN DE ACTIVOS EKONOPHARMA S.A.C				CRITERIOS				
Ámbito	**Categoría**	**ID**	**Activo**	**C**	**I**	**D**	**Total**	**Impacto**
	[D] Datos	[D-001]	Base de Datos del personal	7	7	7	7	**A**
	[D] Datos	[D-002]	Base de Datos de los medicamentos y productos sanitarios	10	10	10	10	**A**
	[D] Datos	[D-003]	Datos de los clientes concurrentes	7	8	8	8	**A**
Datos	[D] Datos	[D-004]	Base de datos de fórmulas magistrales	9	9	9	9	**A**

	[D] Datos	[D-005]	Datos de Inventariado de PF, DM Y PS	9	9	9	9	**A**
	[D] Datos	[D-006]	Control de salarios	5	8	8	7	**A**
	[D] Datos	[D-007]	Formatos de entrevista	3	4	3	3	**B**
	[D] Datos	[D-008]	Listas de asistencia	3	4	3	3	**B**
	[D] Datos	[D-009]	Listas de medicamentos vencidos y deteriorados	9	8	8	8	**A**
	[D] Datos	[D-010]	Control de políticas	3	8	9	7	**A**
	[D] Datos	[D-011]	Control de procedimiento	5	6	7	6	**M**
Servicios	[S] Servicios	[S-001]	Correo Electrónico	7	6	5	6	**M**
	[S] Servicios	[S-002]	Pago a servicios de terceros	6	7	7	7	**A**
	[S] Servicios	[S-003]	Internet	7	7	7	7	**A**
	[S] Servicios	[S-004]	Boletas de ventas y compras emitidas	5	7	9	7	**A**
Software	[SW] Software	[SW-001]	Sistema de Ventas Ekonopharma	7	9	9	8	**A**
	[SW] Software	[SW-002]	Antivirus	3	4	3	3	**B**
	[SW] Software	[SW-003]	Licencias Office 365	3	4	3	3	**B**
Hardware	[HW] Hardware	[HW-001]	Monitores	6	6	5	6	**M**
	[HW] Hardware	[HW-002]	computadoras	6	7	7	7	**A**
	[AUX] Equipamiento auxiliar	[AUX-001]	Impresora	6	8	8	7	**A**
Equipamiento auxiliar	[AUX] Equipamiento auxiliar	[AUX-002]	Equipamiento de cámaras	8	9	8	8	**A**
	[AUX] Equipamiento auxiliar	[AUX-003]	Discos externos	4	6	4	5	**M**
Redes de Comunicación	[COM] Redes de comunicaciones	[COM-001]	Sistema de Red	5	5	3	4	**M**
	[COM] Redes de comunicaciones	[COM-002]	Red Inalámbrica	4	5	4	4	**A**

Instalación	[I] Instalaciones	[I-001]	Oficinas Botica Ekonopharma	8	6	9	8	**A**
Personal	[I] Personal	[P-001]	Gerente, Técnicos en Farmacia, Regente QF, Coordinadora QF	8	9	9	9	**A**

Nota: Esta tabla detalla los inventarios de activos de Ekonopharma.

Los activos presentes en la tabla son de gran importancia y están asociados al proceso principal de la empresa. Solo cinco activos son de importancia intermedia, ya que no tienen un gran impacto, pero igualmente están relacionados con los procesos principales. Por lo tanto, estos activos serán tomados en cuenta en la evaluación de riesgos.

En cada fase del alcance, es necesario hacer una lista de los recursos de información relacionados. Luego, se analizaron todos los recursos, eligiendo aquellos con impacto significativo y también con impacto moderado, los cuales se identifican como Activos de Información de Importancia.

Tabla 27

Valoración de Activos de información de alto impacto

ACTIVOS DE ALTO IMPACTO EKONOPHARMA SAC				**Criterios**				
ÁMBITO	**CATEGORÍA**	**ID**	**ACTIVO**	**C**	**I**	**D**	**Total**	**Impacto**
Datos	[D] Datos	[D-001]	Base de Datos del personal	7	7	7	7	**A**
	[D] Datos	[D-002]	Base de Datos de los medicamentos y productos sanitarios	10	10	10	10	**A**
	[D] Datos	[D-003]	Datos de los clientes concurrentes	7	8	8	8	**A**
	[D] Datos	[D-004]	Base de datos de fórmulas magistrales	9	9	9	9	**A**
	[D] Datos	[D-005]	Datos de Inventariado de PF, DM Y PS	9	9	9	9	**A**
	[D] Datos	[D-006]	Control de salarios	5	8	8	7	**A**
	[D] Datos	[D-009]	Listas de medicamentos vencidos y deteriorados	9	8	8	8	**A**
	[D] Datos	[D-010]	Control de políticas	3	8	9	7	**A**
	[D] Datos	[D-011]	Control de procedimiento	5	6	7	6	**M**
Servicios	[S] Servicios	[S-001]	Correo Electrónico	7	6	5	6	**M**
	[S] Servicios	[S-002]	Pago a servicios de terceros	6	7	7	7	**A**
	[S] Servicios	[S-003]	Internet	7	7	7	7	**A**
	[S] Servicios	[S-004]	Boletas de ventas y compras emitidas	5	7	9	7	**A**
Software	[SW] Software	[SW-001]	Sistema de Ventas Ekonopharma	7	9	9	8	**A**
Hardware	[HW] Hardware	[HW-001]	Monitores	6	6	5	6	**M**
	[HW] Hardware	[HW-002]	computadoras	6	7	7	7	**A**

Equipamiento auxiliar	[AUX] Equipamiento auxiliar	[AUX-001]	Impresora	6	8	8	7	**A**
	[AUX] Equipamiento auxiliar	[AUX-002]	Equipamiento de cámaras	8	9	8	8	**A**
	[AUX] Equipamiento auxiliar	[AUX-003]	Discos externos	4	6	4	5	**M**
Redes de Comunicación	[COM] Redes de comunicaciones	[COM-001]	Sistema de Red	5	5	5	5	**M**
	[COM] Redes de comunicaciones	[COM-002]	Red Inalámbrica	4	5	4	4	**M**
Instalación	[I] Instalaciones	[I-001]	Oficinas Botica Ekonopharma	8	6	9	8	**A**
Personal	[I] Personal	[P-001]	Gerente, Técnicos, Regente QF, Coordinadora QF	8	9	9	9	**A**

Nota: Esta tabla detalla los inventarios de activos de alto impacto en Ekonopharma.

Se analiza el gráfico anterior para determinar la cantidad y disposición de los activos en términos de confidencialidad, integridad y disponibilidad. Se identificarán los activos clave para poder evaluar los riesgos de seguridad de la información y gestionarlos de forma eficaz.

4.2.17 IDENTIFICACIÓN DE AMENAZAS

En este apartado se realizará una evaluación de los riesgos que podrían afectar los bienes de la compañía Ekonopharma. Los obstáculos que pueden dificultar el funcionamiento normal de una empresa pueden surgir de diversas fuentes. A continuación, se presenta un cuadro que detalla las amenazas de acuerdo con la clasificación de riesgos de MAGERIT.

Tabla 28

Posibles riesgos para los activos de información de gran importancia.

AMENAZAS DE LOS ACTIVOS DE ALTO IMPACTO EKONOPHARMA SAC			
Tipo de activo	activos	Id	Amenazas
Datos	Base de Datos del personal	R1	Alteración intensional de datos
		R2	Acceso no autorizado
		R3	Fuga de información
	Base de Datos de los medicamentos y productos sanitarios	R4	Eliminación de datos
		R2	Acceso no autorizado
		R3	Fuga de información
		R6	Registros incompletos
		R7	Alteración accidental de datos
		R8	Introducción de datos errores
	Datos de los clientes concurrentes	R9	Alteración de datos
		R2	Acceso no autorizado
		R5	Eliminación accidental de datos
	Base de datos de fórmulas magistrales	R4	Eliminación de datos
		R2	Acceso no autorizado

		R3	Fuga de información
		R6	Registros incompletos
		R1	Alteración intensional de datos
		R7	Alteración accidental de datos
	Datos de Inventariado de PF, DM Y PS	R5	Eliminación accidental de datos
		R2	Acceso no autorizado
		R3	Fuga de información
		R6	Registros incompletos
		R1	Alteración intensional de datos
		R7	Alteración accidental de datos
		R8	Introducción de datos erróneos
	Control de salarios	R4	Eliminación de datos
		R2	Acceso no autorizado
		R3	Fuga de información
		R6	Registros incompletos
		R8	Introducción de datos errores
	Lista de medicamentos vencidos y deteriorados	R10	Error en el desarrollo de las listas
		R4	Eliminación de datos
		R7	Alteración accidental de datos
		R3	Fuga de información
	control de políticas	R11	Equivocación al momento de crear documentos
		R3	Fuga de información
		R12	Manipulación de los datos de los documentos
		R4	Eliminación de datos
	control de procedimiento	R9	Alteración de datos
		R11	Equivocación al momento de crear documentos
		R3	Fuga de información
		R12	Manipulación de los datos de los documentos
		R7	Alteración accidental de datos
		R4	Eliminación de datos
Servicios	Correo electrónico	R13	Negación de haber recibió un mensaje
		R14	Uso incorrecto
		R15	Expansión de virus
	Pago a servicios de terceros	R4	Eliminación de datos
		R3	Fugas de información
		R12	Manipulación de los datos de los documentos
		R9	Alteración de datos
	Internet	R11	Caída de los servicios de internet
		R2	Acceso no autorizado
		R16	Abuso de beneficios de acceso
	Boletas de ventas y compras emitidas	R3	Fugas de información
		R12	Manipulación de los datos de los documentos
		R4	Eliminación de datos
Hardware	Monitores	R17	posibilidad de que el fuego acabe
		R18	Desgaste debido a su uso
		R19	Avería del hardware
		R20	Corte de suministro eléctrico
	Computadoras	R17	posibilidad de que el fuego dañe
		R18	Desgaste debido a su uso
		R19	Avería del hardware
		R21	Uso ilícito
		R22	Desconexión del equipo
		R23	Errores en el mantenimiento actualización del equipo
		R24	Contaminación mecánica polvo
		R20	Corte de suministro eléctrico
	Impresoras	R18	Desgaste debido a su uso

Equipamiento auxiliar		R19	Avería del hardware
		R22	Desconexión del equipo
		R23	Errores en el mantenimiento actualización del equipo
		R20	Corte de suministro eléctrico
		R17	Posibilidad de ocurrir un incendio y dañar
	Equipamiento de cámaras	R17	Posibilidad de ocurrir un incendio y dañar
		R24	Contaminación mecánica polvo
		R23	Errores en el mantenimiento actualización del equipo
		R22	Desconexión del equipo
	Discos externos	R23	Errores en el mantenimiento actualización del equipo
		R24	Contaminación mecánica polvo
		R25	Robo de Disco
		R26	Destrucción deliberada del disco
		R27	Degradación por consecuencia del tiempo
Redes de Comunicación	Sistema de red	R28	Posibilidad de equivocaciones en la instalación
		R22	Desconexión del equipo
		R17	Posibilidad de ocurrir un incendio y dañar
		R29	Posibilidad de que las fugas de agua inunden y dañen
	Red inalámbrica	R31	Interceptación de red
		R32	Monitorización del trafico
		R2	Acceso no autorizado
Software	Sistema de ventas Ekonopharma	R2	Acceso no autorizado
		R3	Fuga de información
		R8	Introducción de datos errores
Instalación	Oficinas Botica Ekonopharma	R2	Acceso no autorizado
		R30	Posibilidad de ocurrir sismo o terremoto
		R29	Posibilidad de que las fugas de agua inunden y dañen
		R17	Posibilidad de ocurrir un incendio y dañar
Personal	Trabajadores	R33	Indisponibilidad por ausencia o despido inmediato
		R34	Extorsión por obligar a obrar en mal sentido
		R35	Ingeniería social aprovechamiento de buena fe

Nota: Esta tabla detalla las amenazas a la que estarían expuestas los activos de alto impacto en Ekonopharma.

4.2.18 EVALUACIÓN DE RIESGOS

Después de completar la revisión de los activos de información, se lleva a cabo la valoración de riesgos, la cual consiste en determinar el efecto de las posibles amenazas y la probabilidad de que estas ocurran, con el fin de calcular el nivel de riesgo al combinar ambos factores. Asimismo, se identifica la zona de riesgos, que señala qué activos están en una situación de riesgo elevado. Esta evaluación nos permite determinar qué acciones de control deberíamos implementar y considerar para gestionar, prevenir, disminuir o transferir dicho riesgo.

4.2.18.1 ESTIMACIÓN DEL RIESGO

Se emplearán escalas numéricas para medir el grado de riesgo, considerando tanto la importancia del impacto como la probabilidad de que cada activo sea impactado por distintas amenazas

.

El impacto se refiere al daño que sufriría el activo luego de que se materialice una amenaza. En la tabla se detalla la estimación del impacto, la probabilidad y el riesgo asociado al activo La estimación del riesgo se calcula: Riesgo = Probabilidad*Impacto.

Tabla 29

Estimación de probabilidad e impacto

ESCALAS			
IMPACTO		**PROBABILIDAD**	
Valor	Tasación	Valor	Tasación
5	MA: Muy alto	5	MA: Muy alto
4	A: Alto	4	A: Alto
3	M: Medio	3	M: Medio
2	B: Bajo	2	B: Bajo
1	MB: Muy bajo	1	MB: Muy bajo

Nota: Esta tabla detalla la estimación de probabilidad e impacto. Elaboración propia.

Tabla 30

Niveles del riesgo

Riesgo	
Escala	Tasación
15-25	MA: Muy alto
9-14	A: Alto
5-8	M: Medio
3-4	B: Bajo
1-2	MB: Despreciable

Nota: Esta tabla detalla las escalas del riesgo.

Tabla 31

Estimación de Riesgo

RIESGO	**Probabilidad**				
Riesgo = Probabilidad*Impacto	Bajo	Medio	Alto		
	1	2	3	4	5

Impacto	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5

Nota. La tabla representa estimación de riesgo para Ekonopharma.

La tabla siguiente presenta la valoración del riesgo para cada peligro y recurso de información de la compañía Ekonopharma. Es importante identificar rápidamente los activos que sean calificados como críticos en la escala de riesgo.

LEYENDA:

Impacto [Im]: Se refiere a las posibles consecuencias negativas que podrían surgir de un evento, y se relaciona con el daño potencial que podría resultar para la empresa.

Probabilidad [Prob]: Hace referencia a la posibilidad de que ocurra un evento.

Riesgo [R]: Se habla de la posibilidad de que un riesgo detectado se materialice y genere perjuicios en una organización.

Tabla 32

Estimación del Riesgo

ESTIMACIÓN DEL RIESGO DE LOS ACTIVOS DE ALTO IMPACTO EKONOPHARMA SAC

Tipo de activo	Activos	Amenazas	[Im]	[P]	[R]
Datos	Base de Datos del personal	Alteración intensional de datos	4	2	8
		Acceso no autorizado	3	2	6
		Fuga de información	4	3	12
	Base de Datos de los medicamentos y productos sanitarios	Eliminación de datos	5	5	25
		Acceso no autorizado	4	3	12
		Fuga de información	3	2	6
		Registros incompletos	5	3	15
		Alteración accidental de datos	4	2	8
		Introducción de datos erróneos	4	3	12
	Datos de los clientes concurrentes	Alteración de datos	2	1	2
		Acceso no autorizado	2	1	2
		Eliminación accidental de datos	3	3	9
	Base de datos de fórmulas magistrales	Eliminación de datos	5	4	20
		Acceso no autorizado	5	3	15
		Fuga de información	5	4	20
		Registros incompletos	5	3	15

		Alteración intensional de datos	4	2	8
		Alteración accidental de datos	4	2	8
	Datos de Inventariado de PF, DM Y PS	Eliminación accidental de datos	5	3	15
		Acceso no autorizado	3	3	9
		Fuga de información	3	2	6
		Registros incompletos	5	3	15
		Alteración intensional de datos	3	2	6
		Alteración accidental de datos	3	2	6
		Introducción de datos erróneos	5	3	15
	Control de salarios	Eliminación de datos	4	3	12
		Acceso no autorizado	3	2	6
		Fuga de información	3	2	6
		Registros incompletos	3	3	9
		Introducción de datos erróneos	3	3	9
	Lista de medicamentos vencidos y deteriorados	Error en el desarrollo de las listas	5	4	20
		Eliminación de datos	5	4	20
		Alteración accidental de datos	4	4	16
		Fuga de información	4	4	16
	control de políticas	Equivocación al momento de crear documentos	3	3	9
		Fuga de información	3	3	9
		Manipulación de los datos de los documentos	3	3	9
		Eliminación de datos	3	3	9
	control de procedimiento	Alteración de datos	3	2	6
		Equivocación al momento de crear documentos	3	2	6
		Fuga de información	3	2	6
		Manipulación de los datos de los documentos	3	1	3
		Alteración accidental de datos	3	2	6
		Eliminación de datos	3	2	6
Servicios	Correo electrónico	Negación de haber recibió un mensaje	4	3	12
		Uso incorrecto	3	3	9
		Expansión de virus	4	3	12
	Pago a servicios de terceros	Eliminación de datos	4	3	12
		Fugas de información	3	3	9
		Manipulación de los datos de los documentos	3	2	6
		Alteración de datos	3	3	9
	Internet	Caída de los servicios de internet	3	2	6
		Acceso no autorizado	3	2	6
		Abuso de beneficios de acceso	3	3	9
	Boletas de ventas y compras emitidas	Fugas de información	3	2	6
		Manipulación de los datos de los documentos	3	2	6
		Eliminación de datos	3	2	6
Hardware	Monitores	posibilidad de que el fuego acabe	5	3	15
		Desgaste debido a su uso	4	3	12
		Avería del hardware	4	3	12
		Corte de suministro eléctrico	4	3	12

	Computadoras	posibilidad de que el fuego dañe	5	3	15
		Desgaste debido a su uso	4	3	12
		Avería del hardware	4	3	12
		Uso ilícito	4	3	12
		Desconexión del equipo	4	3	12
		Errores en el mantenimiento actualización del equipo	4	3	12
		Contaminación mecánica polvo	5	3	15
		Corte de suministro eléctrico	4	3	12
Equipamiento auxiliar	Impresoras	Desgaste debido a su uso	4	3	12
		Avería del hardware	4	3	12
		Desconexión del equipo	4	3	12
		Errores en el mantenimiento actualización del equipo	4	3	12
		Corte de suministro eléctrico	4	2	8
		Posibilidad de ocurrir un incendio y dañar	5	3	15
	Equipamiento de cámaras	Posibilidad de ocurrir un incendio y dañar	5	3	15
		Contaminación mecánica polvo	5	3	15
		Errores en el mantenimiento actualización del equipo	4	3	12
		Desconexión del equipo	4	3	12
	Discos externos	Avería del hardware	4	3	12
		Contaminación mecánica por polvo suciedad	4	3	12
		Robo de Disco	4	3	12
		Destrucción deliberada del disco	4	3	12
		Degradación por consecuencia del tiempo	4	3	12
Redes de Comunicación	Sistema de red	Posibilidad de equivocaciones en la instalación	4	3	12
		Desconexión del equipo	4	3	12
		Posibilidad de ocurrir un incendio y dañar	5	3	15
		Posibilidad de que las fugas de agua inunden y dañen	4	3	12
	Red inalámbrica	Interceptación de red	4	3	12
		Monitorización del trafico	4	3	12
		Acceso no autorizado	4	3	12
Software	Sistema de Ventas Ekonopharma	Acceso no autorizado	5	4	20
		Fuga de información	4	3	12
		Introducción de datos erróneos	5	3	15
Instalación	Oficinas Botica Ekonopharma	Acceso no autorizado	5	4	20
		Posibilidad de ocurrir sismo o terremoto	5	2	10
		Posibilidad de que las fugas de agua inunden y dañen	5	4	20
		Posibilidad de ocurrir un incendio y dañar	5	4	20
Personal	Trabajadores	Indisponibilidad por ausencia o despido inmediato	5	4	20
		Extorsión por obligar a obrar en mal sentido	5	3	15
		Ingeniería social aprovechamiento de buena fe	5	3	15

Nota. La tabla representa Estimación del Riesgo en Ekonopharma.

4.2.19 TRATAMIENTO DEL RIESGO

Después de evaluar los peligros, se tomará una decisión sobre qué acciones tomar o qué medidas implementar para proteger los activos de los riesgos identificados. Para lograr esto, se seguirán las estrategias detalladas en la siguiente tabla.

Tabla 33

Medidas frente al riesgos

FORMAS DE MITIGAR	EXPLICACIÓN
ASUMIR/ ACEPTAR	Aceptar la posibilidad de que el riesgo pueda materializarse sin implementar acciones concretas.
REDUCIR	Disminuir la posibilidad de que ocurra un evento tomando precauciones adecuadas.
ELIMINAR	Eliminar la causa de la amenaza para reducir el riesgo, especialmente cuando la actividad que la genera no es crucial para el negocio y puede ser eliminada sin afectar negativamente a la entidad.
COMPARTIR/ TRANSFERIR	Desplazar la responsabilidad del riesgo hacia entidades externas, como compañías de seguros o proveedores de servicios, se emplea en situaciones donde no es posible disminuir la posibilidad de que ocurra un riesgo, pero su efecto es inevitable.

Nota. La tabla representa medidas frente al riesgo para Ekonopharma.

Se elegirán las medidas o acciones a implementar para detener los riesgos, se identificarán los riesgos de alto nivel que requieran una intervención inmediata debido a ser los activos con mayor nivel de riesgo. En la siguiente tabla se detallan las medidas que se llevarán a cabo para reducir los riesgos seleccionados.

Tabla 34

Medidas frente al riesgos

MEDIDAS FRENTE AL RIESGO DE LOS ACTIVOS DE ALTO IMPACTO EKONOPHARMA SAC						
Tipo de activo	Activos	Amenazas	[Im]	[P]	[R]	Formas de mitigar
Datos	Base de Datos del personal	Alteración intensional de datos	4	2	8	Reducir
		Acceso no autorizado	3	2	6	Reducir
		Fuga de información	4	3	12	Eliminar
	Base de Datos de los medicamentos y productos sanitarios	Eliminación de datos	5	5	25	Eliminar
		Acceso no autorizado	4	3	12	Eliminar
		Fuga de información	3	2	6	Reducir

		Registros incompletos	5	3	15	Eliminar
		Alteración accidental de datos	4	2	8	Reducir
		Introducción de datos erróneos	4	3	12	Reducir
	Datos de los clientes concurrentes	Alteración de datos	2	1	2	Reducir
		Acceso no autorizado	2	1	2	Reducir
		Eliminación accidental de datos	3	3	9	Eliminar
	Base de datos de las fórmulas magistrales	Eliminación de datos	5	4	20	Eliminar
		Acceso no autorizado	5	3	15	Eliminar
		Fuga de información	5	4	20	Eliminar
		Registros incompletos	5	3	15	Eliminar
		Alteración intensional de datos	4	2	8	Reducir
		Alteración accidental de datos	4	2	8	Reducir
	Datos de Inventariado de PF, DM Y PS	Eliminación accidental de datos	5	3	15	Eliminar
		Acceso no autorizado	3	3	9	Eliminar
		Fuga de información	3	2	6	Eliminar
		Registros incompletos	5	3	15	Reducir
		Alteración intensional de datos	3	2	6	Reducir
		Alteración accidental de datos	3	2	6	Reducir
		Introducción de datos erróneos	5	3	15	Eliminar
	Control de salarios	Eliminación de datos	4	3	12	Eliminar
		Acceso no autorizado	3	2	6	Reducir
		Fuga de información	3	2	6	Reducir
		Registros incompletos	3	3	9	Reducir
		Introducción de datos erróneos	3	3	9	Eliminar
	Lista de medicamentos vencidos y deteriorados	Error en el desarrollo de las listas	5	4	20	Eliminar
		Eliminación de datos	5	4	20	Eliminar
		Alteración accidental de datos	4	4	16	Eliminar
		Fuga de información	4	4	16	Eliminar
	control de políticas	Equivocación al momento de crear documentos	3	3	9	Eliminar
		Fuga de información	3	3	9	Reducir
		Manipulación de los datos de los documentos	3	3	9	Reducir
		Eliminación de datos	3	3	9	Eliminar
	control de procedimiento	Alteración de datos	3	2	6	Eliminar
		Equivocación al momento de crear documentos	3	2	6	Reducir
		Fuga de información	3	2	6	Reducir
		Manipulación de los datos de los documentos	3	1	3	Eliminar
		Alteración accidental de datos	3	2	6	Reducir
		Eliminación de datos	3	2	6	Eliminar
Servicios	Correo electrónico	Negación de haber recibió un mensaje	4	3	12	Reducir
		Uso incorrecto	3	3	9	Reducir
		Expansión de virus	4	3	12	Reducir
	Pago a servicios de terceros	Eliminación de datos	4	3	12	Eliminar
		Fugas de información	3	3	9	Reducir

		Manipulación de los datos de los documentos	3	2	6	Eliminar
		Alteración de datos	3	3	9	Reducir
	Internet	Caída de los servicios de internet	3	2	6	Transferir
		Acceso no autorizado	3	2	6	Reducir
		Abuso de beneficios de acceso	3	3	9	Reducir
	Boletas de ventas y compras emitidas	Fugas de información	3	2	6	Reducir
		Manipulación de los datos de los documentos	3	2	6	Reducir
		Eliminación de datos	3	2	6	Reducir
Hardware	Monitores	posibilidad de que el fuego acabe	5	3	15	Reducir
		Desgaste debido a su uso	4	3	12	Reducir
		Avería del hardware	4	3	12	Transferir
		Corte de suministro eléctrico	4	3	12	Transferir
	Computadoras	posibilidad de que el fuego dañe	5	3	15	Reducir
		Desgaste debido a su uso	4	3	12	Reducir
		Avería del hardware	4	3	12	Transferir
		Uso ilícito	4	3	12	Reducir
		Desconexión del equipo	4	3	12	Reducir
		Errores en el mantenimiento actualización del equipo	4	3	12	Transferir
		Contaminación mecánica polvo	5	3	15	Reducir
		Corte de suministro eléctrico	4	3	12	Transferir
Equipamiento auxiliar	Impresoras	Desgaste debido a su uso	4	3	12	Reducir
		Avería del hardware	4	3	12	Transferir
		Desconexión del equipo	4	3	12	Reducir
		Errores en el mantenimiento actualización del equipo	4	3	12	Transferir
		Corte de suministro eléctrico	4	2	8	Reducir
		Posibilidad de ocurrir un incendio y dañar	5	3	15	Reducir
	Equipamiento de cámaras	Posibilidad de ocurrir un incendio y dañar	5	3	15	Reducir
		Contaminación mecánica polvo	5	3	15	Reducir
		Errores en el mantenimiento actualización del equipo	4	3	12	Transferir
		Desconexión del equipo	4	3	12	Reducir
	Discos externos	Avería del hardware	4	3	12	Transferir
		Contaminación mecánica por polvo suciedad	4	3	12	Reducir
		Robo de Disco	4	3	12	Aceptar
		Destrucción deliberada del disco	4	3	12	Aceptar
		Degradación por consecuencia del tiempo	4	3	12	Aceptar
Redes de Comunicación	Sistema de red	Posibilidad de equivocaciones en la instalación	4	3	12	Reducir
		Desconexión del equipo	4	3	12	Reducir
		Posibilidad de ocurrir un incendio y dañar	5	3	15	Reducir
		Posibilidad de que las fugas de agua inunden y dañen	4	3	12	Aceptar
	Red inalámbrica	Interceptación de red	4	3	12	Reducir
		Monitorización del trafico	4	3	12	Reducir
		Acceso no autorizado	4	3	12	Reducir

Software	Sistema de Ventas Ekonopharma	Acceso no autorizado	5	4	20	Eliminar
		Fuga de información	4	3	12	Reducir
		Introducción de datos erróneos	5	3	15	Reducir
Instalación	Oficinas Botica Ekonopharma	Acceso no autorizado	5	4	20	Reducir
		Posibilidad de ocurrir sismo o terremoto	5	2	10	Aceptar
		Posibilidad de que las fugas de agua inunden y dañen	5	4	20	Aceptar
		Posibilidad de ocurrir un incendio y dañar	5	4	20	Reducir
Personal	Trabajadores	Indisponibilidad por ausencia o despido inmediato	5	4	20	Aceptar
		Extorsión por obligar a obrar en mal sentido	5	3	15	Reducir
		Ingeniería social aprovechamiento de buena fe	5	3	15	Reducir

Nota. La tabla representa Medidas frente al riesgo para Ekonopharma.

4.2.20 CONTROLES PARA ASEGURAR LA INFORMACIÓN

En este informe se describen las medidas de seguridad que se implementarán para reducir los riesgos que afectan la seguridad de la información de la empresa Ekonopharma, así como las vulnerabilidades y amenazas que pueden comprometer la integridad de los activos de información. Cada riesgo ha sido vinculado a controles de seguridad que cumplen con los requisitos de la norma ISO 27001, con el objetivo de evitar posibles incidentes. Se ha llevado a cabo un análisis exhaustivo de los controles de seguridad de la información en relación con las amenazas y activos de Ekonopharma, el cual se detalla en el Anexo I.

4.2.21 PLAN DE TRATAMIENTO DE RIESGOS

Una vez que se definen los estándares de riesgo aceptables, es fundamental crear el "Plan de Tratamiento de Riesgos". En este plan se asigna responsabilidades para la implementación de medidas de control, se establecen los plazos para su ejecución y se desarrolla un plan de acción para garantizar su cumplimiento. Es esencial contar con la aprobación de la alta dirección, ya que la implementación puede requerir mucho tiempo y esfuerzo, especialmente si los controles son complejos, y sin su apoyo los recursos necesarios podrían no estar disponibles. Es imprescindible tener en cuenta todos los aspectos abordados anteriormente para identificar, clasificar, analizar y evaluar las posibles amenazas a los activos, así como para determinar la probabilidad y el impacto de su ocurrencia. Estos procesos deben estar respaldados por un plan de gestión de riesgos que dirija las acciones, tareas, responsabilidades y recursos necesarios para mitigar los riesgos identificados. El Plan de Tratamiento de Riesgos detallado se encuentra en el Anexo J.

4.2.22 DECLARACIÓN DE APLICABILIDAD

Se describen los objetivos de control alineados con los controles mencionados en el Anexo 1 de la norma ISO/IEC 27002, con el fin de identificar los controles relevantes para la empresa y justificar su elección. El propósito de este documento es establecer los controles necesarios, definir sus metas y su implementación, así como evaluar los riesgos restantes y la efectividad de los controles implementados. Todos los controles especificados en el Anexo A de la norma ISO 27001 son considerados y se aplican en todo el Sistema de gestión de seguridad de la información de EKONOPHARMA S.A.C. Los empleados que forman parte del SGSI son los usuarios principales de este documento.

Tabla 35

Cuadro de declaración de aplicabilidad

A.5 POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN			
A.5.1 DIRECCIÓN DE LA GERENCIA PARA LA SEGURIDAD DE LA INFORMACIÓN			
Objetivo: Proporcionar guía y respaldo de la gerencia en relación con la protección de datos conforme a las normativas internas y legales correspondientes.			
ID	Controles según la norma ISO 27001	Aplicabilidad (SÍ/NO)	Razón para seleccionar/ no seleccionar.
A.5.1.1	Políticas para seguridad de la información	SI	La norma UNE-EN ISO/IEC 27001 exige la creación de protocolos de seguridad como elemento esencial en la puesta en marcha del Sistema de Gestión de Seguridad de la Información (SGSI). Es crucial que estas directrices sean difundidas y conocidas por todos los empleados de Ekonopharma.
A.5.1.2	Revisión de políticas para seguridad de la información	SI	La norma UNE-EN ISO/IEC 27001 estipula que las políticas de seguridad de la información necesitan ser revisadas y aprobadas por la Alta Dirección para asegurar que se ajusten adecuadamente a las necesidades de la empresa.
A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN			
6.1 ORGANIZACIÓN INTERNA			
Objetivo: Definir pautas de gestión para dar inicio y supervisar la ejecución y funcionamiento de las medidas de protección de datos en la empresa.			
A.6.1.1	Roles y responsabilidades sobre seguridad de la información	SI	La empresa debe implementar roles de seguridad de la información según lo requiere la normativa UNE-EN ISO/IEC 27001 con el fin de evitar cambios no autorizados.
A.6.1.2	Separación de deberes	si	Es importante dividir las responsabilidades entre los diferentes roles de la empresa para evitar las cargas por demasiadas labores.
A.6.1.3	Contacto con autoridades	no	No se cree que la implementación de este nivel de control contribuya a disminuir la probabilidad de pérdida de los activos.

A.6.1.4	Contacto con grupos de interés especial	si	Es fundamental establecer relaciones con grupos específicos, entidades u organizaciones que promuevan acciones relacionadas con la protección de la información en línea.
A.6.1.5	Seguridad de la información en gestión de proyectos	no	Aún no realizan proyectos en la empresa
6.2 DISPOSITIVOS MÓVILES Y TELETRABAJO			
Objetivo: Velar por la protección en la realización de labores a distancia y la utilización de aparatos portátiles.			
A.6.2.1	Política sobre dispositivos móviles	SI	Los dispositivos móviles pueden o no manejarse para guarda datos.
A.6.2.2	Teletrabajo	NO	No se trabaja de forma remota.
A.7 SEGURIDAD RELATIVA A LOS RECURSOS HUMANOS			
7.1 ANTES DEL EMPLEO			
Objetivo: Garantizar que los empleados y colaboradores entiendan sus deberes y sean adecuados para las funciones que desempeñan.			
A.7.1.1	Investigación de antecedentes	SI	Durante el proceso de selección y contratación, es fundamental examinar los registros criminales y policiales de los candidatos, especialmente si se trata de una posición de liderazgo.
A.7.1.2	Términos y condiciones de empleo	SI	Se documentan en los contratos
7.2 DURANTE EL EMPLEO			
Objetivo: Asegurar que tanto los empleados como los contratistas estén al tanto de sus responsabilidades respecto a la protección de la información y las cumplan de manera correcta.			
A.7.2.1	A.7.2.1 Gestión de responsabilidades	SI	Es importante tener un registro y hacer saber las tareas que deben llevar a cabo antes de entrenar al personal.
A.7.2.2	Toma de concienciación, educación y capacitación en seguridad de la información	SI	Según la evaluación de riesgos, una situación común que representa un peligro es la carencia de capacitación en seguridad.
A.7.2.3	Proceso disciplinario	SI	Es necesario implementar consecuencias para los trabajadores que no cumplan con las regulaciones de seguridad de la información establecidas o que incurran en alguna vulneración de la seguridad.
7.3 FINALIZACIÓN DEL EMPLEO O CAMBIO EN EL PUESTO DE TRABAJO			
Objetivo: Proteger los intereses de la empresa durante el proceso de cambio o terminación de un contrato de trabajo.			
A.7.3.1	Terminación o cambio de condiciones del empleo	SI	Después de que el contrato de un empleado finalice, es importante que las obligaciones y acciones de protección de la información continúen vigentes incluso luego de que haya finalizado o cambiado de trabajo.
A.8 GESTIÓN DE ACTIVOS			
A.8.1 RESPONSABILIDAD DE LOS ACTIVOS			
Objetivo: Reconocer los bienes de la organización y establecer las responsabilidades necesarias para su cuidado.			
A.8.1.1	Inventario de activos	SI	Es imprescindible elaborar un inventario de los recursos de información de la empresa para poder administrarlos y controlarlos de manera efectiva.
A.8.1.2	Propiedad de los activos	SI	La información del activo es reservada y solo un selecto grupo de empleados tienen permiso para acceder a ella, su divulgación podría

			afectar a la empresa.
A.8.1.3	Uso aceptable de los activos	SI	Se establecerán directrices para el uso de los recursos.
A.8.1.4	Devolución de activos	SI	Es fundamental implementar un procedimiento para la devolución de activos, en el cual los trabajadores deben entregar todos los recursos de la empresa que hayan estado a cargo de ellos al concluir su contrato laboral.
8.2 CLASIFICACIÓN DE LA INFORMACIÓN			
Objetivo: Asegurarse de que la información reciba la protección necesaria en función de su relevancia para la empresa.			
A.8.2.1	Clasificación de la información	SI	Será importante reconocer la información más importante para implementar las medidas apropiadas.
A.8.2.2	Etiquetado de la información	SI	Se requiere establecer y seguir un proceso adecuado para etiquetar la información, asignando etiquetas específicas y manteniendo un registro centralizado que señale qué recursos de información están disponibles en cada área.
A.8.2.3	Manejo de activos	SI	Para determinar la clasificación y establecer las medidas de seguridad correspondientes.
8.3 MANIPULACIÓN DE LOS SOPORTES			
Objetivo: Evitar que la información almacenada en dispositivos sea difundida, modificada, borrada o accedida sin autorización..			
A.8.3.1	Gestión de medios removibles	SI	Es indispensable implementar procedimientos para gestionar los dispositivos de almacenamiento que se pueden desconectar.
A.8.3.2	Eliminación de medios	SI	Es imprescindible crear procedimientos para gestionar los dispositivos de almacenamiento portátiles, de acuerdo con la jerarquía de clasificación establecida en la empresa.
A.8.3.3	Transferencia de medios físicos	NO	No se podrían obtener documentos significativos fuera de las instalaciones.
A.9 CONTROL DE ACCESO			
9.1 REQUISITOS DE LA EMPRESA PARA EL CONTROL DE ACCESO			
A.9.1.1	Política de control de acceso	SI	Es necesario crear, registrar y actualizar constantemente una política de control de acceso que se ajuste a los requerimientos de la compañía y asegure la protección de los datos.
A.9.1.2	Acceso a redes y a servicios de red	SI	La gestión del acceso a los servicios de red se basa en las necesidades individuales de cada usuario.
A.9.2 GESTIÓN DE ACCESO DE USUARIO			
Objetivo: Asegurar que solo las personas autorizadas puedan acceder a sistemas y servicios para prevenir el ingreso de personas no autorizadas.			
A.9.2.1	Registración y baja de usuarios	SI	El control se vuelve esencial debido a los cambios constantes de usuarios en los sistemas, que entran y salen de manera continua.
A.9.2.2	Concesión de acceso de usuarios	SI	Los permisos son asignados o revocados de acuerdo a los requerimientos de acceso de los usuarios.
A.9.2.3	Gestión de derechos de acceso privilegiado	SI	Los permisos se otorgan en el nivel del sistema operativo.
A.9.2.4	Gestión de información secreta de autenticación de usuarios	SI	Dado lo que se encontró en el análisis de riesgos, sería aconsejable llevar a cabo esta acción de control.

A.9.2.5	Revisión de los derechos de acceso del usuario	SI	Se lleva a cabo a solicitud del encargado directo del usuario.
A.9.2.6	Eliminación o ajuste de derechos de acceso	SI	Cuando se produce una disminución de empleados o cambios en sus responsabilidades, se procede a desactivar las cuentas o ajustar los permisos correspondientes.
9.3 RESPONSABILIDADES DEL USUARIO			
Objetivo: Responsabilizar a los usuarios de proteger su información de acceso de forma segura.			
A.9.3.1	Uso de información secreta de autenticación	SI	Los usuarios deben acatar las normas de la empresa respecto al tratamiento de datos confidenciales para la autenticación.
9.4 CONTROL DE ACCESO A SISTEMA Y APLICACIÓN			
Objetivo: Prevenir el ingreso no autorizado a sistemas y programas.			
A.9.4.1	Restricción al acceso a la información	No	No es válido porque carecen de un departamento de desarrollo, por lo tanto, no disponen de sistemas ni aplicaciones.
A.9.4.2	Procedimiento de registro en el terminal	No	No se aplica ya que no cuentan con un área de desarrollo, por lo tanto, no cuentan con sistemas ni aplicaciones.
A.9.4.3	Sistema de gestión de claves	No	No aplica ya que no cuentan con un área de desarrollo, por lo tanto, no cuentan con sistemas ni aplicaciones
A.9.4.4	Uso de programas de utilidad privilegiada	No	No aplica ya que no cuentan con un área de desarrollo, por lo tanto, no cuentan con sistemas ni aplicaciones
A.9.4.5	Control de acceso al código fuente del programa	No	No es necesario ya que no tienen una sección de crecimiento.
A.10 CRIPTOGRAFÍA			
10.1. CONTROLES CRIPTOGRÁFICOS			
Objetivo: Asegurar que la criptografía se aplique de manera correcta y eficiente para proteger la confidencialidad, autenticidad y/o integridad de la información.			
A.10.1.1	Política del uso de controles criptográficos	NO	No se utilizan técnicas criptográficas en Ekonopharma.
A.10.1.2	Gestión clave	NO	Las claves criptográficas no se están manejando.
A.11 SEGURIDAD FÍSICA Y DEL ENTORNO			
11.1 ÁREAS SEGURAS			
Finalidad: Impedir que individuos no autorizados puedan ingresar de forma física a la información y a las instalaciones de procesamiento de datos de la entidad, y prevenir posibles perjuicios e interrupciones.			
A.11.1.1	Perímetro de seguridad física	SI	Es necesario implementar y seguir protocolos de seguridad en el perímetro de áreas que contengan información confidencial, como centros de datos.
A.11.1.2	Controles físicos de ingreso	SI	Es fundamental garantizar que solamente las personas autorizadas puedan acceder a las áreas seguras a través de sistemas de control de acceso adecuados.
A.11.1.3	Seguridad de oficinas, habitaciones e instalaciones	SI	Es necesario planificar y llevar a cabo medidas para asegurar la protección física en oficinas, recintos e instalaciones.

A.11.1.4	Protección contra amenazas externas y ambientales	Si	Este control tiene un efecto positivo en la disminución de los riesgos identificados.
A.11.1.5	Trabajo en áreas seguras	NO	No es necesario aun este control
A.11.1.6	Áreas de entrega y carga	NO	En la recepción se destina un área específica para llevar a cabo la carga y descarga.
A.11.2 SEGURIDAD DE LOS EQUIPOS			
Propósito: Evitar que los activos de la organización sufran pérdidas, daños, robos o compromisos, así como evitar la interrupción de sus operaciones.			
A.11.2.1	Emplazamiento y protección de los equipos	SI	Es necesario situar los equipos en zonas seguras, resguardados de posibles riesgos y amenazas externas.
A.11.2.2	Servicios de suministro	SI	Es de vital importancia garantizar la seguridad de los dispositivos ante posibles fallos eléctricos y cortes de energía causados por problemas en los servicios.
A.11.2.3	Seguridad en el cableado	SI	La colocación de los cables se realiza de forma segura.
A.11.2.4	Mantenimiento de equipo	SI	Es necesario mantener los equipos adecuadamente para garantizar que estén disponibles y en buen estado de funcionamiento de forma constante.
A.11.2.5	Retirada de materiales propiedad de la empresa	NO	No se revelará información confidencial de la organización en los materiales divulgados.
A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones	NO	Los equipos permanecen dentro de las instalaciones de la compañía.
A.11.2.7	Disposición o reutilización de equipos	SI	Cuando se vuelven a utilizar, los equipos que han sido descartados son formateados e instalados de nuevo.
A.11.2.8	Equipo de usuario desatendido	SI	Sería recomendable tomar medidas para prevenir accesos no autorizados.
A.11.2.9	Política de escritorio limpio y pantalla limpia	SI	Para prevenir de esta manera fugas de información no deseadas.
A.12 SEGURIDAD DE LAS OPERACIONES			
A.12.1 PROCEDIMIENTOS Y RESPONSABILIDADES OPERACIONALES			
Objetivo: Asegurar que los centros de procesamiento de datos operen de manera eficiente y segura.			
A.12.1.1	Procedimientos documentados de operación	NO	Se cree que la inversión necesaria para instalar este sistema de control sería mayor que los beneficios que generaría.
A.12.1.2	Gestión de cambios	NO	Se cree que la inversión necesaria para instalar este sistema de control sería mayor que los beneficios que generaría.
A.12.1.3	Gestión de capacidad	NO	Se cree que la inversión necesaria para instalar este sistema de control sería mayor que los beneficios que generaría.
A.12.1.4	Separación de ambientes de desarrollo, prueba y operacionales	NO	La entidad no desarrolla Software

A.12.2 PROTECCIÓN CONTRA EL SOFTWARE MALICIOSO (MALWARE)			
Objetivo: Garantizar que los datos y sistemas de información estén seguros ante la amenaza de malware.			
A.12.2.1	Controles contra software malicioso	SI	Deberían establecerse medidas de seguridad para el uso de correo electrónico y la visita de sitios web con contenido sospechoso.
A.12.3 COPIAS DE SEGURIDAD DE LA INFORMACIÓN			
Objetivo: Garantizar la seguridad de la información para evitar su pérdida.			
A.12.3.1	Copia de seguridad de la información	SI	Los equipos cuentan con software de protección contra virus.
A.12.4 REGISTRO DE EVENTOS			
Objetivo: Documentar sucesos y crear pruebas.			
A.12.4.1	Registro de eventos	NO	No se puede aplicar ya que los costos para implementar este control serían mayores que los beneficios que se podrían obtener.
A.12.4.2	Protección de la información del registro	NO	
A.12.4.3	Registros del administrador y operador	NO	
A.12.4.4	Sincronización de relojes	NO	
A.12.5 CONTROL DEL SOFTWARE OPERACIONAL			
Propósito: Garantizar la seguridad y fiabilidad de los sistemas operativos.			
A.12.5.1	Instalación de software en sistemas operativos	NO	No se puede aplicar ya que los costos para implementar este control serían mayores que los beneficios que se podrían obtener.
A.12.6 GESTIÓN DE VULNERABILIDAD TÉCNICA			
Propósito: Evitar la explotación de las debilidades técnicas.			
A.12.6.1	Gestión de vulnerabilidades técnicas	No	No se puede aplicar ya que los costos para implementar este control serían mayores que los beneficios que se podrían obtener.
A.12.6.2	Restricciones sobre instalación de software	No	
A.12.7 CONSIDERACIONES PARA LA AUDITORIA DE LOS SISTEMAS DE INFORMACIÓN			
Objetivo: Reducir el efecto de las actividades de auditoría en los sistemas operativos.			
A.12.7.1	Controles de auditoría sobre los sistemas de información	NO	No se puede aplicar ya que los costos para implementar este control serían mayores que los beneficios que se podrían obtener.
A.13.1 GESTIÓN DE LA SEGURIDAD DE LA RED			
Objetivo: Asegurar la protección de la información en los sistemas informáticos y en las estructuras de almacenamiento y tratamiento de datos.			
A.13.1.1	Controles de red	NO	No se puede aplicar ya que los costos para implementar este control serían mayores que los beneficios que se podrían obtener.
A.13.1.2	Seguridad de los servicios de red	NO	
A.13.1.3	Segregación en redes	NO	
A.13.2 TRANSFERENCIA DE INFORMACIÓN			
Objetivo: Garantizar la protección de los datos compartidos tanto dentro de una empresa como con otras entidades.			

A.13.2.1	Procedimientos y políticas sobre transferencia de información	NO	No se puede aplicar ya que los costos para implementar este control serían mayores que los beneficios que se podrían obtener.
A.13.2.2	Acuerdos sobre transferencia de información	NO	Es necesario llegar a consensos para intercambiar información empresarial con los empleados internos y con socios externos.
A.13.2.3	Mensajes electrónicos	SI	Es imprescindible definir procedimientos acerca de la manera en que se comparte la información.
A.13.2.4	Acuerdos de confidencialidad o no divulgación	SI	Estamos desarrollando medidas internas para asegurar la privacidad de la información de nuestros clientes en nuestra organización.
A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS			
14.1 REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN			
Propósito: Asegurar que la seguridad de la información sea una prioridad en cada fase de creación de sistemas de información, incluso en aquellos que brindan servicios a través de Internet.			
A.14.1.1	Análisis y especificación de los requerimientos de seguridad de la información	NO	En este momento, no se está contemplando incluir este control en el alcance del SGSI, ya que resultaría en mayores costos.
A.14.1.2	Seguridad de servicios de aplicación en redes públicas	NO	
A.14.1.3	Protección de transacciones de servicios de aplicaciones	NO	
A.14.2 Seguridad en los procesos de desarrollo y soporte			
Propósito: Garantizar que la protección de la información se incorpore de manera planificada y ejecutada en todas las etapas del desarrollo de los sistemas de información.			
A.14.2.1	Política de desarrollo seguro	NO	La falta de implementación de esta medida se debe a que en la actualidad no se toma en cuenta esta consideración, y también a la ausencia de sistemas de información en la empresa.
A.14.2.2	Procedimientos para control en cambio de sistema	NO	
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma operativa	NO	
A.14.2.4	Restricciones sobre los cambios en los paquetes de software	NO	
A.14.2.5	Principios de ingeniería para sistema seguro	NO	

A.14.2.6	Ambiente de desarrollo seguro	NO	
A.14.2.7	Desarrollo externalizado	NO	
A.14.2.8	Prueba de seguridad del sistema	No	
A.14.2.9	Prueba de aceptación del sistema	NO	
14.3 DATOS DE PRUEBA			
Objetivo: Garantizar la seguridad de la información utilizada en ensayos.			
A.14.3.1	Protección de datos de prueba	NO	En la actualidad, este control no se está tomando en cuenta para la puesta en marcha del Sistema de Gestión de Seguridad de la Información (SGSI).
A.15 RELACIONES CON LOS PROVEEDORES			
15.1 SEGURIDAD DE LA INFORMACIÓN EN LAS RELACIONES CON LOS PROVEEDORES			
Objetivo: Garantizar la seguridad de los bienes de la empresa que estén al alcance de los proveedores.			
A.15.1.1	Política de seguridad de la información para relaciones con proveedores	NO	No se ve factible llevar a cabo esta medida de control ya que se cree que los gastos serían mayores que las ventajas que se obtendrían.
A.15.1.2	Tratamiento de la seguridad en contratos con proveedores	SI	Es fundamental poner en marcha políticas con los proveedores para acordar el correcto uso de la información que se almacena.
A.15.1.3	Cadena de suministro de tecnología de información y comunicación	SI	Los acuerdos con los proveedores deben contener especificaciones que impidan posibles peligros relacionados con la seguridad de la información.
15.2 GESTIÓN DE ENTREGA DE SERVICIOS DEL PROVEEDOR			
Meta: Asegurar que se respete el nivel de seguridad de la información y la prestación del servicio conforme a los convenios establecidos con los proveedores.			
A.15.2.1	Monitoreo y revisión de los servicios de proveedores	NO	En este momento, no se está considerando incluir este control en el ámbito del Sistema de Gestión de Seguridad de la Información.
A.15.2.2	Gestión de cambios en los servicios de proveedores	NO	Actualmente no se está considerando incluir este control en el ámbito del Sistema de Gestión de Seguridad de la Información.
A.16 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN			
A. 16.1 Gestión de incidentes de seguridad de la información y mejoras			
Propósito: Asegurar la implementación de un método coherente y efectivo para abordar incidentes de seguridad de la información y para comunicar de forma adecuada eventos de seguridad y vulnerabilidades.			
A.16.1.1	Responsabilidades y procedimientos	SI	Es fundamental contar con la participación del equipo en la administración de contratiempos.
A.16.1.2	Reporte de eventos en la seguridad de la información	SI	Es imprescindible documentar cada ocasión en la que se presente un incidente de seguridad con el fin de establecer un historial de acontecimientos que será de utilidad para aprender de ellos en el futuro. Asimismo, resulta crucial mantener al día los procedimientos en este ámbito.

A.16.1.3	Reporte de debilidades en la seguridad de la información	SI	Es necesario comunicar los incidentes detectados con el fin de determinar si constituyen un problema o no.
A.16.1.4	Evaluación y decisión sobre eventos de seguridad de la información	SI	Se requiere la creación de protocolos específicos basados en las decisiones tomadas respecto a la seguridad de la información, con el objetivo de tener un documento exhaustivo que señale las directrices a seguir en todo momento.
A.16.1.5	Respuesta ante incidentes de seguridad de la información	SI	Identificar de manera prioritaria a la persona adecuada que será responsable de recibir las alertas sobre situaciones de seguridad en la información y colaborar de acuerdo con el encargado de contacto designado.
A.16.1.6	Aprendizaje a partir de los incidentes en la seguridad de la información	SI	Es esencial supervisar y examinar minuciosamente la cantidad, el tamaño y los gastos de los incidentes de seguridad de la información con el fin de poder analizarlos de manera adecuada y aprender de ellos.
A.16.1.7	Recolección de evidencia	SI	La entidad necesita establecer y seguir procesos para detectar, recolectar, obtener y conservar datos que puedan ser utilizados como prueba.
A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO			
A.17.1 Continuidad de seguridad de la información			
Meta: La incorporación de medidas de seguridad de la información en los procesos de gestión de la continuidad del negocio es imprescindible en la empresa.			
A.17.1.1	Planificación de la continuidad de la seguridad de la información	SI	Es esencial identificar posibles vulnerabilidades en el funcionamiento continuo de las operaciones.
A.17.1.2	Implementación de la continuidad de la seguridad de la información	SI	Es esencial asegurar que los servicios sigan funcionando de manera ininterrumpida.
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	SI	**Es imprescindible comprobar si los planes son apropiados.**
17.2 Redundancias			
Objetivo: Garantizar que las instalaciones de procesamiento de datos estén siempre disponibles.			
A.17.2.1	Disponibilidad de instalaciones de procesamiento de información	NO	Se estima que los gastos de implementar estas acciones serían mayores que los beneficios obtenidos.
A.18 CUMPLIMIENTO			
A.18.1 CUMPLIMIENTO CON REQUISITOS LEGALES Y CONTRACTUALES			
Propósito: Evitar el incumplimiento de las obligaciones legales, estatutarias, regulatorias o contractuales relacionadas con la seguridad de la información y cualquier requisito de seguridad.			

A.18.1.1	Identificación de legislación y requerimientos contractuales aplicables	SI	Es esencial identificar y documentar los mandatos legales, normas y acuerdos contractuales relevantes, así como la estrategia empresarial para su cumplimiento, asegurándose de mantenerlos actualizados constantemente.
A.18.1.2	Derechos de propiedad intelectual	SI	Es imprescindible llevar a cabo medidas concretas para garantizar el acatamiento de las leyes, acuerdos contractuales y derechos de propiedad intelectual en relación con obras y programas de software protegidos.
A.18.1.3	Protección de registros	SI	Es imprescindible contar con un sistema de control documentado que permita mantener un registro detallado de toda la información, evitando posibles problemas como pérdida, manipulación o falsificación de datos.
A.18.1.4	Privacidad y protección de información personalmente identificable	SI	Es necesario implementar un acuerdo de confidencialidad que resguarde la privacidad de los individuos y la integridad de la información de la compañía.
A.18.1.5	Regulación de controles criptográficos	NO	En la empresa no se utilizan métodos de encriptación para resguardar la información.
18.2 REVISIONES DE SEGURIDAD DE LA INFORMACIÓN			
Propósito: Asegurar que las políticas y procedimientos organizacionales para la seguridad de la información sean cumplidos y ejecutados adecuadamente.			
A.18.2.1	Revisión independiente de la seguridad de la información	SI	Es indispensable llevar a cabo una evaluación regular de la protección de los datos.
A.18.2.2	Cumplimiento con las políticas y estándares de seguridad	SI	Durante las revisiones se verificará si se han cumplido los procedimientos, políticas y normativas adecuadas.
A.18.2.3	Revisión de cumplimiento técnico	SI	Se estima que los beneficios obtenidos no superarían el coste de implementar estas medidas.

Nota. La tabla representa cuadro de declaración de aplicabilidad en Ekonopharma. Elaboración propia.

4.2.23 Matriz de Comunicación Interna y Externa

En este texto se detallan las directrices para la comunicación interna y externa en relación con el SGSI. Se especifica el contenido de la información a comunicar, los momentos requeridos para hacerlo, los destinatarios pertinentes, la persona encargada de la comunicación y los canales a utilizar. Estos aspectos se encuentran descritos de forma detallada en la tabla del Anexo K.

4.2.24 Plan de Concientización y Capacitación

Es fundamental y necesario mantener al personal informado y concienciado, por lo que se deben llevar a cabo diferentes actividades como charlas y campañas de seguridad cibernética. Asimismo, se ha creado un documento llamado "Plan de sensibilización y capacitación" para este propósito.

El propósito de este programa es instruir y sensibilizar al personal de Ekonopharma con el fin de que adquieran las destrezas requeridas para fortalecer la seguridad de la información. Para alcanzar este objetivo, se describen las tareas a realizar, los plazos a cumplir y los recursos financieros necesarios. La responsabilidad empieza en la cúpula directiva y se extiende a todos los colaboradores implicados en el núcleo del procedimiento y en los procesos conexos.

Beneficios:

a) Mejora en la protección de la información con mayor eficacia.
b) Establecimiento de documentos, modelos y archivos específicos para implementar el Sistema de Gestión de Seguridad de la Información.
c) Normas y directrices establecidas para asegurar la seguridad de la información y aumentar su rendimiento en este aspecto.

Se realizará una charla en persona acerca de la relevancia de mantener la seguridad de los datos.

Tabla 36

Plan de charla y capacitación de SI

CAPACITACIONES DE LA EMPRESA EKONOPHARMA S.A.C	
1.- CHARLA DE CONCIENTIZACION EN SEGURIDAD DE LA INFORMACIÓN: Se realizarán evaluaciones cortas sobre la seguridad de la información antes y después de la charla de concientización, con el objetivo de medir el impacto que haya tenido en los empleados.	
Tiempo:	1 hora
Audiencia:	Todo el personal de Ekonopharma
Asistentes	7

TEMARIO:

- ¿Cómo se puede describir la seguridad de la información?
- ¿Cuál es la diferencia entre la seguridad de la información y la seguridad informática?
- Ejemplos específicos de riesgos para la información
- Factores fundamentales en la protección de la información
- Métodos para garantizar la seguridad de la información
- Maneras de crear conciencia sobre la relevancia de la seguridad de la información
- Reflexiones finales

CAPACITACIÓN SOBRE CÓMO MANTENER LA SEGURIDAD DE LA INFORMACIÓN.

Se realizarán talleres presenciales que abordarán distintos temas relacionados con la protección de la información, como se especifica a continuación:

Tiempo	5 horas
Asistentes	3 personas
Audiencia	Responsables de cada proceso.

TEMARIO:

- ¿Qué implica el Sistema de Gestión de Seguridad de la Información?
- Ventajas del SGSI
- Proceso de supervisión de la información registrada
- Manejo de riesgos
- Medidas de seguridad de datos
- Manejo de situaciones imprevistas
- Revisión interna
- Resultados finales y sugerencias

CAMPAÑA SOBRE LA IMPORTANCIA DE PROTEGER LA INFORMACIÓN

El propósito es fomentar en el personal de Ekonopharma una conciencia de seguridad de la información a través de diferentes iniciativas, como la introducción de salvapantallas, boletines electrónicos, folletos, trípticos, posters y afiches que aborden esta temática. Estas acciones buscan que los empleados comprendan la relevancia de proteger la información de la empresa.

Tiempo	1 hora
Audiencia	Todo el personal
Asistentes	7 personas

TEMARIO:

La campaña durará una semana de manera continua y después se llevará a cabo cada dos meses de forma regular. El desarrollo de la campaña se dividirá en tres fases.

Diseño de la campaña

En esta fase se llevarán a cabo la fabricación y organización de los recursos requeridos para ejecutar la campaña de concienciación acerca de la protección de los datos. Se realizarán las actividades previstas para este intervalo de tiempo:

- Desarrollo de un logo y lema para impulsar la seguridad de datos.
- Elaboración de tres diseños de salvapantallas relacionados con la protección de información.
- Diseño de tres carteles que promuevan la importancia de mantener segura la información.
- Creación de trípticos y folletos dirigidos al personal para concientizar sobre la seguridad de la información.

Promoción de la campaña

Promoveremos la campaña de concienciación sobre seguridad de la información enviando carteles y/o afiches por correo electrónico:

- Se llevará a cabo la difusión del logo y lema de seguridad de la información.
- Se implementará la instalación de salvapantallas en todos los equipos de trabajo de los empleados de Ekonopharma.
- Se pondrán carteles de seguridad de la información en las instalaciones de la oficina de Ekonopharma y se distribuirán trípticos o folletos físicos al personal externo.

Nota. La tabla muestra el plan de charlas y capacitación sobre seguridad de la información en Ekonopharma.

Tabla 37

Presupuesto para charla y capacitación por día

Recursos	**Empresa**	**Descripción**	**Cantidad**	**Monto total s/.**
break	Local principal de Ekonopharma	sándwich (1) bebida (1)	10 personas	s/ 100.00
Impresiones y folletos	gráfica	impresión: 10 folletos calidad: full color tamaño: a4	10 hojas	s/ 2.00
		costo total		s/ 102.00

Fuente: La tabla representa el presupuesto de charla y capacitación por día.

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

Según los resultados obtenidos en el estudio realizado, se concluye que EKONOPHARMA enfrenta dificultades en la organización y almacenamiento de la información, debido a la falta de procedimientos implementados actualmente. La falta de un sistema adecuado dificulta la realización de las tareas de la empresa, lo que conlleva a una gestión administrativa ineficiente con problemas como la pérdida de datos, duplicación de información, falta de centralización y descontento del personal. Por lo tanto, es esencial asegurar la implementación adecuada de un Sistema de Gestión de Seguridad de la Información (SGSI), ya que la falta de manejo correcto de la información puede resultar en consecuencias negativas y daños económicos para la organización.

Es crucial fijar objetivos y políticas claras, reducir riesgos y contar con la implicación activa de los directivos. La mejora continua y el monitoreo constante del sistema son clave para evaluar su desempeño y realizar ajustes necesarios. La implementación de un SGSI en EKONOPHARMA SAC es crucial para garantizar la seguridad de los activos y cumplir con los objetivos del negocio, mediante controles efectivos y acciones concretas.

Es fundamental no solo tener medidas de seguridad en lugar, sino también establecer políticas y procedimientos que refuercen la seguridad en el ámbito informático y garanticen una defensa eficaz.

Se puede ajustar los procedimientos y políticas a distintas empresas, adaptándolos a sus necesidades específicas con el fin de disminuir el riesgo que enfrentan sus activos identificados y alcanzar un menor nivel residual de riesgo.

No basta con tener medidas de seguridad implementadas, es necesario contar con políticas y procedimientos que fortalezcan la seguridad informática y brinden una defensa efectiva.

5.2 RECOMENDACIONES

Se aconseja seguir con el plan de trabajo para finalizar la instalación de los controles pendientes. Para lograrlo, es fundamental que la dirección superior garantice la disponibilidad de los recursos requeridos para alcanzar este objetivo clave.

Se aconseja a los altos cargos de la empresa EKONOPHARMA SAC que cada área realice un análisis de los posibles riesgos asociados a sus activos en funcionamiento, los cuales deben ser monitoreados mediante una matriz de riesgos corporativa.

Se sugiere que, cada dos años, la alta dirección implemente programas de concienciación en todos los sectores de la empresa, con el fin de reforzar la relevancia de la seguridad de la información y su impacto en la protección de los datos. Es esencial que todos los empleados comprendan las posibles consecuencias de no cumplir con las normas de seguridad vigentes.

Es esencial para las empresas de tamaño pequeño y mediano tener en cuenta la importancia de emplear software legítimo, instalar un antivirus de calidad, actualizar programas con regularidad y detectar posibles riesgos de seguridad al abordar por primera vez la protección de la información.

Es fundamental instruir a los trabajadores sobre los conceptos de la seguridad cibernética, fomentar la creación de contraseñas robustas, restringir la navegación en internet durante el horario laboral, implementar reglas para el uso seguro de teléfonos móviles y realizar respaldos periódicos de la información corporativa como medidas de protección.

Es aconsejable continuar empleando la técnica de gestión de riesgos, ya que ayudará a detectar de forma eficiente los riesgos relacionados con la empresa y tomar medidas adecuadas para mitigarlos.

Se recomienda que investigaciones futuras investiguen y pongan a prueba nuevas herramientas tecnológicas para situaciones específicas, ya que la información sobre el uso de tecnologías para reducir riesgos es escasa a nivel nacional.

BIBLIOGRAFÍA

Abad M. (2015). *Cómo gestionar la seguridad de la información (según ISO 27001: 2013 en una PYME del sector de las tecnologías de la información y la comunicación.* Tesis de pregrado, Universidad de VALLADOLID,, Valladolid, España.

AENOR. (2014). *Structure of the ISO/IEC 27001:2013 Standard.*

Amutio, M., Candau, J., & Mañas, J. (2012). *MAGERIT – versión 3.0.Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (Vol. III). (J. González, Ed.).* Madrid, Madrid, España: Ministerio de Hacienda y Administraciones Públicas. Obtenido de https://bit.ly/3Mw4PiT

Buendía, R. (2013). *Seguridad de la Información.*

Calder A. (2013). *Información de seguridad y ISO 27001*. Libro Verde de Gobierno de TI.

Camero y Carbajal. (2020). *Mypes en peru.*

Carpentier. (2016). Amenazas de la informacion.

Carrasco, S. (2019). *Metodología de la investigación científica. Pautas metodológicas para diseñar y elaborar el proyecto de investigación* (Vol. 19ava ed). Lima: Editorial San Marcos.

M. y. (2019). *Propuesta de un modelo de sistema de gestion de la seguridad de la informacion en una pyme basado en la norma ISO/IEC 27001.* Peru.

Chopra A. y Chaudhary M. . (2020). *Implementing an Information Security Management System.*

COMPENDIO. (2006). *Sistema de gestión de la seguridad de la información (SGSI).* CONTEC. Obtenido de www.Icontec.org.com

Eset . (2023). Security Report.

Francisco Nicolás Solarte. (s.f.). *Revista Tecnologica ESPOL*.

Hernández, Fernández y Baptista. (2014). *Metodologia de investigación.*

Iso Tools Excellence chile. (2016). Obtenido de https://isotools.org/isotools/normas/sistema-de-gestion-de-riesgos-y-seguridad/iso-27001/

Jeimy J. y Cano Gonzales. (2020). *Seguridad de la informacion y ciberseguridad empresarial.* doi:10.29236/sistemas.n155a1.

Ministerio de Hacienda y Administraciones Públicas, o. 2.-N.-1.-1.-8. (2012). *MAGERIT-V3.0 Metodología para el Análisis y Gestión de Riesgos en Sistemas de Información.* Obtenido de Tomado de MAGERIT-V3.0 Metodología para el Análisis y Gehttps://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

Miranda K. (2013). *Guía Metodológica para implementar un Sistema de Gestión de Seguridad en Instituciones* . (Tesis de Maestría), Universidad de Piura, Piura, Perú.

Revista Global de Seguridad de la Información. (2022). Encuesta Global de Seguridad de la Informacion. *Encuesta Global de Seguridad de la Informacion*.

Roa Buendia y Tori. (2013). *Ciberseguridad.*

Rodríguez Baca, L., Cruzado Puente de la Vega, C., Mejía Corredor, C., & Alarcón Díaz, M. (2020). *Aplicación de ISO 27001 y su influencia en la seguridad de la información de una empresa privada peruana.* Propósitos y Representaciones, 8(3), e786.

Sunat. (2020). *Encuestas generales del Perú.*

Vivian Andrea Garcia Balaguera y Jhon Jarby Ortiza Gonzales. (2017). *Análisis de riesgos según la norma iso 27001:2013 para las aulas virtuales de la universidad santo tomas.* Bogotá.

ANEXOS

ANEXO A - CRONOGRAMA DE ACTIVIDADES

Se elabora un plan de trabajo aproximado teniendo en cuenta las tareas y metas que se deben cumplir en cada una de las etapas de ejecución.

Tabla 38

Cronograma de Actividades para EKONOPHARMA. S.A.C

PROYECTO IMPLEMENTACIÓN DE LA ISO/IEC 27001-Ekonopharma		**180 días**	**Fecha de inicio**	**Fecha de finalización**
FASE 1 – PLANEAR		54 días	16/03/2024	15/05/2024
3	**Realizar el análisis de brecha inicial**	**8 días**	**16/03/2024**	**20/03/2024**
4	Realizar cuestionario de análisis de brecha	3 días	16/03/2024	18/03/2024
5	Responder cuestionario de análisis de brecha	2 días	19/03/2024	20/03/2024
6	Informe de análisis de brecha inicial	0 días		
7	**Compromiso con la alta dirección**	**5 días**	**22/03/2024**	**26/03/2024**
8	Realizar una propuesta del proyecto	3 días	22/03/2024	24/03/2024
9	Realizar acta de compromiso de la alta dirección	1 día	25/03/2024	25/03/2024
10	Revisión de la alta dirección	1 día	26/03/2024	26/03/2024
11	Acta de compromiso de la alta dirección	0 días		
13	**Comprender el contexto de la organización**	**2 días**	**30/03/2024**	**31/03/2024**
14	Análisis del contexto de la organización	2 día	30/03/2024	31/03/2024
16	Informe del contexto de la organización	0 días		
17	**Comprender necesidades y expectativas**	**2 días**	**03/04/2024**	**04/04/2024**
18	Reunión para evaluar las necesidades y expectativas	1 día	03/04/2024	03/04/2024
19	Análisis de necesidades y expectativas	1 día	04/04/2024	04/04/2024
20	Informe de necesidades y expectativas de las partes interesadas	0 días		
21	**Determinar el alcance del SGSI**	**2 días**	**06/04/2024**	**07/04/2024**
22	Evaluar el alcance del SGSI	1 día	06/04/2024	06/04/2024

23	Revisión de la Alta Dirección	1 día	07/04/2024	07/04/2024
24	Declaración del alcance del SGSI	0 días		
25	**Determinar política de seguridad de la información**	**3 días**	**09/04/2024**	**11/04/2024**
26	Desarrollo de la política de seguridad de la información	2 días	09/04/2024	10/04/2024
27	Revisión de la Alta Dirección	1 día	11/04/2024	11/04/2024
28	Política de seguridad de la información	0 días		
29	**Actualizar manual de organización y funciones (ficha de puesto)**	**3 días**	**13/04/2024**	**15/04/2024**
30	Identificar roles y responsabilidades para la seguridad de la información	2 días	13/04/2024	14/04/2024
31	Elaborar ficha de puesto para roles de la seguridad de la información	1 día	15/04/2024	15/04/2024
32	Ficha de puesto para los roles de seguridad de la información	0 días		
33	**Establecer procedimiento de control de documentación**	**3 días**	**16/04/2024**	**18/04/2024**
34	Desarrollo de procedimiento de control de documentación	3 días	16/04/2024	19/04/2024
35	Procedimiento de control de documentación	0 días		
36	**Establecer procedimiento de evaluación y tratamiento de riesgos**	**6 días**	**21/04/2024**	**26/04/2024**
37	Desarrollo de procedimiento de evaluación y tratamiento de riesgos	2 días	21/04/2024	22/04/2024
38	Procedimiento de evaluación y tratamiento de riesgos	0 días		
39	Establecer procedimiento de gestión de incidentes	2 días	23/04/2024	24/04/2024
40	Desarrollo de procedimiento de gestión de incidentes	2 días	25/04/2024	26/04/2024
41	Procedimiento de gestión de incidentes	0 días		
42	**Establecer procedimiento de auditoría interna**	**2 días**	**27/04/2024**	**28/04/2024**
43	Desarrollo del procedimiento de auditoría interna	2 días	27/04/2024	28/04/2024
44	Procedimiento de auditoría interna	0 días		
45	**Gestión de Riesgos**	**14 días**	**29/04/2024**	**12/05/2024**

46	Realizar metodología de evaluación de riesgos	2 días	29/04/2024	30/04/2024
47	Metodología de evaluación de riesgos	0 días		
48	Realizar el inventario de activos de información	6 días	01/05/2024	05/05/2024
49	Inventario de activos de información	0 días		
50	Determinar amenazas y vulnerabilidades de los activos de información	6 días	06/05/2024	12/05/2024
51	Evaluación de riesgos	0 días		
52	**Elaborar plan de tratamiento de Riesgos**	**6 días**	**15/05/2024**	**20/05/2024**
53	Realizar plan de tratamiento de riesgos	5 días	15/05/2024	19/05/2024
54	Realizar informe de gestión de riesgos	1 día	19/05/2024	19/05/2024
55	Plan de tratamiento de riesgos	0 días		
56	Informe de la gestión de riesgos	0 días		
57	**Elaborar declaración de aplicabilidad de controles**	**6 días**	**21/05/2024**	**26/05/2024**
58	Elaborar declaración de aplicabilidad de controles	6 días	21/05/2024	26/05/2024
59	Declaración de aplicabilidad de controles	0 días		
60	**Elaborar matriz de comunicación interna y externa**	**2 días**	**01/06/2024**	**02/06/2024**
61	Realizar matriz de comunicación interna	2 días	01/06/2024	02/06/2024
62	Matriz de comunicación interna	0 días		
63	**Elaborar plan de capacitación y concientización**	**4 días**	**04/06/2024**	**07/06/2024**
64	Realizar plan de capacitación y concientización	4 días	04/06/2024	07/06/2024
65	Plan de capacitación y concientización	0 días		
FASE 2 – HACER		82 días	12/06/2024	14/08/2024
67	**Implementar plan de capacitación y concientización**	**11 días**	**12/06/2024**	**13/06/2024**
68	Ejecución del plan de capacitación y concientización	10 días	02/05/2024	12/05/2024
69	Realizar informe de ejecución del plan	1 día	14/05/2024	14/05/2024

70	Informe de plan de capacitación y concientización	0 días		
71	**Implementar plan de tratamiento de riesgos**	**84 días**	**14/05/2024**	**04/08/2024**
72	**Ejecución del plan de tratamiento de riesgos**	**82 días**	**14/05/2024**	**02/08/2024**
73	Grupo uno de controles	12 días	14/05/2024	26/05/2024
74	Grupo dos de controles	50 días	06/06/2024	02/08/2024
75	Realizar informe de ejecución de plan de tratamiento de riesgos	2 días	03/08/2024	04/08/2024
76	Informe de plan de tratamiento de riesgos	0 días		
77	**FASE 3 – VERIFICAR**	**13 días**	**06/08/2024**	19/08/2024
78	**Auditoría externa**	**13 días**	**06/08/2024**	**18/08/2024**
79	Preparar auditoría externa	4 días	06/08/2024	09/08/2024
80	Ejecutar auditoría externa	7 días	10/08/2024	17/08/2024
81	Informe de resultados de la auditoría externa	0 días		
82	Revisión por la Alta Dirección	2 día	18/08/2024	19/08/2024
83	Acta de revisión por la Alta Dirección	0 días		
FASE 4 – ACTUAR		**33 días**	**20/08/2024**	25/09/2024
85	**Elaborar plan de acciones correctivas y mejoras**	**14 días**	**20/08/2024**	**04/08/2024**
86	Identificar las acciones por cada observación	4 días	20/08/2024	23/08/2024
87	Realizar el plan de acciones correctivas y mejoras	10 días	24/08/2024	04/09/2024
88	Plan de acciones correctivas y mejoras	0 días		
89	**Implementar plan de acciones correctivas y mejoras**	**16 días**	**05/09/2024**	**21/09/2024**
90	Aplicar el plan de acciones correctivas, levantamiento de observaciones y oportunidades de mejora	16 días	05/09/2024	21/09/2024
91	**Realizar el análisis de brecha final**	**3 días**	**22/09/2024**	**25/09/2024**
92	Responder cuestionario de análisis de brecha	3 días	22/09/2024	25/09/2024
93	Informe de análisis de brecha final	0 días		

ANEXO B

RECOPILACION DE DATOS PARA ANALISIS DE BRECHA EN EKONOPHARMA

Los resultados logrados en las pruebas y la puesta en marcha son los que se detallan a continuación:

a) Entrevistas: Las entrevistas iniciales documentadas fueron a todos los jefes de área de la empresa.

Tabla 39

Plantilla de entrevista general

ENTREVISTA SGSI		
Fecha:	Oficina:	Responsable
ítem	pregunta	respuesta: si /no
1	¿conoce el termino SGSI?	
2	¿su área cuenta o participa en el SGSI?	
3	¿conoce los controles de seguridad?	
4	¿tienen identificados sus activos de información?	
5	¿cuenta con políticas de seguridad de información?	
6	¿tiene controles o políticas de contraseñas?	
7	¿se realizan mantenimiento preventivo a los equipos informáticos de su área?	
8	¿ha tenido incidentes de seguridad informática?	
9	¿ha tenido incidentes de seguridad de información?	

ANEXO C -CUESTIONARIOS REALIZADOS

Tabla 40

Resultado de las entrevista y cuestionarios realizados

N.º	Responsable / Pregunta	Gerente General	Coordinador de Calidad QF	Coordinadora de RRHH y Logística	QF Regente	Tecnico1	Tecnico2	si	no
1	¿Conoce el termino SGSI?	si	no	no	no	no	no	1	5
2	¿Su área cuenta o participa en el SGSI?	no	no	no	no	no	no	0	6
3	¿Conoce los controles de seguridad?	si	si	si	si	no	no	4	2
4	¿Tienen identificados sus activos de información?	no	no	no	no	no	no	0	6
5	¿Cuenta con políticas de seguridad de información?	no	no	no	no	no	no	0	6
6	¿tiene controles o políticas de contraseñas?	si	si	si	si	si	si	6	0
7	¿Se realizan mantenimiento preventivo a los equipos informáticos de su área?	no	no	no	no	no	no	0	6
8	¿Ha tenido incidentes de seguridad informática?	si	si	si	si	si	si	6	0
9	¿ha tenido incidentes de seguridad de información?	si	si	si	si	si	si	6	0

ANEXO D

A partir de la documentación generada se obtuvieron los siguientes resultados:

Los resultados obtenidos a través de la documentación mostraron que existen importantes deficiencias en los controles implementados, lo cual fue evidenciado mediante el análisis de brechas. Se destacó la utilidad de utilizar un cuadro de resumen final para facilitar la identificación de las deficiencias. Se recomienda alcanzar un nivel de madurez 3 en la mayoría de los casos, ya que de lo contrario el desarrollo sería costoso en términos de tiempo y recursos.

1. INFORME DE ANALISIS DE CONTROLES:

Tabla 41

Análisis de Brecha de Requisitos

PREGUNTAS		RESPONSABLE	EJEMPLOS DE EVIDENCIAS	NIVEL DE APLICACIÓN			
				0	1	2	3
4. ENTORNO/CONTEXTO DE LA ORGANIZACIÓN							
4.1	¿La organización revisa regularmente su entorno para identificar los factores que pueden tener un impacto en ella?	Alta dirección	La revisión administrativa se lleva a cabo, aunque no de forma regular.		1		
4.2.	¿Han sido identificadas y especificadas cuáles son las diferentes personas involucradas en la organización?	Alta dirección	Las partes interesadas son reconocidas, a pesar de que sus responsabilidades pueden variar en la empresa.		1		
4.2.	¿La entidad reconoce, examina y mantiene al día datos acerca de los requerimientos y deseos de sus clientes, proveedores, colaboradores y demás partes involucradas pertinentes al Sistema de Gestión de Seguridad de la Información?	Alta dirección	Se entienden las demandas de los clientes, proveedores y trabajadores, sin embargo, el SGSI carece de políticas adecuadas.		1		
4.1.	¿La organización tiene una planificación estratégica basada en la información relevante tanto interna como externa?	Alta dirección	No existe	0			
4.3.	¿Se ha definido el alcance del Sistema de Gestión de Seguridad de la Información por parte de la organización?	Alta dirección	No existe	0			
4.4	¿La Organización sigue, lleva a cabo, conserva y perfecciona constantemente su Sistema de Gestión de la Seguridad de la Información?	Coordinadora de Calidad	No, ya que está en proceso de implementación en la empresa.	0			
4. ENTORNO/CONTEXTO DE LA ORGANIZACIÓN - NIVEL DE APLICACIÓN				10%			
5. LIDERAZGO							
5.1	¿Se lleva a cabo una evaluación por parte de la dirección sobre el acatamiento de los objetivos de seguridad de la información con el fin de orientar la dirección estratégica según las necesidades identificadas?	Alta dirección	No, ya que se está comenzando a implementar en la empresa.	0			

5.1	¿Garantiza la alta dirección que los requisitos del Sistema de Gestión de Seguridad de la Información se integren en los procesos de la empresa?	Alta dirección	No, ya que se encuentra en proceso de implementación en la compañía.	0	
5.1	¿El personal directivo garantiza que se cuente con los recursos requeridos para el Sistema de Gestión de Seguridad de la Información (SGSI)?	Alta dirección	No, porque no hay suficiente personal.	0	
5.1	¿Se transmite al personal la relevancia de una adecuada administración de la seguridad de la información y el cumplimiento de los estándares del Sistema de Gestión de Seguridad de la Información?	Alta dirección	No, ya que se está llevando a cabo la implementación en la compañía.	0	
5.1	¿El liderazgo del equipo ha establecido, revisado y difundido la Política de Seguridad de la Información y se asegura de que sea de fácil acceso?	Alta dirección	No, ya que se encuentra en proceso de implementación en la organización.	0	
5.1	¿El liderazgo del equipo garantiza que el sistema de Gestión de Seguridad de la Información logre sus objetivos planeados?	Alta dirección	No, ya que todavía se está introduciendo en la compañía.	0	
5.1	¿El Equipo Directivo guía y respalda a los individuos para que aporten a la eficiencia del Sistema de Gestión de Seguridad de la Información?	Alta dirección	No, ya que está en proceso de ser implementado en la compañía.	0	
5.1	¿El liderazgo del equipo directivo se manifiesta a través de la promoción de la mejora continua y el respaldo a otros roles importantes?	Alta dirección	No existe una mejora continua, solo un apoyo al personal para la atención.	0	
5.2	¿Ha sido creada por el equipo de dirección una política de seguridad de la información?	Alta dirección	No, dado que recién se está poniendo en marcha en la compañía.	0	
5.3.	¿Se han establecido y revisado los roles, funciones y niveles de autoridad pertinentes para garantizar la seguridad de la información?	Alta dirección/ Coordinador de RRHH y Logística	Sí, se llevó a cabo una reunión, pero no se llegó a implementar las funciones adecuadas.		1
5. LIDERAZGO – NIVEL DE APLICACIÓN				3%	
6. PLANIFICACION					

6.1.1.	¿Se incorpora en el sistema de gestión de seguridad la evaluación de los riesgos asociados a la actividad de la empresa?	Coordinador de Calidad	No existe	0	
6.1.2.	¿La organización establece y lleva a cabo un procedimiento para evaluar los riesgos de seguridad de la información?	Coordinador de Calidad	No existe	0	
6.1.3	¿Se ha diseñado un plan para gestionar los riesgos asociados a las operaciones de la organización?	Coordinador de Calidad	No existe	0	
6.2	¿Se han establecido y registrado claramente los propósitos de Seguridad de la Información?	Alta dirección	No, porque recién se está implementando en la empresa	0	
6.2	¿Se ha establecido un plan de mejora centrado en lograr metas específicas?	Coordinador de Calidad	No, porque recién se está implementando en la empresa	0	
6. PLANIFICACIÓN - NIVEL DE APLICACIÓN				0%	
7. SOPORTE					
7.1	¿La organización ha identificado y garantiza la disponibilidad de los recursos esenciales para administrar el Sistema de Gestión de Seguridad de la Información (SGSI)?	Alta dirección / Coordinador de Calidad	Aunque se han identificado los recursos aún no han sido entregados o proporcionados.		1
7.2.	¿Se lleva a cabo una evaluación y monitoreo de cómo se desempeñan las personas?	Coordinadora de RRHH y Logística	Se realiza un seguimiento de forma informal, pero no se lleva a cabo de manera formal.		1
7.3.	¿El equipo está al tanto de la política de seguridad de la información, los objetivos, las ventajas del sistema de gestión de seguridad de la información y las oportunidades de mejora?	Coordinador de Calidad	No, existe	0	
7.4.	¿Han sido establecidas cuáles son las comunicaciones internas y externas que son importantes para el sistema de gestión de Seguridad de la Información?	Coordinador de Calidad	No se llegó a definir	0	
7.5.1.	¿Se ha recopilado la información necesaria del SGSI para garantizar su eficacia?	Coordinador de Calidad	No, porque recién se está implementando en la empresa	0	
7.5.2.	¿Se garantiza la correcta identificación, descripción, formato y revisión de los documentos que han sido creados o actualizados?	Coordinador de Calidad	Si existe un formato establecido y se realiza una revisión, pero no hay una identificación por parte de los líderes de la empresa.		1

7.5.3.	¿Se garantiza la protección y disponibilidad de la información necesaria para la gestión de seguridad?	Coordinador de Calidad	No existe	0
7. SOPORTE - NIVEL DE APLICACIÓN				10%
8. OPERACIÓN				
8.1.	¿Se lleva a cabo la planificación, implementación y supervisión de los procesos del Sistema de Gestión de Seguridad de la Información?	Alta dirección / Coordinador de Calidad	No, porque recién se está implementando en la empresa	0
8.2.	¿Se llevan a cabo evaluaciones de riesgos de seguridad de la información de manera regular programada o cuando surgen modificaciones importantes?	Coordinador de Calidad	No, existe	0
8.3.	¿La organización tiene un plan establecido para abordar los riesgos?	Coordinador de Calidad	No existe	0
8. OPERACIÓN - NIVEL DE APLICACIÓN				0%
9. EVALUACIÓN DEL DESEMPEÑO				
9.1	¿La organización lleva a cabo el monitoreo, medición, análisis y evaluación del Sistema de Gestión de la Seguridad de la Información?	Alta dirección / Coordinador de Calidad	No, porque recién se está implementando en la empresa	0
9.2	¿La organización lleva a cabo auditorías internas en momentos programados previamente?	Alta dirección / Coordinador de Calidad	No, los procesos apenas están comenzando.	0
9.2	¿La organización tiene previsto, establece, ejecuta y conserva un programa de auditorías?	Alta dirección / Coordinador de Calidad	No cuenta con un plan de auditoria	0
9.3	¿Se revisa el sistema de gestión de seguridad de la información por la dirección para garantizar su efectividad?	Alta dirección	No, porque recién se está implementando en la empresa	0
9.3	¿La dirección toma decisiones y lleva a cabo acciones según los resultados obtenidos de la evaluación del Sistema de Gestión de Seguridad de la Información?	Alta dirección	No, porque recién se está implementando en la empresa	0

9. EVALUACIÓN DEL DESEMPEÑO - NIVEL DE APLICACIÓN				0%
10. MEJORAS				
10.1.	¿La organización se encarga de supervisar y enmendar las no conformidades?	Coordinador de Calidad	No, porque recién se está implementando en la empresa.	0
10.1.	La organización examina las no conformidades y toma medidas para eliminar sus causas a través de acciones correctivas.	Coordinador de Calidad	No, porque recién se está implementando en la empresa	0
10.2.	¿La organización busca constantemente mejorar la practicidad, idoneidad y eficacia del SGSI?	Coordinador de Calidad	No, porque recién se está implementando en la empresa	0
10. MEJORA - NIVEL DE APLICACIÓN →				**0%**
SGC- ISO 27001:2013 - REQUISITOS - NIVEL DE APLICACIÓN →				**5%**

Nota: La tabla muestra los resultados de la revisión de los requisitos de la empresa Ekonopharma

INFORME DE ANÁLISIS DE CONTROLES

Tabla 42

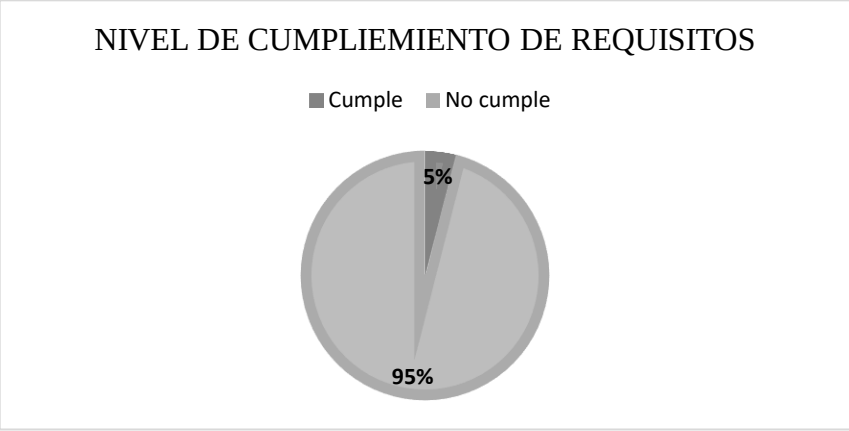
Análisis de Brecha de Controles

Control	Preguntas	¿Es necesario?	Rango 1-4	Comentario
A.5 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN				
A.5.1. DIRECCIÓN DE LA GERENCIA PARA LA SEGURIDAD DE LA INFORMACIÓN				
A.5.1.1 Políticas de seguridad de la información	¿Existe un documento aprobado por la alta dirección que se conoce como Política de Seguridad de la Información?	SI	0	Dado que no había un departamento de tecnología en la empresa, la dirección consideró que no era imprescindible implementar políticas de seguridad.
	¿Opina que los trabajadores están al tanto de las normas de seguridad que debe seguir su empresa?	SI	1	No, únicamente aquellos empleados de la parte administrativa.
A.5.1.2 Revisión de las políticas de	¿Su empresa establece períodos de tiempo específicos para revisar las políticas de seguridad de la información?	SI	0	No, ya que la compañía está empezando a aplicarlas recientemente.

seguridad de la información	¿Se analiza la eficacia, idoneidad y pertinencia de las políticas de seguridad de la información durante las revisiones?	SI	0	Todavía no, ya que solamente se centraron en la administración del acceso de los usuarios.

Figura 16

Gráfico de Resultados del Análisis Inicial de Brechas

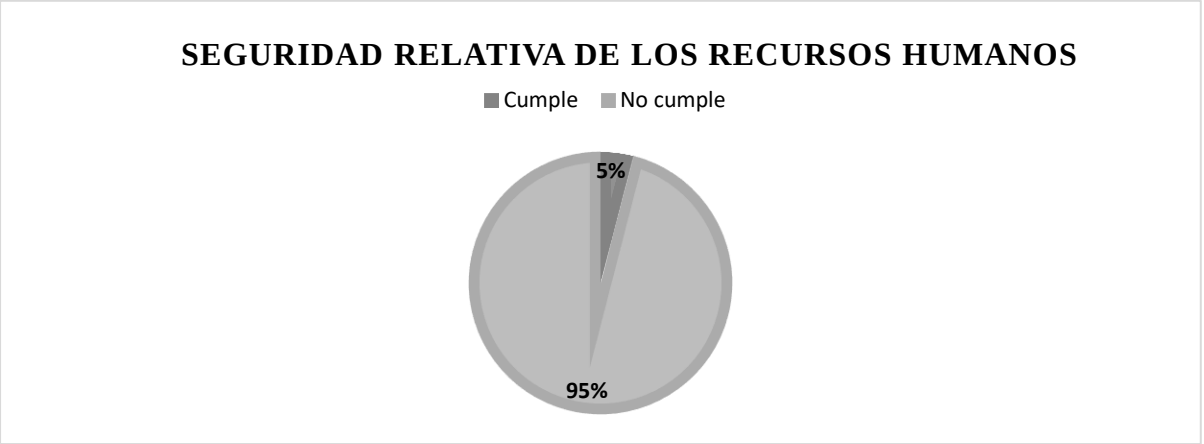


A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN				
A.6.1. ORGANIZACIÓN INTERNA				
A.6.1.1 Roles y responsabilidades para la seguridad de la información	¿Están claros los roles relacionados con la seguridad de la información en la organización?	SI	0	Hay roles, pero no para la seguridad de la información.
	¿Han sido designadas funciones y tareas específicas a los diferentes puestos dentro de la empresa en lo que respecta a la protección de la información?	SI	0	Ausencia de designación
A.6.1.2 Segregación de funciones	¿La organización asignó ciertas responsabilidades específicas a los distintos roles dentro de los activos de información?	SI	0	Aún está en revisión.
A.6.1.3 Contacto con autoridades	¿Hay un registro que detalle las autoridades a las que se debe contactar en caso de ocurrir un incidente de seguridad de la información?	SI	0	No existe ese documento

A.6.1.4 Contacto con grupos especiales de interés	¿La organización cuenta con algún vínculo con un grupo de interés para recibir asesoramiento en materia de seguridad de la información?	SI	0	Se ha consultado con expertos, pero no se ha logrado llegar a un consenso.
A.6.1.5 Seguridad de la información en la gestión de proyectos	¿Se está incorporando la seguridad de la información en el enfoque de gestión de proyectos de la empresa?	SI	0	No, ya que la compañía está en proceso de implantación
A.6.2 DISPOSITIVOS MOVILES Y TELETRABAJO				
A.6.2.1 Política de dispositivos móviles	¿Se implementan medidas de protección en los dispositivos móviles de la empresa para prevenir riesgos de seguridad?	SI	0	No, existe un control de seguridad
A.6.2.2 Teletrabajo	¿Se implementan precauciones con la información que es transmitida, recibida o guardada durante el teletrabajo?	SI	0	No existe medidas de seguridad

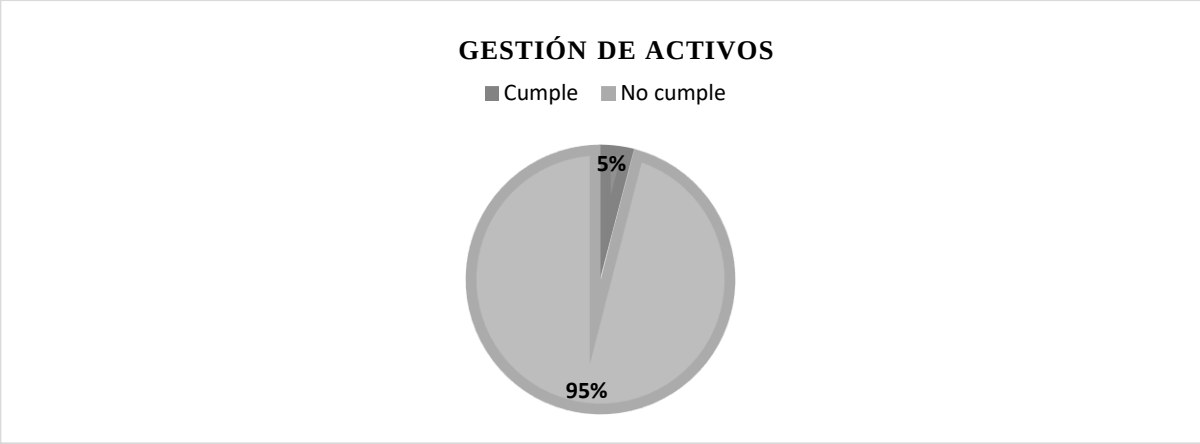
A.7. SEGURIDAD RELATIVA A LOS RECURSOS HUMANOS				
A.7.1. ANTES DEL EMPLEO				
A.7.1.1 Investigación de antecedentes	¿Los responsables de la contratación revisan los registros previos de los posibles empleados y contratistas con el fin de evitar posibles situaciones de explotación de información de la empresa (por ejemplo, referencias, documento de identidad, verificación del currículum, entre otros)?	SI	1	Si se valida esa información.

A.7.1.2 Términos y condiciones del empleo	¿En el acuerdo se establecen los compromisos tanto del colaborador como de la organización en lo que respecta a la protección de la información?	SI	0	Dado que no se ha especificado adecuadamente en las condiciones del acuerdo.
A.7.2. DURANTE EL EMPLEO				
A.7.2.1 Responsabilidades de gestión	¿El equipo directivo requiere que los empleados y colaboradores sigan las normas y procedimientos establecidos en materia de seguridad de la información?	SI	0	No hay tal registro/documento.
A.7.2.2 Conciencia, educación y capacitación sobre la seguridad de la información	¿Se ha proporcionado formación a los empleados sobre la importancia de la seguridad de la información?	SI	0	No hay programas de formación sobre la protección de la información.
	¿Se informa a los empleados sobre las actualizaciones en las políticas o procedimientos de seguridad de la información que sean pertinentes a su función laboral?	SI	0	Dado que la política de seguridad de información no ha sido formalizada.
A.7.2.3 Proceso disciplinario	¿La empresa cuenta con un procedimiento disciplinario establecido para los empleados que utilicen incorrectamente la información?	SI	0	No se encuentra sometido a un procedimiento disciplinario.
	¿Los colaboradores han sido informados sobre este proceso disciplinario?	SI	0	No se encuentra sometido a un procedimiento disciplinario
A.7.3. FINALIZACIÓN DEL EMPLEO O CAMBIO EN EL PUESTO DE TRABAJO				
A.7.3.1 Responsabilidad antes la finalización o cambio	¿Las responsabilidades y obligaciones en materia de seguridad de la información se establecen y comunican claramente y continúan en efecto incluso después de que cambia o finaliza el empleo?	SI	0	Las responsabilidades no están claramente definidas ni comunicadas.



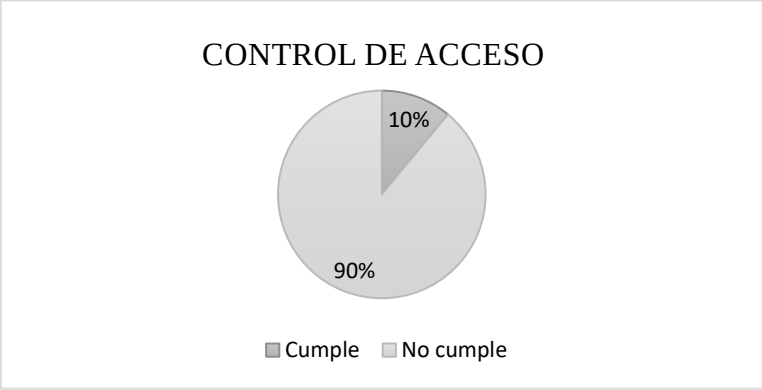
A.8. GESTIÓN DE ACTIVOS				
A.8.1 RESPONSABILIDAD SOBRE LOS ACTIVOS				
A.8.1.1 Inventario de activos	¿Se han establecido qué activos están identificados?	SI	1	Los activos fueron ingresados en el registro, pero no se cuenta con documentación formal de todos ellos.
A.8.1.2 Propiedad de los activos	¿Existe algún documento que detalle quiénes son los responsables de gestionar los activos de información en la organización?	SI	0	No se cuenta con ello.
A.8.1.3 Uso aceptable de los activos	¿Se han creado, registrado y aplicado normativas con el fin de garantizar la adecuada utilización de los recursos de información?	SI	0	
A.8.1.4 Devolución de activos	¿Disponen de alguna documentación que detalle los activos de información y recursos utilizados durante la ejecución del proyecto?	SI	0	
	¿Existe algún tipo de formulario oficial que garantice la devolución de cualquier activo físico o electrónico que pertenezca a la empresa durante el proceso de desvinculación?	SI	0	
A.8.2. CLASIFICACIÓN DE LA INFORMACIÓN				

A.8.2.1 Clasificación de la Información	¿La empresa ha categorizado su información de acuerdo a cuán crucial es su divulgación?	SI	0	No se cuenta con ello.
A.8.2.2 Etiquetado de Información	¿Siguen un conjunto de instrucciones para clasificar la información?	SI	0	
A.8.2.3 Manipulado de la información	¿Hay alguna guía para gestionar la información?	SI	0	No se cuenta con ello.
A.8.3. MANIPULACIÓN DE LOS SOPORTES				
A.8.3.1 Gestión de medios removibles	¿Existe un protocolo establecido para el manejo de dispositivos extraíbles en forma documentada?	SI	0	No se cuenta con ello.
A.8.3.2 Disposición de medios	¿Cuentan con un protocolo establecido para eliminar o destruir la información contenida en los dispositivos electrónicos de la empresa de manera formal?	SI	0	
A.8.3.3 Transferencia de medios físicos	¿Se cuentan con medidas de protección para el empleo de dispositivos físicos tanto dentro como fuera de la compañía?	SI	0	



A.9. CONTROL DE ACCESO				
A.9.1 REQUISITOS DE NEGOCIO PARA EL CONTROL DE ACCESO				
A.9.1.1 Política de control de acceso	¿Se implementan normas en la organización para gestionar el acceso de acuerdo con las prioridades de protección?	SI	1	Se cuenta únicamente con el control de acceso que se mantiene con los clientes.
A.9.1.2 Acceso a redes y servicios de red	¿Supervisan los usuarios en la organización los servicios de red?	SI	0	No se cuenta con ello.
A.9.2. GESTIÓN DE ACCESO DE USUARIO				
A.9.2.1 Registro y baja de usuarios	¿Existe algún procedimiento oficial que facilite la inscripción y eliminación de usuarios con el fin de autorizar el acceso?	SI	0	No se cuenta con ello.
A.9.2.2 Aprovisionamiento de acceso a usuario	¿Se emplea algún mecanismo que facilite la entrada y salida de los usuarios?	SI	0	
A.9.2.3 Gestión de privilegios de acceso	¿Existe algún tipo de supervisión sobre el uso de accesos privilegiados?	SI	0	
A.9.2.4 Gestión de la información secreta de autentificación de los Usuarios	¿Existen normas o directrices establecidas para la generación de contraseñas?	SI	0	
A.9.2.5 Revisión de derechos de acceso de usuarios	¿Se lleva a cabo la supervisión de los accesos de los usuarios en la empresa?	SI	0	
A.9.2.6 Retirada o reasignación de los derechos de acceso	¿Se ha celebrado algún contrato o convenio que restrinja el acceso a la información a los empleados?	SI	0	No se cuenta con ello.
A.9.3. RESPONSABILIDADES DE LOS USUARIOS				
A.9.3.1 Uso de información secreta de autentificación secreta	¿Hay algún acuerdo en la empresa que asegure que la información sea tratada de forma confidencial?	SI	1	Solo se ha establecido un compromiso de mantener la información en secreto.
A.9.4. CONTROL DE ACCESO A SISTEMA Y APLICACIÓN				
A.9.4.1 Restricción de acceso a la información	¿La organización restringe el acceso a la información relevante?	NO	0	no es pertinente
A.9.4.2 Procedimientos de ingreso seguro	¿Existe una manera segura para que los trabajadores puedan ingresar de forma segura a los sistemas de la empresa?	NO	0	

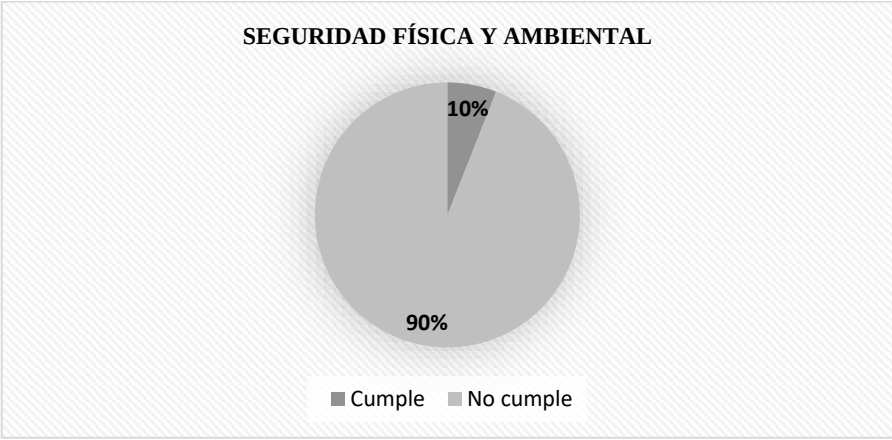
A.9.4.3 Sistema de gestión de Contraseñas	¿Tienen un sistema de gestión que les permita crear contraseñas de forma segura y fuerte?	NO	0	
9.4.4 Uso de programas utilitarios privilegiados	¿Se limita o supervisa de manera estricta el uso de herramientas que puedan desactivar o eludir los controles del sistema?	NO	0	
A.9.4.5 Control de acceso al código fuente de los programas	¿Hay algún código fuente dentro de la organización que esté restringido para su manipulación?	NO	0	



A.10. CRIPTOGRAFÍA				
A.10.1 CONTROLES CRIPTOGRÁFICOS				
A.10.1.1 Política de uso de los controles criptográficos	¿La empresa tiene una política establecida sobre el uso de medidas de seguridad criptográficas para proteger la información?	NO	0	no es pertinente
A.10.1.2 Gestión de claves	¿Hay expertos disponibles para evaluar cuál es el grado adecuado de protección necesario?	NO	0	
A.11. SEGURIDAD FISICA Y AMBIENTAL				
A.11.1. ÁREAS SEGURAS				

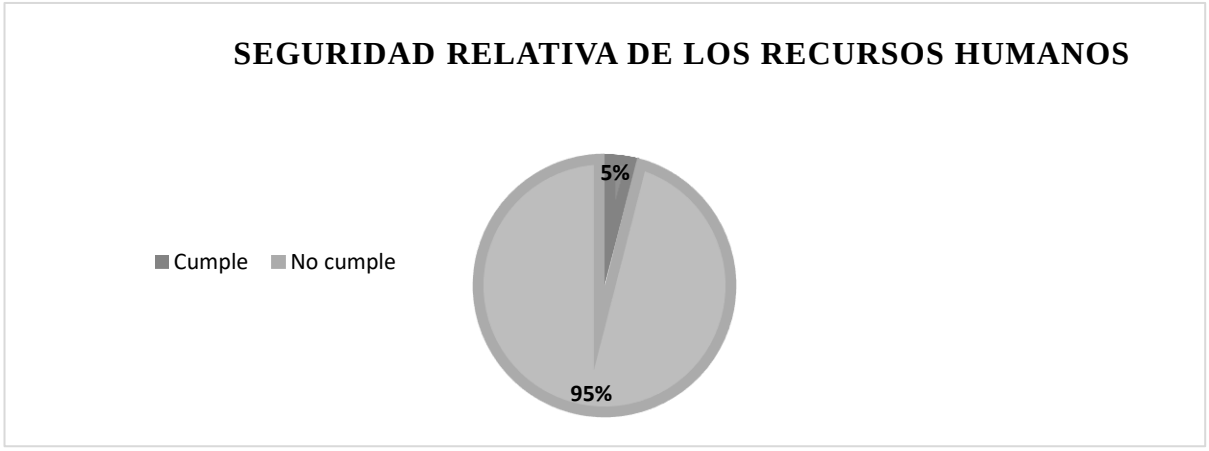
A.11.1.1 Perímetro de Seguridad Física	¿La implementación de medidas de seguridad en áreas donde se maneja información delicada garantiza el control del riesgo de pérdida o robo de datos?	NO	0	no es pertinente
A.11.1.2 Controles de Ingreso Físico	¿Se identifica el ingreso no permitido, es decir, se utiliza un método de autenticación exclusivamente para el personal autorizado?	SI	0	No se cuenta con ello.
A.11.1.3 Asegurar oficinas, áreas e instalaciones	¿Se implementan medidas para evitar filtraciones en lugares de trabajo como oficinas y despachos que impidan el acceso al público en general y así prevenir posibles pérdidas o robos de información?	SI	0	No se cuenta con ello.
A.11.1.4 Protección contra amenazas externas y ambientales	¿Se implementan medidas de política para hacer frente a las amenazas provenientes del exterior y del medio ambiente?	SI	0	No se cuenta con ello.
A.11.1.5 Trabajo en áreas Seguras	¿La zona laboral de la empresa es segura?	NO	0	no es pertinente
A.11.1.6 Áreas de despacho y carga	¿En la organización hay espacios designados para cargar y descargar mercancías?	NO	0	no es pertinente
A.11.2. SEGURIDAD DE EQUIPOS				
A.11.2.1 Emplazamiento y protección de los equipos	¿Crees que es relevante la ubicación y seguridad de los equipos?	NO	0	no es pertinente
A.11.2.2 Servicio de suministro	¿Se lleva a cabo una revisión de las instalaciones de suministros para garantizar su correcto funcionamiento en la organización?	SI	0	No se inspecciona
A.11.2.3 Seguridad del cableado	¿Están disponibles de manera segura los servicios de cableado eléctrico y de telecomunicaciones en la organización?	SI	0	Sí, pero en el caso de los equipos.

A.11.2.4 Mantenimiento de equipos	¿Llevan a cabo mantenimientos de forma regular en los equipos?	SI	1	Comenzó a enviar los equipos para su mantenimiento.
A.11.2.5 Remoción de equipos	¿Se ejecuta una logística eficiente en la protección de los equipos fuera de la empresa?	SI	0	No se llevan a cabo
A.11.2.6 Seguridad de equipos y activos fuera de las instalaciones	¿Tienen un plan de seguridad para proteger los activos que están fuera de las instalaciones?	SI	0	No se cuenta con ello.
A.11.2.7 Disposición o reutilización segura de equipos	¿Dispone de un proceso seguro para reutilizar o desechar equipos de manera adecuada?	SI	0	
A.11.2.8 Equipos de usuario desatendidos	¿Se implementan precauciones de seguridad cuando el equipo no está siendo supervisado?	SI	1	Comenzó indicando que es necesario bloquear los equipos cuando no estén siendo utilizados.
A.11.2.9 Política de escritorio limpio y pantalla limpia	¿Crees que la ubicación y la seguridad de los equipos son aspectos importantes a tener en cuenta?	SI	0	No están cumpliendo.



A.12 SEGURIDAD DE LAS OPERACIONES				
A.12.1.1 Procedimientos operativos documentados	¿Están registrados los procedimientos de operación?	SI	1	Se encuentra en desarrollo.
	¿Están disponibles para aquellos usuarios que los requieran?	SI	0	No se cuenta con ello.
A.12.1.2 Gestión del cambio	¿Existe algún instrumento para supervisar las modificaciones en los sistemas de procesamiento de datos?	SI	0	
A.12.1.3 Gestión de la capacidad	¿Monitorea el uso de recursos de la organización?	NO	0	Todo se hace de forma manual.
A.12.1.4 Separación de los entornos de desarrollo, pruebas y operaciones	¿Cuenta la organización con ambientes dedicados al desarrollo, pruebas y operación?	NO	0	No es relevante ya que no se está realizando la creación de software.
A.12.2. PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS				
A.12.2.1 Controles contra códigos maliciosos	¿Existe un programa informático para resguardarse de los peligros cibernéticos?	SI	1	Se cuentan con licencias de software antivirus, sin embargo, no se realiza la supervisión correspondiente.
A.12.3. RESPALDO				
A.12.3.1 Respaldo de la información	¿La información se respalda de manera automática o manualmente?	SI	0	La información se almacena, pero no se realiza de forma automática.
A.12.4. REGISTROS Y MONITOREO				
A.12.4.1 Registro de eventos	¿Se revisan de manera regular los registros vinculados a las actividades de los usuarios?	NO	0	No es aplicable
A.12.4.2 Protección de información de registros	¿Poseen un sistema de almacenamiento de datos de respaldo para toda la empresa?	NO	0	No se puede contar con eso.
A.12.4.3 Registros del administrador y del operador	¿Existe un sistema para detectar la presencia de invasores?	NO	0	
A.12.4.4 Sincronización de reloj	¿Existe un servidor designado para la sincronización de la hora en los sistemas de la empresa?	NO	0	
A.12.1. CONTROL DEL SOFTWARE OPERACIONAL				

A.12.5.1 Instalación de software en sistemas operacionales	¿Se requieren medidas específicas que deban llevarse a cabo para gestionar la instalación de software en sistemas operativos?	NO	0	No se dispone de eso.
A.12.6. GESTIÓN DE VULNERABILIDAD TÉCNICA				
A.12.6.1 Gestión de vulnerabilidades técnicas	¿Existe un sistema para registrar, controlar y vigilar las vulnerabilidades de los activos de información?	SI	0	No se puede contar con eso.
A.12.6.2 Restricción en la instalación de software	¿Existe un protocolo de seguimiento y supervisión del uso del software que se encuentra instalado?	SI	0	
A.12.7. CONSIDERACIONES PARA LA AUDITORÍA DE LOS SISTEMA DE INFORMACIÓN				
A.12.7.1 Controles de auditoría de sistemas de información	¿Existe un documento que contenga el historial de auditorías realizadas en los sistemas de información?	NO	0	No se dispone de eso.



A.13. SEGURIDAD DE LA COMUNICACIONES				
A.13.1. GESTION DE SEGURIDAD DE LA RED				
A.13.1.1 Controles de la red	¿La gestión y control de las redes de la organización están a cargo?	NO	0	No se cuenta con ello.

A.13.1.2 Seguridad de servicios de red	¿Los servicios de red son manejados en casa o se externalizan a terceros?	NO	0	
A.13.1.3 Segregación en redes	¿La red está dividida en secciones? ¿Cómo se ha planificado la división de la red?	NO	0	
A.13.2. TRANSFERENCIA DE INFORMACIÓN				
A.13.2.1 Políticas y procedimientos de transferencia de la información	¿Hay políticas o procesos definidos para compartir información de manera establecida?	NO	0	No se cuenta con ello.
A.13.2.2 Acuerdo sobre transferencia de información	¿La organización comparte información con entidades externas? ¿Se sigue el mismo procedimiento con todas las entidades?	SI	0	No se cuenta con ello.
A.13.2.3 Mensajes electrónicos	¿Existe un mecanismo para proteger los mensajes electrónicos que sean considerados como sospechosos?	SI	1	Se cuenta con el programa de protección Avast.
A.13.2.4 Acuerdos de confidencialidad o no divulgación	¿Se emplea algún tipo de documentación de especificaciones para los contratos de confidencialidad?	SI	1	Las políticas se refieren a las normas establecidas por el gobierno en relación con las telecomunicaciones.

A.14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN
A.14.1. REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

A.14.1.1 Análisis de requisitos y especificaciones de seguridad de la información	Garantía de seguridad en las operaciones realizadas en aplicaciones de servicios.	NO	0	No es relevante.
A.14.1.2 Asegurar los de servicios de aplicaciones en redes públicas	Seguridad en las transacciones de servicios de aplicaciones	NO	0	
A.14.1.3 Protección de transacciones en servicios de aplicaciones	Proteger las transacciones realizadas en servicios de aplicaciones.	NO	0	
A.14.2. SEGURIDAD EN EL DESARROLLO Y EN LOS PROCESOS DE SOPORTE				
A.14.2.1 Política de desarrollo seguro	¿La organización tiene políticas enfocadas en el desarrollo de sistemas de software?	NO	0	No es relevante.
A.14.2.2 Procedimientos de control de cambios del	¿Se consideran las políticas de la organización durante todo el ciclo de vida del desarrollo de software/sistemas?	NO	0	
A.14.2.3 Revisión técnica de aplicaciones tras efectuar cambios en el sistema operativo	¿Se lleva a cabo la evaluación técnica de aplicaciones que son fundamentales para el funcionamiento del negocio?	NO	0	
A.14.2.4 Restricciones sobre cambios a los paquetes de software	¿Existe alguna restricción de acceso al editar el código fuente de los programas informáticos?	NO	0	No es relevante.
A.14.2.5 Principios de ingeniería de sistemas seguros	¿Implementan métodos para el diseño de sistemas de información?	NO	0	
A.14.2.6 Entorno de desarrollo seguro	¿Se lleva a cabo la protección del entorno de desarrollo para la integración de sistemas?	NO	0	
A.14.2.7 Externalización del desarrollo de software	¿Se lleva a cabo seguimiento a los sistemas que han sido contratados externamente?	NO	0	
A.14.2.8 Pruebas funcionales de la seguridad de sistemas	¿Se llevan a cabo las pruebas de seguridad requeridas durante el proceso de desarrollo del sistema?	NO	0	
A.14.2.9 Pruebas de aceptación de los Sistemas	¿Implementan alguna estrategia de pruebas de aceptación para los sistemas?	NO	0	
A.14.3. DATOS DE PRUEBA				
A.14.3. Protección de datos de prueba	¿Se resguardan los datos de prueba?	NO	0	No es relevante.

A.15. RELACION CON LOS PROVEEDORES				
A.15.1. SEGURIDAD EN LAS RELACIONES CON PROVEEDORES				
A.15.1.1 Política de seguridad de la información en las relaciones con los proveedores	¿El proveedor implementa medidas de protección de la información para resguardar los activos de la organización?	SI	0	No se fija
A.15.1.2 Requisitos de seguridad en contratos con terceros	¿Define los criterios de protección de datos con los proveedores respecto a la tecnología de la información?	SI	0	No se fija
A.15.1.3 Cadena de suministro de tecnología de la información y de las comunicaciones	¿Se establecen condiciones en los acuerdos con los proveedores para enfrentar los posibles peligros relacionados con la seguridad de la información?	SI	0	No hay consenso en cuanto a la protección de la información.
A.15.2. GESTIÓN DE LA PROVISIÓN DE SERVICIOS DEL PROVEEDOR				
A.15.2.1 Control y revisión de la provisión de servicios del proveedor	¿Se supervisa y/o verifica la prestación de servicios por parte de los proveedores?	NO	0	No es relevante.
A.15.2.2 Gestión de cambios en la provisión del servicio del proveedor	¿Tienen algún tipo de control para supervisar la manera en que los proveedores gestionan los cambios en la provisión de bienes o servicios?	NO	0	

A.16. GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN				
A.16.1. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN Y MEJORAS				

A.16.1.1 Responsabilidades y procedimientos	¿Tienen establecidos protocolos y medidas para gestionar incidentes de seguridad de la información?	SI	0	no son tomados en consideración
A.16.1.2 Notificación de los eventos de seguridad de la información	¿Se elaboran informes sobre los sucesos relacionados con la seguridad de la información?	SI	0	no son tomados en consideración
A.16.1.3 Notificación de puntos débiles de la seguridad	¿Se generan informes sobre las vulnerabilidades en la seguridad de la información?	SI	0	No llevan a cabo
A.16.1.4 Evaluación y decisión sobre los eventos de seguridad de la información	¿Lleva a cabo análisis de sucesos relacionados con la seguridad de la información?	SI	0	No llevan a cabo
A.16.1.5 Respuesta a incidentes de seguridad de la información	¿Se toman medidas ante los incidentes de seguridad de la información en la organización?	SI	0	No llevan a cabo
A.16.1.6 Aprendizaje de los incidentes de seguridad de la información	¿Solucionas los problemas con la información que has aprendido?	SI	0	
A.16.1.7 Recolección de evidencias	¿Acostumbra a recopilar pruebas e información con regularidad?	SI	0	
A.17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTION DE CONTINUIDAD DEL NEGOCIO				
A.17.1. CONTINUIDAD DE SEGURIDAD DE LA INFORMACIÓN				
A.17.1.1 Planificación de continuidad de seguridad de la información	¿Tienen establecido un plan que define los criterios de seguridad de la información?	SI	1	Sí, se encuentra en proceso de evaluación.
A.17.1.2 Implementación de continuidad de seguridad de la información	¿La entidad posee documentación que tiene como objetivo establecer procesos, métodos y medidas de control para garantizar la continuidad de la seguridad de la información?	SI	0	No llevan a cabo
A.17.1.3 Verificación revisión y evaluación de continuidad de seguridad de la información	¿Se lleva a cabo una inspección, análisis y valoración de los mecanismos de seguridad de la información para garantizar su continuidad?	SI	0	
A.17.2. REDUNDANCIAS				
A.17.2.1 Instalación de procesamiento de la información	¿Se ha establecido algún plan para garantizar que la información esté siempre disponible?	NO	0	no son tomados en consideración
A.18. CUMPLIMIENTO				

A.18.1. CUMPLIMIENTO CON REQUISITOS LEGALES Y CONTRACTUALES				
A.18.1.1 Identificación de requisitos contractuales y de legislación aplicables	¿Se encuentran en posesión de los requisitos exigidos por los estatutos, regulaciones y contratos correspondientes?	SI	0	no son tomados en consideración
A.18.1.2 Derechos de propiedad intelectual DPI	¿Se asegura de que al llevar a cabo los procedimientos se cumplan con todas las regulaciones legales, normativas y contractuales correspondientes?	NO	0	no son tomados en consideración
	¿La entidad cuenta con protocolos para garantizar la seguridad de los derechos de propiedad intelectual?	NO	0	
	¿Se compra software de proveedores reconocidos y de confianza?	NO	0	
A.18.1.3 Protección de registros	¿Tienen un plan en donde protegen los registros de la organización contra pérdidas, falsificación y publicaciones no autorizadas?	SI	0	no son tomados en consideración
A.18.1.4 Privacidad y protección de datos personales	¿Se cuenta con un mecanismo para garantizar la seguridad y confidencialidad de los datos personales?	SI	0	No está presente, pero es crucial convenir en un pacto de confidencialidad.
A.18.1.5 Regulación de controles criptográficos	¿Se utiliza una protección encriptada de los datos en la empresa para garantizar el cumplimiento de las regulaciones, leyes y acuerdos actuales?	NO	0	El control no se aplica actualmente en la evaluación del alcance del SGSI.
A.18.2. REVISIONES DE SEGURIDAD DE LA INFORMACIÓN CUMPLIMIENTO CON REQUISITOS LEGALES Y CONTRACTUALES				
A.18.2.1 Revisión independiente de la seguridad de la información	¿Se lleva a cabo una evaluación imparcial de la seguridad de la información?	SI	0	No llevan a cabo inspecciones.
A.18.2.2 Cumplimiento de políticas y normas de seguridad	¿Se han determinado las razones por las cuales las políticas y normas de seguridad no se están cumpliendo en la organización?	SI	1	Se inició porque no están debidamente establecidas.
A.18.2.3 Revisión del cumplimiento técnico	¿Se han llevado a cabo pruebas de intrusión y análisis de vulnerabilidades?	NO	0	No se puede aplicar porque no hay un sistema de información en funcionamiento.

Nota. La tabla representa los resultados específicos para los controles de la ISO/IEC. Elaboración propia.

ANEXO E

ACTA DE COMPROMISO

ACTA DE COMPROMISO DE LA GERENCIA PARA LA IMPLEMENTACION DE LA NORMA ISO 27001-SISTEMA DE GESTION DE LA SEGURIDAD DE LA INFORMACION(SGSI)

En mi calidad de Gerente de la empresa, manifiesto nuestro compromiso y respaldo a la implementación del Sistema de Gestión de Seguridad de la Información (SGSI), en cumplimiento de la ISO27001:2013 EKONOPHARMA S.A.C

Para dicho fin nos comprometemos a:

a) Asignar los recursos necesarios para la implementación del SGSI.
b) Realizar reuniones periódicas para verificar que la política seguridad y los objetivos de la seguridad de información estén alineados con la dirección estratégica de la organización.
c) Realizar reuniones para identificar oportunidades de mejora en el SGSI
d) Verifica que los requisitos del SGSI estén integrados en los procesos pertinentes de la organización mediante reuniones.
e) Comunicar la importancia de la Gestión de la información mediante correos y reuniones.
f) Garantizar que el SGSI va a lograr alcanzar los resultados previstos mediante un seguimiento continuo.
g) Apoyar a otros roles relevantes de gestión para demostrar su liderazgo aplicado a sus áreas de responsabilidad mediante capacitaciones.
h) Motivar al personal para que contribuya con la efectividad de la implementación del SGSI.

Firman en señal de conformidad, en la ciudad de Ayacucho, a los 25 días del mes de febrero del 2024

BOTICA EKONOPHARMA
Pool Rudy Chávez Moscoso
PROPIETARIO
Gerente General

BOTICA EKONOPHARMA
Q.F. Ruben Coral Cisneros
C.Q.F.P. 14379
Coordinador de Calidad

Tema:	DESARROLLO DE LOS ANÁLISIS DE BRECHAS INICIAL		
Lugar	AV. RAMÓN CASTILLA, SAN JUAN BAUTISTA (306)		
Fecha	18/03/2024		
Hora de Inicio	07:00 p.m	**Hora de Fin**	08:00 P.M
CARGO		**FIRMA**	
GERENTE GENERAL			
COORDINADOR DE CALIDAD			
COORDINADORA DE RECURSOS HUMANOS Y LOGISTICA			
JEFE DE PROYECTO			

TEMAS TRATADOS

* Analisis de Brechas Inial de Contioles y Requisitos 1) ANALISIS DE BRECHAS DE REQUISITOS ▸ Se respondieron los cuestionarios del analisis de brechas ▸ Se identificaron bajos niveles de cumplimiento, en general se tiene 5 % de cumplimiento de Requisitos. ▸ Se requiere elevar el porcentaje del cumplimiento. ▸ El contexto de Ekonopharma y el soporte y Contexto son los mas altos pero no es Suficiente.	2) ANALISIS DE BRECHAS INICIAL DE CONTROLES ▸ Se ha respondido los cuestionarios de Analisis de Brechas. ▸ Se identificó el porcentaje bajo en complimiento de contioles de 9% ▸ Se identificaron que contioles son aplicables (necesarios) y cuales no lo son. Se requiere implementar los contioles de activos que sean prioritarios y necesarios para la Empresa EKONOPHARMA

ANEXO F

PROCESO DE SUPERVISIÓN DE LA INFORMACIÓN REGISTRADA EN DOCUMENTOS.

Tabla 43

Procedimiento documentario

N.º	Actividad	Descripción	Realiza	Registro
1	Transmitir las exigencias de elaboración o modificación de documentos.	Informa al encargado del proceso sobre la necesidad de crear o modificar un documento a través de un correo electrónico.	Integrante de la organización	Correo electrónico
2	Analizar solicitud	Evaluar la petición de crear o modificar un documento y, si es aprobada de pedir al encargado del procedimiento que designe a un experto quien será responsable de realizar las modificaciones.	Coordinadora de RRHH y Logística	Correo electrónico
3	Elaborar y modificar documentos	Si es necesario redactar un documento, el encargado de su elaboración será la persona que lo cree.	Responsable del documento	-
4	Revisar el documento	Verifica que los documentos estén adecuadamente redactados.	Coordinadora de RRHH y Logística	-
5	Aprobar el documento	Se requiere la aprobación después de verificar el contenido del documento.	Gerente	-

6	Registrar en Lista Maestra	Una vez que un documento ha sido aprobado, se incluye en la Lista Maestra de documentos físicos originales en la carpeta "Documentos Vigentes", ya sea que se trate de documentos nuevos o modificados. En caso de que los documentos modificados se vuelvan obsoletos, se trasladan a la categoría de "Lista Maestra de documentos obsoletos".	Coordinador de calidad	Inventario principal de archivos internos, Inventario principal de archivos desactualizados.
7	Difundir el documento	Existen dos formas de distribuir documentos: • A través de medios electrónicos: Se convierte el documento a formato digital y se comunica a las partes interesadas por correo electrónico, indicando su ubicación. • A través de medios físicos: Se proporcionan copias físicas controladas del documento.	Coordinador de Calidad	Lista de Distribución de documentos

Nota. La tabla representa el procedimiento documentario de Ekonopharma.

ANEXO G PROCEDIMIENTO DE GESTIÓN DE RIESGOS

Tabla 44

Documentos y registros

N.º	Actividad	Descripción	Realiza	Registro
1	Identificar lista de activos	Realizar un listado de los recursos de información utilizando la metodología de identificación y evaluación de riesgos.	Equipo de Seguridad de la información	Inventario de Activos
2	Determinar amenazas	Encontrar los riesgos potenciales relacionados con cada recurso, los cuales pueden ser similares.	Equipo de Seguridad de la información	Evaluación de Riesgos
3	Evaluar el riesgo	Llevar a cabo la evaluación de riesgos utilizando el formulario "Evaluación de Riesgos" y siguiendo las pautas establecidas en la "Metodología de Gestión de Riesgos".	Equipo de Seguridad de la información	Evaluación de Riesgos
4	Aplicar los criterios de aceptación aprobados	Determinar los parámetros para evaluar los posibles riesgos utilizando la técnica de gestión de riesgos y tomar medidas para disminuir la posibilidad y gravedad de los mismos.	Coordinador de Seguridad de información	Evaluación de Riesgos
5	Asignar propietarios de los riesgos	Identificar la persona responsable de cada riesgo y quién será encargado de implementar el control correspondiente, aunque no necesariamente sean la misma persona que el dueño del activo en cuestión.	Coordinador de Seguridad de información	Evaluación de Riesgos
6	Elaborar Plan de Tratamiento de riesgos	Elabora un plan detallado para manejar los riesgos, definiendo el tiempo requerido, asignando responsabilidades a las personas correspondientes y estableciendo las acciones a seguir frente a cada riesgo.	Equipo de Seguridad de la información	Plan de Tratamiento de riesgos
7	Realizar Informe de Gestión de riesgos	Redacta un informe que resuma los recursos más importantes, los riesgos que se presentan y las acciones de protección que se llevarán para garantizar su seguridad.	Coordinador de Seguridad de información	Informe sobre la gestión de los riesgos.
8	Ejecutar el plan de acción para abordar los riesgos identificados.	Sigue aplicando las acciones de control que se han establecido en el plan de gestión de riesgos.	Equipo de Seguridad de la información	-
9	Determinar el nivel de riesgo restante	Determinar el riesgo residual considerando la evaluación de los controles existentes.	analista de Seguridad de información	Evaluación de Riesgos
10	Realizar Informe de Plan de Tratamiento de riesgos	Redactar un reporte sobre las acciones de control implementadas y definidas en el documento del "Plan de Gestión de riesgos".	Coordinador de Seguridad de información	Plan de Tratamiento de riesgos

Nota. La tabla detalla procedimientos de gestión de riesgos en Ekonopharma.

ANEXO H PROCEDIMIENTO DE LA AUDITORÍA

Tabla 45

Auditoría proceso

N.º	Actividad	Descripción	Realiza	Registro
1	Planificar la auditoría	Se planifican mediante el "Programa de Auditoría Interna", el cual determina los procedimientos a revisar y su duración. Tanto las auditorías internas como externas deben realizarse de forma anual y contar con la aprobación del Gerente General.	Coordinador de Seguridad de la Información	Programa de Auditoría Interna
2	Seleccionar Auditor	Elige, estructura y nombra al equipo que llevará a cabo la auditoría, formado por personas capacitadas, ya sea internas o externas, que cumplan con los requisitos necesarios para realizar auditorías y que no estén involucradas directamente en la actividad a examinar.	Coordinador de Seguridad de la Información	Programa de Auditoría Interna
3	Preparar auditoría	Antes de realizar la auditoría, se comunica a los encargados de los procesos los pormenores de cómo se llevará a cabo a través del "Plan de Auditoría Interna", con al menos cinco días hábiles de anticipación.	Auditor	Plan para realizar una auditoría interna.
4	Ejecutar auditoría	La auditoría se inicia con una reunión inicial en la que se explica a los auditados el objetivo y las actividades que se llevarán a cabo. Luego, los auditores recopilan pruebas a través de entrevistas, observaciones y revisión de registros para comprobar la implementación y eficacia del sistema. Al finalizar, se lleva a cabo una reunión de cierre donde se explican los resultados de la auditoría, se resumen las no conformidades y hallazgos encontrados, y se presentan las conclusiones del proceso de auditoría.	Auditor	
5	Elaborar informe	El equipo de auditoría interna trabaja en conjunto con el líder de auditoría para crear el "Informe de Auditoría Interna".	Auditor	Informe de revisión interna de cuentas
6	Comunicar informe	El informe se entrega durante una junta con los directivos de alto rango y luego se debe transmitir la información.	Coordinador de Seguridad de la Información	Acta de Reunión
7	Generar no conformidades, y oportunidades de mejora	Durante la auditoría interna, se categorizan las no conformidades encontradas de acuerdo a su tipo y se documentan de manera minuciosa en un documento llamado "Seguimiento de No Conformidades y Acciones Correctivas". Aparte, cualquier sugerencia de mejora o hallazgo debe ser registrado como acciones preventivas para reducir riesgos.	Analista de Seguridad de la información	El seguimiento de situaciones de incumplimiento y las medidas correctivas.

Nota. La tabla proceso de auditoría en Ekonopharma.

ANEXO I MEDIDAS DE SEGURIDAD EN LA GESTIÓN DE LA INFORMACIÓN

Tabla 46

Controles de seguridad de información

CONTROLES DE SEGURIDAD DE EKONOPHARMA SAC				
TIPO DE ACTIVO	**ACTIVOS**	**ID RIESGO**	**AMENAZAS**	**CONTROLES SEGÚN ISO 27001**
Datos	Base de Datos del personal	R1	Alteración intensional de datos	A.7.2.3 Proceso disciplinario A.9.1.1 Política de control de acceso A.7.1.2Términos y condiciones de empleo A.7.2.1 Gestión de responsabilidades
		R2	Acceso no autorizado	A.9.1.1 Política de control de acceso A.9.4.1 Restricción al acceso a la información A.11.1.2 Controles físicos de ingreso
		R3	Fuga de información	A.5.1.1 Políticas para seguridad de la información A.5.1.2 Revisión de políticas para seguridad de la información A.6.2.1 Política sobre dispositivos A.8.3.1 Gestión de medios removibles móviles A.18.1.3 Protección de registros A.18.1.4 Privacidad y protección de información personalmente identificable A.13.2.4 Acuerdos de confidencialidad o no divulgación A.7.2.1 Gestión de responsabilidades A.7.2.2 Toma de concienciación, educación y capacitación en seguridad de la información
Datos	Base de Datos de los medicamentos y productos sanitarios	R4	Eliminación de datos	A.9.1.1 Política de control de acceso A.9.2.6 Eliminación o ajuste de derechos de acceso A.7.2.3Proceso disciplinario
		R2	Acceso no autorizado	A.9.4.1 Restricción al acceso a la información A.9.1.1 Política de control de acceso A.11.1.2 Controles físicos de ingreso
		R3	Fuga de información	A.8.3.1 Gestión de medios removibles A.5.1.1 Políticas para seguridad de la información A.5.1.2Revisión de políticas para seguridad de la información la información A.13.2.4 Acuerdos de confidencialidad o no divulgación A.7.2.1 Gestión de responsabilidades A.7.2.2 Toma de concienciación, educación y capacitación en seguridad d la información
		R6	Registros incompletos	A.18.2.3 Revisión de cumplimiento técnico A.6.1.2 Separación de deberes A.7.2.1Gestión de responsabilidades A.7.2.1 Gestión de responsabilidades
		R7	Alteración accidental de datos	A.9.1.1 Política de control de acceso A.9.2.6 Eliminación o ajuste de derechos de acceso A.8.2.1 Clasificación de la información A.7.2.1 Gestión de responsabilidades
		R8	Introducción de datos erróneos	A.9.1.1 Política de control de acceso A.9.4.5 Control de acceso al código fuente del programa A.7.2.1 Gestión de responsabilidades
Datos	Datos de los clientes concurrentes	R9	Alteración de datos	A.9.1.1 Política de control de acceso A.8.2.1 Clasificación de la información A.7.2.1 Gestión de responsabilidades A.7.2.3Proceso disciplinario
		R2	Acceso no autorizado	A.9.4.1 Restricción al acceso a la información A.11.1.2 Controles físicos de ingreso
		R5	Eliminación accidental de datos	A.9.1.1 Política de control de acceso A.9.2.6 Eliminación o ajuste de derechos de acceso A.7.2.1 Gestión de responsabilidades

Datos	Base de datos de fórmulas magistrales	R4	Eliminación de datos	A.9.1.1 Política de control de acceso A.9.2.6 Eliminación o ajuste de derechos de acceso A.7.2.3Proceso disciplinario
		R2	Acceso no autorizado	A.9.4.1 Restricción al acceso a la información A.9.1.1 Política de control de acceso A.11.1.2 Controles físicos de ingreso
		R3	Fuga de información	A.5.1.1 Políticas para seguridad de la información A.8.3.1 Gestión de medios removibles A.13.2.4 Acuerdos de confidencialidad o no divulgación A.7.2.1 Gestión de responsabilidades A.7.2.2 Toma de concienciación, educación y capacitación en seguridad de la información
		R6	Registros incompletos	A.8.2.2 Etiquetado de la información A.8.2.1 Clasificación de la información A.18.2.3 Revisión de cumplimiento técnico A.6.1.2 Separación de deberes A.7.2.1Gestión de responsabilidades A.7.2.1 Gestión de responsabilidades
		R1	Alteración intensional de datos	A.7.2.3 Proceso disciplinario A.9.1.1 Política de control de acceso A.7.2.3Proceso disciplinario
		R7	Alteración accidental de datos	A.9.1.1 Política de control de acceso A.9.4.5 Control de acceso al código fuente del programa A.7.2.1 Gestión de responsabilidades
Datos	Datos de Inventariado de PF, DM Y PS	R5	Eliminación accidental de datos	A.9.1.1 Política de control de acceso A.9.2.6 Eliminación o ajuste de derechos de acceso
		R2	Acceso no autorizado	A.9.4.1 Restricción al acceso a la información A.9.1.1 Política de control de acceso
		R3	Fuga de información	A.5.1.1 Políticas para seguridad de la información A.8.3.1 Gestión de medios removibles A.5.1.2 Revisión de políticas para seguridad de la información A.13.2.4 Acuerdos de confidencialidad o no divulgación A.7.2.1 Gestión de responsabilidades A.7.2.2 Toma de concienciación, educación y capacitación en seguridad de la información
		R6	Registros incompletos	A.8.1.2 Propiedad de los activos A.6.1.2 Separación de deberes A.8.1.1 Inventario de activos A.18.2.3Revisión de cumplimiento técnico A.7.2.1Gestión de responsabilidades
		R1	Alteración intensional de datos	A.7.2.3Proceso disciplinario A.9.1.1 Política de control de acceso
		R7	Alteración accidental de datos	A.9.1.1 Política de control de acceso A.7.2.1 Gestión de responsabilidades
		R8	Introducción de datos erróneos	A.18.2.3 Revisión de cumplimiento técnico A.7.2.1 Gestión de responsabilidades
datos	Control de salarios	R4	Eliminación de datos	A.9.1.1 Política de control de acceso A.9.2.6 Eliminación o ajuste de derechos de acceso
		R2	Acceso no autorizado	A.9.4.1 Restricción al acceso a la información A.9.1.1 Política de control de acceso

		R3	Fuga de información	A.5.1.1 Políticas para seguridad de la información A.5.1.2 Revisión de políticas para seguridad de la información la información A.6.2.1 Política sobre dispositivos móviles A.8.3.1 Gestión de medios removibles A.13.2.4 Acuerdos de confidencialidad o no divulgación A.7.2.1 Gestión de responsabilidades A.7.2.2 Toma de concienciación, educación y capacitación en seguridad de la información
		R6	Registros incompletos	A.18.2.3 Revisión de cumplimiento técnico A.18.1.3 Protección de registros A.6.1.2 Separación de deberes A.7.2.1Gestión de responsabilidades
		R8	Introducción de datos erróneos	A.18.2.3 Revisión de cumplimiento técnico A.18.1.3 Protección de registros A.7.2.1 Gestión de responsabilidades
datos	Lista de medicamentos vencidos y deteriorados	R10	Error en el desarrollo de las listas	A.18.2.3 Revisión de cumplimiento técnico A.7.2.1 Gestión de responsabilidades
		R4	Eliminación de datos	A.9.1.1 Política de control de acceso A.9.2.6 Eliminación o ajuste de derechos de acceso
		R7	Alteración accidental de datos	A.9.1.1 Política de control de acceso A.7.2.1 Gestión de responsabilidades
		R3	Fuga de información	A.5.1.1 Políticas para seguridad de la información A.5.1.2 Revisión de políticas para seguridad de la información A.6.2.1 Política sobre dispositivos móviles A.8.3.1 Gestión de medios removibles A.13.2.4 Acuerdos de confidencialidad o no divulgación A.7.2.1 Gestión de responsabilidades A.7.2.2 Toma de concienciación, educación y capacitación en seguridad de la información
Datos	control de políticas	R9	Alteración de datos	A.9.1.1 Política de control de acceso A.9.2.6 Eliminación o ajuste de derechos de acceso
		R11	Equivocación al momento de crear documentos	A.18.2.3 Revisión de cumplimiento técnico A.7.2.1 Gestión de responsabilidades
		R3	Fuga de información	A.6.2.1 Política sobre dispositivos móviles A.5.1.1 Políticas para seguridad de la información A.5.1.2 Revisión de políticas para seguridad de la información A.8.3.1 Gestión de medios removibles A.13.2.4 Acuerdos de confidencialidad o no divulgación A.7.2.1 Gestión de responsabilidades A.7.2.2 Toma de concienciación, educación y capacitación en seguridad de la información
		R12	Manipulación de los datos de los documentos	A.9.1.1 Política de control de acceso A.9.2.6 Eliminación o ajuste de derechos de acceso A.15.1.2 Tratamiento de la seguridad en contratos con proveedores A.15.1.3 Cadena de suministro de tecnología de información y comunicación A.16.1.1 Responsabilidades y procedimientos A.16.1.2Reporte de eventos en la seguridad de la información A.16.1.3 Reporte de debilidades en la seguridad de la información
		R7	Alteración accidental de datos	A.9.1.1 Política de control de acceso A.9.2.6 Eliminación o ajuste de derechos de acceso A.7.2.1 Gestión de responsabilidades
		R4	Eliminación de datos	A.9.1.1 Política de control de acceso A.9.2.6 Eliminación o ajuste de derechos de acceso
	control de procedimiento	R9	Alteración de datos	A.9.1.1 Política de control de acceso A.9.2.6 Eliminación o ajuste de derechos de acceso

		R11	Equivocación al momento de crear documentos	A.18.2.3 Revisión de cumplimiento técnico A.6.1.2 Separación de deberes A.7.2.1Gestión de responsabilidades
		R3	Fuga de información	A.6.2.1 Política sobre dispositivos móviles A.5.1.1 Políticas para seguridad de la información A.8.3.1 Gestión de medios removibles A.13.2.4 Acuerdos de confidencialidad o no divulgación A.7.2.1 Gestión de responsabilidades A.7.2.2 Toma de concienciación, educación y capacitación en seguridad de la información
		R12	Manipulación de los datos de los documentos	A.9.1.1 Política de control de acceso A.9.2.6 Eliminación o ajuste de derechos de acceso A.15.1.2 Tratamiento de la seguridad en contratos con proveedores A.15.1.3 Cadena de suministro de tecnología de información y comunicación A.16.1.1 Responsabilidades y procedimientos A.16.1.2 Reporte de eventos en la seguridad de la información A.16.1.3 Reporte de debilidades en la seguridad de la información A.7.2.3 Proceso disciplinario
		R7	Alteración accidental de datos	A.9.1.1 Política de control de acceso A.9.2.6 Eliminación o ajuste de derechos de acceso
		R4	Eliminación de datos	A.9.1.1 Política de control de acceso A.9.2.6 Eliminación o ajuste de derechos de acceso A.7.2.3 Proceso disciplinario
Servicios	Correo electrónico	R13	Negación de haber recibió un mensaje	A.7.2.2Toma de concienciación, educación y capacitación en seguridad de la información A.9.1.1 Política de control de acceso A.7.1.2 Términos y condiciones de empleo A.7.2.3 Proceso disciplinario
		R14	Uso incorrecto	A.9.1.1 Política de control de acceso A.7.1.2 Términos y condiciones de empleo A.13.2.3Mensajes A.7.2.3 Proceso disciplinario
		R15	Expansión de virus	A.7.2.2Toma de concienciación, educación y capacitación en seguridad de la información A.12.2.1 Controles contra software malicioso
	Pago a servicios de terceros	R4	Eliminación de datos	A.9.1.1 Política de control de acceso A.9.2.6 Eliminación o ajuste de derechos de acceso A.7.2.3Proceso disciplinario A.7.2.3 Proceso disciplinario
		R3	Fugas de información	A.6.2.1 Política sobre dispositivos móviles A.5.1.1 Políticas para seguridad de la información A.5.1.2 Revisión de políticas para seguridad de la información A.8.3.1 Gestión de medios removibles A.13.2.4 Acuerdos de confidencialidad o no divulgación A.7.2.1 Gestión de responsabilidades A.7.2.2 Toma de concienciación, educación y capacitación en seguridad de la información A.7.2.3 Proceso disciplinario
		R12	Manipulación de los datos de los documentos	A.9.1.1 Política de control de acceso A.9.2.6 Eliminación o ajuste de derechos de acceso A.7.2.1 Gestión de responsabilidades A.7.2.3 Proceso disciplinario
		R9	Alteración de datos	A.7.2.3 Proceso disciplinario A.9.1.1 Política de control de acceso A.9.2.6 Eliminación o ajuste de derechos de acceso
	Internet	R11	Caída de los servicios de internet	A.12.1.1 Procedimientos documentados de operación

		R2	Acceso no autorizado	A.9.1.2 Acceso a redes y a servicios de red A.9.4.1 Restricción al acceso a la información
		R16	Abuso de beneficios de acceso	A.9.2.5 Revisión de los derechos de acceso del usuario A.7.2.1 Gestión de responsabilidades
	Boletas de ventas y compras emitidas	R3	Fugas de información	A.6.2.1 Política sobre dispositivos móviles A.5.1.1 Políticas para seguridad de la información A.5.1.2 Revisión de políticas para seguridad de la información A.8.3.1 Gestión de medios removibles A.13.2.4 Acuerdos de confidencialidad o no divulgación A.7.2.2 Toma de concienciación, educación y capacitación en seguridad de la información
		R12	Manipulación de los datos de los documentos	A.9.1.1 Política de control de acceso A.9.2.6 Eliminación o ajuste de derechos de acceso A.7.2.1 Gestión de responsabilidades
		R4	Eliminación de datos	A.9.1.1 Política de control de acceso A.9.2.6 Eliminación o ajuste de derechos de acceso A.7.2.3 Proceso disciplinario
Hardware	Monitores	R17	posibilidad de que el fuego acabe	A.11.1.4 Protección contra amenazas externas y ambientales A.11.2.1 Emplazamiento y protección de los equipos A.12.3.1 Copia de seguridad de la información
		R18	Desgaste debido a su uso	A.11.2.4 Mantenimiento de equipo A.8.1.3 Uso aceptable de los activos
		R19	Avería del hardware	A.15.1.2 Tratamiento de la seguridad en contratos con proveedores A.12.3.1 Copia de seguridad de la información
		R20	Corte de suministro eléctrico	A.11.2.1 Ubicación y protección del equipo A.11.2.9 Política de pantalla y escritorio limpio A.11.2.2 Servicios de suministro
Hardware	Computadoras	R17	posibilidad de que el fuego dañe	A.11.1.4 Protección contra amenazas externas y ambientales A.11.2.1 Emplazamiento y protección de los equipos A.12.3.1 Copia de seguridad de la información
		R18	Desgaste debido a su uso	A.11.2.4 Mantenimiento de equipo A.11.2.8 Equipo de usuario. 8.1.3 Uso aceptable de los activos desatendido
		R19	Avería del hardware	A.15.1.2 Tratamiento de la seguridad en contratos con proveedores
		R21	Uso ilícito	A.9.1.1 Política de control de acceso A.7.1.2 Términos y condiciones de empleo A.7.2.1 Gestión de responsabilidades A.7.2.3 Proceso disciplinario
		R22	Desconexión del equipo	A.11.2.4 Mantenimiento de equipo A.11.2.2 Servicios de suministro
		R23	Errores en el mantenimiento actualización del equipo	A.11.2.4 Mantenimiento de equipo
		R24	Contaminación mecánica polvo	A.12.3.1 Copia de seguridad de la información A.11.2.1 Emplazamiento y protección de los equipos
		R20	Corte de suministro eléctrico	A.11.2.1 Ubicación y protección del equipo A.11.2.9 Política de pantalla y escritorio limpio A.11.2.2 Servicios de suministro
Equipamiento auxiliar	Impresoras	R18	Desgaste debido a su uso	A.11.2.4 Mantenimiento de equipo A.8.1.3 Uso aceptable de los activos
		R19	Avería del hardware	A.11.2.4 Mantenimiento de equipo

		R22	Desconexión del equipo	A.11.2.2 Servicios de suministro
		R23	Errores en el mantenimiento actualización del equipo	A.12.3.1 Copia de seguridad de la información A.11.2.4 Mantenimiento de equipo
		R20	Corte de suministro eléctrico	A.11.2.4 Mantenimiento de equipo A.11.2.2 Servicios de suministro
		R17	Posibilidad de ocurrir un incendio y dañar	A.11.1.4 Protección contra amenazas externas y ambientales A.11.2.1 Emplazamiento y protección de los equipos
	Equipamiento de cámaras	R17	Posibilidad de ocurrir un incendio y dañar	A.11.1.4 Protección contra amenazas externas y ambientales A.11.2.1 Emplazamiento y protección de los equipos A.12.3.1 Copia de seguridad de la información
		R24	Contaminación mecánica polvo	A.11.2.1 Emplazamiento y protección de los equipos A.12.3.1 Copia de seguridad de la información
		R23	Errores en el mantenimiento actualización del equipo	A.12.3.1 Copia de seguridad de la información A.11.2.4 Mantenimiento de equipo
		R22	Desconexión del equipo	A.11.2.4 Mantenimiento de equipo A.11.2.2 Servicios de suministro
	Discos externos	R23	Errores en el mantenimiento actualización del equipo	A.11.2.4 Mantenimiento de equipo
		R24	Contaminación mecánica polvo	A.11.2.1 Emplazamiento y protección de los equipos A.12.3.1 Copia de seguridad de la información
		R25	Robo de Disco	A.9.1.1 Política de control de acceso A.9.2.6 Eliminación o ajuste de derechos de acceso A.12.3.1 Copia de seguridad de la información A.7.2.3 Proceso disciplinario
		R26	Destrucción deliberada del disco	A.9.1.1 Política de control de acceso
		R27	Degradación por consecuencia del tiempo	A.11.2.4 Mantenimiento de equipo
Redes de Comunicación	Sistema de red	R28	Posibilidad de equivocaciones en la instalación	A.13.1.2 Seguridad de los servicios de red A.11.2.3 Seguridad en el cableado A.11.2.1 Emplazamiento y protección de los equipos
		R22	Desconexión del equipo	A.11.2.2 Servicios de suministro
		R17	Posibilidad de ocurrir un incendio y dañar	A.11.1.4 Protección contra amenazas externas y ambientales A.11.2.1 Emplazamiento y protección de los equipos
		R29	Posibilidad de que las fugas de agua inunden y dañen	A.11.1.4 Protección contra amenazas externas y ambientales A.11.2.1 Emplazamiento y protección de los equipos
	Red inalámbrica	R31	Interceptación de red	A.13.1.2 Seguridad de los servicios de red
		R32	Monitorización del tráfico	A.13.1.2 Seguridad de los servicios de red
		R2	Acceso no autorizado	A.9.2.5 Revisión de los derechos de acceso del usuario
Software		R2	Acceso no autorizado	A.9.2.5 Revisión de los derechos de acceso del usuario

	Sistema de Ventas Ekonopharma	R3	Fuga de información	A.6.2.1 Política sobre dispositivos móviles A.5.1.1 Políticas para seguridad de la información A.5.1.2 Revisión de políticas para seguridad de la información A.8.3.1 Gestión de medios removibles A.13.2.4 Acuerdos de confidencialidad o no divulgación A.7.2.1 Gestión de responsabilidades A.7.2.2 Toma de concienciación, educación y capacitación en seguridad de la información A.7.2.3 Proceso disciplinario
		R8	Introducción de datos erróneos	A.18.2.3 Revisión de cumplimiento técnico A.18.1.3 Protección de registros
Instalación	Oficinas Botica Ekonopharma	R2	Acceso no autorizado	A.9.4.1 Restricción al acceso a la información A.9.1.1 Política de control de acceso A.11.1.2 Controles físicos de ingreso A.11.1.3 Seguridad de oficinas, habitaciones e instalaciones
		R30	Posibilidad de ocurrir sismo o terremoto	A.11.1.1 Perímetro de seguridad física A.11.2.1 Emplazamiento y protección de los equipos
		R29	Posibilidad de que las fugas de agua inunden y dañen	A.11.1.4 Protección contra amenazas externas y ambientales A.11.2.1 Emplazamiento y protección de los equipos
		R17	Posibilidad de ocurrir un incendio y dañar	A.11.1.4 Protección contra amenazas externas y ambientales
Personal	Trabajadores	R33	Indisponibilidad por ausencia o despido inmediato	A.8.1.4 Devolución de activos A.7.1.2 Términos y condiciones de empleo A.7.3.1 Terminación o cambio de condiciones del empleo A.7.2.1 Gestión de responsabilidades
		R34	Extorsión por obligar a obrar en mal sentido	A.6.1.1Roles y responsabilidades sobre seguridad de la información. A.6.1.2 Separación de deberes A.7.3.1Terminación o cambio de condiciones del empleo
		R35	Ingeniería social aprovechamiento de buena fe	A.7.1.2 Términos y condiciones de empleo

Nota. La tabla representa los controles de seguridad de información para Ekonopharma. Elaboración propia.

ANEXO J PLAN DE TRATAMIENTO DE RIESGOS DE EKONOPHARMA S.A.C

Tabla 47

PLAN DE TRATAMIENTO DE RIESGOS EKONOPHARMA S.A.C

ID del riesgo	Descripción del riesgo	Activos	Niveles del riesgo	Tratamiento del Riesgo	Propietario del Riesgo	Personal / Recursos	Registro Asociado
R1	Alteración intensional de datos	Base de Datos del personal	medio	Formación tanto interna como externa del personal, incluyendo estímulos. Concientización a través de charlas y recursos de seguridad, advertencias, supervisión del personal, fomento del sentido de identidad y compromiso con la institución.	1.-Analista de de la Seguridad de la información. /Coordinadora de RRHH y Logística 2.- Coordinador de Calidad/ Coordinador de Seguridad de la información	Tiempo, área de conferencias	Formato de registro y Cronograma de Capacitaciones y actividades o incentivos
		Base de datos de fórmulas magistrales	medio				
		Datos de Inventariado de PF, DM Y PS	medio				
R2	Acceso no autorizado	Base de Datos de los medicamentos y productos sanitarios	alto	1.-Informar a todo el personal sus funciones y roles dentro de la empresa Ekonopharma. 2.-Estblecer un plan de sanciones por violar un acceso no autorizado. 3.- Contar dispositivos que controles los accesos de personas que no pertenecen a la empresa. 4.-establecer funciones y prohibiciones de acceso a documentos o áreas no autorizados a los trabajadores de la empresa.	1.-Coordinador de Calidad/ Coordinador de Seguridad de la información	1. Información detallada sobre las responsabilidades, funciones, sanciones y consecuencias de no respetar las políticas de seguridad de la información en Ekonopharma.	11.- Directrices sobre roles y responsabilidades 2.- Normativas de Seguridad de datos.
		Datos de los clientes concurrentes	bajo				
		Base de datos de fórmulas magistrales	muy alto				
		Datos de Inventariado de PF, DM Y PS	alto				
		Sistema de ventas Ekonopharma	alto				
		Base de Datos del personal	medio				
		Control de salarios	medio				
		Internet	medio				
		Red inalámbrica	alto				
		Oficinas Botica Ekonopharma	muy alto				
R3	Fuga de información	Boletas de ventas y compras emitidas	medio	Normas y protocolos para mantener la confidencialidad en la información contenida en documentos y contratos laborales, capacitación tanto interna como	1.-Coordinador de Calidad/ Coordinador de Seguridad de la información	N. A	Procedimiento confidencialidad y política de datos personales
		control de políticas	alto				
		Datos de Inventariado de PF, DM Y PS	medio				

		Plan estratégico	medio	externa para los empleados, monitoreo del tráfico en la red y restricción de puertos de comunicación innecesarios, con implementación de contraseñas necesarias.	2.-Analista de la Seguridad de la información. /Coordinador de RRHH y Logística		
		Base de Datos del personal	alto				
		control de procedimiento	medio				
		Lista de medicamentos vencidos y deteriorados	muy alto				
		Control de salarios	medio				
		Sistema de ventas Ekonopharma	medio				
		Base de datos de fórmulas magistrales	muy alto				
		Base de Datos de los medicamentos y productos sanitarios	medio				
		Pago a servicios de terceros	alto				
R4	Eliminación de datos	Boletas de ventas y compras emitidas	medio	Supervisar las modificaciones en los sistemas y la documentación, gestionar los accesos de usuarios y restringir el acceso a las bases de datos.	1.-Coordinador de Calidad/ Coordinador de Seguridad de la información	N. A	Directrices de protección de datos.
		Pago a servicios de terceros	alto				
		Plan estratégico	medio				
		control de políticas	alto				
		control de procedimiento	medio				
		Lista de medicamentos vencidos y deteriorados	muy alto				
		Control de salarios	alto				
		Base de datos de fórmulas magistrales	muy alto				
		Base de Datos de los medicamentos y productos sanitarios	muy alto				
R5	Eliminación accidental de datos	Datos de Inventariado de PF, DM Y PS	muy alto	Formación tanto interna como externa del personal, incluyendo estímulos. Concientización a través de charlas y recursos de seguridad, advertencias, supervisión del personal, fomento del sentido de identidad y compromiso con la institución.	1.-Analista de la Seguridad de la información. Coordinadora de RRHH y Logística	Tiempo, área de conferencias	Formato de registro y Cronograma de Capacitaciones y actividades o incentivos
		Datos de los clientes concurrentes	alto				
R6	Registros incompletos	Datos de Inventariado de PF, DM Y PS	muy alto	Capacitar al personal en sus actividades y esclarecer sus funciones y tareas dentro de la empresa.	1.-Analista de la Seguridad de la información. Coordinadora de RRHH y Logística	Tiempo para capacitaciones de sus funciones y tareas	Políticas de responsabilidades y funciones
		Base de datos de fórmulas magistrales	muy alto				
		Base de Datos de los medicamentos y productos sanitarios	muy alto				
		Control de salarios	alto				

R7	Alteración accidental de datos	control de procedimiento	medio	Formación tanto interna como externa del personal, incluyendo estímulos. Concientización a través de charlas y recursos de seguridad, advertencias, supervisión del personal, fomento del sentido de identidad y compromiso con la institución.	1.-Analista de la Seguridad de la información. Coordinadora de RRHH y Logística	Tiempo, área de conferencias	Formato de registro y Cronograma de Capacitaciones y actividades o incentivos
		Lista de medicamentos vencidos y deteriorados	muy alto				
		Base de Datos de los medicamentos y productos sanitarios	medio				
		Datos de Inventariado de PF, DM Y PS	medio				
		Base de datos de fórmulas magistrales	medio				
R8	Introducción de datos errores	Sistema de ventas Ekonopharma	alto	Formación tanto interna como externa del personal, incluyendo estímulos. Concientización a través de charlas y recursos de seguridad, advertencias, supervisión del personal, fomento del sentido de identidad y compromiso con la institución.	1.-Analista de de la Seguridad de la información. /Coordinadora de RRHH y Logística	Tiempo, área de conferencias	Formato de registro y Cronograma de Capacitaciones y actividades o incentivos
		Base de Datos de los medicamentos y productos sanitarios	alto				
		Control de salarios	alto				
R9	Alteración de datos	Datos de los clientes concurrentes	bajo	Supervisar las modificaciones en los sistemas, gestionar los accesos de los usuarios, mantener el firewall actualizado y promover la participación del personal en la institución.	1.-Coordinador de Calidad/ Coordinador de Seguridad de la información	N.A Licenciamiento de antivirus	Procedimiento para determinar roles y privilegios de usuarios
		Pago a servicios de terceros	alto				
		control de procedimiento	medio alto				
R10	Error en el desarrollo de las listas	Lista de medicamentos vencidos y deteriorados	muy alto	Formación tanto interna como externa del personal, incluyendo estímulos. Concientización a través de charlas y recursos de seguridad, advertencias, supervisión del personal, fomento del sentido de identidad y compromiso con la institución.	1.-Analista de de la Seguridad de la información. /Coordinadora de RRHH y Logística	Tiempo, área de conferencias	Formato de registro y Cronograma de Capacitaciones y actividades o incentivos
R11		control de procedimiento	medio	Formación tanto interna como externa del personal,		Tiempo, área de conferencias	Formato de registro y Cronograma de

	Equivocación al momento de crear documentos	control de políticas	alto	incluyendo estímulos. Concientización a través de charlas y recursos de seguridad, advertencias, supervisión del personal, fomento del sentido de identidad y compromiso con la institución.			Capacitaciones y actividades o incentivos
R12	Manipulación de los datos de los documentos	control de procedimiento	bajo	Supervisar las modificaciones en los sistemas y la documentación, gestionar los accesos de usuarios y restringir el acceso a las bases de datos.	1.-Coordinador de Calidad/ Coordinador de Seguridad de la información	N. A	Normas de seguridad de la información.
		Pago a servicios de terceros	medio				
		Boletas de ventas y compras emitidas	medio				
		control de políticas	alto				
R13	Negación de haber recibió un mensaje	Correo electrónico	alto	Guía de responsabilidades y procedimientos establecidos, Normas de protección de datos.	1.-Coordinador de Calidad/ Coordinador de Seguridad de la información	N. A	Normas de seguridad de la información.
R14	Uso incorrecto	Correo electrónico	alto				
R15	Expansión de virus	Correo electrónico	alto				
R16	Abuso de beneficios de acceso	Internet	alto				
R17	posibilidad de que el fuego dañe	Sistema de red	muy alto	Realizar inspecciones regulares para identificar y corregir posibles riesgos de incendio, No fumar en áreas donde haya material inflamable, No fumar en áreas donde haya material inflamable Tener un plan de evacuación en caso de incendio	1.-Alta dirección/ Gerente General	aparatos de medidas contra incendios	Plan contra incendios
		Equipamiento de cámaras	muy alto				
		Monitores	muy alto				
		Computadoras	muy alto				
		Impresoras	muy alto				
		Oficinas Botica Ekonopharma	muy alto				
R18	Avería del hardware	Monitores	alto	Actualizar regularmente el Antivirus, abstenerse de instalar programas sin permiso del	1.-Coordinador de Calidad/ Coordinador	Adquirir Licenciamiento de antivirus	Plan de instalación y difusión
		Computadoras	alto				

		Impresoras	alto	administrador. Cumplir con las políticas de seguridad actualizadas. Implementar un servidor para usuarios y controlar el acceso por usuario. Asegurar la configuración correcta del firewall de seguridad.	de Seguridad de la información		de Software
R19	Posibilidad de ocurrir un incendio y dañar	Computadoras	muy alto	Tener a disposición una compañía externa que se encargue de proteger contra incendios y brindar asesoramiento al personal para actuar adecuadamente en caso de una emergencia. Compañías aseguradoras que ofrecen cobertura contra diferentes tipos de desastres, tanto naturales como provocados por el hombre (como incendios, inundaciones, cortocircuitos, etc.). Contar con una aseguradora que proteja al negocio de posibles incidentes como incendios, terremotos, actos de terrorismo, huelgas, inundaciones, cortocircuitos, entre otros.	1.-Alta dirección/ Gerente General	N. A	Política contra desastres
		Equipamiento de cámaras	muy alto				
		Impresoras	muy alto				
		Monitores	muy alto				
R20	Corte de suministro eléctrico	Computadoras	alto	Realizar copias de seguridad regularmente. Asegurar un suministro constante de energía para evitar interrupciones en los procesos.	1.-Alta dirección/ Gerente General	N. A	cronograma de mantenimiento y backup
		Monitores	alto				
		Impresoras	medio				
R21	Uso ilícito	Computadoras	alto	Normas para proteger información sensible y prevenir su exposición indebida o pérdida. Establecer directrices para resguardar la información de accesos no autorizados o divulgaciones. Documento de entrega de dispositivos. Registro que incluye el nombre del empleado, las características del equipo asignado, las reglas de uso, estado del equipo y otros accesorios, así como la fecha de entrega del dispositivo.	1.-Coordinador de Calidad/ Coordinador de Seguridad de la información		Formato de confidencialidad y declaración jurada.

R22	Desconexión del equipo	Impresoras	alto	Realizar copias de seguridad regularmente. Asegurar un suministro constante de energía para evitar interrupciones en los procesos.	1.-Coordinador de Calidad/ Coordinador de Seguridad de la información	N. A	Plan de mantenimiento, cronograma de mantenimiento y backup
		Computadoras	Muy alto				
		Equipamiento de cámaras	Muy alto				
		Sistema de red	Muy alto				
R23	Errores en el mantenimiento actualización del equipo	Impresoras	alto				
		Computadoras	Muy alto				
		Equipamiento de cámaras	alto				
R24	Contaminación mecánica polvo	Equipamiento de cámaras	Muy alto	Contratar a una empresa externa que se encargue de realizar tanto el mantenimiento preventivo como correctivo de los dispositivos tecnológicos, tales como portátiles, impresoras, monitores, cargadores, entre otros. Esta empresa llevará a cabo de manera regular el mantenimiento, diagnóstico y reparación de los equipos, asegurando su óptimo funcionamiento.	1.-Alta dirección/ Gerente General	N. A	Acta de Contrato para el mantenimiento respectivo de Equipos
		Discos externos	alto				
		Computadoras	Muy alto				
R25	Robo de Disco	Discos externos	alto	Redactar un documento de entrega a la persona encargada del equipo	1.-Coordinadora de RRHH y logística/ Analista de SI	N. A	Acta de recibo y entrega Equipo, inventario de activos, acta de custodia de equipo
R26	Destrucción deliberada del disco	Discos externos	alto	Realizar copias de seguridad regularmente. Asegurar un suministro constante de energía para evitar interrupciones en los procesos.	1.-Coordinador de Calidad/ Coordinador de Seguridad de la información	N. A	Plan de mantenimiento, cronograma de mantenimiento y backup
R27	Degradación por consecuencia del tiempo	Discos externos	alto				
R28	Posibilidad de equivocaciones en la instalación	Sistema de red	alto	Contratar servicios externos de asistencia técnica para llevar a cabo el mantenimiento preventivo y correctivo de los dispositivos. Se busca una empresa especializada que se encargue de mantener, diagnosticar y reparar los diferentes equipos tecnológicos de forma periódica (como portátiles, impresoras, monitores, cargadores, entre otros).	1.-Alta dirección/ Gerente General	N. A	Acta de Contrato para el mantenimiento respectivo de Equipos

R29	Posibilidad de que las fugas de agua inunden y dañen	Oficinas Botica Ekonopharma	Muy alto	Tener a disposición una compañía externa que se encargue de proteger contra incendios y brindar asesoramiento al personal para actuar adecuadamente en caso de una emergencia. Compañías aseguradoras que proporcionan protección contra una variedad de desastres, ya sean causados por la naturaleza o por el ser humano (como incendios, inundaciones, cortocircuitos, etc.). Tener una compañía de seguros que resguarde al negocio de posibles eventos como incendios, terremotos, terrorismo, huelgas, inundaciones, cortocircuitos, entre otros, es fundamental.	1.-Alta dirección/ Gerente General	N. A	Política contra desastres
R30	Posibilidad de ocurrir sismo o terremoto	Oficinas Botica Ekonopharma	alto				
R31	Interceptación de red	Red inalámbrica	alto	Se debe Cambia las contraseñas del Wi-Fi y de todos los dispositivos conectados a ella. Actualizando el firmware y todos los dispositivos conectados para corregir posibles vulnerabilidades. Escanear la red en busca de dispositivos desconocidos que podrían estar comprometiendo la seguridad de la red.	1.-Coordinador de Calidad/ Coordinador de Seguridad de la información	N. A	Medidas de Seguridad de la Información
R32	Monitorización del trafico	Red inalámbrica	alto				
R33	Indisponibilidad por ausencia o renuncia inmediato	Trabajadores	Muy alto	Contar con un plan de contingencia que incluya la incorporación de personal adicional para cubrir ausencias y garantizar la continuidad de las operaciones de la empresa.	1.-Analista de Seguridad de la Información/ Coordinadora de RRHH y Logística	N. A	Plan de contingencia
R34	Extorsión por obligar a obrar en mal sentido	Trabajadores	Muy alto	Capacitar al personal vulnerable en las estrategias de los atacantes y promover la denuncia de cualquier caso.	1.-Analista de Seguridad de la Información/ Coordinadora de RRHH y Logística	N. A	Acta de reunión y Acta de capacitación n.
R35	Ingeniería social aprovechamiento de buena fe	Trabajadores	Muy alto				

ANEXO K

MATRIZ DE COMUNICACIÓN INTERNA Y EXTERNA EKONOPHARMA S.A.C

Tabla 48

N.º	¿Qué información es necesaria transmitir?	¿En qué momento es adecuado comunicar?	¿Quién tiene la responsabilidad de transmitir información?	¿Con quién debo comunicarme?	Tipo	Registro	Proceso de Comunicación
1	La política de Seguridad de la información establece los objetivos que se deben cumplir en el manejo y protección de la información de una organización.	Cuando se actualiza y se aprueba la Política de Seguridad de la Información.	Analista de SI	Todos los empleados de Ekonopharma	Interna	Correo electrónico institucional	Comunicación de las normas de seguridad de la información a través del correo electrónico por parte del Coordinador de la compañía.
2	Organización de la SI (Roles y Responsabilidad des) MOF	Cuando se analizan y se aprueban las funciones y obligaciones dentro del Sistema de Gestión de Seguridad de la Información (SGSI).	Analista de SI	Todos los empleados de Ekonopharma	Interna	Correo electrónico institucional	Comunicación de información por parte de la Organización de Seguridad de la Información a través del correo electrónico del Coordinador.
3	Manual del SGSI	Cuando se examina y se aprueba el Manual del Sistema de Gestión	Coordinador de la seguridad de la información.	Todos los empleados de Ekonopharma	Interna	Correo electrónico institucional	Envío del Manual del Sistema de Gestión de Seguridad de la Información a través del correo electrónico del Coordinador de la organización.

		de la Seguridad de la Información.					
4	Programa de formación y sensibilización en protección de datos.	Semestral	Coordinador de Seguridad de la información	Todos los empleados de Ekonopharma	Interna	Correo electrónico institucional	Transmisión del programa de formación y sensibilización mediante un mensaje electrónico.
5	Informe sobre la situación de la implementación de los controles de Seguridad de la Información.	Mensual	Coordinador de Seguridad de la información	Alta dirección y Analista de SI	Interna	Acta de reunión	Informe del progreso de la aplicación de medidas de control, mediante una junta de trabajo.
6	Informe sobre la evaluación del Sistema de Gestión de Seguridad de la Información llevada a cabo por la alta dirección.	Bimestral	Coordinador de Seguridad de la información	Alta dirección	Interna	Acta de reunión	Reporte de evaluación del Sistema de Gestión de Seguridad de la Información expuesto en una reunión con los líderes empresariales más importantes.
7	Informe sobre el manejo de contratiempos de seguridad informática	Bimestral	Coordinador de Seguridad de la información	Alta dirección Todos los colaboradores	Interna	Correo electrónico institucional	Dar cuenta de los incidentes de seguridad de la información ocurridos durante las reuniones. Enviar el reporte de estos incidentes por medio del correo electrónico institucional.
8	Informe sobre los resultados obtenidos en las auditorías internas del Sistema de Gestión de la	De acuerdo con el Programa de Auditorías Internas	Coordinador de Seguridad de la Información	Alta Dirección	Interna	Acta de reunión Correo electrónico	Comunicación de los resultados obtenidos en las revisiones internas del Sistema de Gestión de Seguridad de la Información durante una reunión. Compartir el informe de las inspecciones internas del SGSI a través de un correo electrónico con el Coordinador de la organización.

	Seguridad de la Información.						
9	Reporte sobre las medidas correctivas y de mejora	Después de las auditorias	Coordinador de Seguridad de la Información	Alta Dirección y Analista de SI	Interna	Acta de reunión Correo electrónico	Transmitir la información sobre las medidas correctivas y de mejora durante una reunión. Enviar por email el informe actualizado sobre el progreso de las solicitudes de acción correctiva.
10	Conclusiones de la inspección de certificación del Sistema de Gestión de Seguridad de la Información.	Según lo planificado	Coordinador de Seguridad de la Información	Alta Dirección y Analista de SI	Interna	Acta de reunión Correo electrónico	Transmisión de los resultados de la auditoría de certificación del Sistema de Gestión de Seguridad de la Información en una reunión. Divulgación del informe de la auditoría de certificación del SGSI mediante el uso del correo electrónico corporativo.

Nota. La tabla representa Matriz de comunicación interna y externa en Ekonopharma.

PRESUPUESTO

Tabla 49

Bienes

BIENES	COSTO (S/.)
Un ordenador personal	4500.00
Unidad de almacenamiento	300.00
Impresora	365.00
Otros	200.00
TOTAL	**5365.00**

Nota. La tabla representa el presupuesto de la inversión en bienes

Tabla 50

Servicios

SERVICIOS	COSTO (S/.)
Fluido eléctrico	650.00
Internet	320.00
Servidor de la nube	1000.00
Asesoría de expertos	2500.00
TOTAL	**4470.00**

Nota. La tabla representa el presupuesto de la inversión en servicios

Tabla 51

Resumen del presupuesto

RESUMEN DE INVERSIÓN	
Total, bienes	5365.00
Total, servicios	4470.00
TOTAL	**9835.00**

Nota. La tabla representa el resumen del presupuesto

UNSCH FACULTAD DE INGENIERÍA DE MINAS, GEOLOGIA Y CIVIL

ACTA DE SUSTENTACION DE TESIS N° 058-2024-FIMGC

PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERA DE SISTEMAS

En la Universidad Nacional de San Cristóbal de Huamanga de la ciudad de Ayacucho, en cumplimiento a la **Resolución Decanal N° 592-2024-FIMGC-D** y al **Memorando N° 436-2024-FIMGC/UNSCH,** a los diez días del mes de setiembre de 2024, siendo las 10:00 a.m, reunidos en el Auditorio de la Escuela Profesional de Ingeniería de Minas, bajo la presidencia del MSc. Ing. Karel PERALTA SOTOMAYOR y los miembros; Mg. Ing. Eloy VILA HUAMÁN y Mg. Ing. Hubner JANAMPA PATILLA, actuando como secretario docente el MSc. Ing. Kelvis BERROCAL ARGUMEDO, para proceder a la sustentación de tesis para optar el Título Profesional de Ingeniero de Sistemas, del bachiller:

Lisset Karen LIMA LOAYZA

Quien presentó la tesis denominada:

Sistema de gestión de seguridad de la información según ISO/IEC 27001 para las pymes del Perú, 2024

Los señores miembros del jurado luego de expuesto la tesis y absueltas las preguntas, delibera y lo declaran:

APROBADO CON NOTA DIECISEIS (16)

Siendo las 11:50 a.m. del día 10 de setiembre de 2024, culmina el acto de sustentación de tesis, y en conformidad a lo actuado los miembros del jurado firmamos al pie del presente.

MSc. Ing. Karel PERALTA SOTOMAYOR
Presidente

Mg. Ing. Eloy VILA HUAMÁN
Miembro

Dr. Ing. Hubner JANAMPA PATILLA
Miembro

Mg. Ing. Kelvis BERROCAL ARGUMEDO
Secretario docente de la FIMGC

cc:
Archivo

FACULTAD DE INGENIERIA
DE MINAS, GEOLOGÍA Y CIVIL
Av. Independencia S/N
Ciudad Universitaria
Central Tel 066 312510
Anexo 151

CONSTANCIA DE ORIGINALIDAD DE TRABAJO DE INVESTIGACIÓN

CONSTANCIA Nº 012-2024-KPS-FIMGC/UNSCH

El que suscribe; responsable verificador de originalidad de trabajos de tesis de pregrado con el software Turnitin, en segunda instancia para las **Escuelas Profesionales** de la **Facultad de Ingeniería de Minas, Geología y Civil**; en cumplimiento a la **Resolución de Consejo Universitario Nº 039-2021-UNSCH-CU**, Reglamento de Originalidad de Trabajos de Investigación de la Universidad Nacional San Cristóbal de Huamanga y **Resolución Decanal Nº 473-2023-FIMGC-D**, deja constancia de originalidad de trabajo de investigación, que el/la Sr./Srta.

Nombres y Apellidos	:	Lisset Karen LIMA LOAYZA
Escuela Profesional	:	INGENIERÍA DE SISTEMAS
Título de la Tesis	:	Sistema de gestión de seguridad de la información según ISO/IEC 27001 para las pymes del Perú, 2024
Evaluación de la Originalidad	:	**24%** Índice de Similitud
Identificador de la entrega	:	2474899363

Por tanto, según los Artículos 12, 13 y 17 del Reglamento de Originalidad de Trabajos de Investigación, es **PROCEDENTE** otorgar la **Constancia de Originalidad** para los fines que crea conveniente.

En señal de conformidad y verificación se firma la presente constancia

Ayacucho, 09 de octubre de 2024

FIRMA DIGITAL

Firmado digitalmente por: PERALTA SOTOMAYOR Karel FAU 20143660754 soft
Motivo: Soy el autor del documento
Fecha: 09/10/2024 22:10:41-0500

Con depósito para Sustentación y Tramites
C.c. Archivo

FACULTAD DE INGENIERIA DE MINAS, GEOLOGIA Y CIVIL
Av. Independencia S/N Ciudad Universitaria
Central Tel. 066 312510
Anexo 151

Sistema de gestión de seguridad de la información según ISO/IEC 27001 para las pymes del Perú, 2024

por Lisset Karen Lima Loayza

Fecha de entrega: 04-oct-2024 09:26a.m. (UTC-0500)
Identificador de la entrega: 2474899363
Nombre del archivo: Lisset_Karen_Lima_Loayza.pdf (3.6M)
Total de palabras: 42120
Total de caracteres: 224831

Sistema de gestión de seguridad de la información según ISO/IEC 27001 para las pymes del Perú, 2024

INFORME DE ORIGINALIDAD

24%	24%	8%	15%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	repositorio.usmp.edu.pe Fuente de Internet	8%
2	repository.unad.edu.co Fuente de Internet	1%
3	Submitted to Universidad Internacional de la Rioja Trabajo del estudiante	1%
4	Submitted to Universidad Nacional Abierta y a Distancia, UNAD,UNAD Trabajo del estudiante	1%
5	repositorio.unne.edu.ar Fuente de Internet	1%
6	vsip.info Fuente de Internet	1%
7	repositorio.unamba.edu.pe Fuente de Internet	1%
8	repositorio.upn.edu.pe Fuente de Internet	1%

9	repositorio.espe.edu.ec Fuente de Internet	1 %
10	repositorio.uta.edu.ec Fuente de Internet	1 %
11	repositorio.pucesa.edu.ec Fuente de Internet	1 %
12	bibdigital.epn.edu.ec Fuente de Internet	1 %
13	repository.unipiloto.edu.co Fuente de Internet	1 %
14	stadium.unad.edu.co Fuente de Internet	1 %
15	repositorio.undac.edu.pe Fuente de Internet	1 %
16	www.adinelsa.com.pe Fuente de Internet	1 %
17	cybertesis.unmsm.edu.pe Fuente de Internet	<1 %
18	www.slideshare.net Fuente de Internet	<1 %
19	openaccess.uoc.edu Fuente de Internet	<1 %
20	repositorio.ug.edu.ec Fuente de Internet	<1 %

21	Submitted to Universidad Tecnológica Centroamericana UNITEC Trabajo del estudiante	<1 %
22	Submitted to UDELAS: Universidad Especializada de las Americas Panama Trabajo del estudiante	<1 %
23	Submitted to Universidad Cesar Vallejo Trabajo del estudiante	<1 %
24	Submitted to Universidad Distrital FJDC Trabajo del estudiante	<1 %
25	Bernal, Jennyfer Ospina. "T.I.l (Tiempo de Interacción y Lectura) Desarrollo de la Lectura en Estudiantes Con Discapacidad Intelectual Límite de Segundo Grado", Universidad Distrital Francisco José de Caldas (Colombia), 2024 Publicación	<1 %
26	uvadoc.uva.es Fuente de Internet	<1 %
27	Submitted to Fundacion Universitaria Juan de Castellanos Trabajo del estudiante	<1 %
28	Submitted to Universidad de Santiago de Chile Trabajo del estudiante	<1 %

29	Cossio Medina, Jorge Alberto. "Implementacion de un sistema integrado de gestion de monitoreo del circuito consultorio-farmacia-logistica en la atencion ambulatoria del hospital central PNP. Luis N Saenz de la direccion de sanidad PNP, en la ciudad de Lima.", Pontificia Universidad Catolica del Peru - CENTRUM Catolica (Peru), 2021 Publicación	<1 %
30	repositorio.unprg.edu.pe Fuente de Internet	<1 %
31	Submitted to Universidad Nacional de Colombia Trabajo del estudiante	<1 %
32	Submitted to consultoriadeserviciosformativos Trabajo del estudiante	<1 %
33	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 %
34	repositorio.uisrael.edu.ec Fuente de Internet	<1 %
35	Submitted to Universidad Pontificia Bolivariana	<1 %

Trabajo del estudiante

36	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 %
37	Jezreel Mejia, Mima Munoz, Heltton Ramirez. "Proposed framework for the CSIRT protection", 2016 11th Iberian Conference on Information Systems and Technologies (CISTI), 2016 Publicación	<1 %

Excluir citas	Activo	Excluir coincidencias	< 30 words
Excluir bibliografía	Activo		