UNIVERSIDAD NACIONAL DEL SANTA

ESCUELA DE POSGRADO

Programa de Doctorado en Ingeniería de Sistemas e Informática

Modelo de buenas practicas para aplicar la seguridad de información para hospitales públicos nivel II, caso la Caleta Chimbote

Tesis para optar el grado de Doctor en Ingeniería de Sistemas e Informática

Autor:

Mg. Carranza Lujan, Jorge Luis

Código ORCID: 0009-0006-9524-4973

Asesor:

Dr. Gutiérrez Gutiérrez, Jorge Luis

DNI. N° 18135227

Código ORCID: 0000-0002-4989-1196

Línea de Investigación:

Sistemas de Información y Gestión Sanitaria

Nuevo Chimbote - PERÚ

2026

UNS
ESCUELA DE POSGRADO

CONSTANCIA DE ASESORAMIENTO DE TESIS

Yo, Dr. Gutierrez Gutierrez, Jorge Luis, a través del presente documento, hago constar mi asesoramiento de la tesis titulado: **"Modelo de buenas prácticas para aplicar la seguridad de información para hospitales públicos nivel II, caso la caleta Chimbote"** que tiene como autor a **Jorge Luis Carranza Lujan**, alumno del Doctorado en Ingeniería de Sistemas e Informática, ha sido elaborado de acuerdo al Reglamento de Normas y Procedimientos para optar el Grado de **Doctor** en la Escuela de Posgrado de la Universidad Nacional del Santa.

Nuevo Chimbote, mayo del 2026

Dr. Gutiérrez Gutiérrez, Jorge Luis
Asesor
DNI: 18135227
Código ORCID: 0000-0002-4989-1196

AVAL DE CONFORMIDAD DEL JURADO

Tesis titulado: **"Modelo de buenas prácticas para aplicar la seguridad de información para hospitales públicos nivel II, caso la caleta Chimbote"** que tiene como autor a **Jorge Luis Carranza Lujan**.

Revisado y Aprobado por el Jurado Evaluador:

Dr. Ramírez Milla, Luis Enrrique
Presidente
DNI: 32956519
Código ORCID: 0000-0002-2259-1070

Dr. Apestegui Florentino , Yim Isaías
Secretario
DNI: 32541215
Código ORCID 0000-0003-2873-1748

Dr. Gutierrez Gutierrez, Jorge Luis
Vocal
DNI: 18135227
Código ORCID: 0000-0002-4989-1196

UNS
ESCUELA DE POSGRADO

ACTA DE EVALUACIÓN DE SUSTENTACIÓN DE TESIS

A los quince días del mes de mayo del año 2026, siendo las 18:00 horas, en el aula P-02 de la Escuela de Posgrado de la Universidad Nacional del Santa, se reunieron los miembros del Jurado Evaluador, designados mediante Resolución Directoral Nº 239-2026-EPG-UNS de fecha 26.03.2026, conformado por los docentes: Dr. Luis Enrique Ramírez Milla (Presidente), Dr. Yim Isaias Apestegui Florentino (Secretario) y Dr. Jorge Luis Gutiérrez Gutiérrez (Vocal); con la finalidad de evaluar la tesis intitulada: "***MODELO DE BUENAS PRACTICAS PARA APLICAR LA SEGURIDAD DE INFORMACIÓN PARA HOSPITALES PÚBLICOS NIVEL II, CASO LA CALETA CHIMBOTE***"; presentado por el tesista **Jorge Luis Carranza Lujan** egresado del programa de Doctorado en Ingeniería de Sistemas e Informática.

Sustentación autorizada mediante Resolución Directoral N° 362-2026-EPG-UNS de fecha 06 de mayo de 2026.

El presidente del jurado autorizó el inicio del acto académico; producido y concluido el acto de sustentación de tesis, los miembros del jurado procedieron a la evaluación respectiva, haciendo una serie de preguntas y recomendaciones al tesista, quien dio respuestas a las interrogantes y observaciones.

El jurado después de deliberar sobre aspectos relacionados con el trabajo, contenido y sustentación del mismo y con las sugerencias pertinentes, declara la sustentación como APROBADO, asignándole la calificación de 18.

Siendo las 16:10 horas del mismo día se da por finalizado el acto académico, firmando la presente acta en señal de conformidad.

Dr. Luis Enrique Ramírez Milla
Presidente

Dr. Yim Isaías Apestegui Florentino
Secretario

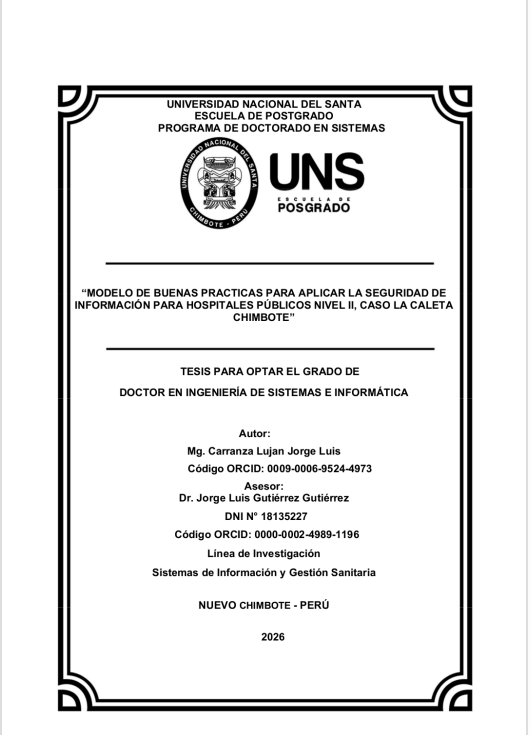
Dr. Jorge Luis Gutiérrez Gutiérrez
Vocal/Asesor

Recibo digital

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

La primera página de tus entregas se muestra abajo.

Autor de la entrega:	Jorge Luis CARRANZA LUJAN
Título del ejercicio:	DOCTORADO 2026
Título de la entrega:	MODELO DE BUENAS PRACTICAS PARA APLICAR LA SEGURIDA...
Nombre del archivo:	TESIS_FINAL_2026_Jorge_Carranza_23.04.2026.docx
Tamaño del archivo:	4.86M
Total páginas:	146
Total de palabras:	32,898
Total de caracteres:	194,205
Fecha de entrega:	28-may-2026 02:43p. m. (UTC-0500)
Identificador de la entrega:	2971464146



UNIVERSIDAD NACIONAL DEL SANTA
ESCUELA DE POSTGRADO
PROGRAMA DE DOCTORADO EN SISTEMAS

UNS
ESCUELA DE POSGRADO

"MODELO DE BUENAS PRACTICAS PARA APLICAR LA SEGURIDAD DE INFORMACIÓN PARA HOSPITALES PÚBLICOS NIVEL II, CASO LA CALETA CHIMBOTE"

TESIS PARA OPTAR EL GRADO DE
DOCTOR EN INGENIERÍA DE SISTEMAS E INFORMÁTICA

Autor:
Mg. Carranza Lujan Jorge Luis
Código ORCID: 0009-0006-9524-4973
Asesor:
Dr. Jorge Luis Gutiérrez Gutiérrez
DNI N° 18135227
Código ORCID: 0000-0002-4989-1196
Línea de Investigación
Sistemas de Información y Gestión Sanitaria

NUEVO CHIMBOTE - PERÚ

2026

MODELO DE BUENAS PRACTICAS PARA APLICAR LA SEGURIDAD DE INFORMACIÓN PARA HOSPITALES PÚBLICOS NIVEL II, CASO LA CALETA CHIMBOTE

INFORME DE ORIGINALIDAD

18%	17%	7%	8%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	repositorio.uta.edu.ec Fuente de Internet	4%
2	hdl.handle.net Fuente de Internet	4%
3	Submitted to Universidad San Marcos Trabajo del estudiante	1%
4	tesis.ipn.mx Fuente de Internet	1%
5	repositorio.unjfsc.edu.pe Fuente de Internet	1%
6	Submitted to Universidad Internacional de la Rioja Trabajo del estudiante	1%
7	repository.unad.edu.co Fuente de Internet	1%
8	mafiadoc.com Fuente de Internet	<1%
9	repositorio.unitec.edu Fuente de Internet	<1%
10	Submitted to Universitat Oberta de Catalunya Trabajo del estudiante	<1%
11	repositorio.unprg.edu.pe Fuente de Internet	<1%

Dedicatoria

A mi Madre, raíz que sostiene mi paso y mi fe,

su amor es luz constante en cada amanecer del esfuerzo.

A Mi Padre ausente, pero eterno en mi rumbo,

este logro lleva tu nombre escrito en silencio y gratitud.

A mi esposa, compañera de desvelos y paciencia infinita,

su amor es refugio cuando el camino se hizo largo.

A mis dos hijas, Angie y Martha, luz que da sentido a cada meta,

este logro late por ustedes, razón y alegría de mi vida.

Agradecimientos

A mi asesor el Dr. Jorge Luis Gutiérrez Gutiérrez

por conducirme por la senda de la ciencia de los datos.

A mis jurados

por sus acertadas y necesarias apreciaciones

INDICE

INDICE DE TABLAS

INDICE DE FIGURAS

INDICE DE ANEXOS

RESUMEN

La seguridad de la información tiene un papel importante en las organizaciones, por ello en el presente informe tesis titulado “Modelo de buenas prácticas para aplicar la seguridad de la información para hospitales públicos nivel II, caso Hospital La Caleta Chimbote”, quiere contribuir en la búsqueda de una solución a través de buenas prácticas que contribuirán a reducir significativamente los riesgos de perdida de información. es por ello que se inició seleccionando los atributos más relevantes para proponer un modelo de aprendizaje con políticas, procedimientos y mecanismos necesarios para salvaguardar la información.

A medida que se implemente una buena práctica, ayudará a gestionar la seguridad de la información a través de controles y procedimientos formales para evitar la pérdida de información que puede ocurrir debido a los riesgos y vulnerabilidades que enfrenta el Hospital Nivel 2 La Caleta. Las buenas prácticas ayudarán a crear una cultura organizacional de seguridad de la información y respaldarán la continuidad del negocio al reducir la incidencia de cambios o pérdidas de información que ocurren durante procesos comerciales críticos ocasionales.

Palabras claves: Buenas Prácticas, Sistemas de información.

ABSTRACT

Information security plays a crucial role in organizations. Therefore, this thesis report, entitled "A Best Practices Model for Implementing Information Security in Level II Public Hospitals: The Case of La Caleta Hospital in Chimbote," aims to contribute to finding a solution through best practices that will significantly reduce the risk of information loss. To this end, the most relevant attributes were selected to propose a learning model with the necessary policies, procedures, and mechanisms to asegurad information.

As a best practice is implemented, it will help manage information security through formal controls and procedures to prevent information loss that can occur due to the risks and vulnerabilities faced by La Caleta Level II Hospital. These best practices will help create an organizational culture of information security and support business continuity by reducing the incidence of changes or data loss that occur during occasional critical business processes.

Keywords: Best Practices, Information Systems

CAPÍTULO I

Problema de Investigación

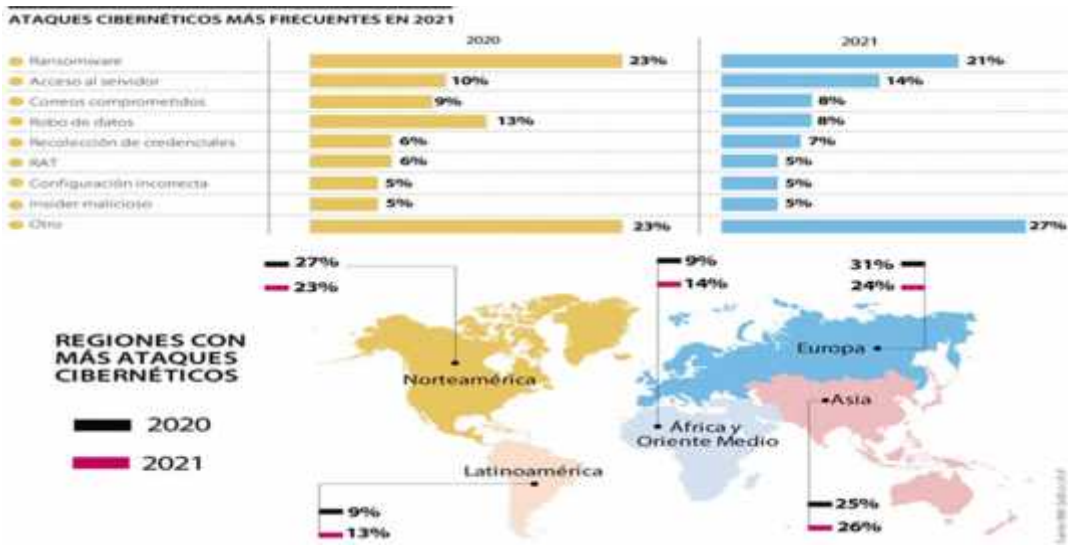
1.1. Planteamiento y fundamentación del problema de investigación

Según (IBM Security, 2022). En la actualidad la seguridad de información es una preocupación relevante en las empresas; donde no interesa el rubro en el cual desarrollen sus actividades. A todo ello se suma que en dichas actividades que se desarrollan diariamente se hace uso de las tecnologías de la información y comunicaciones (TICs); con el uso de las TICs ha permitido que aparezcan mas activos que seran necesarios proteger. Cada activo tambien esta expuesto a las amenazas y vulnerabilidades de su entorno. Un caso comun que se presenta a diario son los ciberataques, los cuales son cada vez mas complejos y por lo consiguiente llegan a tener consecuencias muy graves como es la revelación de información. (catalogado como confidencial)

Los esfuerzos de la compañía para mejorar la seguridad de los equipos informaticos se enfrentan a muchos obstáculos. Las empresas deben defender múltiples áreas y funciones, así como los desafíos de seguridad. Uno de los puntos de defensa más desafiantes enumerados es el dispositivo móvil, los datos almacenados en la nube pública (infraestructura que está disponible para el público) y, lo más importante, el comportamiento del usuario. En la Figura 1, podemos ver el aumento de los ataques en los ultimos años.

Figura 1

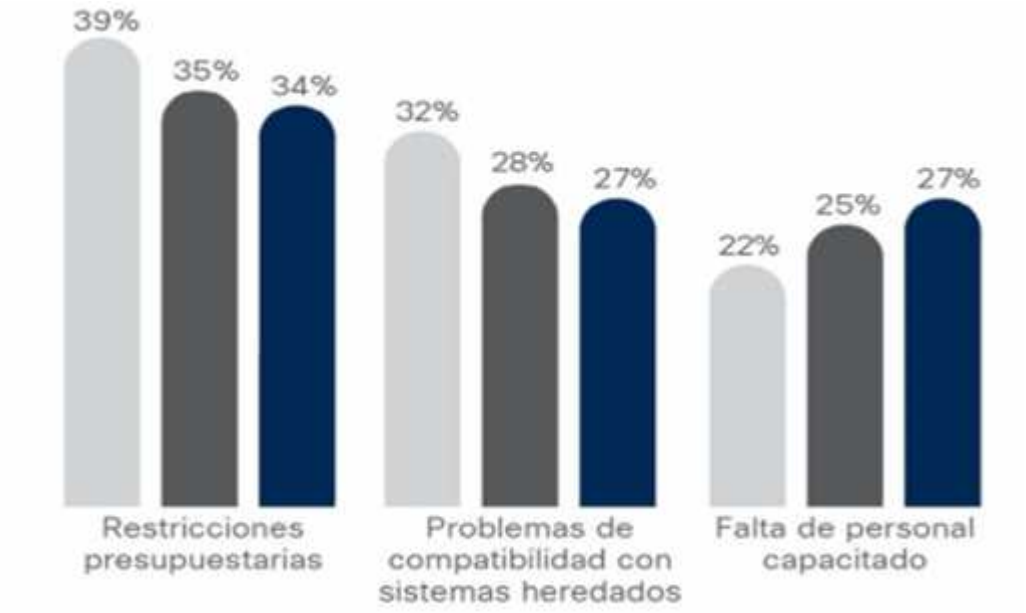
Áreas más difíciles de defender: dispositivos móviles y datos en la nube



Por ello las empresas para lograr implementar medidas de seguridad sobre las areas dificiles de controlar necesitan contar con los recursos economicos necesarios para adquirir o mejorar servicios de seguridad que ayuden mitigar las amenazas y vulneralidades. Es por ello que en el contexto de latinoamerica aun en el presupuesto anual que planifican las empresas no consideran el tema de seguridad como una actividad relevante; por ello al no contar con recursos provoca brechas de seguridad. Asi mismo el desconocimiento del alcance de funcionamiento de sistemas informaticos heredados por la empresa representa una fuente de un sin numero de fallos de seguridad informatica que pueden estar sucediendo sin tener control de ellos y por ultimo algo que es mas comun es no contar con el personal ideal sobre temas de seguridad dentro de la empresa, asi como lo podemos obserbar en la figura 2.

Figura 2

Restricciones presupuestarias de seguridad



Nota: Estudio de referencia de las capacidades de seguridad Cisco 2018

Las empresas pueden aumentar sus posibilidades de gestionar con éxito los factores que ayudan a precisar que la seguridad de la información esté integrada en todas las áreas de la empresa, no de manera integral. También deben evitarse las modificaciones de mejoras de producto o tecnología para reparar, mantener la seguridad. Para que un producto tenga éxito, la empresa necesita comprender e implementar las políticas y procesos tecnológicos ideales. Como resultado, el panorama moderno de desafíos de exposición de información y las personas

comprometidas con el crimen se están volviendo cada vez más profesionales. Porque tienen herramientas más efectivas (como el cifrado) y estrategias inteligentes más avanzadas (como el abuso de servicios legítimos de Internet) para ocultar sus actividades y violar las tecnologías de seguridad tradicionales.

En la mayoría de instituciones de salud pública y privada a nivel nacional, las políticas que ayudan a garantizar la seguridad de la información no están establecidas de manera formal, lo cual deja como responsabilidad a cada institución de salud perteneciente a establecer sus propias políticas que ayuden a gestionar la seguridad de información. En el caso de los establecimientos de salud, Nivel II, caso Hospital La Caleta el escenario es similar debido que a pesar de los años de antigüedad del hospital existe pocas políticas para asegurar que la información que se genera en los diferentes procesos de la unidad productora de servicios. La falta de políticas es responsabilidad de la dirección ejecutiva que por carecer un bajo nivel de conocimiento sobre la importancia de la seguridad de la información. Cada año el número de incidencias va en aumento y se presentan de manera frecuente en las diferentes áreas administrativas y asistenciales, según la información recopilada, podemos mencionar las incidencias que se presentan con mayor frecuencia que han presentado pérdida y/o alteración accidental de la información, también existe pocos registros de evidencias de los incidentes reportados y de las vulnerabilidades en cada uno de los procesos de seguridad de información del establecimiento asistencial..

Esta realidad problemática posee las siguientes características:

a.- Los hospitales públicos de Nivel II gestionan datos clínicos y administrativos que son muy sensibles. En el Hospital La Caleta se observan deficiencias en las políticas de seguridad, en el control de accesos, en el respaldo de información y en la sensibilización del personal, lo que eleva los riesgos de pérdida, modificación o divulgación no autorizada de datos, comprometiendo la continuidad del servicio y la privacidad del paciente.

b.- En nuestra región los hospitales nivel II es común que cada año se presente un número considerable de incidencias asociadas a fallas de computadoras causados por diferentes factores (fallas, desgaste mecánicas y de circuitos digitales en los discos duros, humedad, brisa; hacen que las computadoras no funciones por estar

cerca al mar etc.), El fallo de estas computadoras conlleva a perder datos relevantes para los usuarios y sobre todo para el Hospital. A pesar de la existencia de políticas las cuales son omitidas por el personal responsable de cada equipo y también del personal técnico, caso hospital La Caleta.

c.- Un aspecto que pocas organizaciones y como también es el caso de los Hospitales Nivel II de la región no tienen las políticas establecidas para garantizar la continuidad del negocio. Como por ejemplo garantizar disponibilidad del servicio de Internet en cada oficina administrativa y asistencial donde es muy necesario contar con dicho servicio. Otro de las incidencias que afectan el normal desenvolvimiento de los procesos informáticos del establecimiento hospitalario es la interrupción de servicio eléctrico provocado por fallos en el suministro externo, que son de manera recurrente. Para dar solución a esta contingencia se cuenta con grupos electrógenos pero que no cubren la demanda total y solo se centran en ciertas áreas asistenciales relevantes.

d.- En los hospitales nivel II de la región que empezaron a usar tecnología de información como soporte a sus actividades diarias es frecuente encontrar que se presente ataques de virus donde su origen puede ser externo o interno. Así mismo el tener servicios expuestos en una red pública como el internet es muy probable que se presenten ataques informáticos, pudiendo afectar la web institucional. A pesar que las recomendaciones sobre Ciberseguridad se encuentren implementadas en los documentos de gestión, es necesario hacer una revisión periódica de dichos controles y realizar las mejoras en el caso de encontrar ciertas deficiencias y vulnerabilidades sobre la seguridad de la información.

e.- Las tecnologías de la información de los hospitales donde se encuentran los sistemas de escritorio y web deben ser manipulados por los usuarios acreditados y autenticados por el sistema de gestión gerencial, no permitiendo el uso por terceras personas que se pueden convertir en nuevas amenazas de los sistemas computarizados.

f.- Actualmente el hospital la caleta cuenta en su infraestructura tecnológica cerca de 180 computadoras e 150 impresoras que se interconectan a un servidor en una arquitectura cliente-Servidor. Además, se cuenta con una línea de Internet

dedicada de 200 Mbps y una central digital de 10 canales telefónicos para atender las llamadas de la población.

Las incidencias que se presentan son muchas entre ellas tenemos: 4,320 interrupciones a los sistemas en el último año.

Los principales incidentes tenemos: Acceso no autorizado a información clínica, Pérdida o filtración de datos de pacientes, ataques de malware o ransomware, caída de sistemas críticos hospitalarios, errores humanos del personal y uso indebido de dispositivos médicos conectados

Estas incidencias son críticas en un hospital por que impactan sobre la atención al paciente, historias clínicas electrónicas, equipos y biomédicos conectados

A continuación, se realizó un diagnóstico cuantitativo inicial sobre la situación de la seguridad de informacion del Hospital La Caleta, que ha sido creado a partir de datos internos proporcionados por la sección de TI, entrevistas técnicas y comparación con métricas empleadas en hospitales públicos de categoría II del Ministerio de Salud.

Entre enero y diciembre de 2024, el Hospital La Caleta reportó cerca de 145 eventos relacionados con la protección de la información personal. Estos eventos fueron categorizados como incidentes de seguridad de la información, conforme a los criterios determinados, como se muestra en la Tabla 1.

En cuanto a la infraestructura tecnológica, la entidad cuenta con alrededor de 180 dispositivos operativos, los cuales se especifican en la Tabla 2. Además, se detectaron varios sistemas informáticos que se comunican con el servidor de la institución, cuya información está disponible en la Tabla 3.

Con base en el análisis de estos elementos, se realizó una valoración del nivel de avance en protección de datos, teniendo en cuenta tanto los factores técnicos como organizativos. Los resultados que se obtuvieron se presentan de forma organizada en la Tabla 4.

Tabla 1

Incidentes de seguridad de la informacion.

Tipo de Incidente	Nro de Casos	Porcentaje (%)
Infecciones por malware/virus	50	32.4 %
Fallas de disponibilidad de sistemas	15	10.3 %
Accesos no autorizados	20	13.7 %
Pérdida o corrupción de información	24	16.5%
Otros (errores humanos, configuración)	36	24.8%
Total	145	100%

Nota: Elaboración Propia

Tabla 2

Estado de equipos informáticos

Tipo de Incidente	valor
Computadoras con fallas técnicas recurrentes	100
Porcentaje de equipos con fallas	55.5%
Computadoras sin antivirus actualizado	180
Computadoras sin políticas de respaldo automático	120
Equipos con sistemas operativos obsoletos	30

Nota: Elaboración Propia

Tabla 3

Disponibilidad de los sistemas críticos

Sistema	Horas de indisponibilidad/año	Impacto
Sistemas de Historias Clínicas	24 h	alto
Módulo de Farmacia	19 h	alto
Módulo de Laboratorio	35 h	alto
Sistema SIAF	8 h	Medio
Sistema SIGA	7 h	Medio
Sistema Hismis	6 h	Medio

Nota: Elaboración Propia

Tabla 4

Grado de desarrollo en la protección de datos

Dimensión evaluada	Nivel de cumplimiento
Políticas de seguridad	Bajo
Gestión de accesos	Medio
Gestión de incidentes	Medio
Continuidad del negocio	Alto
Concienciación del personal	Bajo

Nota: Elaboración Propia

1.2. Antecedentes de la Investigación.

Actualmente se puede observar cómo la seguridad de información ha originado de forma significativa un cambio en las organizaciones; trayendo consigo una preocupación latente de la forma eficiente de cómo administrar los activos de información. Las organizaciones se ven obligadas a encontrar el mecanismo más apropiado para enfrentar las causas de las amenazas y los riesgos.

Según los resultados obtenidos por (Baldera, 2025) en su investigación de análisis se basa en el desafío de la administración de la seguridad de la información en lo que respecta a la gestión de registros clínicos dentro de las instituciones que brindan servicios de salud, las cuales han sido poco exploradas tanto en investigaciones como en modelos de seguridad. El objetivo de esta investigación es crear un modelo de seguridad de la información basado en un enfoque de gestión de riesgos en tecnologías de la información, tomando como base las recomendaciones y buenas prácticas de normas como la ISO/IEC 27001, ISO/IEC 27002 y la metodología española Magerit. Este modelo se aplicará en tres IPRESS ubicadas en Chiclayo, Perú, como ejemplos de estudio. Para construir el modelo propuesto, se consideró la normativa actual de Perú relacionada con la gestión de registros clínicos electrónicos, viéndolos como el núcleo de los procesos hospitalarios, de consultas ambulatorias y de emergencias. La metodología empleada en la investigación fue descriptiva y propositiva, detallando cada actividad y tarea para establecer un marco de trabajo que facilite la identificación y gestión de riesgos, abarcando incluso el cálculo del nivel de exposición a dichos riesgos. A partir de los hallazgos obtenidos, se concluyó que las amenazas

derivadas de actos maliciosos o de errores y faltas del personal son las que presentan un mayor nivel de riesgo; en contraste, las amenazas relacionadas con acciones sobre los sistemas y datos son las que muestran una menor exposición al riesgo.

Según los resultados obtenidos por (Vega, 2025) en su investigación detalla un estudio aplicado que se llevó a cabo en la Gerencia Regional de Salud Lambayeque, centrado en las áreas de Estadística e Informática. El propósito de este estudio fue diseñar e implementar un Sistema de Gestión de Seguridad de la Información (SGSI) alineado con normas ISO, con el objetivo de fortalecer la seguridad de la información ante el aumento de las amenazas cibernéticas y la falta de controles, políticas y buenas prácticas. La metodología empleada fue de tipo aplicada, con un enfoque cuantitativo, un alcance descriptivo y un diseño no experimental. Se utilizó el ciclo de Deming y los estándares ISO/IEC 27001, 27002 y 27005, respaldándose en dos cuestionarios dirigidos al personal de tecnologías de la información y a los jefes de oficina para diagnosticar la situación actual y evaluar el grado de cumplimiento de los controles de seguridad.

Los resultados más relevantes mostraron que la implementación del SGSI facilitó el establecimiento de controles, procedimientos y documentación formal, alcanzando una mejora significativa en la gestión de la seguridad de la información y en el manejo de los riesgos identificados. En conclusión, el estudio evidenció que la adopción de un SGSI conforme a estándares internacionales refuerza la confidencialidad, integridad y disponibilidad de la información, además de adaptarse a las necesidades específicas de una entidad del sector salud. En relación al presente estudio, este antecedente proporciona un marco teórico y metodológico valioso, demostrando empíricamente la efectividad de las buenas prácticas y normas ISO en la gestión de la seguridad de la información, y sirviendo como punto de referencia para investigaciones similares que busquen evaluar o mejorar la seguridad de la información en instituciones de salud u organizaciones públicas.

Según los resultados obtenidos por (Herrera, 2025). En su investigación en el Hospital II-1 de Moyobamba, en el transcurso del año 2024, se llevó a cabo un estudio con un enfoque cuantitativo y un diseño no experimental de tipo transversal,

cuyo objetivo era determinar la conexión entre el sistema de administración de la seguridad de la información y la privacidad de los datos. Este estudio fue de carácter aplicado, con un alcance relacional y un método deductivo, y se llevó a cabo con una muestra de 16 empleados, a quienes se les realizó una encuesta utilizando un cuestionario estructurado. Los hallazgos indicaron que el sistema de administración de la seguridad de la información logró un porcentaje de efectividad del 62,5%, mientras que la confidencialidad de los datos obtuvo un nivel alto del 56,3%. Además, se observó una correlación positiva y significativa en las dimensiones tecnológica y de procesos y políticas, aunque no ocurrió lo mismo en la dimensión cultural y organizacional, lo que indica ciertas debilidades en la concienciación del personal. Finalmente, se llegó a la conclusión de que hay una relación positiva y estadísticamente relevante entre el sistema de administración de la seguridad de la información y la privacidad de los datos (Rho = 0,757; p).

Según los resultados obtenidos por (Arenas, 2025). En su investigación se refiere a la implementación de un Sistema de Información Hospitalaria (HIS) en una clínica privada de Lima, Perú. Su propósito fue mejorar los procesos clínicos y administrativos, elevando así la calidad del servicio al paciente. La metodología utilizada fue de enfoque aplicado y descriptivo, apoyándose en la metodología ágil SCRUM. Se emplearon herramientas tecnológicas como HL7 v2. x para facilitar la interoperabilidad, MySQL para la gestión de bases de datos, y Mirth Connect para la integración y transformación de mensajes. Esto se complementó con actividades de análisis funcional, gestión del cambio y capacitación de los usuarios. Los resultados más destacados incluyeron la digitalización completa (100%) de los historiales clínicos, una reducción del 90% en el uso de papel, la mejora en la programación de citas médicas con una disminución del 50% en los tiempos de espera, una interoperabilidad del 98% entre sistemas, un aumento del 20% en la satisfacción del paciente, y la formación de más de 200 usuarios. En conclusión, el estudio evidenció que la implementación de un HIS, con el respaldo de tecnologías de interoperabilidad y metodologías ágiles, produce mejoras notables en la eficiencia operativa y en la calidad de atención en las instituciones de salud. Por último, la relación con el estudio actual radica en que este antecedente proporciona pruebas empíricas sobre los beneficios de los sistemas de información hospitalaria y la gestión tecnológica en el sector salud, contribuyendo a analizar y reforzar la

importancia de modelos de gestión y mejores prácticas para la optimización de procesos en hospitales.

Según los resultados obtenidos por (Fernández, 2024). En su investigación tuvo como objetivo diseñar e implementar un Sistema de Gestión de Seguridad de la Información (SGSI) que garantice la confidencialidad, integridad y disponibilidad de la información en el proceso de emisión de certificados médicos de aptitud, especialmente en un entorno de alta demanda de exámenes ocupacionales tras la pandemia de COVID-19. La metodología utilizada fue de carácter aplicado, con un enfoque descriptivo y propositivo, fundamentada en el análisis del proceso actual, la identificación de riesgos a la seguridad de la información y la selección de controles del estándar ISO/IEC 27001:2022. Se consideró la combinación de procedimientos manuales y un sistema de información adaptado, además de la incorporación de firmas digitales para disminuir los riesgos de falsificación. Entre los resultados destacados se definieron políticas, procedimientos y controles específicos del SGSI alineados al proceso de emisión de certificados, logrando fortalecer la trazabilidad, la auditoría y la protección de los datos de los pacientes. Las conclusiones mostraron que la implementación del SGSI mejora de manera significativa la seguridad del proceso, reduce los riesgos relacionados con la manipulación de información médica y aumenta la confianza de los pacientes en la clínica. Por último, la relación con el estudio actual radica en que este trabajo proporciona un marco metodológico y normativo basado en ISO/IEC 27001:2022, aplicable al sector salud, actuando como referencia para la gestión de la seguridad de la información en instituciones sanitarias que desean optimizar sus procesos críticos y fortalecer la protección de datos sensibles.

Según los resultados obtenidos por (Rosero, 2024) En su investigación buscó recomendar las mejores prácticas de ciberseguridad que sean aplicables a hospitales públicos en Colombia, fundamentándose en marcos de trabajo, estándares y guías reconocidas, con el objetivo ese fortalecer la protección de información crítica y sensible. La metodología utilizada fue analítica y descriptiva, apoyándose en el análisis del contexto de los hospitales públicos colombianos, la revisión de marcos de ciberseguridad, así como la identificación de vulnerabilidades y amenazas frecuentes en el sector salud. Los resultados principales mostraron que, a pesar de contar con medidas tecnológicas y

recomendaciones de seguridad, los hospitales han experimentado un aumento considerable de ciberataques en el último año, lo que ha impactado la continuidad en la atención al paciente, la confianza de los usuarios y la reputación de las instituciones, resaltando la falta de políticas integrales, procedimientos formalizados y programas de concienciación del personal. En conclusión, el estudio determinó que la adopción de marcos de ciberseguridad y buenas prácticas permite desarrollar políticas y procedimientos enfocados en la gestión de riesgos, así como implementar estrategias técnicas avanzadas y programas de sensibilización que refuercen la integridad, disponibilidad, confidencialidad, autenticidad y trazabilidad de la información. Finalmente, la conexión con el estudio actual reside en que este antecedente respalda la necesidad de aplicar modelos de buenas prácticas y planes integrales de seguridad de la información en hospitales públicos, ofreciendo un marco conceptual y metodológico que avala la realización e identificación de la gestión de la seguridad de la información en contextos hospitalarios similares.

Según los resultados obtenidos por (Nicho, 2024), en su investigación, tuvo como objetivo diseñar un modelo de gestión de riesgos que permita fortalecer la seguridad de la información en los servicios de emergencia de los hospitales públicos de dicha región. La investigación se desarrolló bajo un enfoque aplicado y propositivo, empleando como metodología el análisis y evaluación de riesgos mediante la identificación de activos críticos, amenazas y vulnerabilidades, alineando estándares y marcos internacionales como la NTP ISO 27005, COBIT 5 para Gestión de Riesgos, Magerit y OCTAVE, adaptados al contexto hospitalario. Los resultados evidenciaron deficiencias significativas en la capacitación del personal en seguridad de la información, ausencia de controles formales, falta de identificación sistemática de riesgos y debilidades en la disponibilidad e integridad de los sistemas informáticos del área de emergencias, lo cual generaba demoras en la atención y afectaba la calidad del servicio. El estudio concluyó que la implementación de un modelo estructurado de gestión de riesgos, con definición clara de roles y participación activa del personal, permite priorizar activos críticos y garantizar la confidencialidad, integridad y disponibilidad de la información las 24 horas del día. Este antecedente se relaciona con la presente investigación, ya que aporta fundamentos metodológicos y normativos para la aplicación de un modelo

de buenas prácticas orientado a mejorar la gestión de la seguridad de la información y reducir riesgos en hospitales de nivel II.

Según los resultados obtenidos por (Sánchez, 2024). En la investigación titulada “Implementación de un sistema de gestión de información y eventos de seguridad para la detección de amenazas en una entidad pública del sector salud”, se tuvo como objetivo implementar un sistema SIEM (Security Information and Event Management) en una entidad pública peruana del sector salud, con la finalidad de fortalecer la supervisión de la infraestructura tecnológica y mejorar la detección temprana de amenazas de ciberseguridad, en concordancia con lo establecido en el Decreto Supremo N.º 132-2018-PCM, que aprueba la Estrategia Nacional de Ciberseguridad. La metodología empleada fue de tipo aplicada, con un enfoque práctico-tecnológico, iniciando con el diagnóstico de la infraestructura existente y la identificación de las limitaciones del monitoreo previo basado en protocolos SNMP y NetFlow, los cuales no permitían una adecuada correlación de eventos ni visibilidad integral de incidentes. Posteriormente, se procedió al diseño, instalación y configuración del SIEM, incluyendo la integración de fuentes de registros (logs), activación de reglas de correlación, configuración de controles de seguridad perimetral y validación operativa del sistema mediante pruebas de monitoreo en tiempo real. Los resultados evidenciaron un incremento del 60% en el nivel de seguridad de la infraestructura tecnológica, así como una mejora sustancial en la visualización, análisis y respuesta ante incidentes, permitiendo anticipar amenazas y reducir tiempos de reacción. En conclusión, el estudio demuestra que la implementación de herramientas avanzadas de gestión y correlación de eventos constituye una estrategia efectiva para fortalecer la seguridad de la información en entidades del sector salud, superando las limitaciones de los métodos tradicionales de supervisión. Este antecedente se relaciona directamente con el estudio actual, ya que respalda la necesidad de implementar modelos de buenas prácticas y controles tecnológicos dentro de un Sistema de Gestión de Seguridad de la Información (SGSI), evidenciando que la adopción de mecanismos de monitoreo continuo impacta positivamente en la gestión del riesgo y en la mejora de los niveles de seguridad institucional.

Según los resultados obtenidos por (Almanza, 2023) En el estudio titulado “Buenas prácticas en la seguridad del paciente en el servicio de urgencia. CAMU Prado,

Cereté (septiembre 2021–2022)", se analizó la implementación de la guía de buenas prácticas en seguridad del paciente en el servicio de urgencias, tomando como referencia las directrices del Ministerio de Salud y Protección Social de Colombia y de la Organización Mundial de la Salud (OMS). El objetivo principal fue evaluar la adherencia a las políticas institucionales y medir su impacto en la calidad de la atención y en la reducción de eventos adversos evitables. La investigación se desarrolló bajo un enfoque descriptivo y evaluativo, mediante la medición periódica de indicadores de desempeño establecidos en el Sistema Obligatorio de Garantía de Calidad en Salud (SOGC), así como la revisión documental y el análisis de procesos asistenciales relacionados con la gestión del riesgo. Los resultados evidenciaron que la aplicación sistemática de indicadores permite identificar debilidades en el cumplimiento de protocolos, fortalecer la cultura de seguridad y promover mejoras continuas en la prestación del servicio. Asimismo, se destacó la importancia de consolidar una cultura organizacional no punitiva, orientada al aprendizaje y a la prevención del daño, superando modelos históricos basados en la sanción y avanzando hacia prácticas fundamentadas en evidencia científica. El estudio concluye que la seguridad del paciente constituye un componente esencial de la calidad en salud pública y un compromiso compartido entre las Instituciones Prestadoras de Servicios de Salud y el Estado, siendo indispensable la evaluación constante de las buenas prácticas para garantizar resultados sostenibles. Este antecedente se relaciona directamente con investigaciones actuales sobre gestión de la seguridad en entornos hospitalarios, ya que demuestra que la medición de indicadores, el cumplimiento normativo y la mejora continua son factores determinantes para fortalecer los sistemas de gestión y reducir riesgos institucionales.

Según los resultados obtenidos por (chiquito, 2023), El estudio titulado "Implementación de políticas de seguridad en la infraestructura tecnológica del Hospital Básico Jipijapa mediante un appliance Fortinet 80E" tuvo como objetivo establecer medidas de seguridad de la información que permitan salvaguardar los recursos tecnológicos y mitigar los riesgos presentes en la infraestructura tecnológica hospitalaria, partiendo de la evaluación del estado actual de las políticas de seguridad, la identificación de vulnerabilidades y la formulación de estrategias orientadas a fortalecer la protección de la información en entidades

públicas de salud. La investigación se desarrolló bajo un enfoque cualitativo, con perspectiva interpretativa y diseño de estudio de caso, empleando métodos como la revisión bibliográfica, el análisis inductivo y el análisis descriptivo; asimismo, se aplicaron entrevistas mediante cuestionarios estructurados y herramientas tecnológicas para el escaneo periódico de la red de datos, lo que permitió diagnosticar debilidades en la configuración, control de accesos y protección perimetral. Los resultados evidenciaron deficiencias significativas en la gestión de la seguridad y la necesidad urgente de implementar políticas formales respaldadas por tecnología especializada, destacándose la incorporación del appliance Fortinet 80E como solución integral para el control de amenazas, filtrado de tráfico y fortalecimiento de la infraestructura tecnológica. Se concluye que la adopción de políticas de seguridad apoyadas en herramientas tecnológicas robustas mejora considerablemente la protección de la información sensible de los pacientes y reduce los riesgos cibernéticos, siendo este modelo replicable en otros hospitales y organizaciones del sector salud. En relación con el estudio actual, esta investigación aporta un referente práctico y tecnológico que respalda la implementación de modelos de buenas prácticas en seguridad de la información hospitalaria, evidenciando que la combinación de diagnóstico organizacional y soluciones tecnológicas fortalece la gestión del riesgo y contribuye a la consolidación de un Sistema de Gestión de Seguridad de la Información (SGSI).

Según los resultados obtenidos por (Reyes, 2023). En la investigación titulada “Modelo de buenas prácticas para la calidad de atención del personal de enfermería del Instituto Nefro Urológico del Norte, Chiclayo” (2022), se tuvo como objetivo presentar un Modelo de Buenas Prácticas orientado a mejorar la atención brindada por el personal de enfermería en dicha institución. El estudio se desarrolló bajo un enfoque cuantitativo, de tipo descriptivo con carácter propositivo y diseño no experimental. La población estuvo conformada por 88 pacientes y la muestra por 85, a quienes se les aplicó la técnica de encuesta mediante el instrumento Caring Assessment Instrument (Care-Q) para evaluar la percepción sobre la calidad del cuidado recibido. Los resultados evidenciaron que el 41% de los pacientes tenía entre 60 y 69 años, el 66% eran hombres, el 74% estaban casados y el 64% contaba con educación secundaria; además, el 51% llevaba entre 1 y 5 años en tratamiento. En cuanto a la calidad de atención, el 58.3% la calificó como regular,

el 29.8% como deficiente y el 11.9% como aceptable, lo que refleja una percepción predominantemente intermedia y evidencia oportunidades de mejora en la prestación del servicio. Se concluyó que la calidad de atención requería fortalecimiento, proponiéndose un Modelo de Buenas Prácticas basado en la teoría interpersonal de Hildegard Peplau, estructurado en cuatro fases: orientación, identificación, aprovechamiento y resolución, con el fin de mejorar la relación enfermero–paciente y optimizar la experiencia asistencial. Este antecedente se relaciona con el estudio actual porque parte de un diagnóstico cuantitativo para sustentar la formulación de un modelo de mejora institucional, demostrando que la implementación de buenas prácticas fundamentadas teóricamente contribuye al fortalecimiento de la gestión y calidad en instituciones de salud.

Según los resultados obtenidos por (Cabello, 2022). La investigación tuvo como objetivo analizar e implementar tres iniciativas estratégicas de tecnologías de la información en el Centro Internacional de la Papa (CIP): un Sistema de Gestión de Seguridad de la Información (SGSI), una solución de firma electrónica y un sistema de gestión de servicios de TI bajo el marco ITIL, con la finalidad de fortalecer la transformación digital institucional y garantizar el alineamiento con los Objetivos de Desarrollo Sostenible (ODS). La metodología empleada fue de enfoque aplicado y descriptivo, basada en la gestión por proyectos, implementación de buenas prácticas internacionales (ISO 27001 para SGSI e ITIL para ITSM), atención a recomendaciones de auditoría, elaboración de políticas institucionales y adopción progresiva por parte de las áreas usuarias, todo ello en un contexto de trabajo remoto impuesto por la pandemia del COVID-19 durante los años 2019 y 2020. Entre los principales resultados se evidenció la aprobación e implementación de la política de seguridad de la información estructurada por dominios, la creación de una cultura organizacional orientada a la comprensión de responsabilidades en ciberseguridad, la adopción progresiva de la firma electrónica como mecanismo de no repudio y optimización de procesos de aprobación, y la modernización de la gestión de servicios TI mediante procesos de gestión de cambios, solicitudes y activos alineados a ITIL. Se concluye que el éxito de las iniciativas radicó en el alineamiento estratégico entre TI y la alta dirección, en la gestión del cambio organizacional y en la capacidad de adaptación ante restricciones presupuestarias y desafíos operativos derivados del trabajo remoto. En relación con el estudio

actual sobre seguridad de la información y modelos de buenas prácticas en entornos institucionales, esta experiencia demuestra que la implementación integrada de SGSI e ITSM no solo fortalece la gestión del riesgo y la gobernanza de TI, sino que también contribuye directamente a la eficiencia organizacional, continuidad operativa y sostenibilidad institucional, constituyéndose en un antecedente empírico relevante para investigaciones aplicadas en hospitales u organizaciones públicas que buscan mejorar su nivel de madurez en seguridad de la información.

Según los resultados obtenidos por (Sandoval, 2022), La investigación titulada “Desarrollo de un modelo de gestión de incidentes de TI basado en estándares de buenas prácticas para mejorar el servicio de TI en las Direcciones Regionales de Salud del Perú” tuvo como objetivo desarrollar un modelo que permita elevar la calidad del servicio de tecnología de la información en la gestión de incidentes dentro de las DIRESA, respondiendo a la interrogante sobre cómo optimizar dicho servicio en entidades públicas del sector salud. El estudio partió de la problemática relacionada con deficiencias en la identificación, tratamiento y control de incidentes tecnológicos, así como la necesidad de incorporar estándares sustentados en buenas prácticas de ingeniería de seguridad y normativas gubernamentales para garantizar la protección de los datos institucionales. Metodológicamente, adoptó un enfoque aplicado con estrategia de ingeniería, sustentado en la revisión de teorías y modelos previos, a partir de los cuales se estructuró un modelo compuesto por las fases de recepción, registro, diagnóstico, resolución y cierre del incidente. El modelo fue implementado en un caso de estudio en la DIRESA Piura y evaluado mediante una encuesta aplicada a los trabajadores de la institución para medir el nivel de satisfacción respecto al servicio de TI. Los resultados evidenciaron que los incidentes fueron adecuadamente filtrados y gestionados a través de formularios establecidos en cada fase del proceso, logrando proporcionar soluciones organizacionales efectivas; asimismo, se obtuvo un nivel de satisfacción del 74.38 %, ubicándose en la categoría de “Bueno”. En conclusión, el estudio demostró que la adopción de un modelo basado en estándares de buenas prácticas mejora la gestión de incidentes y fortalece la calidad del servicio de TI en el sector salud, constituyéndose en un antecedente relevante para investigaciones orientadas a la implementación de modelos de buenas prácticas y Sistemas de Gestión de

Seguridad de la Información (SGSI) en hospitales públicos, como el Hospital Nivel II La Caleta, al evidenciar que la estructuración formal de procesos tecnológicos contribuye a la reducción de riesgos y al fortalecimiento de la seguridad organizacional.

Según los resultados obtenidos por (Villegas, 2022). En la investigación titulada Modelo de gestión de riesgos de TI que contribuye en la protección de los activos de información en hospitales de nivel II-I de la región Amazonas, se tuvo como objetivo principal diseñar un modelo de gestión de riesgos de tecnologías de la información orientado a proteger los activos informativos en hospitales de dicho nivel, debido a que estas instituciones enfrentan constantes incidentes relacionados con el uso inapropiado de los activos tecnológicos y la falta de conocimiento sobre riesgos tanto por parte de los usuarios como de la alta dirección. La metodología empleada fue de enfoque aplicado y propositivo, iniciándose con un diagnóstico situacional en hospitales seleccionados, seguido de un análisis comparativo de marcos y estándares de gestión de riesgos en TI, los cuales fueron adaptados al contexto del sector salud. El modelo propuesto fue validado mediante juicio de cinco expertos, utilizando el alfa de Cronbach para determinar su confiabilidad y el coeficiente de concordancia de Kendall para medir la consistencia de las evaluaciones. Tras su validación, el modelo se implementó en un hospital de nivel II-I de la muestra, donde se identificaron 258 riesgos asociados a los activos informáticos, de los cuales 137 fueron clasificados como críticos para su tratamiento, y se formularon 11 proyectos orientados a la supervisión y mejora de la gestión de riesgos. Los resultados evidenciaron que la aplicación sistemática del modelo permite identificar, priorizar y tratar riesgos de manera estructurada, fortaleciendo la protección de los activos críticos y promoviendo una cultura de gestión de riesgos en el ámbito hospitalario. Este antecedente se relaciona directamente con el estudio actual, ya que sustenta la necesidad de implementar modelos de buenas prácticas en la gestión de la seguridad de la información en hospitales de nivel II, aportando bases metodológicas y empíricas para el diseño de estrategias que reduzcan vulnerabilidades y mejoren la protección de la información institucional.

Según los resultados obtenidos por (Villanueva, 2021), La investigación titulada “Implementación de un Sistema Informático para mejorar la atención de pacientes

en los servicios de Emergencia y Hospitalización del Hospital Carlos Lanfranco La Hoz” tuvo como objetivo principal diseñar e implementar un Sistema de Gestión Hospitalaria que permita optimizar el manejo de la información clínica y administrativa, garantizando seguridad, integridad, disponibilidad y accesibilidad de los registros médicos electrónicos, con el fin de mejorar la calidad del servicio y la eficiencia operativa. La metodología empleada fue de tipo aplicada, con enfoque tecnológico y diseño preexperimental, iniciando con un diagnóstico situacional del sistema informático existente, el análisis de requerimientos funcionales y no funcionales, el modelado del nuevo sistema y su posterior implementación y evaluación en los servicios de Emergencia y Hospitalización. Entre los resultados principales se evidenció que el sistema anterior presentaba limitaciones en seguridad, capacidad de procesamiento, conectividad e integración tecnológica, lo que generaba reprocesos, demoras en la atención, falta de acceso oportuno a historias clínicas, dificultades en el control concurrente de la Unidad de Seguros y riesgos económicos frente a las IAFAS; tras la implementación del nuevo sistema, se logró centralizar la información, facilitar el acceso seguro a los registros clínicos, reducir tiempos de espera, mejorar el control de prestaciones y optimizar la coordinación entre áreas como Diagnóstico y Farmacia, especialmente en el contexto de la pandemia por COVID-19. En conclusión, el estudio demuestra que la implementación de un Sistema de Gestión Hospitalaria moderno y seguro impacta positivamente en la eficiencia institucional, la calidad de atención y la sostenibilidad financiera, al reducir errores, reprocesos y riesgos de auditoría. La relación con el estudio actual radica en que ambos trabajos abordan la necesidad de fortalecer la gestión de la información hospitalaria mediante modelos tecnológicos que integren seguridad de la información, disponibilidad y control de procesos, constituyendo un antecedente directo para investigaciones orientadas a mejorar la gestión de la seguridad y el riesgo en hospitales de nivel II bajo un enfoque de buenas prácticas o SGSI.

Según los resultados obtenidos por (Izquierdo, 2021). La investigación titulada “Modelo basado en la gestión de seguridad de la información para contribuir en los procesos de las farmacias de los hospitales II-I en la región Amazonas” tuvo como objetivo desarrollar un modelo de gestión de seguridad de la información alineado y armonizado con los procesos operativos de las farmacias hospitalarias de nivel

II-I, buscando fortalecer la protección de los activos críticos y mejorar la eficiencia en la gestión de riesgos. La metodología empleada fue de enfoque aplicado y diseño descriptivo-propositivo, basada en la armonización de estándares de gestión de seguridad de la información, estructurando el modelo en cuatro fases, catorce procesos, seis subprocesos, quince plantillas y una herramienta de seguimiento y control. Para validar su funcionalidad, el modelo fue sometido a evaluación por expertos en la materia mediante indicadores técnicos, alcanzando un nivel de aceptación del 91%, lo que evidenció su pertinencia y viabilidad. Posteriormente, se realizó una aplicación piloto en un hospital de muestra, donde se efectuó un diagnóstico previo para identificar la situación problemática y obtener una visión integral del estado de los procesos farmacéuticos. Los resultados principales demostraron una mejora significativa en la gestión de la seguridad de la información, especialmente en la identificación y protección de activos críticos, así como en la implementación de un plan de mejora continua orientado a mantener y superar el nivel de control alcanzado. Se concluye que el modelo propuesto es funcional, adaptable y aplicable en entornos hospitalarios de nivel II-I, contribuyendo al fortalecimiento del control interno y la gestión del riesgo informático. En relación con el estudio actual, esta investigación sirve como base conceptual y metodológica, ya que demuestra la efectividad de un modelo estructurado de buenas prácticas en contextos hospitalarios, aportando evidencia empírica sobre la influencia positiva de la gestión sistemática de la seguridad de la información en la mejora de procesos organizacionales.

Según los resultados obtenidos por (Correa, 2020). La investigación titulada “Manual de Buenas Prácticas en Seguridad de la Información para entornos hospitalarios” tuvo como objetivo principal diseñar un manual de buenas prácticas que permita fortalecer la protección de la información en instituciones hospitalarias de primer y segundo nivel en Colombia, considerando la alta vulnerabilidad del sector salud frente a ataques informáticos y la exposición de datos sensibles como la información clínica protegida. La metodología empleada fue de enfoque descriptivo–propositivo, desarrollada en tres etapas: una revisión bibliográfica de normas, protocolos y directrices internacionales de seguridad de la información; la construcción del manual basado en estándares y lineamientos técnicos; y finalmente su evaluación para validar su aplicabilidad en el contexto hospitalario

colombiano. Los resultados principales evidencian que el sector hospitalario es altamente vulnerable debido a la configuración de sus sistemas, la interacción constante de múltiples usuarios y el alto valor comercial de los datos médicos, lo que incrementa riesgos como accesos no autorizados, interrupciones del servicio, pérdidas económicas y afectación reputacional. Como conclusión, el estudio determina que la implementación de un manual estructurado de buenas prácticas permite reducir vulnerabilidades, fortalecer la gestión de riesgos y mejorar la protección de la información clínica, contribuyendo a la continuidad operativa y a la confianza institucional. La relación con el estudio actual radica en que proporciona un modelo base para estructurar propuestas de mejora en la gestión de la seguridad de la información en hospitales, especialmente en investigaciones que buscan evaluar la influencia de modelos de buenas prácticas o implementar un SGSI bajo estándares como ISO 27001 en establecimientos de salud.

1.3 Formulación del problema de investigación

Todo lo descrito anteriormente constituye la situación problemática que da origen al siguiente problema científico:

¿En qué medida un modelo de buenas prácticas permite gestionar la seguridad de la información en hospitales Nivel II, caso la Caleta?

1.4 Delimitación de estudio

El estudio consideró el hospital la Caleta nivel II, Chimbote.

1.5 Justificación e importancia de la investigación

La presente investigación se justifica de forma operativa porque mediante la implementación de un modelo de buenas prácticas ayudara a mejorar la seguridad de Información en los hospitales Nivel II se conseguiría minimizar considerablemente el riesgo donde su productividad se vea afectada debido a la ocurrencia de un evento que comprenda la confidencialidad, disponibilidad e integridad de la información o de alguno de los sistemas informáticos. Logrando reducir las amenazas que puedan afectar los procesos “Core” de los hospitales Nivel II, caso Hospital La Caleta y, en caso se logre materializar, que los daños que

pueda ocasionar sean mínimos, de tal manera que apoye a la continuidad del negocio.

Con respecto a la justificación social podemos decir que la implementación de un Sistema de gestión de la seguridad de la información para los Hospitales Nivel II beneficiará a sus trabajadores y sus clientes porque ayudara a mantener segura la información que se encuentra almacenada y que frecuentemente es procesada cuando es requerida para la toma de decisiones que son realizadas por los diferentes niveles jerárquicos de los Hospital Nivel II, caso La Caleta, convirtiéndose de esta manera en un proyecto de impacto social.

Con respecto a la justificación económica habrá un ahorro significativo en recursos económicos, recursos humanos y también en recursos materiales

En los hospitales Nivel II no se cuenta con mecanismos de protección de seguridad de los sistemas de información. Asimismo, el incremento de pérdidas de datos, debido a la vulnerabilidad tecnológica y ataques cibernéticos por parte de hacker hacen que los sistemas de información sean vulnerables, por esta razón se hace necesario que se implementen estrategias para la gestión de seguridad de información: generación, manejo, tratamiento y disposición final de estos datos.

La presente investigación pretende desarrollar una propuesta de modelo de buenas prácticas para aplicar la seguridad de la información que facilite la prevención, reducción, mediante la seguridad de los sistemas y de esta manera contribuya al desarrollo sustentable a la protección y conservación de los datos, contribuyendo a mejorar la calidad de vida de la población en el ámbito sanitario, social y económico.

El Modelo de buenas prácticas de seguridad de la información permite que los responsables en la toma de decisiones cuenten con un soporte de forma oportuna y aprovechen las oportunidades que ofrece el mercado, así como analizar el comportamiento y dinámica del sector, así mismo permite entender mejor a los usuarios, al mercado y demás factores que interactúan con sus instituciones. De ahí radica la importancia de contar con modelos, plataformas, herramientas, esquemas y formas de trabajo para obtener la información relevante y oportuna.

1.6 Objetivos de la investigación

Objetivo general

Elaborar un modelo de buenas prácticas para gestionar la seguridad de la información en hospitales nivel II, caso hospital la Caleta.

Objetivos específicos

a) Conocer la seguridad de la información en el Hospital nivel II, la Caleta de Chimbote.

b) Caracterizar el modelo de buenas prácticas para gestionar la seguridad de información en hospitales nivel II, la Caleta Chimbote

c) Determinar la influencia del Modelo de las buenas prácticas en la gestión de la seguridad y el riesgo en el Hospital nivel II, la Caleta de Chimbote.

CAPÍTULO II

MARCO TEORICO

2.1. Fundamentos teóricos de la investigación

2.1.1. Modelo de gestión

Según (ISO/IEC 27001:2022), Un sistema de gestión es un esquema organizado que guía a una entidad en la programación, estructuración, supervisión y regulación de sus recursos (humanos, tecnológicos, económicos y procesos) con el propósito de lograr metas estratégicas de manera eficaz y duradera.

Este sistema establece el modo en que se realizan las decisiones, cómo se manejan los riesgos, de qué manera se evalúa el rendimiento y cómo se lleva a cabo la mejora continua de la entidad. En áreas como la salud o la tecnología de la información, el sistema de gestión resulta fundamental para garantizar calidad, seguridad y adherencia a las normativas.

Es un esquema o marco de referencia para la administración de una entidad. Los modelos de gestión pueden ser aplicados tanto en las empresas y negocios privados como en la administración pública.

2.1.2. Seguridad

(Samaniego, E., Ponce, J. 2021). La seguridad se define como una situación que otorga la posibilidad de estar libre de amenazas. Su propósito fundamental es resguardar contra los enemigos; por ejemplo, en el ámbito de un país, es vital resguardar su independencia, sus recursos y su población para prevenir agresiones.

En el contexto de una entidad, lograr un nivel apropiado de seguridad demanda la instauración de un sistema compuesto por múltiples capas que estén estratégicamente interconectadas y que compartan elementos en común. Por eso, es responsabilidad de la entidad garantizar que posea enfoques cuidadosamente diseñados y estructurados

Las ramas de seguridad abarcan:

• Área física: Se ocupa de salvaguardar a las personas, los bienes materiales y el entorno laboral

• Seguridad en las operaciones: Permite que las entidades realicen sus actividades cotidianas sin interrupciones.

• Seguridad en las comunicaciones: Resguarda los canales de comunicación y la tecnología dentro de una entidad

• Seguridad en red: Protege los dispositivos de la red, las conexiones y la información.

2.1.3 Seguridad Informática

Según (Faliero, 2023). La seguridad informática es una disciplina encargada de proteger los sistemas, redes, dispositivos y datos informáticos de accesos no autorizados, ataques maliciosos o errores que amenacen su funcionamiento. Integra medidas técnicas, legales y organizativas encaminadas a mantener la confidencialidad, integridad y disponibilidad de la información digital en infraestructuras tecnológicas complejas. En este sentido, cubre no sólo la protección del software y hardware, sino también las comunicaciones, bases de datos y servicios digitales que son importantes para las organizaciones. De forma complementaria, esta disciplina busca prevenir, detectar y dar respuesta a incidentes que puedan afectar la continuidad del negocio y la protección de datos, convirtiéndose en un componente estratégico de la gestión de riesgos tecnológicos en la era digital.

2.1.4. Seguridad de la información

(Aguilera y Ramos, 2023). Se refiere a un grupo de directrices, procedimientos y medidas diseñadas para salvaguardar los recursos informáticos contra riesgos tanto dentro como fuera de la organización, asegurando su privacidad, precisión y accesibilidad.

La protección de la información se describe como el conjunto de normas, procedimientos y medidas destinados a resguardar los recursos informativos de una entidad, con el objetivo de asegurar la privacidad, la calidad y el acceso a la información frente a peligros dentro y fuera de la organización, en contextos tanto

físicos como virtuales .Este enfoque capacita a las entidades a minimizar amenazas, garantizar la continuidad de sus operaciones y satisfacer las obligaciones legales y normativas relacionadas, transformándose en un componente clave para la gestión contemporánea de organizaciones .

(Peltier, 2023) La protección de datos es un conjunto sistemático de normas y métodos que busca resguardar la información de la organización frente a accesos no permitidos, alteraciones inadecuadas, divulgaciones o eliminaciones, en consonancia con las metas comerciales.

Según (ISO/IEC 27001:2022), El resguardo de datos en un hospital de II nivel sigue la regla de la C. I. A.: Confidencialidad, Integridad y Disponibilidad. Esto es clave para proteger la información de pacientes, temas administrativos y procesos de operación. La confidencialidad asegura que solo la gente autorizada vea los expedientes clínicos; la integridad comprueba que los datos no se modifiquen sin permiso al guardarse o enviarse; y la disponibilidad mantiene prendidos los sistemas del hospital para dar cuidados correctos y sin peligro a los enfermos. Poner en práctica buenas rutinas y normas internacionales de seguridad de la información reduce peligros, cumple leyes y optimiza el manejo de los centros de salud, asegurando que sigan funcionando y manteniendo la confianza de la gente.

La protección de la información consiste en un conjunto de principios, políticas, procedimientos y medidas que buscan resguardar la información contra accesos no permitidos, modificaciones inapropiadas, pérdidas o interrupciones. Su meta fundamental es asegurar la confidencialidad, integridad y disponibilidad de la información, sin importar el soporte en que se encuentre (digital, físico o verbal). En las organizaciones contemporáneas, especialmente en el ámbito de la salud, la protección de la información es esencial para salvaguardar datos sensibles, garantizar la continuidad del servicio y cumplir con regulaciones y requisitos legales.

(Whitman & Mattord, 2022) La protección de la información implica salvaguardar datos y sus componentes esenciales, abarcando los sistemas y equipos que manejan, almacenan y envían dicha información, a través de la implementación de métodos para gestionar riesgos y establecer medidas de seguridad.

(Von Solms & Van Niekerk, 2022) La protección de datos se entiende como un elemento clave en la administración de la organización, el cual tiene como objetivo garantizar un uso ético, fiable y seguro de la información a través de sistemas de supervisión, adherencia a normativas y administración de riesgos. Ver Tabla 5.

Tabla 5

Seguridad Informática VS Seguridad de la informacion

Seguridad Informática	Seguridad de la informacion
Seguridad informática: Se enfoca en proteger los sistemas informáticos (hardware, software, redes).	Se refiere a un grupo de directrices, procedimientos y medidas diseñadas para proteger los recursos informáticos de riesgos tanto dentro como fuera de la organización y para garantizar su privacidad, precisión y disponibilidad

2.1.5. Fundamentos de la Información

Según (ISO/IEC 27001:2022). Los principios de la gestión de la información son aquellos aspectos esenciales que aseguran que la información sea segura, accesible y valiosa para una entidad. Estos principios determinan la manera en la cual se debe manejar, resguardar y aprovechar la información, sobre todo en ámbitos sensibles como el de la salud, donde los datos tanto clínicos como administrativos son extremadamente delicados.

Los activos de información presentan muchos peligros: la divulgación o el robo de datos confidenciales, la manipulación, modificación de archivos, interrupción del acceso a los archivos y las transacciones o la destrucción completa de los mismos debido a causas naturales o provocadas por el hombre Los tres principios básicos de la gestión de seguridad, son: confidencialidad, integridad y disponibilidad (Confidentiality, Integrity, Availability o CIA), están controlados para implementar los mecanismos necesarios para proteger la información y salvaguardar la información de los tipos de ataques y amenazas. Por lo tanto, cualquier sistema de seguridad debe tener los tres principios del CID.

2.1.5.1 Confidencialidad: Solo personal autorizado debe acceder a esta información.

(Samaniego y Ponce, 2021). La Confidencialidad garantiza que únicamente el personal con permiso pueda acceder a los datos necesarios para realizar sus funciones, así que para mantener esta privacidad se requieren tres elementos:

a) Verificación de usuarios: Esto posibilita confirmar que quien ingresa a la información es realmente quien dice ser.

b) Administración de accesos: Asegura que la información solo sea utilizada por aquellos que tienen autorización para ello y de la manera establecida

c) Encriptación de datos: Impide que la información sea visible para quienes no tienen permiso, convirtiendo los datos de un formato legible a uno ilegible.

Este principio de protección ayuda a salvaguardar la información de la divulgación a personas o sistemas no autorizados, así que solo aquellos que poseen los derechos y privilegios pueden acceder a la información necesaria.

2.1.5.2 Integridad: Asegurar la exactitud e integridad de la información. En otras palabras, debe permanecer intacto (integra) y no sujeto a sufrir un accidente accidental o deliberado.

(Samaniego y Ponce, 2021). Se trata de asegurar que los datos se mantengan seguros y no se vean comprometidos, puesto que trabajar con datos incorrectos puede generar una serie de errores y conducir a decisiones erróneas. Para proteger la información, se deben considerar los siguientes aspectos:

a) Vigilar la red para identificar posibles infiltraciones.

b) Establecer procedimientos de auditoría para revisar los sistemas

c) Aplicar métodos de control de modificaciones.

d) Realizar copias de seguridad para preservar los datos.

La información se considera íntegra cuando es completa y sin alteraciones, por lo que cualquier daño o modificación a su estado original puede suceder durante su almacenamiento o transferencia debido a virus y malware diseñados para dañar los datos Por esta razón, una técnica fundamental para identificar un virus o malware es observar variaciones en la integridad del archivo, como el tamaño

2.1.5.3 Disponibilidad: Asegúrese de que los usuarios tengan acceso a información y recursos relacionados cuando sea necesario. En otras palabras, mientras sea necesario, debe ser accesible en cualquier momento.

(Samaniego y Ponce, 2021). La accesibilidad asegura que los datos sean accesibles para aquellos que los requieren; por eso, se deben llevar a cabo las acciones necesarias para que tanto los datos como las autorizaciones sean accesibles .Por ejemplo, un ataque DDoS puede inhabilitar un comercio virtual, mientras que los correos no deseados pueden impedir que los destinatarios adecuados reciban sus mensajes .Para evitar que estas situaciones ocurran, es esencial establecer acuerdos de niveles de servicio, implementar balanceadores de carga que reduzcan el efecto del DDoS, realizar copias de seguridad y contar con alternativas ante posibles situaciones que puedan afectar la disponibilidad de la información .

Figura 3

Principios fundamentales de la Seguridad confidencialidad, Integridad y Disponibilidad.

Nota: Fuente. (Samaniego y Ponce, 2021), Guía práctica para el desarrollo de planes de contingencia de los sistemas de información

2.1.6. Gestión de la seguridad de la Información

(Calder, 2022), en su libro Implementing Information Security Based on ISO/IEC 27001, enfatiza que la gestión de la seguridad de la información se implementa mediante la implementación de un sistema de gestión de seguridad de la información (SGSI), que permite crear controles basados en riesgos, monitorear su efectividad y promover la mejora continua. Este enfoque garantiza que la seguridad de la información no sea un acto aislado, sino un proceso continuo y mensurable según los estándares internacionales.

(Peltier, 2023). En su libro Information Security Risk Analysis, sostiene que la gestión de la seguridad de la información debe adaptarse a un entorno digital altamente dinámico donde el aumento de las ciber amenazas requiere una visión integral y proactiva. El autor enfatiza que la gestión moderna combina análisis de riesgos, cumplimiento legal y resiliencia organizacional, lo que permite a las instituciones responder eficazmente a los incidentes de seguridad y minimizar su impacto en las operaciones y la reputación.

Whitman y Mattord (2022) en su libro Principles of Information Security. La gestión de la seguridad de la información se entiende como un proceso sistemático encaminado a proteger los activos de información de la organización contra amenazas internas y externas, garantizando la confidencialidad, integridad y disponibilidad de la información. Señalan que esta gestión no se limita a controles tecnológicos, sino que integra políticas, procedimientos, estructuras organizacionales y concientización de los empleados, permitiendo alinear la seguridad con los objetivos estratégicos de la empresa.

Según (ISO/IEC 27001:2022). La Administración de la Seguridad de la Información comprende un conjunto de políticas, procedimientos, procesos y controles diseñados para salvaguardar la información de una organización contra amenazas tanto internas como externas, asegurando así la confidencialidad, integridad y disponibilidad de los datos. Este enfoque se basa en un sistema metódico que implica la identificación, evaluación y manejo de riesgos, lo que permite que la información, en particular la que es crítica y sensible, se maneje de forma segura y efectiva. En ámbitos como el sector de la salud, la administración de la seguridad de la información es esencial para proteger datos clínicos y

administrativos, garantizar la continuidad operativa y cumplir con las normativas y leyes aplicables.

Un marco ampliamente aceptado para la administración de la seguridad de la información es el Sistema de Gestión de Seguridad de la Información (SGSI), que ofrece directrices para establecer, aplicar, mantener y mejorar de manera continua la seguridad de la información dentro de una organización.

Todos los usuarios de computadoras, ya sean usuarios público o privado, tienen expectativas informales respecto a las computadoras: Cuando se presiona el botón de encendido, esperan que la computadora retendrá todos los datos restantes del día anterior; cuando envían un correo electrónico, esperan que llegue o transfiera a su destinatario legal dentro de un tiempo razonable; cuando Acceden a la base de datos salariales y esperan que el salario y el nombre del empleado. Es verdad, nada ha cambiado.

En resumen, los usuarios albergan una gran esperanza, pero desafortunadamente siempre no cumple con las expectativas: falla de hardware Puede perder los datos en el disco; el mensaje de correo electrónico y archivos adjuntos pueden ser interceptados por intrusos; empleados injustos con los muchos privilegios pueden manipular el acceso a las aplicaciones de nómina.

La mayoría de las expectativas informáticas se verán defraudadas sino se cumplen con las medidas de seguridad. Ya que la información está expuesta a innumerables amenazas y es necesaria protegerla. Son muchas probalidades de ocurrencia y riesgo como: espías externos, programas malignos y intrusos, empleados desmotivados o sobornados, fallos de hardware o de software, interrupciones en energía, fuegos, incendios e inundaciones, la lista sería interminable. La seguridad de la información es una disciplina que se ocupa de los riesgos dentro de los sistemas informáticos. En otras palabras, al aplicar sus principios, las medidas de seguridad que pueden responder a las amenazas que enfrentan los problemas de la organización se implementarán en el sistema informático: la información y los elementos de hardware y software que respaldan el activo. Esto no debe implementarse sin rima o medidas de seguridad (como cortafuegos o cifrado de datos) porque la tecnología o la tecnología es popular o porque se cree que sería más seguro hacerlo. Se trata más bien de evaluar los

riesgos reales a los que la información está expuesta y mitigarlos mediante la aplicación de las medidas necesarias y en el grado adecuado, con el fin de satisfacer las expectativas de seguridad generadas.

2.1.7. Sistemas de Información

(Laudon y Laudon, 2022). Los sistemas de información se definen como un conjunto organizado de componentes (personas, procesos, datos y tecnología) que interactúan para recopilar, procesar, almacenar y distribuir información para respaldar la toma de decisiones, la coordinación y el control dentro de una organización. En este sentido, señalan que los sistemas de información permiten no sólo automatizar las operaciones, sino también crear valor estratégico al mejorar la eficiencia operativa, facilitar el análisis de grandes cantidades de datos y fortalecer la competitividad de la organización. Asimismo, los autores destacan que los sistemas de información en el contexto digital actual están estrechamente integrados con la gestión del conocimiento, la ciberseguridad y la transformación digital y se convierten en un elemento clave para la sostenibilidad y el cumplimiento de los objetivos institucionales (Management Information Systems: Management the Digital Firm).

Según (Laudon & Laudon, 2022). Los Sistemas de Información (SI) constituyen una agrupación estructurada de individuos, procedimientos, datos y herramientas tecnológicas que se comunican entre sí para reunir, analizar, archivar y difundir información. Su objetivo principal es facilitar el proceso de toma de decisiones, la coordinación, el control y la administración de las organizaciones, lo que les permite aumentar la eficiencia tanto operativa como estratégica. En ámbitos como el sector salud, los sistemas de información son esenciales para asegurar la calidad, la puntualidad y la seguridad de la información tanto clínica como administrativa, como muestra la figura 4.

Los Sistemas de información tienen en común muchas cosas. En muchos casos están formados por equipos, personas y procedimientos.

Figura 4.

Sistemas de Información

Nota: Guía práctica para el desarrollo de planes de contingencia de los sistemas de información

La figura 4 nos muestra una dirección capaz que se puede considerar un Sistema de Información (SI) como una agrupación de elementos que interactúan para que la empresa pueda alcanzar sus metas beneficiosos. Los integrantes de un SI son los siguientes:

- Datos: En general se consideran datos tanto los estructurados como los no estructurados, las imágenes, los sonidos, etc.
- Aplicaciones: Se incluyen los manuales y las aplicaciones informáticas.
- Tecnología: El software y el hardware; los sistemas operativos; los sistemas de gestión de bases de datos; los sistemas de red, etc.
- Instalaciones: En ellas se ubican y se mantienen los sistemas de información.
- Personal: Los conocimientos específicos que ha de tener el personal de los sistemas de información para planificarlos, organizarlos, administrarlos y gestionarlos. Políticas de Seguridad de Información (PSI)

2.1.8. Aumento de los niveles de seguridad en las organizaciones

Whitman y Mattord (2022). Los crecientes niveles de seguridad en las organizaciones responden a la necesidad de proteger los activos de información frente a un entorno digital cada vez más complejo y expuesto a ciber amenazas

avanzadas. Las organizaciones han evolucionado desde enfoques reactivos hacia modelos integrales de seguridad de la información que incluyen controles técnicos, administrativos y físicos bajo la gestión de riesgos. Este aumento en el nivel de seguridad significa no sólo la implementación de tecnologías de protección, sino también el fortalecimiento de políticas, procedimientos y concientización de los empleados, que permita garantizar la confidencialidad, integridad y disponibilidad de la información. De esta manera, la seguridad se consolida como un componente estratégico que contribuye a la continuidad del negocio y la confianza de los stakeholders en el contexto organizacional actual.

La implementación de unas Políticas de Seguridad de Información", permite a las Organizaciones cumplir una gestión efectiva de los recursos de información críticos e instalar y administrar los mecanismos de protección adecuados, determinando qué conductas son permitidas y cuáles no son permisibles.

Esto redundará en una efectiva reducción de los niveles de riesgo y de las vulnerabilidades, lo cual, en definitiva, se traduce en ahorro de tiempo y dinero, genera mayor confianza y un fortalecimiento de la imagen institucional.

Planificación de actividades

A través del desempeño de diferentes participantes, las organizaciones pueden programar de manera efectiva las actividades que se llevarán a cabo para hacer que sus sistemas sean más seguros.

Esto es importante porque no solo garantiza que se cubran todas las áreas relevantes, sino que también se logran los objetivos.

2.1.9 Mejora Continua

(Aguilera & Ramos, 2023, La mejora continua es un enfoque sistemático que tiene como objetivo optimizar constantemente los procesos, productos y servicios de la organización identificando constantemente oportunidades de mejora, evaluando el desempeño y aplicando acciones correctivas y preventivas. Este concepto se basa en la retroalimentación continua, el aprendizaje organizacional y la participación activa de los stakeholders, la satisfacción con la calidad y la efectividad de los empleados. Desde el punto de vista de la gestión moderna, la

mejora continua no se limita a corregir errores, sino que es un proceso estratégico integrado a la cultura organizacional y alineado con los objetivos institucionales, que permite una adaptación efectiva a un entorno cambiante y competitivo.

La mejora continua es un método de gestión que se centra en optimizar constantemente los procesos, productos y servicios, a través de pequeñas modificaciones sistemáticas y duraderas en el tiempo. El propósito es mejorar la calidad, eficiencia y satisfacción del cliente, disminuyendo errores, desperdicios y riesgos. Este método se fundamenta en la valoración continua del rendimiento, el aprendizaje dentro de la organización y la implicación activa de los individuos que participan en los procesos.

2.1.10 Involucramiento

(Laudon y Laudon, 2022). La participación se refiere al grado en que los miembros de la organización participan activamente, están involucrados y se sienten responsables de los procesos, decisiones y resultados asociados con el uso y gestión de los sistemas de información. Según, la participación de los usuarios y del personal de gestión es un factor crítico en el éxito de los sistemas de información porque promueve la adopción de tecnología, mejora la calidad de los datos y fortalece el ajuste entre la tecnología y los objetivos organizacionales. Los autores también sostienen que cuando el compromiso es alto, se fomenta una cultura de corresponsabilidad y mejora continua, reduciendo la resistencia al cambio y optimizando el desempeño organizacional.

Usted es muy importante para la organización, por lo que debe participar en el cumplimiento de las Políticas de Seguridad de Información.

2.1.11 Conocimiento

(Alavi y Leidner, 2022). El conocimiento se define como el resultado de una integración sistemática de información, experiencia y comprensión contextual que permite a las personas interpretar la realidad y tomar decisiones efectivas en diferentes contextos organizacionales y sociales. Según el conocimiento, va más allá de los datos y la información, ya que incluye la capacidad humana de interpretar, utilizar y transformar la información en acciones significativas, especialmente en un entorno organizacional apoyado en la tecnología de la

información. En este sentido, el conocimiento puede ser tácito cuando puede documentarse y transferirse fácilmente, o tácito cuando reside en experiencias y habilidades individuales que son la base tanto del aprendizaje organizacional como de la creación de valor.

Necesario Conozca y comprenda las Políticas de Seguridad de la Información de su organización.

2.1.12 Marco conceptual

(Hernández-Sampieri y Mendoza, 2022), el marco conceptual permite al investigador organizar el conocimiento existente, evitar ambigüedades conceptuales y asegurar que la investigación se desarrolle dentro de un referente teórico claramente definido y adaptado a los objetivos y metodología de la investigación.

El marco conceptual viene a ser la representación general de la información que se utilizará en el proceso de investigación y que aporta una visión de conjunto para la investigación.

2.1.13 Proteger

Según (ISO/IEC 27001:2022), Proteger se refiere a la implementación de estrategias, directrices y procedimientos diseñados para evitar, disminuir o evitar daños, accesos no autorizados, pérdidas o modificaciones en relación con individuos, propiedades, datos o infraestructuras. En el contexto de la seguridad de la información, proteger significa resguardar los recursos contra peligros tanto internos como externos, asegurando que estos sean utilizados únicamente en conformidad con los propósitos y reglas definidas, así como manteniendo su continuidad y fiabilidad.

(Michael E. Whitman & Herbert J. Mattord, 2022). La defensa es una función central de la gestión de la seguridad de la información que se centra en desarrollar e implementar medidas de seguridad adecuadas para garantizar la prestación de servicios críticos y contener o limitar el impacto de posibles incidentes de seguridad. Esta función incluye controles técnicos, administrativos y físicos como control de acceso, sensibilización y formación del personal, protección de datos,

procedimientos operativos y mantenimiento de tecnologías de seguridad. Desde una perspectiva organizacional, Proteger asegura que los activos de información –personas, procesos, tecnología y datos– cuenten con mecanismos preventivos que reduzcan la probabilidad de que las amenazas se materialicen, contribuyendo directamente al logro de los objetivos del Sistema de Gestión de Seguridad de la Información (SGSI).

2.1.14 Los Virus Informáticos

Según (Valverde, 2025). Un virus informático es un programa malicioso diseñado para infiltrarse en los sistemas sin el consentimiento de los usuarios.

Estos programas se copian a sí mismos modificando archivos legítimos. Se distribuyen a través de medios extraíbles, correo electrónico y descargas de Internet.

Cuando están activos, pueden destruir datos importantes en su computadora. También pueden ralentizar significativamente el rendimiento del sistema.

Algunos virus están diseñados para robar información personal o contraseñas. Esto supone un riesgo tanto para las personas como para las organizaciones.

El propósito de un virus informático puede ser financiero o malicioso. Los creadores de virus suelen aprovechar las vulnerabilidades del software vulnerable.

Las actualizaciones periódicas ayudan a reducir la exposición a este tipo de amenazas. El término "virus" se utiliza porque estos programas actúan como agentes biológicos.

No todos los virus son iguales; Existen variantes con diferentes propósitos. Los antivirus modernos detectan patrones inusuales de archivos y procesos.

La higiene digital, como no abrir archivos sospechosos, es clave para la prevención. Un clic en un enlace malicioso puede provocar una infección.

Esto puede llevar a un compromiso total del sistema. Las copias de seguridad frecuentes reducen el impacto de un ataque.

La educación en seguridad digital es tan importante como las herramientas técnicas. Los virus informáticos evolucionan y se vuelven más complejos con el tiempo.

A medida que las redes crecen, también lo hacen los ataques. La cooperación internacional es esencial para combatir estos programas.

Los desarrolladores de software también desempeñan un papel en el fortalecimiento de las defensas. Comprender qué es un virus informático le ayudará a tomar decisiones más seguras.

Cada usuario es responsable de proteger sus dispositivos. Así, los virus informáticos son una amenaza constante en el mundo digital.

Según (William Stallings, 2024), un virus informático se define como un tipo de software malicioso diseñado para insertarse deliberadamente en otros programas, archivos o sectores del sistema con la intención de replicarse y realizar acciones no autorizadas que amenacen la confidencialidad, integridad y disponibilidad de la información. Según el autor, un virus se caracteriza por su capacidad de propagarse en respuesta a la intervención del usuario o a un evento del sistema, y se diferencia de otras amenazas como gusanos o troyanos en que requiere la activación del ordenador anfitrión. Stallings señala que los virus informáticos pueden modificar, destruir o alterar datos críticos, degradar el rendimiento del sistema y facilitar el acceso no autorizado a la infraestructura tecnológica. También destaca que estas amenazas representan un riesgo significativo para las organizaciones, ya que son capaces de eludir los controles de seguridad básicos si no existen políticas adecuadas de gestión de riesgos. En el contexto de la seguridad de la información, el autor destaca que los virus son una de las principales fuentes de incidentes de seguridad, especialmente en entornos donde no se utilizan mecanismos de actualización, control de acceso y notificación al usuario. Finalmente, Stallings confirma que una comprensión conceptual de un virus informático es esencial en el desarrollo e implementación de sistemas de gestión de seguridad de la información, ya que permite establecer controles preventivos, defectivos y correctivos de acuerdo con estándares internacionales como ISO/IEC 27001.

Según (Rodríguez Rodríguez, 2023). En el mundo digital, un virus informático es un programa malicioso diseñado para infiltrarse y multiplicarse en sistemas o archivos sin el consentimiento del usuario, amenazando el normal funcionamiento de dispositivos y redes. Estas sustancias nocivas actúan como virus biológicos: se

adhieren a programas legítimos, se propagan y provocan efectos no deseados. Un virus informático puede destruir datos, ralentizar los sistemas, cambiar la configuración o incluso permitir el acceso no autorizado a los ciberdelincuentes. La propagación ocurre cuando un archivo infectado se comparte, ejecuta o transfiere entre computadoras y redes. Muchas veces quienes lo padecen no detectan su presencia hasta que aparecen síntomas como errores, pérdida de información o comportamientos extraños. Los métodos de infección varían desde correos electrónicos engañosos hasta descargas de software no confiables. Una vez dentro, algunos virus se esconden para evitar ser detectados por los programas antivirus, lo que dificulta su eliminación. La educación digital y las herramientas de seguridad son esenciales para prevenir infecciones. El análisis continuo de amenazas ayuda a identificar patrones de comportamiento malicioso antes de que se conviertan en epidemias digitales. Las actualizaciones de software proporcionan parches que corrigen las vulnerabilidades utilizadas por estos virus.

Un virus informático es una amenaza activa en la era tecnológica actual, capaz de alterar la integridad y disponibilidad de los sistemas de información. Comprender su naturaleza, métodos de distribución y medidas preventivas es fundamental para proteger los datos personales y corporativos en un entorno cada vez más conectado. Es responsabilidad de los desarrolladores y usuarios finales mantener un ecosistema digital seguro y resiliente frente a estas constantes amenazas.

Según (Stallings, 2021). Los virus informáticos son softwares dañinos creados para comprometer dispositivos de computación sin el permiso del usuario, alterando su operación estándar. Se enlazan a documentos o aplicaciones legítimas y se propagan cuando el sistema ejecuta el archivo afectado. Sus objetivos pueden ir desde causar daños, modificar o borrar datos, hasta interrumpir servicios, robar información o permitir accesos no autorizados al sistema.

En la actualidad, los virus informáticos han experimentado un considerable desarrollo, fusionándose con otras variantes de malware como ransomware, spyware y troyanos, lo que potencia su capacidad de ocultarse y su efecto, especialmente en entornos críticos como los sistemas de salud, financieros y gubernamentales.

Cuando hablamos de virus informáticos decimos que es un software completo o fragmentos de un programa que tiene un conjunto de instrucciones sencillas o complejas que tiene como finalidad dañar o destruir la información o cambiar el funcionamiento de una computadora.

Un virus informático puede realizar muchas cosas como: Colisionar el computador, robo de la información, eliminar archivos, impresión de caracteres no deseados, evitar accesos a las Pc, bloqueo del acceso a los sistemas operativos y daño de programas dentro del computador.

2.1.15 Vulnerabilidad

Según (Aguilera, 2026). Una vulnerabilidad se define como una debilidad inherente en un activo, proceso, sistema o conjunto de controles que puede ser explotada por una amenaza interna o externa, con consecuencias adversas para la confidencialidad, integridad y disponibilidad de la información. la vulnerabilidad no debe entenderse sólo como una falla técnica, sino como una condición multidimensional resultante de la interacción de factores tecnológicos, humanos, organizacionales y regulatorios que, si no se abordan adecuadamente, aumentan el nivel de riesgo institucional. Desde esta perspectiva, las vulnerabilidades pueden manifestarse como una mala configuración del sistema, falta de políticas de seguridad, falta de capacitación del personal, deficiencias en los procedimientos operativos o controles inadecuados de monitoreo y respuesta. Aguilera sostiene que las vulnerabilidades no son incidentes aislados, sino estados latentes que permanecen en los sistemas hasta que una amenaza los activa, lo que explica por qué muchas organizaciones experimentan incidentes repetidos a pesar de contar con una infraestructura tecnológica avanzada. Además, el autor enfatiza que identificar y evaluar vulnerabilidades es un proceso continuo y estratégico en la gestión de la seguridad de la información, ya que se desarrollan continuamente bajo la influencia de cambios tecnológicos, nuevas formas de ataque y transformaciones de procesos organizacionales. En este sentido, una adecuada gestión de la vulnerabilidad nos permite reducir la superficie de ataque, fortalecer los controles preventivos y correctivos y apoyar la toma de decisiones basada en riesgos de acuerdo con los principios de los sistemas de gestión de seguridad de la información y estándares internacionales como ISO/IEC 27001.

Una vulnerabilidad es una debilidad en un activo.

2.1.16 Amenaza

Según (Ross, 2024). Una amenaza se define como cualquier circunstancia, evento o agente que puede explotar una vulnerabilidad y causar daño a los activos de información de una organización, afectando la confidencialidad, integridad o disponibilidad de la información. la amenaza no es solo un evento aislado, sino un factor dinámico resultante de la interacción de personas, procesos, tecnología y el entorno organizacional, aumentando su complejidad en los sistemas de información modernos. El autor señala que las amenazas pueden ser de origen natural, humano o tecnológico y pueden ser intencionadas o no, y las amenazas humanas intencionadas –como los ciberataques, el espionaje o el sabotaje– son las más críticas en el contexto digital actual. De manera similar, Ross explica que la globalización, el teletrabajo y la cada vez mayor interconexión de los sistemas han ampliado la superficie de exposición de las organizaciones, contribuyendo a la materialización de amenazas complejas y persistentes. En este sentido, las amenazas no deben analizarse de forma aislada, sino como parte de un escenario de riesgo que requiere identificación, análisis y tratamiento continuo. El autor enfatiza que comprender la naturaleza de las amenazas es un paso fundamental para la implementación efectiva de un Sistema de Gestión de Seguridad de la Información (SGSI), ya que permite establecer prioridades de control, distribuir eficazmente los recursos y fortalecer la resiliencia de la organización. Finalmente, Ross sostiene que la gestión proactiva de amenazas promueve la continuidad del negocio, el cumplimiento normativo y protege la confianza de las partes interesadas en un entorno cada vez más vulnerable y cambiante.

Según (Ali Dehghantanha, Mauro Conti, Tooska Dargahi, 2018). En el ámbito de la seguridad de la información, se define una amenaza como cualquier situación o evento que pueda impactar de forma adversa a sistemas, datos o procesos de tecnología de la información. Esto puede suceder a través de acceso ilegal, destrucción, alteración o interrupción de servicios.

Dicho de otra manera:

Una amenaza no debe ser vista necesariamente como un ataque consumado, sino como una circunstancia que podría provocar daño si se aprovecha una vulnerabilidad existente.

En el campo de la seguridad de la información y la ciberseguridad, este término se utiliza para categorizar y administrar riesgos antes de que se materialicen incidentes perjudiciales.

Una amenaza es una violación potencial de la seguridad. No es necesario que la violación ocurra para que la amenaza exista. Las amenazas “explotan” vulnerabilidades.

En el lenguaje informático, se denomina ‘amenaza’ a la violación de la seguridad (confidencialidad, integridad, disponibilidad o uso legítimo), tal como lo muestra la figura 5, que podría efectuar una persona, máquina, suceso o idea, dada una oportunidad. Un ataque no es más que la realización de una amenaza.

Figura 5.

Amenazas a Sistemas de Información

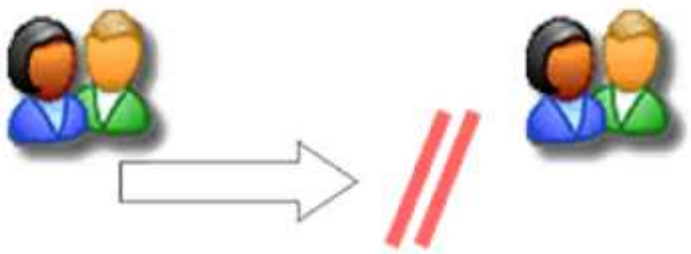
Nota. *Manual del Instructor de seguridad de la información*

Las cuatro categorías generales de amenazas o ataques son las siguientes:

2.1.17 Interrupción: Este es un ataque a los recursos del sistema que se destruyen o deshabilitan regularmente. Ver Figura 6. Por ejemplo, destruya el disco duro, corte la línea de comunicación o desactive el sistema de consulta

Figura 6.

Interrupción/Disponibilidad

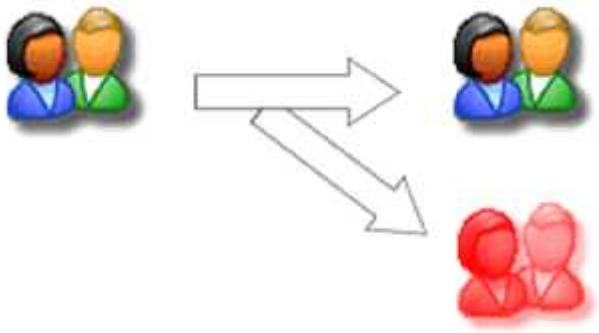


Nota: ARcert (2007), Manual del Instructor de seguridad de la información

2.1.18 Intercepción: Este es un ataque a una entidad que obtiene acceso a recursos no autorizados. Ver figura 7.Dicha entidad puede ser una persona, un programa o una computadora. Ejemplos de cuentos ataques son: interceptar una línea para obtener información y copiar ilegalmente archivos o programas distribuidos por la red, o leer el encabezado del mensaje para descubrir la identidad de uno o más usuarios que participan en la comunicación. Fue interceptado ilegalmente

Figura 7

Intercepción - Confidencialidad



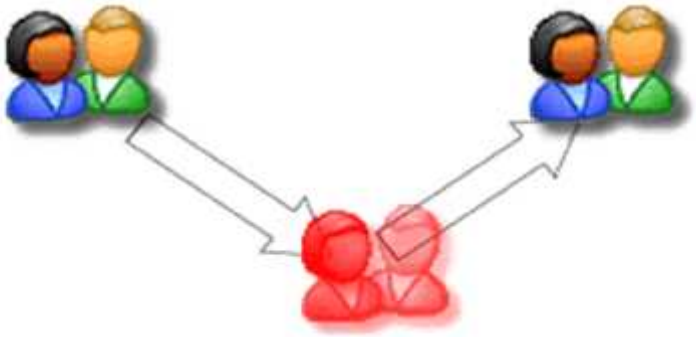
Nota. ARcert (2007), Manual del Instructor de seguridad de la información

2.1.19 Modificación: Este es un ataque de una entidad no autorizada que puede acceder a los recursos y modificarlos. Ver Figura 8.Ejemplos de ataques que incluyen cambios en los valores de los archivos de datos, cambios en los programas para

que funcionen de diferentes maneras y modificación del contenido de los mensajes transmitidos a través de la red.

Figura. 8.

Modificación - Integridad

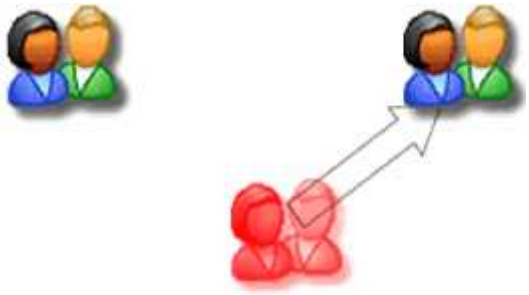


Nota. ARcert (2007), Manual del Instructor de seguridad de la información

2.1.20 Fabricación: Este es un ataque de una entidad no autorizada que agrega mensajes, archivos u otros objetos extraños al sistema. Ver figura 9. Ejemplos de ataques son insertar spam en la red o agregar registros a los archivos.

Figura 9.

Producción - Integridad



Nota: ARcert (2007), Manual del Instructor de seguridad de la información

2.1.21 Riesgo

Según (Martínez, 2024), se define como la posibilidad de que un evento ocurra y cause consecuencias negativas que afecten el logro de objetivos personales o sociales. El autor afirma que el riesgo no es simplemente una amenaza aislada, sino una interacción entre la probabilidad de un evento y el alcance de sus consecuencias, lo que significa que puede variar de persona a persona. Martínez señala que el riesgo no es necesariamente negativo, pues también puede representar oportunidades si se gestiona adecuadamente, pero centra su análisis en los riesgos que amenazan la seguridad, la salud o el bienestar. En este sentido,

el autor enfatiza la importancia de identificar, evaluar y priorizar riesgos para tomar decisiones informadas y reducir la incertidumbre. Además, enfatiza que el riesgo es una característica inherente a la actividad humana, ya sea en el trabajo, en la educación o en la vida cotidiana, y que su percepción depende de factores culturales, sociales y personales. Por ello, Martínez (2024) sostiene que comprender el riesgo desde una perspectiva individual permite que cada persona evalúe sus circunstancias y contextos, reconociendo sus limitaciones y fortalezas en relación a las amenazas potenciales. El autor también distingue entre riesgo objetivo y riesgo percibido, donde el primero es medible y el segundo está influenciado por las emociones y la experiencia personal. En general, la visión de Martínez ofrece un marco que ayuda a comprender de manera integral los riesgos, promoviendo la concientización y la preparación como herramientas clave para reducir los impactos negativos.

Según (ISO/IEC 27005:2022), La administración de riesgos en TI es un procedimiento organizado y permanente que tiene como objetivo detectar, examinar, valorar y gestionar los peligros que pueden influir en los activos informativos, la infraestructura tecnológica y los servicios digitales de una empresa. En el contexto institucional, especialmente en sectores críticos como el de la salud, esta gestión ayuda a prever amenazas, disminuir vulnerabilidades y reducir el efecto de incidentes tecnológicos que podrían poner en riesgo la continuidad operativa, la seguridad de la información y el cumplimiento de normativas. La implementación de metodologías reconocidas, basadas en controles técnicos, organizativos y legales, apoya la toma de decisiones fundamentadas, refuerza la capacidad de adaptación tecnológica y garantiza que los riesgos de TI se mantengan dentro de límites aceptables para la empresa.

2.1.22 Incidente

Según (Aguilera, 2025) en su obra Gestión Integral de Incidentes de Seguridad de la Información en Entornos Organizacionales, un incidente se define como cualquier evento inesperado o no deseado que compromete o tiene el potencial de comprometer la confidencialidad, integridad o disponibilidad de la información y de los sistemas que la procesan. El autor sostiene que un incidente no necesariamente implica un ataque exitoso, sino que puede tratarse de una vulnerabilidad explotada,

un error humano, una falla técnica o una acción deliberada que altera el funcionamiento normal de los procesos institucionales. Aguilera enfatiza que la identificación oportuna del incidente es fundamental para reducir su impacto operativo, financiero y reputacional, especialmente en organizaciones que dependen de infraestructuras tecnológicas críticas, como hospitales o entidades públicas. Asimismo, explica que un incidente debe analizarse desde una perspectiva sistémica, considerando sus causas raíz, los activos afectados, el nivel de riesgo asociado y las medidas de contención implementadas. El autor diferencia claramente entre evento e incidente, señalando que el primero es cualquier suceso observable en un sistema, mientras que el segundo implica una afectación real o potencial a la seguridad. Además, plantea que la gestión adecuada de incidentes requiere procedimientos documentados, equipos de respuesta especializados y mecanismos de monitoreo continuo. En este sentido, resalta la importancia de contar con políticas alineadas a estándares internacionales como ISO/IEC 27001 para fortalecer la capacidad de reacción institucional. Finalmente, Aguilera concluye que un incidente no debe entenderse solo como una amenaza, sino como una oportunidad de mejora, ya que su análisis permite fortalecer controles, actualizar protocolos y consolidar una cultura organizacional orientada a la prevención y resiliencia digital.

Según (ISO/IEC 27035-1:2023). Un incidente relacionado con la seguridad de la información se define como un suceso o una serie de acontecimientos inesperados o no deseados en el ámbito de la seguridad de la información que tienen una probabilidad considerable de poner en riesgo las actividades de la organización y de amenazar la protección de la información.

En otras palabras, no es suficiente con que algo suceda; debe contar con la capacidad de impactar la confidencialidad, integridad o disponibilidad de los datos o las operaciones de la empresa.

Los incidentes de seguridad son eventos adversos que pueden afectar los sistemas informáticos o las redes. Puede ser tratado por la falla de ciertos mecanismos de seguridad, intentos o amenazas (designadas o no especificadas) de romper el mecanismo de seguridad, etc.

2.1.23 Ciberataques

Según (Pérez, 2024). Los ciberataques son una de las amenazas más sofisticadas y dinámicas de la era digital actual, caracterizada por el uso de técnicas avanzadas para piratear sistemas, redes y dispositivos con fines disruptivos o maliciosos. En su sentido más amplio, un ciberataque incluye la intención de obtener acceso no autorizado a información, alterar o destruir datos y manipular infraestructuras tecnológicas críticas que respaldan el funcionamiento de gobiernos, empresas y servicios esenciales. La naturaleza de estos ataques ha cambiado significativamente durante la última década, pasando de simples intrusiones de bajo nivel a operaciones organizadas a gran escala con sofisticación técnica y objetivos estratégicos. Estas actividades pueden ser llevadas a cabo por individuos, grupos delictivos organizados o incluso entidades estatales, con motivos que van desde el beneficio económico hasta el espionaje político o la interferencia en procesos democráticos. Para comprender la dimensión de los ciberataques, es importante reconocer que no se limitan al robo de datos personales, sino que también pueden amenazar la integridad de los sistemas médicos, financieros y energéticos, provocando consecuencias tangibles en la vida cotidiana de millones de personas. Además, la rápida expansión y la interconexión global del Internet de las cosas (IoT) aumentan exponencialmente la superficie de ataque disponible para los adversarios digitales. Los mecanismos de defensa tradicionales, como los cortafuegos y los antivirus, ya no son suficientes por sí solos; Las organizaciones se ven obligadas a implementar estrategias de ciberseguridad más profundas, que incluyen inteligencia artificial, monitoreo continuo y capacitación humana especializada. Al mismo tiempo, la cooperación internacional en el ámbito de la ciberseguridad se ha consolidado como un elemento esencial para disuadir y mitigar las amenazas, ya que las fronteras digitales no coinciden con la geopolítica. En este contexto, la educación y la concientización sobre buenas prácticas de seguridad digital se han convertido en componentes críticos para reducir la vulnerabilidad individual y colectiva a ataques cada vez más sofisticados. Por lo tanto, los ciberataques no son sólo un desafío técnico, sino también un fenómeno social que requiere respuestas integrales de la tecnología, las políticas, la ética y la educación para proteger los activos y la privacidad en un mundo cada vez más conectado.

Según (García, 2024). Los ciberataques son una de las amenazas más importantes del siglo XXI, definido como acciones deliberadas de individuos o grupos para comprometer sistemas, red o datos con fines maliciosos para robar información, causar daño o influir en procesos críticos. Según García (2024), estos ataques explotan vulnerabilidades debido a software, hardware o error humano para ingresar al entorno digital, causando consecuencias que van desde pérdidas financieras hasta el colapso infraestructura. El autor explica que el desarrollo tecnológico ha ampliado la superficie de ataque al permitir que actores estatales y criminales trabajar con mayores recursos y sofisticación. Ataques de ransomware, . Roban datos críticos y exigen pago por su liberación, afectando a empresas y usuarios. Asimismo, los ataques de denegación de servicio (DDoS).

Pueden paralizar todos los servicios en línea, interrumpir las operaciones y las comunicaciones. García destaca que la ingeniería social, al igual que el phishing, explota la confianza humana para engañar a las personas y obtener acceso no autorizado subrayando que la ciberseguridad no es sólo un problema técnico, sino también educativo. El autor enfatiza la necesidad de estrategias integrales que combinen tecnologías, políticas claras y capacitación continua para anticipar y mitigar amenazas. También señala que la cooperación internacional es muy importante la naturaleza global de los ciberataques, ya que no están limitados por fronteras físicas acciones de los atacantes. Aquí es donde entra en juego la resiliencia digital la prioridad de gobiernos y organizaciones, obligándolos a invertir en sistemas robustos y protocolos de respuesta rápida. García concluye que, Si bien la prevención completa de los ciberataques es imposible, la preparación es necesaria Un seguimiento adecuado y una ciberinteligencia pueden reducir significativamente su impacto, proporcionar un entorno digital más seguro para todos. Puedo adaptarme a un estilo académico, técnico o más sencillo si lo prefieres.

2.1.24 CIBERATAQUES MAS COMUNES

Según (Steinberg, 2022). Los ciberataques más comunes son acciones maliciosas realizadas por atacantes para dañar, interrumpir o robar información de sistemas informáticos, redes y dispositivos conectados

a Internet. Estos ataques incluyen métodos como malware, phishing, ransomware, robo de datos y denegación de servicio (DDoS).

El "malware", que es todo aquello que se considera un software malicioso que entra al sistema de manera inadvertida con un propósito específico y no deseado. La Tabla 6 muestra una variedad de tipos dentro de esta definición.

T**abla 6**

Tipos de malware

Tipo de Ciberataque	Descripción	Ejemplos Famosos (2019-2024)
Phishing	Engaños para robar credenciales, datos bancarios o información sensible.	2022: Phishing masivo simulando notificaciones de bancos europeos. 2023: Ataques de phishing a empresas con suplantación de CEO (“CEO fraud”).
Ransomware	Malware que cifra archivos o sistemas y exige rescate.	2022: Ataques a empresas de logística y salud en EE. UU. y Europa. 2023: Brecha masiva de la compañía japonesa de videojuegos Capcom.
Malware / Virus / Troyanos	Programas maliciosos que dañan o controlan sistemas.	2022: Uso de malware BazarLoader en empresas financieras. 2023: Ataques de malware a dispositivos IoT en hogares y oficinas.
Robo de datos / Ataques a credenciales	Explotación de accesos o filtración de información sensible.	2022: Fuga de información en la

		cadena de hoteles Marriott. 2023: Robo masivo de datos de usuarios de Discord y Reddit.
Ataques DDoS (Denegación de Servicio)	Saturar redes o servicios para dejarlos inoperables.	2022: DDoS a bancos europeos y servicios financieros online. 2023: Campañas DDoS contra gobiernos de Europa del Este.
Ataques a la cadena de suministro	Infiltración mediante software o proveedores para afectar a múltiples víctimas.	2022: Vulnerabilidades explotadas en proveedores de servicios en la nube. 2023: Brechas vía software de gestión empresarial en Asia y Europa.

Nota: Tipos de Malware (Elaboración propia, 2026).

Los ataques más comunes combinan phishing + malware/ransomware, mostrando que la ingeniería social sigue siendo la puerta de entrada más utilizada. Además, la tendencia de ataques a la cadena de suministro y DDoS masivos ha crecido en complejidad y alcance.

2.1.25 Ciberseguridad

Según (Robin Sharp, 2024), La ciberseguridad se define como el conjunto de enfoques, herramientas y procesos destinados a salvaguardar los sistemas informáticos, las redes y la información contra accesos no autorizados, ataques, fallos y cualquier acción que pueda poner en riesgo la confidencialidad, la integridad y la disponibilidad de los datos en entornos digitales .Esta área es crucial en la actualidad debido al crecimiento acelerado del uso de internet, dispositivos

interconectados y servicios en la nube, que han ampliado las oportunidades y también los peligros en el entorno cibernético. En el libro Introduction to Cybersecurity: A Multidisciplinary Challenge la ciberseguridad se describe como un reto que abarca múltiples disciplinas, integrando elementos técnicos, éticos y legales para resguardar la infraestructura digital a nivel global y reducir los riesgos relacionados con ciberataques en diversas áreas de la sociedad.

Según (Sam Grubb, 2021). La seguridad informática abarca las técnicas, herramientas y procedimientos diseñados para salvaguardar sistemas computacionales, redes y datos contra accesos indebidos, amenazas maliciosas y otros peligros digitales, con la finalidad de asegurar la privacidad, integridad y accesibilidad de la información en un contexto cada vez más conectado

2.1.26 Cloud Security / Arquitectura de Seguridad en la Nube

Según (Nolle, 2023). La seguridad en la nube es un conjunto integral de políticas, controles, tecnologías y prácticas de TI diseñadas para proteger datos, aplicaciones, plataformas e infraestructuras que operan en entornos de computación en la nube. Una arquitectura de seguridad en la nube define cómo se estructuran y aplican estos controles para garantizar confidencialidad, integridad y disponibilidad (CIA) en entornos SaaS, PaaS e IaaS, soportando estrategias como IAM (Identity and Access Management), cifrado de datos, detección de amenazas, cumplimiento normativo y un modelo de responsabilidad compartida entre proveedor y cliente. Esta arquitectura también incorpora enfoques como Zero Trust para reforzar controles de acceso en entornos distribuidos.

2.1.27 Dispositivo Médico

Según (Carr, 2022). Un dispositivo medico abarca cualquier instrumento, dispositivo, equipo, software, implante o sustancia que el fabricante destina a su uso en personas para diagnóstico, prevención, vigilancia, tratamiento o alivio de una patología o lesión, y cuyo efecto primordial no se obtiene mediante medios farmacéuticos, inmunológicos o metabólicos, aunque pueda complementarse con ellos, los dispositivos médicos forman la base tecnológica de los sistemas de salud contemporáneos, ya que facilitan desde la evaluación de signos vitales hasta intervenciones quirúrgicas avanzadas, y están sujetos a rigurosos estándares

globales de calidad y seguridad con el fin de asegurar la protección del paciente y la eficacia clínica .

Según (Hemanth, 2022). Un Dispositivo médico se define como cualquier instrumento, herramienta, equipo, software, implante o material que, según el fabricante, está diseñado para ser usado en humanos para diagnosticar, prevenir, supervisar, tratar o aliviar una enfermedad o lesión. Esta función no se lleva a cabo a través de medios farmacológicos, inmunológicos o metabólicos, sino mediante métodos físicos o tecnológicos. Los dispositivos médicos contemporáneos incorporan sensores, conectividad y análisis de datos para mejorar la precisión en la clínica, la seguridad de los pacientes y la gestión dentro de hospitales, especialmente en entornos digitalizados donde la interoperabilidad y la ciberseguridad son aspectos cruciales .Este enfoque subraya que los dispositivos médicos actuales no solo desempeñan roles asistenciales, sino que son parte de ecosistemas tecnológicos complejos en los sistemas de información de salud .

Según (OMS, 2014). La Organización Mundial de la Salud (OMS) describe un dispositivo médico como "un objeto, herramienta, aparato o máquina que se utiliza para prevenir, diagnosticar o tratar enfermedades o condiciones, así como para detectar, medir, restaurar, corregir o alterar la estructura o función del cuerpo con fines de salud". Generalmente, el uso de un dispositivo médico no se logra mediante métodos farmacológicos, inmunológicos o metabólicos

Los dispositivos médicos son esenciales para garantizar que la prevención, diagnóstico, tratamiento y rehabilitación de enfermedades y condiciones de salud sean eficaces y seguros. En el contexto de los objetivos de desarrollo sostenible, alcanzar la meta de salud y bienestar depende en gran medida de que estos dispositivos sean diseñados, fabricados, regulados, evaluados, adquiridos, gestionados y utilizados de forma segura y adecuada a su entorno de aplicación.

Según (INNDUX, 2020). Muchos de estos dispositivos utilizan algún tipo de software para su funcionamiento y están conectados a una red, lo que permite que se realicen configuraciones o actualizaciones de manera remota; así como añadir, controlar o eliminar funciones e ingresar o extraer datos desde otros dispositivos.

Desde dispositivos implantados hasta escáneres de cuerpo completo, el número de dispositivos médicos conectados a la red está aumentando rápidamente, debido a los importantes beneficios en términos de información y toma de decisiones que ofrece tanto para los pacientes como para las instituciones de salud. No obstante, los ataques a dispositivos interconectados también están aumentando rápidamente, especialmente aquellos que realizan diagnósticos o controlan funciones vitales. Por esta razón, la ciberseguridad de los dispositivos médicos es una gran responsabilidad que requiere la colaboración de todos los involucrados, incluyendo fabricantes de estos dispositivos médicos, distribuidores, diversas agencias gubernamentales, instituciones de salud, profesionales de la salud, agencias de seguridad de la información, investigadores en ciberseguridad, usuarios de dispositivos médicos y sus cuidadores si los tienen.

2.1.28 INTEROPERABILIDAD DE EQUIPOS MÉDICOS

Según (Monteiro & Cruz-Correia, 2022). Es la capacidad de los dispositivos médicos para funcionar en conjunto dentro de sistemas de salud contemporáneos que posibilita la transmisión y el intercambio de información entre varios aparatos médicos y redes de información clínica, favoreciendo la integración confiable de datos clínicos producidos por equipos diversos y promoviendo resultados más efectivos en la atención de los pacientes .En este sentido, la interoperabilidad se describe como la habilidad de intercambiar y utilizar información entre equipos médicos y plataformas digitales de salud de manera segura y eficiente, lo cual es fundamental para mejorar la calidad de la atención y respaldar decisiones clínicas en tiempo real

2.1.29 Historia Clínica Electrónica.

Goldstein (2023). Define la historia clínica electrónica (Electronic Health Record, EHR) como “la recopilación organizada de información médica de un individuo, que se guarda en formato digital y se puede compartir y analizar en diversos entornos de atención médica”, abarcando información personal, historial médico, resultados de pruebas, tratamientos y otros datos importantes para garantizar la continuidad y la calidad del cuidado médico. Estos registros digitales no solo sustituyen la

documentación en papel, sino que también permiten la interoperabilidad, la coordinación entre los proveedores de salud y el uso de la información para la investigación y la toma de decisiones clínicas, promoviendo una atención más segura y eficaz.

Según el (Ministerio de Salud, 2009). Una Historia Clínica Electrónica (HCE) es un registro médico digital que abarca de manera integral, estructurada y segura la información de salud de un individuo, abarcando datos clínicos, diagnósticos, tratamientos, resultados de laboratorio y notas de atención. Este registro es creado y modificado por profesionales de la salud que tienen autorización, se almacena en sistemas informáticos específicos y se accede a través de métodos que aseguran la protección, privacidad, integridad y disponibilidad de la información, facilitando una atención continua y coordinada entre distintos servicios y centros de salud.

2.2. Marco conceptual

2.2.1 SEGURIDAD INFORMATICA

Según (Faliero, 2023), Describe la seguridad informática como el conjunto de métodos, estrategias y normativas diseñadas para resguardar los sistemas informáticos, redes y datos de accesos no permitidos, abusos de debilidades y otras formas de riesgos cibernéticos, con el objetivo de proteger la confidencialidad, integridad y disponibilidad de la información en contextos digitales actuales.

Según (Whitman & Mattord, 2022). La seguridad informática se refiere al conjunto de estrategias, herramientas y métodos diseñados para salvaguardar los recursos informáticos contra riesgos en el ámbito digital, garantizando la privacidad, consistencia y acceso a la información a través de medidas técnicas, administrativas y físicas, además de la administración de riesgos dentro de las organizaciones para mantener un funcionamiento seguro en un contexto digital global.

2.2.2 SEGURIDAD DE LA INFORMACIÓN EN EL SECTOR SALUD

Según (Gupta, Kapoor, & Debnath, 2025). Con el aumento de la utilización de soluciones de inteligencia artificial en el sector salud, la protección de la información

se vuelve extremadamente importante. Las herramientas de IA pueden optimizar la seguridad de los datos del paciente, identificar riesgos en tiempo real y aumentar la reacción ante situaciones críticas, siempre que se utilicen con principios éticos y medidas de privacidad efectivas. Este tipo de protección avanzada tiene como objetivo asegurar que la información médica sensible no sea accesible para personas no autorizadas, sin comprometer la calidad del servicio ni la efectividad operativa en el ámbito de la salud.

Según (Herzmann, Lashkari & Parizadeh, 2024). La seguridad de información en el ámbito de la salud requiere una administración táctica y operativa de datos delicados, considerando factores como la defensa contra ataques cibernéticos, la preservación de la veracidad de los registros digitales, la privacidad del paciente y la adherencia a las leyes correspondientes. Los trabajadores del sector salud necesitan estar al tanto de los riesgos tecnológicos como de las medidas de defensa para crear políticas sólidas que prevengan filtraciones y aseguren la continuidad de los sistemas de salud digitalizados. Esta administración demanda una fusión de tecnologías, capacitación del personal y tácticas organizacionales para reducir riesgos y reaccionar de forma adecuada ante eventos de seguridad.

Según (Sharma, Lashkari & Parizadeh, 2024). La seguridad de la informacion de los datos en la industria de la salud no solo se encuentra con problemas clásicos como el acceso indebido o la pérdida de información, sino que también necesita ajustarse a desarrollos recientes como la telemedicina, los dispositivos interconectados y las amenazas sofisticadas como el ransomware. Las infraestructuras sanitarias actuales demandan métodos renovados de ciberseguridad que tomen en cuenta la evaluación de riesgos, la formación constante del personal y la adopción de Normas internacionales para salvaguardar de manera efectiva la privacidad y la disponibilidad de los datos clínicos.

Según (Reyes, Vera & Mendoza de los Santos, 2022). La protección de la información en el ámbito sanitario es esencial para asegurar la privacidad, la integridad y el acceso a los datos clínicos y administrativos que administran las instituciones de salud.

Los hospitales y clínicas tratan con información muy delicada, como historiales médicos electrónicos, diagnósticos, resultados de pruebas de laboratorio y datos identificativos de los pacientes, lo cual requiere su resguardo por motivos éticos y legales.

Desde el punto de vista de la tecnología de la información, los controles de seguridad en el ámbito de la salud deben ser abordada de manera holística, integrando controles técnicos, administrativos y organizacionales. Algunas de las acciones más importantes incluyen la gestión de acceso basada en roles, el uso de encriptación para datos almacenados y en tránsito, copias de seguridad regulares, planes para la continuidad del servicio y políticas claras para el uso de los sistemas de información en los hospitales. Además, la formación continua del personal sanitario es esencial, dado que el elemento humano representa una de las mayores fuentes de riesgo.

En el ámbito hospitalario, implementar estándares internacionales, como la norma ISO/IEC 27001, permite crear un Sistema de Gestión de Seguridad de la Información (SGSI) que se adhiera a las mejores prácticas reconocidas en todo el mundo. Esto ayuda a identificar, analizar y gestionar riesgos, lo que a su vez contribuye a reducir incidentes de seguridad, pérdidas de datos y afectaciones en la atención de los pacientes. Por lo tanto, una adecuada gestión de la seguridad de la información refuerza la confianza de los usuarios y eleva la calidad de los servicios de salud.

La seguridad de la información no se limita a la seguridad de datos en los computadores; en esencia, debe centrarse en proteger la propiedad intelectual y la información confidencial de las organizaciones y las personas. Cuando se combinan dos factores: amenazas y vulnerabilidades, se produce un riesgo de información. Las amenazas y las vulnerabilidades están relacionadas entre sí y no pueden existir sin la presencia de ambas. Las amenazas deben tomar ventaja de las vulnerabilidades y pueden venir de cualquier parte relacionada con el entorno de las organizaciones, interna o externa. Las vulnerabilidades son deficiencias en la tecnología o los procesos relacionados con la información y se consideran características específicas de los sistemas de información o de la infraestructura.

En términos simples, una amenaza es cualquier circunstancia o evento que pueda afectar directamente la posibilidad de que las personas o las organizaciones puedan desarrollar sus actividades afectando directamente la información o los sistemas que la procesan.

En general, podemos clasificar las amenazas a la información en cuatro categorías principales:

- ✓ Factores humanos (errores involuntarios)
- ✓ Desastres naturales,
- ✓ Fallas en los sistemas de procesamiento de información
- ✓ Acciones malintencionadas

J Algunas de estas amenazas incluyen

- ✓ Virus o código malicioso en los sistemas informáticos,
- ✓ Robo de información,
- ✓ Fraudes basados en el uso de computadores,
- ✓ Suplantación de identidad,
- ✓ Denegación de Servicios (DoS),
- ✓ Ataques de Fuerza Bruta,
- ✓ Alteración de la información, datos,
- ✓ Divulgación de información,
- ✓ Desastres naturales,
- ✓ Sabotaje,
- ✓ Vandalismo
- ✓ Espionaje.

2.2.3 BUENAS PRACTICAS

Según (Kerzner,2023). Las buenas prácticas son técnicas o métodos organizados que han demostrado ser más eficaces que otras opciones para lograr resultados exitosos en un contexto específico; en el ámbito de la gestión de proyectos, por ejemplo, las prácticas efectivas abarcan la clara definición de metas, la elaboración minuciosa de un plan de trabajo, la constante evaluación de riesgos y una comunicación clara entre los integrantes del equipo, lo que facilita la mejora en la

calidad, la disminución de errores y la optimización de recursos a lo largo de todo el ciclo del proyecto.

Según (Gómez & Luna, 2022). Las prácticas efectivas en la administración de proyectos son esenciales para lograr resultados que sean tanto eficientes como perdurables. Estas prácticas abarcan la definición precisa de metas, la comunicación fluida entre los integrantes del equipo, la revisión constante de posibles riesgos y la capacidad de ajustarse a las modificaciones que surjan a lo largo del proyecto. Asimismo, la adopción de enfoques fundamentados en evidencias y la utilización de herramientas que faciliten la colaboración contribuyen a elevar la calidad y la productividad, fomentando un ambiente laboral más estructurado y responsable.

Toda experiencia guiada por principios, objetivos, procedimientos o pautas aconsejables que se ajustan a una perspectiva normativa o a un parámetro consensuado, así como toda experiencia que ha producido resultados positivos, demostrando su eficacia y utilidad en un contexto específico, se considera "buenas prácticas".

El término "buenas prácticas" se usa en una variedad de contextos para referirse a las formas ideales de llevar a cabo un proceso, que pueden servir como modelo para otras empresas. Las buenas prácticas sistematizadas permiten aprender de las experiencias y aprendizajes de otras personas y aplicarlos en contextos más amplios. También pueden fomentar nuevas ideas o sugerir cambios y brindar una guía sobre la manera más efectiva de mostrar los diversos efectos de una intervención en las comunidades.

Los planteamientos actuales sobre los criterios de calidad y eficiencia de las intervenciones sociales, que abarcan no solo la gestión y los procedimientos, sino fundamentalmente la satisfacción de las necesidades de las personas afectadas y la superación de sus problemas, están directamente relacionados con la búsqueda de buenas prácticas.

Diversas organizaciones han ideado y seleccionado buenas prácticas con diferentes enfoques: inclusión social, perspectiva de género, trabajo con jóvenes,

urbanismo social, superación de conflictos, etc. Y cada una de estas propuestas utiliza diferentes puntos de vista y criterios para identificar y elegir las buenas prácticas. Podríamos decir que un programa, proyecto o intervención que cumpla con al menos una de las siguientes características sería una buena práctica al sistematizar los criterios comunes a todas las evaluaciones revisadas:

- Responden a una necesidad determinada, son el resultado de una evaluación minuciosa de una característica en una población específica que necesita ser modificada y mejorada, y por lo tanto tienen un objetivo claro, relevante y alcanzable.

- Desarrollan estrategias basadas en evidencia y son innovadores en su aplicación, demostrando capacidad de cuestionamiento y creatividad; Las estrategias y acciones parten de principios y valores básicos y responden a una visión o perspectiva definida del problema que atiende;

- Los recursos humanos que implementan la iniciativa están calificados y especializados;

- proponen un sistema riguroso de seguimiento a los procesos y resultados de la iniciativa.

- Cuentan con una amplia base de participación, principalmente de los beneficiarios y de la comunidad, con fuertes alianzas interinstitucionales. Pueden probar una mejora sustantiva de la situación que el dio origen. Incorpora estrategias de sostenibilidad de la iniciativa, propiciando su institucionalización. Sistematiza los procesos y resultados. De alguna manera fomenta la replicación de la experiencia.

- Las “Buenas Prácticas” en seguridad de la información, protegen a esta contra una amplia gama de amenazas, tanto de orden fortuito (destrucción parcial o total por incendio, inundaciones, eventos eléctricos y otros) como de orden deliberado, tal como fraude, espionaje, sabotaje, vandalismo, etc.

- Las buenas prácticas son recomendaciones o métodos probados que han demostrado ser eficaces en contextos reales, pero cuya adopción es flexible y no obligatoria; representan “formas recomendadas de actuar” basadas en la experiencia profesional y la mejora continua

2.2.4 Estándar

Según (Axelos, 2023). Los estándares son normas formales, generalmente emitidas por organismos internacionales, que establecen requisitos específicos, medibles y verificables que deben cumplirse para garantizar calidad, interoperabilidad o seguridad, pudiendo incluso dar lugar a certificaciones

2.2.5 Frameworks

Según (Axelos, 2023). Constituyen marcos estructurados de referencia que integran principios, procesos, roles y prácticas para guiar la implementación y gestión de un área determinada —como la gobernanza de TI o la seguridad—, ofreciendo una estructura metodológica adaptable más que requisitos obligatorios. Según ITIL 4 Edition, las organizaciones suelen combinar estos tres elementos: emplean frameworks para estructurar la gestión, estándares para asegurar cumplimiento y buenas prácticas para optimizar la operación según su contexto específico.

2.2.6 Activo de informacion

Según (Whitman y Mattord, 2022), un activo de información es cualquier dato o conjunto de datos que tiene valor para una organización y debe ser protegido independientemente del entorno en el que resida (digital, físico o verbal), incluidos registros médicos, bases de datos, documentos, conocimientos del personal o información estratégica.

2.2.7 Activo informático

Según (Whitman y Mattord, 2022), una instalación informática se refiere a los recursos tecnológicos que permiten almacenar, procesar o transmitir esta información, como servidores, computadoras, redes, sistemas operativos, aplicaciones y dispositivos de almacenamiento. Esto significa que un activo de TI es el soporte tecnológico, mientras que un activo de información es el contenido de valor que se gestiona y protege.

En la gestión de seguridad actual, la prioridad es identificar los activos de información porque son de valor real para la organización, mientras que los activos

de TI son componentes de infraestructura que facilitan su gestión y requieren controles para evitar el acceso no autorizado, la pérdida o alteración de los datos.

2.2.8 BUENAS PRÁCTICAS EN SEGURIDAD DE LA INFORMACIÓN

Según (Stallings, 2021) Las buenas prácticas de la seguridad de la informacion se componen de un conjunto de tácticas, normativas y procesos que ayudan a salvaguardar los recursos informáticos de una entidad contra amenazas, debilidades y peligros. Estas medidas abarcan la planificación y dirección de la seguridad, la revisión continua de los riesgos, la aplicación de controles tanto tecnológicos como administrativos, el aseguramiento de la privacidad, integridad y disponibilidad de la información, y la capacitación constante del personal para minimizar la posibilidad de accidentes. La adopción de estándares ampliamente reconocidos, así como de marcos de referencia y recomendaciones de buenas prácticas, facilita a las organizaciones en la gestión efectiva de sus políticas de seguridad, alinea sus metas comerciales con la protección de sus activos digitales y optimiza su capacidad de respuesta ante ataques o fallos en la seguridad.

Según (ISO/IEC 27002:2022). Las buenas prácticas adecuadas para la seguridad de la información, forman un conjunto ordenado de medidas organizativas, humanas, físicas y tecnológicas destinadas a reducir los peligros que puedan poner en riesgo la confidencialidad, la integridad y la disponibilidad de los datos .Esta normativa ofrece orientaciones para la instalación de medidas que respaldan un Sistema de Gestión de Seguridad de la Información (SGSI), en conformidad con los criterios establecidos en ISO/IEC 27001 .Su principio se centra en la gestión de riesgos, facilitando a las entidades la elección y aplicación de controles de acuerdo con el ambiente, tamaño, industria y grado de vulnerabilidad ante amenazas. La edición de 2022 reestructura los controles en cuatro áreas clave: organizacionales, humanos, físicos y tecnológicos, mejorando el enfoque contemporáneo hacia la ciberseguridad, la seguridad del entorno en la nube y la defensa contra incidentes como el ransomware y las filtraciones de datos

Así mismo (García-Moliner, 2023) Afirma que aplicar medidas de seguridad basadas en normas globales ayuda a reducir los problemas de seguridad y a

mejorar la administración de TI al combinar políticas, procedimientos y la cultura de la organización.

COBIT (Control Objectives for Information and Related Technology) en TI significa Objetivos de Control para la Información y Tecnologías Relacionadas.
El marco COBIT, que se refiere a los Objetivos de Control para la Información y Tecnologías Relacionadas, representa un esquema completo de supervisión y administración de las tecnologías de la información, con el fin de generar valor dentro de las organizaciones a través de la alineación entre las metas empresariales y los procesos tecnológicos. Creado por ISACA, COBIT 2019 presenta un conjunto organizado de principios, elementos y metas de gobernanza que facilitan la evaluación, dirección y monitoreo de la función de TI dentro de un sistema dinámico y integrado.

Desde el enfoque epistemológico, COBIT va más allá de la visión convencional del control interno, al añadir dimensiones de estrategia, riesgo y rendimiento, estableciéndose como un modelo para la gobernanza corporativa en TI .Este marco hace una clara distinción entre gobernanza y gestión, definiendo roles diferentes y favoreciendo la optimización del balance entre beneficios, riesgos y recursos tecnológicos .Por lo tanto, COBIT se establece como un estándar normativo y metodológico para la ejecución de sistemas de control, conformidad y aseguramiento dentro de ambientes organizacionales complejos, incluidos sectores muy regulados como el de la salud y el financiero .
ITIL (Information Technology Infrastructure Library). Es un conjunto de prácticas recomendadas enfocado en la administración de servicios de TI Su objetivo es sincronizar los servicios tecnológicos con las demandas estratégicas de la empresa, asegurando un servicio de calidad, eficacia y un progreso constante.

Según (Axelos, 2019), ITIL 4 define la gestión de servicios como "un conjunto de capacidades organizativas especializadas para entregar valor a los clientes en forma de servicios".

Según (Claire, 2020), ITIL promueve la co-creación de valor entre el proveedor de servicios y el usuario enfatizando principios como el enfoque en el valor, la mejora continua y la colaboración.

ITIL divide el ciclo de vida del servicio en cinco etapas:

- La identificación de los activos estratégicos de la empresa, que generan valor o la diferencian en el mercado, es la base de la estrategia del servicio.
- El objetivo del diseño de servicios es analizar la cartera de servicios para identificar sus debilidades y fortalezas y establecer estándares y políticas para mejorar su calidad.
- La operación del servicio tiene como objetivo administrar y controlar los procesos necesarios para la puesta en producción de un servicio.
- La transición del servicio cubre el proceso de cambio entre la mejora de servicios existentes o la creación de nuevos servicios si es necesario, según el diseño.
- La mejora continua del servicio tiene como objetivo mejorar la calidad del servicio ofreciendo retroalimentación constante sobre la estrategia, el diseño, la transición y las operaciones para facilitar la adaptación al entorno. Ver Tabla 7.

Tabla 7

comparaciones entre tecnologías

Elemento	COBIT	ITIL	ISO/IEC 27001
Concepto	Marco de gobierno y gestión de TI que integra control, riesgo, seguridad y alineación estratégica.	Marco de gestión de servicios de TI que incluye prácticas para garantizar disponibilidad, continuidad y seguridad.	Norma internacional para implementar un-Sistema de Gestión de Seguridad de la Información (SGSI).
Enfoque principal	Gobierno corporativo de TI y gestión de riesgo.	Gestión del servicio y mejora continua.	Protección de la confidencialidad, integridad y disponibilidad de la información.
Relación con seguridad	Incluye procesos de gestión de ries2.1.27 gos, control interno y cumplimiento normativo.	Integra la seguridad como práctica dentro del ciclo de vida del servicio.	Establece controles y requisitos para gestionar la seguridad basada en riesgos.
Tipo de estándar	Framework de gobierno de TI.	Framework de gestión de servicios.	Norma internacional certificable.

Objetivo en seguridad	Alinear TI con el negocio asegurando control y reducción de riesgos.	Garantizar servicios TI seguros y confiables.	Implementar, mantener y mejorar continuamente un SGSI.
Certificación	Certifica personas, no organizaciones.	Certifica personas, no organizaciones.	Certifica organizaciones mediante auditoría externa.

Nota: Elaboración Propia

2.2.9 Enfoque profesional de Tecnologías de la Información

(Health, 2021). Los sistemas de información hospitalarios son elementos esenciales dentro de las instituciones de salud, ya que se encargan de la gestión de datos clínicos, administrativos y financieros, necesarios para la atención al paciente y la toma de decisiones. La implementación adecuada de prácticas óptimas en tecnología garantiza la protección de la información, la continuidad de las operaciones y la calidad del servicio de salud.

Una de las prácticas esenciales es la gobernanza de TI, que garantiza que la tecnología esté alineada con las metas estratégicas del hospital. Marcos de referencia como COBIT ayudan a establecer responsabilidades, procesos y controles, favoreciendo una gestión clara y eficaz de los recursos tecnológicos.

Además, la seguridad de la información es una prioridad en el sector hospitalario, dado lo delicado de los datos clínicos. La adopción de un Sistema de Gestión de Seguridad de la Información, conforme a la norma ISO/IEC 27001, resguarda la confidencialidad, integridad y disponibilidad de la información, mitigando los riesgos de accesos no autorizados, pérdida de datos o ciber incidentes.

Otra práctica clave es la gestión de riesgos tecnológicos, que tiene como objetivo identificar posibles amenazas que puedan impactar la continuidad de los servicios de atención médica. La aplicación de normas como ISO 31000 ayuda a identificar, abordar y supervisar riesgos relacionados con fallos en los sistemas, desastres naturales o ataques cibernéticos.

La interoperabilidad y estandarización de los sistemas también es crucial. La adopción de normas internacionales como HL7 y DICOM permite un intercambio

seguro y eficaz de datos entre áreas clínicas, laboratorios y sistemas externos, mejorando la atención al paciente y disminuyendo errores médicos.

Por último, la capacitación constante del personal y la mejora continua de los sistemas fomentan una cultura organizacional centrada en la seguridad y el uso ético de la información, garantizando la sostenibilidad tecnológica del hospital.

2.2.10 NORMAS ISO

Según (ISO/IEC 27001:2022). Las normas internacionales requeridas por el comercio, los gobiernos y la sociedad son identificadas por la ISO (Organización Internacional para la Normalización), que las desarrolla junto con los sectores que las van a utilizar, las adopta mediante procedimientos transparentes basados en contribuciones nacionales de múltiples partes interesadas, y las ofrece para ser utilizadas a nivel mundial.

Las normas ISO se derivan de un acuerdo global alcanzado por la mayoría de los grupos de partes interesadas. Los expertos son aquellos que están más cerca de las necesidades de normas y los resultados de su implementación

.

2.2.11 NORMAS ISO 27000

"Requisitos para la especificación de sistemas de gestión de la seguridad de la información (SGSI)" es el nombre de la colección de normas ISO/IEC 27000.
Proporciona un marco de estándares para la seguridad de la información que se puede utilizar en una organización o empresa y abarca los siguientes temas:

- Un sistema para administrar la seguridad de la información.
- Evaluar los riesgos.
- Controles.

2.2.12 ISO/IEC 27001

Según (ISO/IEC 27001:2022). Es la norma que se puede certificar y que establece los requisitos necesarios para la implementación, mantenimiento y mejora de un Sistema de Gestión de Seguridad de la Información (SGSI).
Su Objetivo principal es salvaguardar la información asegurando los tres principios esenciales:

Confidencialidad: solo pueden acceder individuos autorizados.
Integridad: la información es precisa y completa.
Disponibilidad: la información está disponible cuando se requiere.
Otro Aspecto clave es:
Enfoque centrado en la gestión de riesgos.
Especifica políticas, roles, responsabilidades y medidas de control.
Requiere la evaluación, tratamiento y aceptación de riesgos.
Facilita la certificación internacional para la organización.

En hospitales de Nivel II, ISO 27001 contribuye a proteger los registros médicos, los sistemas de atención y los datos administrativos.
La norma 27001 incluye reglas sobre seguridad de la información. La seguridad de la información, según esta norma que es la principal de la serie, es la preservación de la confidencialidad, integridad y disponibilidad, así como de los sistemas involucrados en su tratamiento.

La estructura PHVA (planear, hacer, verificar y actuar) es el modelo utilizado por el sistema de gestión de la seguridad de la información ISO 27001. El proceso comienza con la planificación del alcance del SGSI, que determina las áreas o procesos de la organización en las que el sistema se aplicará.

En la gestión de la información, generalmente se seleccionan las áreas más importantes o susceptibles. Después de definir el alcance, se debe crear y publicar una política de gestión de la seguridad de la información que establezca los estándares generales que la organización debe seguir al abordar los riesgos de la seguridad de la información, teniendo en cuenta los requisitos legales, contractuales y corporativos.

El objetivo principal de la planificación de SGSI (Sistema de gestión de la seguridad de la Información), es identificar los riesgos de la información en relación con las amenazas potenciales y los puntos vulnerables de la organización en términos de confiabilidad, seguridad y disponibilidad de la información.

Los planes de control o tratamiento de riesgos se establecerán a partir de la identificación de estos riesgos, así como de su análisis y evaluación. Además, incluye las instrucciones y procedimientos necesarios para implementar estos

controles, así como la capacitación y capacitación de los empleados sobre la seguridad de la información y los controles que deben implementarse.

La verificación incluye la evaluación del desempeño del SGSI, la evaluación de riesgos y la eficacia de los controles implementados, la realización de auditorías internas al sistema y la recisión del sistema por parte de la dirección.

2.2.13 SECTORES O DOMINIOS DE SEGURIDAD DE LA ISO/IEC 27001

1. Políticas relacionadas con la seguridad.
2. Planificación de la seguridad.
3. Manejo de activos.
4. Seguridad del personal.
5. Protección física y ambiental.
6. Manejo de operaciones y comunicaciones.
7. Sistema para gestionar el acceso.
8. La adquisición, la creación y el mantenimiento de sistemas de información.
9. Manejo de incidentes relacionados con la seguridad de la información.
10. Un plan para la continuidad de la empresa.
11. cumplimiento.
12. Manejo de incidentes de seguridad de datos.
13. Consideraciones sobre la seguridad de la información en la gestión de la continuidad comercial.
14. Eficacia.

2.2.14 ISO/IEC 27002

(ISO/IEC 27002:2022). Se trata de una norma adicional (no sujeta a certificación) que ofrece orientaciones sobre buenas prácticas y medidas de seguridad para facilitar la aplicación de ISO/IEC 27001.

El Propósito principal Ofrecer un listado de medidas y sugerencias prácticas para salvaguardar la información.
Las Áreas clave (sintetizadas) son:
Políticas de seguridad de la información

Seguridad de recursos humanos

Gestión de accesos

Criptografía

Seguridad física y ambiental

Seguridad en la operación

Seguridad en las comunicaciones

Desarrollo y adquisición de sistemas

Manejo de incidentes

Continuidad del negocio

Cumplimiento de normativas y leyes

En el ámbito sanitario, ISO 27002 guía sobre la aplicación de medidas concretas para disminuir los riesgos tecnológicos y operativos. Ver las diferencias de ISO en la tabla 8.

Tabla 8

Diferencia fundamental entre ISO 27001 y 27002

ISO/IEC 27001	ISO/IEC 27002
Norma de requisitos	Norma de buenas prácticas
Certificable	No sujeta a certificación
Establece lo que debe cumplirse	Describe cómo llevarlo a cabo
Enfoque en SGSI	Foco en medidas

Relevancia para hospitales públicos Nivel II

Controles de seguridad sensibles de pacientes.

Minimización de riesgos tecnológicos y jurídicos.

Adherencia a la normativa (protección de información personal).

Fortalecimiento de la confianza institucional.

Apoyo a la continuidad de los servicios sanitarios.

2.2.15 PROCESOS DE SEGURIDAD DE LA INFORMACIÓN

El conocido ciclo de DEMING también conocido como PDCA (Planificación, Hacer, Verificar, Actuar), como se muestra en la Figura 10, es la base de todos los sistemas de gestión de seguridad. Es un enfoque para la mejora continua de la

calidad que se basa en cuatro pasos: planificar, realizar, verificar y actuar. Se describirá la estructura completa:

a) Planificación: Recolectar y analizar datos ayuda a la dirección a tomar conciencia de la situación actual.

b) Hacer: Consiste en implementar procesos basados en análisis y planificación previos.

c) Verificar: Compruebe. Consiste en la supervisión y evaluación de procesos y resultados, relacionándolos con los objetivos y especificaciones iniciales.

d) Actuar: Se realizan las correcciones necesarias y se estandarizan los cambios para asegurarse de que los procesos mejoren continuamente.

Figura. 10

Ciclo de DEMING

Nota: ISO 27001 (2022),

2.2.16 UNA SOLUCIÓN SUGERIDA

Este proyecto propone la implementación de un SGSI basado en la Norma ISO/IEC 27001;27002, que servirá como plan de acción para el mejoramiento de la seguridad para alcanzar un alto grado de eficiencia en las actividades de protección y protección de la información. Además, se tiene como objetivo iniciar el proceso de certificación ISO/IEC 27001:27002 del Hospital La Caleta.

CAPITULO III

MARCO METODOLOGICO

3.1. Hipótesis de la investigación de la investigación

Un modelo de buenas prácticas permite gestionar en forma eficiente la seguridad de la información en los hospitales nivel II.

3.2. Variables e indicadores de la investigación

Las variables propuestas en la presente investigación son:
Variable I: Modelo de Buenas Prácticas.
Variable D: Seguridad de la información en hospitales nivel II
Los indicadores se detallan en la tabla 09 y la matriz de Operacionalización.

Tabla 09

Matriz de Operacionalización

VARIABLE	DEFINICIÓN CONCEPTUAL	DIMENSIÓN	INDICADORES	TIPO	TÉCNICA	INSTRUMENTO
Variable I Independiente Modelo de Buenas Prácticas de Seguridad de la Información	Conjunto estructurado de políticas, procedimientos y controles basados en estándares internacionales para proteger la información organizacional	Gestión organizacional de seguridad	Existencia de políticas, roles definidos, comité de seguridad	Cuantitativo	Encuesta	Cuestionario estructurado
		Gestión de riesgos	Identificación de riesgos, análisis de vulnerabilidades	Cuantitativo	Encuesta	Cuestionario
		Controles técnicos	Antivirus, control de accesos, copias de seguridad	Cuantitativo	Observación / Encuesta	Lista de verificación
		Capacitación y concientización	Programas de formación, campañas de seguridad	Cuantitativo	Encuesta	Cuestionario

Variable II Dependiente Seguridad de la Información	Grado en que la información está protegida frente a accesos no autorizados, alteraciones o interrupciones	Confidencialidad	Control de acceso, privacidad de datos clínicos	Cuantitativo	encuesta	Cuestionario
		Integridad	Exactitud y consistencia de datos	Cuantitativo	Encuesta	Cuestionario
		Disponibilidad	Acceso oportuno a sistemas	Cuantitativo	Encuesta	Cuestionario
		Cumplimiento de políticas	Uso adecuado de normas de seguridad	Cuantitativo	Encuesta	Cuestionario

3.3. Método de la investigación

Este estudio está diseñado con un enfoque cuantitativo, ya que tiene como objetivo medir y analizar el nivel de aplicación de buenas prácticas de seguridad de la información en hospitales públicos de nivel II, recopilando datos numéricos que serán procesados estadísticamente para identificar brechas, falencias y necesidades de mejora. Este enfoque permite una evaluación objetiva de la situación actual de los sistemas de información hospitalarios y apoya la propuesta de un modelo de buenas prácticas basado en evidencia empírica.

- De acuerdo a la orientación de la investigación:

La investigación corresponde a un tipo de investigación aplicada, ya que está enfocada a resolver un problema específico en el contexto real: la insuficiente implementación de medidas de seguridad de la información en los hospitales públicos de nivel II. Su objetivo es desarrollar un modelo de buenas prácticas que ayude a mejorar la protección de datos clínicos, administrativos y tecnológicos, garantizando la confidencialidad, integridad y disponibilidad de la información.

- De acuerdo a la técnica de contratación: La investigación aplicada

El actual proyecto de investigación es de tipo DESCRIPTIVO; ya que la recolección de datos obtenidos a través de instrumentos de investigación nos facilitó observar, entender y detallar la situación en la que se halla el Hospital de nivel II

Nivel de Investigación

La investigación es de nivel descriptivo-proposicional:

Descriptivo porque analiza y caracteriza el estado actual de la seguridad de la información en los hospitales, incluyendo políticas, procedimientos, infraestructura tecnológica, gestión de riesgos y cultura organizacional.

Propositivo ya que ofrece un modelo estructurado de buenas prácticas para fortalecer la gestión de la seguridad de la información en este tipo de instituciones.

3.4 Diseño de la Investigación

El diseño es no experimental transversal
No experimental en el sentido de que las variables de la investigación no se manipulan deliberadamente, sino que se observa la realidad tal como ocurre en su contexto natural. Transversal porque se recopila información en un momento determinado para poder describir la situación actual sin ser longitudinal. Para lo cual, se ha simplificado de la siguiente manera:

M : Muestra de elementos o población de elementos de estudio.
X_i : Variable(s) de estudio, i = 1, 2, 3, ...
O_i : Resultado de medición de la(s) variable(s) de estudio.

M : Representa un muestra con quien o en quien vamos a realizar el estudio.
O_i : Representa la información relevante o de interés que recogemos de la muestra.

3.5 Población y muestra

Población:
La población está formada por personal involucrado en la gestión y uso de los sistemas de información hospitalarios, tales como:
Trabajadores de tecnología de la información
Personal administrativo
Personal Asistencial (médicos, enfermeras, técnicos)

Gerentes o líderes

(Sánchez, 2018) manifiesta que “población es un grupo de unidades con características similares, identificadas en un área determinada, con el fin de ser estudiadas”

Muestra:

Mediante el muestreo no probabilístico por juicio, se tomará como referencia una muestra representativa de 30 personas (este dato corroborar con el cuestionario realizado, elegir un grupo), los cuales son objeto de estudio.

Tabla 10

Grupo representativo por área del hospital la caleta

Áreas	Cantidad (individuos) colocar según las áreas	Muestra representativa (seleccionar cantidad deseada)
Administrativos	49	49/470 ≈ 0.10*30=3
Técnicos de Tecnologías de Información	20	20/470 ≈ 0.04*30 ≈ 1.2 ≈ 1
Médicos	69	69/470 ≈ 0.14*30 ≈ 4.2 ≈ 4
Obstétricas	25	25/470 ≈ 0.05*30 ≈ 1.5 ≈ 2
Otros (Enfermeras, Técnicos de Enfermería)	307	307/470=0.65*30=19.5=30
TOTAL	470	30

3.6 Técnicas e instrumentos de recolección de datos

Se realizaron entrevistas a varios empleados del departamento de TI, junto con personal administrativo y asistencial. Al procesar los datos de las respuestas obtenidas, se observó el proceso laboral del departamento de TI

Tabla 11

Recolección de datos

TECNICA	INSTRUMENTO	DESCRIPCION
Entrevistas	Guía de entrevistas	Dirigido a responsables de TI y autoridades institucionales para profundizar en aspectos estratégicos y organizacionales.
Observación	Ficha de Observación	Evaluación de prácticas operativas relacionadas con la gestión de la información.
Encuestas	Cuestionario de preguntas	Utilizado para medir el nivel de conocimiento, el cumplimiento y la percepción de la seguridad de la información entre el personal del hospital.
Análisis documental	Examinar Informacion	revisar políticas, reglamentos internos, procedimientos, informes de auditoría y documentación institucional.

3.7. Procesamiento de la recolección de datos

Técnicas de procesamiento

Las técnicas de procesamiento de los datos será la tabulación la cual comprende en codificar y verter los datos en una base de datos proporcionada por una herramienta (Excel o SPSS). Todo ello nos permitirá agrupar y estructurar con el fin de responder al propósito de la investigación: Problema, objetivos e hipó investigación.

Análisis de resultados

Mediante la herramienta seleccionada procederemos a realizar el análisis de los datos haciendo uso de estadística descriptiva.

Se evaluará el modelo sin entrenamiento y con entrenamiento por juicio de expertos en función a los rendimientos esperados para la variable dependiente. Para ello se utilizará las herramientas de los ISO 27002

El siguiente es un plan para el procesamiento y análisis de la información:
Revisión crítica de los datos recopilados.
Organización de los datos.
interpretar los resultados, que ayudarán a crear la solución del problema.

3.8 Colección de Datos Caso Estudio

La información es el componente clave necesario para desarrollar un modelo de Buenas prácticas para la seguridad de sistema de información en un hospital nivel II La Caleta
A continuación, explicaremos como se adquirió y como se modificó la información para crear los conjuntos de Datos que faciliten el entrenamiento, evaluación y la validación del modelo de predicción que se presenta en este estudio.

EVOLUCIÓN DEL MODELO

Las siguientes actividades se llevarán a cabo de forma secuencial para completar el desarrollo del proyecto de investigación:

OE1: Conocer la seguridad de la información en el Hospital nivel II, la Caleta de Chimbote.

El presente objetivo específico tiene como finalidad diagnosticar el estado actual de la seguridad de la información en un hospital de Nivel II identificando las fortalezas y vulnerabilidades de sus sistemas y procesos. Su cumplimiento permitirá crear una

base objetiva para la implementación de buenas prácticas. Además, servirá de apoyo para proponer mejoras según los estándares de protección de la información en el entorno hospitalario.

Instrumento: Cuestionario destinado al personal administrativo y sanitario que maneja información, complementado con una lista de verificación basada en controles ISO/IEC 27002.

OE2: Caracterizar el modelo de buenas prácticas para gestionar la seguridad de información en hospitales nivel II.

El propósito de este objetivo es identificar y describir los componentes, principios y lineamientos que constituyen un modelo de buenas prácticas enfocado en la seguridad de la información en hospitales de Nivel II. El cumplimiento de esto le permitirá comprender cómo se deben organizar los procesos, controles y políticas para proteger adecuadamente los datos clínicos y administrativos. Además, es la base para evaluar la relevancia y aplicabilidad del modelo en el contexto de los hospitales públicos.

Instrumento: Análisis de documentos complementado con un cuestionario estructurado adecuado para que el personal administrativo y de TI evalúe el nivel de adopción de buenas prácticas y controles de seguridad de la información.

OE3: Determinar la influencia del Modelo de las buenas prácticas en la gestión de la seguridad y el riesgo en el Hospital nivel II, la Caleta de Chimbote.

Evaluar cómo la implementación del modelo de buenas prácticas afecta directamente a la gestión de la seguridad de la información y la mitigación de riesgos en un hospital de nivel II. La adhesión al mismo permitirá identificar mejoras en los procesos, controles y toma de decisiones relacionados con la protección de los sistemas de información. Además, proporcionará evidencia para validar la efectividad del modelo propuesto en un entorno hospitalario real.

Instrumento: Se recomienda utilizar un cuestionario utilizado para el personal involucrado en la gestión de TI y seguridad, complementado con una lista de verificación basada en ISO/IEC 27001 o 27002.

1. Analizar los procedimientos actuales para el tratamiento de la información y el control de vulnerabilidades.
   - Análisis de la situación actual de la institución
   - Evaluación de los resultados de la encuesta utilizada.

2. Crear un Sistema de Gestión de Seguridad de la Información que reduzca la probabilidad y la ocurrencia de amenazas de acuerdo con los criterios de la Norma ISO/IEC 27001.
   - Gestión de riesgos.
   - Declaración de aplicabilidad.
   - Implementación de procedimientos y controles para la gestión de incidentes de seguridad de la información.

3. Establecer una metodología de evaluación y mejoramiento continuo del SGSI lo cual garantice un adecuado tratamiento de la información.

4.- Monitorización e implementación de mejoras.

METODOLOGIA DE DESARROLLO

Según (Cortés, 2024). Adopta una metodología de desarrollo basada en un Sistema de Gestión de Seguridad de la Información (SGSI) de acuerdo con la norma ISO/IEC 27001:2022 utilizando el ciclo de mejora continua PDCA (Planificar–Hacer–Verificar–Actuar). Este enfoque nos permite desarrollar, implementar, evaluar y mejorar un modelo de buenas prácticas de seguridad de la información adaptado a los hospitales públicos de nivel II. En la fase de planificación se realiza el diagnóstico y análisis de riesgos; Durante la fase de ejecución se implementan controles de seguridad; luego se verifica su eficacia mediante evaluaciones y auditorías; y finalmente, se establecen iniciativas de mejora continua que garanticen la sostenibilidad del modelo.

En los hospitales públicos de nivel II, la implementación de la norma ISO/IEC 27001 permite establecer un sistema de gestión de seguridad de la información destinado a proteger los datos clínicos, administrativos y operativos a través de la gestión de

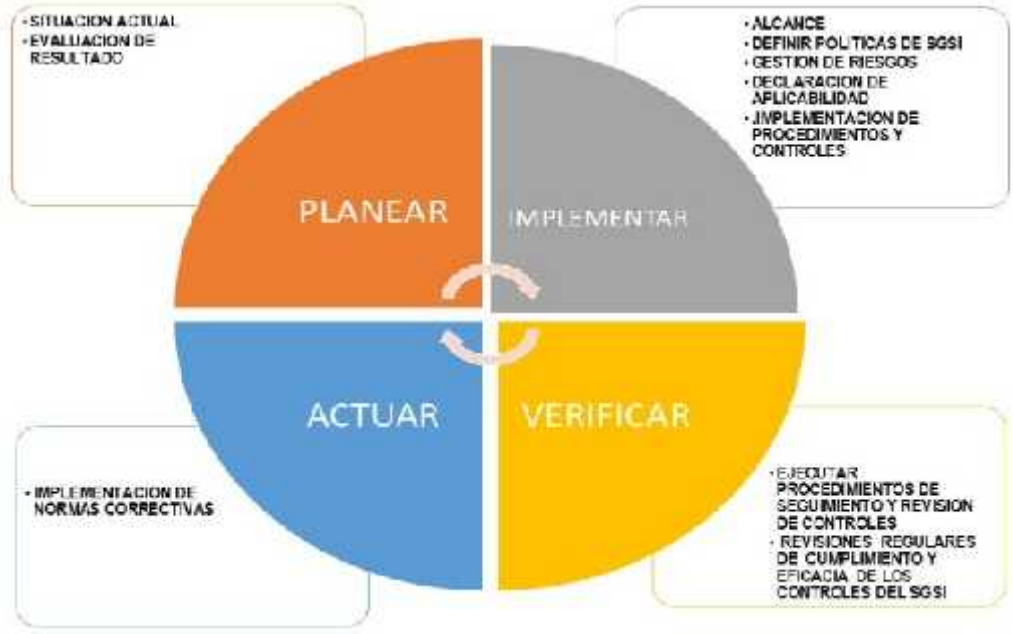
riesgos y la mejora continua. Además, ISO/IEC 27002 proporciona controles específicos (organizativos, humanos, físicos y tecnológicos) necesarios para garantizar la confidencialidad, integridad y disponibilidad de la información hospitalaria, particularmente en sistemas de registros médicos, laboratorios y servicios críticos.

Las normas ISO/IEC 27001:2022 e ISO/IEC 27002:2022 definen las actividades requeridas para la implementación, operación y mejora de un sistema de gestión de seguridad de la información (SGSI). 27001 establece los requisitos obligatorios, mientras que 27002 proporciona buenas prácticas y controles detallados para cumplirlos.

El ciclo de Deming, también conocido como mejora continua (PDCA), se ha utilizado para llevar a cabo la implementación del Sistema de Gestión de Seguridad. Las fases de desarrollo del ciclo se detallan a continuación.

Figura 11.

Mejora continua (PDCA)



PLANEACION

Esta norma organiza sus actividades según el ciclo de mejora continua PDCA (Planificar-Hacer-Verificar-Actuar).

1. Contexto organizacional

Actividad: Comprender el entorno interno y externo del hospital.
Identificación de interesados (pacientes, personal médico, MINSA)
Determinar el alcance del SGSI
Determinación de requisitos legales y reglamentarios.
Sostenibilidad: permite la adaptación del sistema de seguridad a la realidad institucional.

2 Gestión

Actividad: Implicación de la alta dirección.
Política de seguridad de la información
Distribución de roles y responsabilidades.
Apoyo organizacional y recursos
Sostenibilidad: Sin liderazgo, un SGSI no es sostenible ni está integrado en la gestión hospitalaria.

3. Planificación

Actividad: Gestión de riesgos de seguridad.
Identificación de activos de información.
Análisis y evaluación de riesgos.
Gestión de riesgos
Medidas de seguridad
Apoyo: La seguridad se basa en riesgos, no en medidas individuales.

4. Soporte

Actividad: Recursos y capacidades para la operación del SGSI. Incluye:
Formación y sensibilización del personal.
Comunicación interna
Control de información documentada
Soporte: Los usuarios son el factor de seguridad más importante.

5. acción

Acción: Implementación de controles y procesos.
Uso de un plan de gestión de riesgos.
Gestión del cambio
Procedimientos operativos
Soporte: Aquí es donde el modelo pasa del papel a la práctica.

6. Evaluación del desempeño

Actividad: Medir la eficacia del SGSI. Incluye:
Monitoreo y medición
Auditorías internas
Revisión de la gestión
Soporte: Le permite verificar que los controles realmente protegen la información.

7. Mejorar

Actividad: Mejora continua del sistema.
Acciones correctivas
Manejo de incidentes
Optimización SGSI
Soporte: La seguridad es dinámica con nuevas amenazas.

ISO/IEC 27002:2022 - Actividades de implementación de control
Este estándar describe cómo utilizar los controles de seguridad. En la versión 2022 se agrupan en 4 categorías con 93 controles.

A. Controles organizativos (37)
Principales actividades:
Políticas de seguridad
Gestión de riesgos
Gestión de proveedores
Continuidad del negocio
Clasificación de la información
Soporte: Crean gestión de seguridad.

B. Control personal (8)
Principales actividades:
Reclutamiento seguro
Comprensión y formación
Responsabilidad de seguridad
Gestión del trabajo remoto
Sostenibilidad: Reduce las amenazas internas y los errores humanos.

C. Controles físicos (14)
Principales actividades:
Seguridad de objetos
Control de acceso físico
Protección de equipos
Áreas seguras (salas de servidores)
Resiliencia: Protege los activos críticos del acceso no autorizado.

D. Control tecnológico (34)
Principales actividades:
Control de acceso lógico
Criptografía
Seguridad de la red
Copias de seguridad
Gestión de vulnerabilidades
Registro y seguimiento
Soporte: Protege los sistemas informáticos y los datos clínicos.

Analizar la situación actual

a) Conocer la seguridad de la información en el Hospital nivel II, la Caleta de Chimbote.

   El primer paso es realizar una entrevista con el responsable del área de sistemas con el fin de recopilar datos y comprender cómo actualmente maneja la información el departamento de tecnología. Ver Figura 12 ,13 y 14 del modelo.

Luego será esencial realizar un análisis de la entrevista para tener un punto de partida y realizar una gestión adecuada, haciendo hincapié en los aspectos negativos del manejo adecuado de la información.

La entrevista al jefe del Área de Sistemas de TI y Comunicación, Ingeniero Edwin Mantilla Guevara, se llevó a cabo para determinar que el centro de cómputo carece de un plan o sistema de gestión de seguridad para administrar la información de manera adecuada.

Figura 12

Implementación de la propuesta

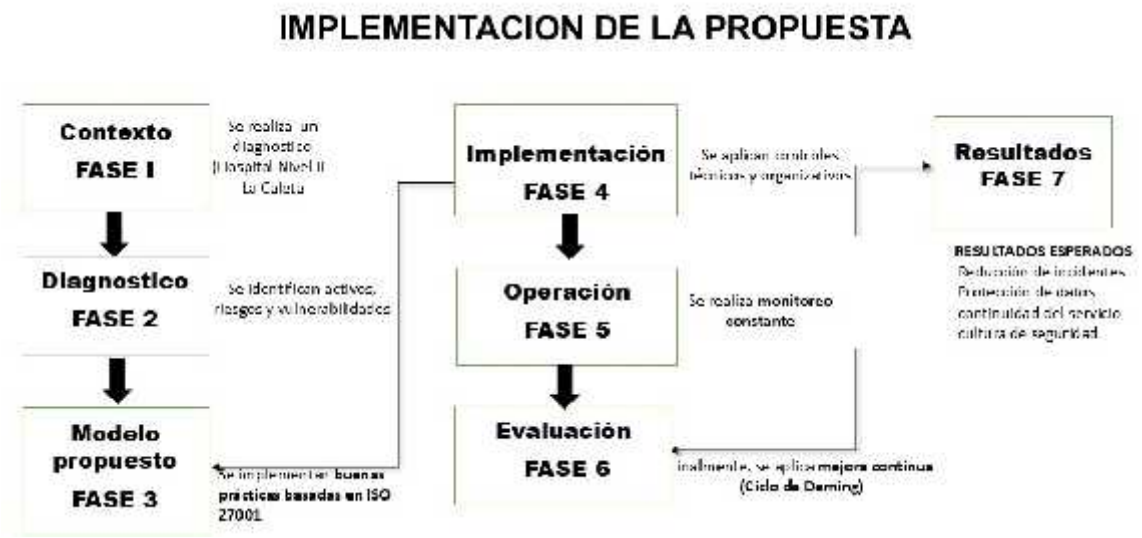


Figura 13

Diagrama del modelo propuesto.

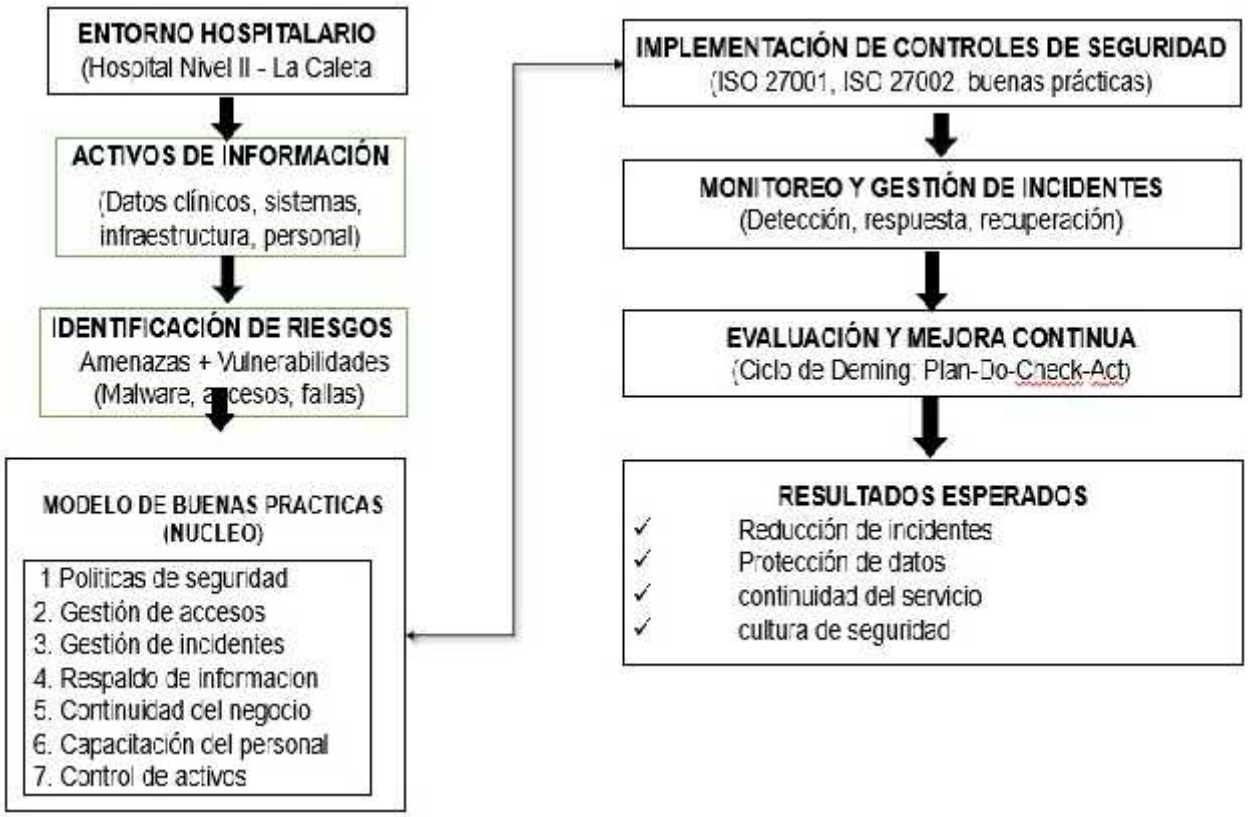
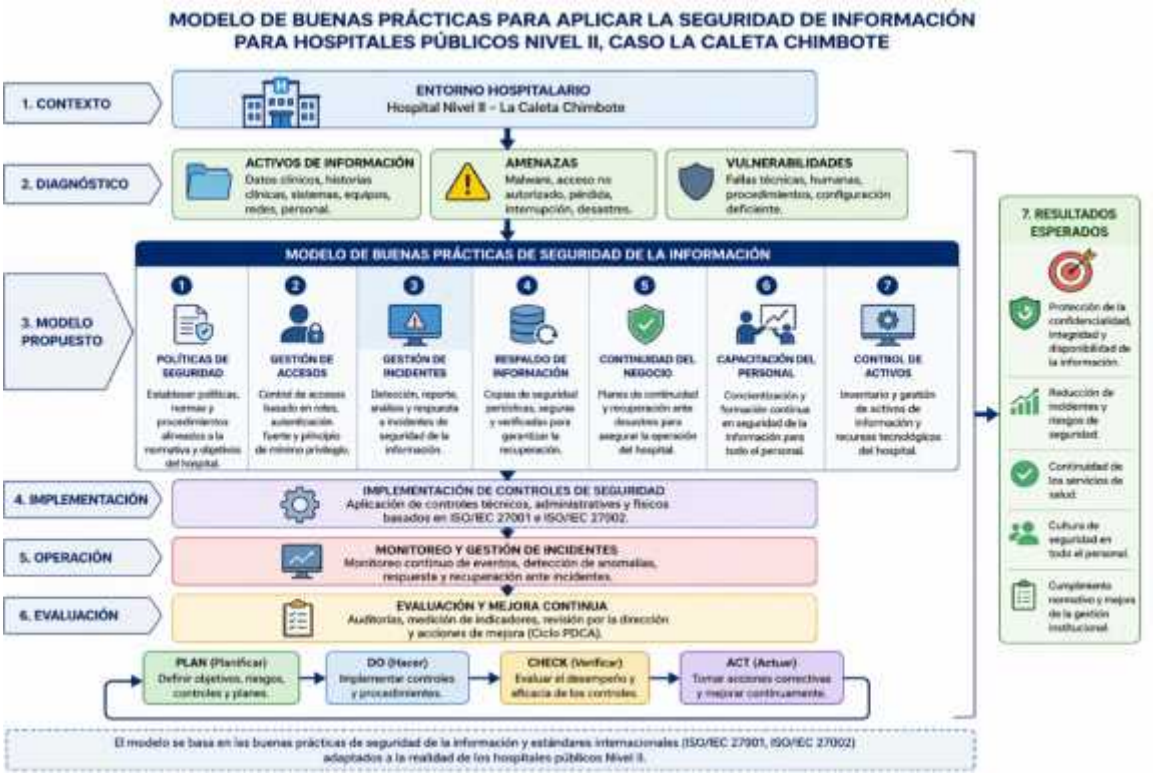


Figura 14

Modelo de buenas prácticas para aplicar la seguridad de informacion.



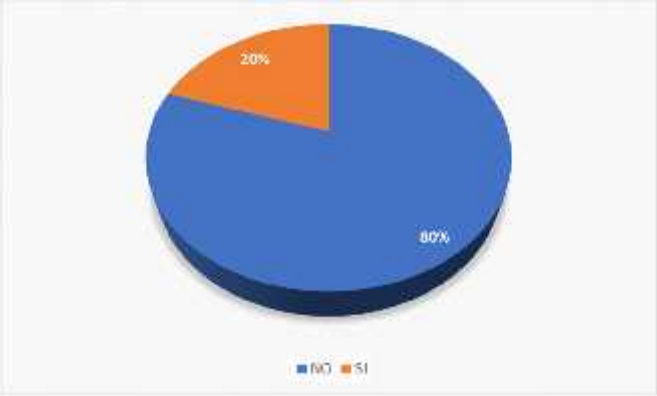
Nota Elaboración propia

RESULTADOS

1.- ¿Existen políticas actuales de seguridad para la gestión de la información?

Figura 15

Políticas de Seguridad



Interpretación:

Dominio ISO/IEC 27001: Sección 5 – Dirección / Anexo A. 5 (Normas de seguridad).

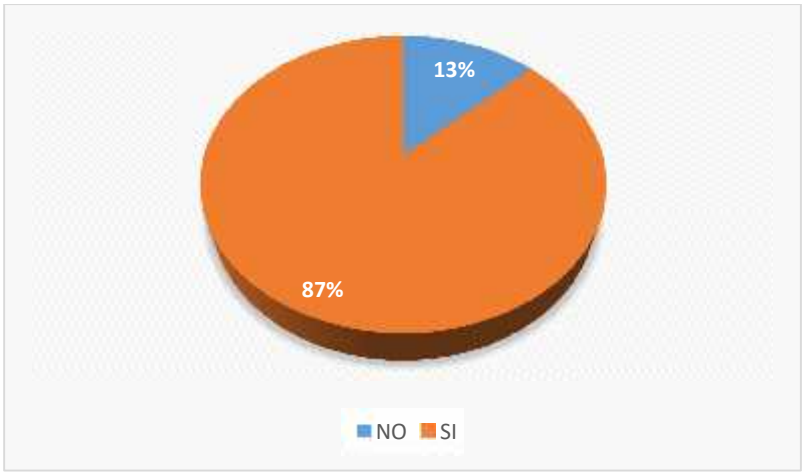
El 80% del personal que participó en la encuesta indica que no hay políticas formales de seguridad de la información, mientras que únicamente un 20% reconoce que sí existen. Este resultado muestra un nivel preocupante de incumplimiento del requisito esencial de la norma, que requiere que existan políticas que sean documentadas, comunicadas y aprobadas por la alta dirección.

Indicador numérico: Existencia de políticas de seguridad: 20% (nivel bajo – crítico)

2.- ¿Están establecidas responsabilidades para los empleados en cuanto al uso adecuado de los recursos?

Figura 16

Responsabilidad de Empleados



Interpretación:

Dominio ISO/IEC 27001: Anexo A. 6 (Estructura de la seguridad de la información)

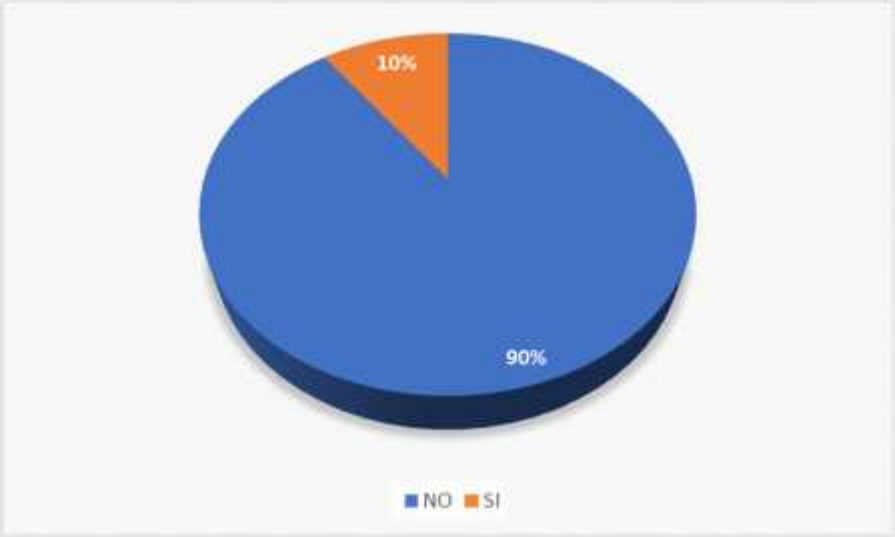
El 80% del personal sostiene que comprende sus deberes en relación con el uso correcto de los recursos tecnológicos, en cambio, el 20% no tiene claridad sobre esas responsabilidades. Aunque el resultado es en su mayoría favorable, la norma establece que el 100% del personal debe tener claramente definidas y formalizadas sus responsabilidades.

Medida numérica: Conocimiento sobre obligaciones: 80% (nivel intermedio)

3.- ¿Existe alguna forma de controlar el acceso no autorizado del personal para proteger los sistemas y equipamiento de la institución?

Figura 17.

Acceso no autorizado



Interpretación:

Dominio ISO/IEC 27001: Anexo A. 9 (Control de accesos) y A. 11 (Seguridad ambiental y física)

El 90 % del personal no autorizado no tiene acceso al Data Center, mientras que solo el 10 % posee acceso autorizado. Este resultado muestra que se han aplicado correctamente controles de acceso físico, cumpliendo con los requisitos establecidos por la norma.

Índice numérico: Acceso regulado al Centro de Datos: 90% (nivel elevado)

4.- ¿Los equipos de la institución reciben mantenimiento regular?

Figura 18

. Mantenimiento de Equipos

Interpretación:

Dominio ISO/IEC 27001: Anexo A. 11 (Protección de los activos)

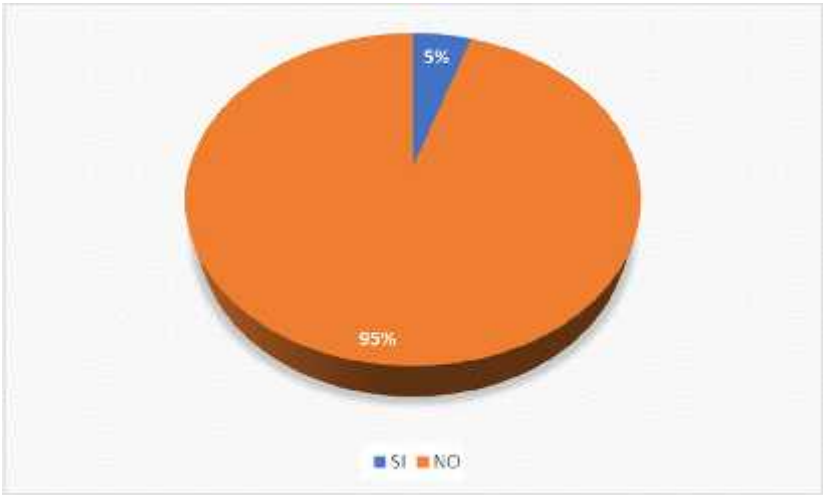
El 87% de las personas encuestadas informa que los equipos cuentan con un mantenimiento preventivo a través de un programa anual, mientras que el 13% indica que dicho mantenimiento no se lleva a cabo. Esto refleja una práctica operativa adecuada, aunque todavía hay áreas que requieren atención.

Indicador numérico: Mantenimiento preventivo de equipos: 87% (nivel medio-alto)

5.- ¿Se han llevado a cabo simulacros de caídas de los sistemas que controlan?

Figura 19

. Caídas de los sistemas



Interpretación:

Dominio ISO/IEC 27001: Anexo A. 17 (Elementos de seguridad de la información en la continuidad del negocio)

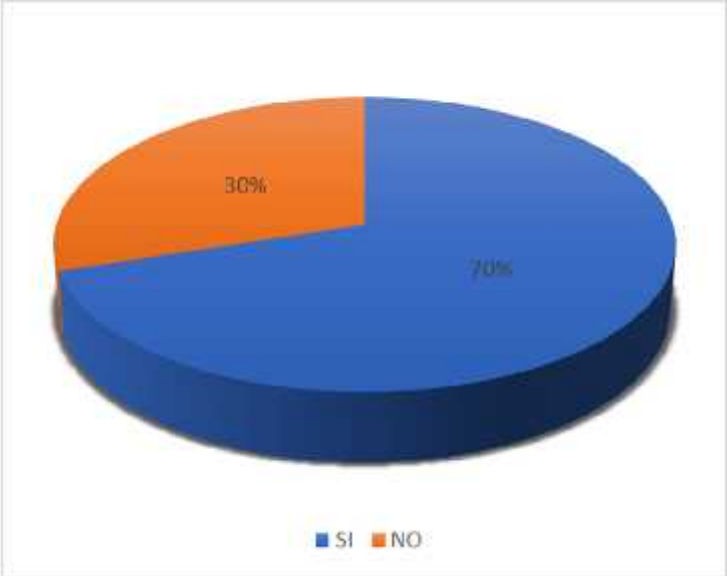
El 95% del personal indica que no se llevan a cabo simulacros de fallos en los sistemas, lo que pone de manifiesto la falta de un plan de continuidad y de pruebas regulares. Este resultado refleja una diferencia importante con respecto a la norma ISO/IEC 27001.

Medida numérica: Simulacros de emergencia: 5% (nivel muy bajo – crítico)

6.- ¿Se monitorean los sistemas de información que administran?

Figura 20

. Monitoreo de Sistemas



Interpretación:

Área ISO/IEC 27001: Anexo A. 12 (Protección de las operaciones)

El 70% de las personas encuestadas sostiene que los sistemas de información están bajo supervisión, mientras que el 30% expresa que no hay un seguimiento constante. Esto indica una aplicación incompleta de los controles de supervisión y registro.

Medida numérica: Supervisión de sistemas: 70% (grado intermedio)

7.- ¿Se implementa gestión de riesgos en relación con la seguridad de la información?

Figura 21

Seguridad de Información

Interpretación:

Dominio ISO/IEC 27001: Cláusula 6 – Planificación / Anexo A.8 (Gestión de activos)

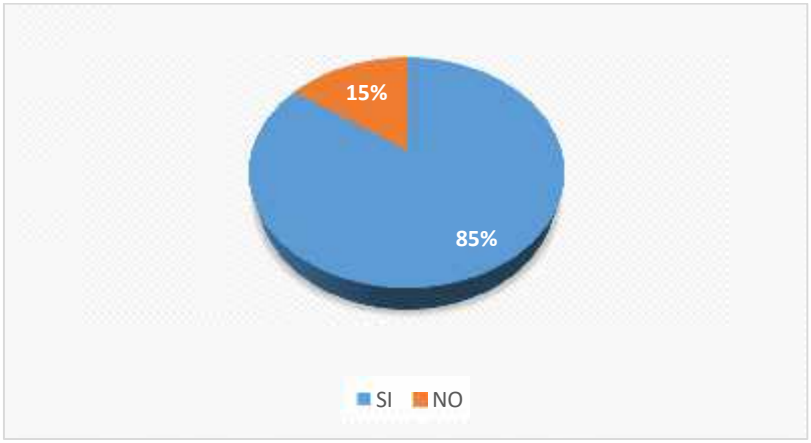
El 95% del personal indica que no se implementa una gestión de riesgos ni planes de contingencia, lo que demuestra la ausencia de uno de los pilares centrales de la norma ISO/IEC 27001: la gestión sistemática de riesgos.

Indicador cuantitativo: Gestión de riesgos: 5% (nivel crítico)

8.- ¿Qué medidas de seguridad se implementan en los sistemas de información y comunicación?

Figura 22.

Medidas de seguridad



Interpretación:

Dominio ISO/IEC 27001: Anexos A. 10 y A. 13 (Criptografía y protección en las comunicaciones)

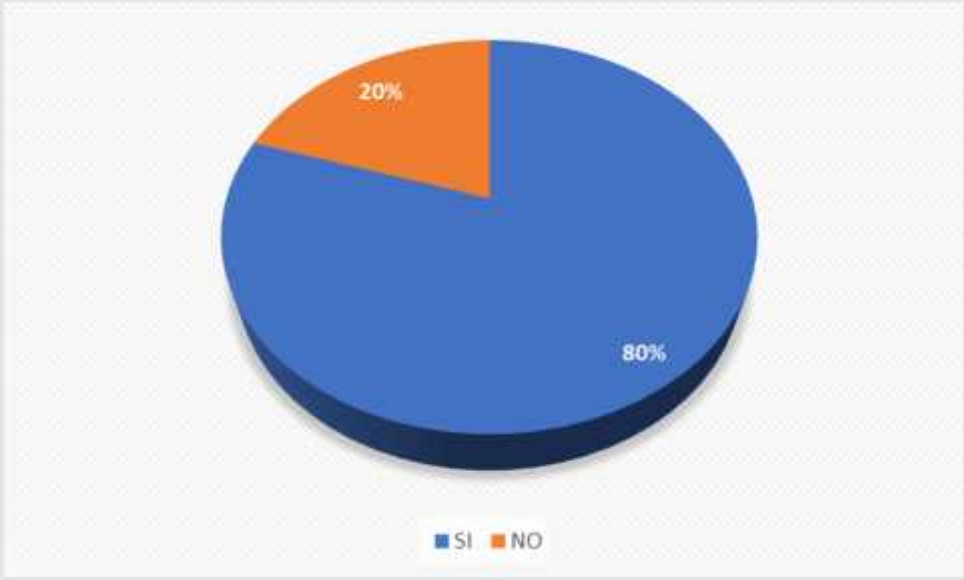
El 85% de los participantes en la encuesta piensa que hay medidas de seguridad, mientras que el 15% tiene una opinión diferente. Este hallazgo indica la existencia de controles técnicos elementales, aunque no cuentan con una estandarización oficial conforme a la norma.

Indicador numérico: Ejecutar medidas de seguridad: 85% (nivel medio-alto)

9.- ¿Tiene control sobre el inventario de la computadora de la institución?

Figura 23.

Control de inventario



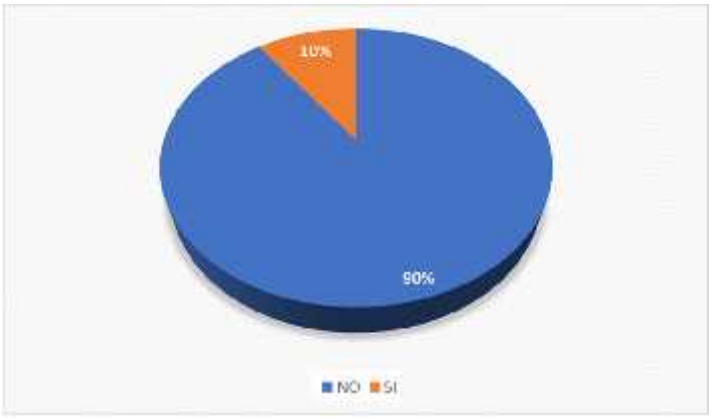
Interpretación:

Dominio ISO/IEC 27001: Anexo A. 8 (Administración de activos)

La mayoría del personal, un 80%, indica que hay un control sobre el inventario de computadoras, mientras que el 20% menciona que no se realiza un control apropiado. La regulación solicita un inventario exhaustivo, actualizado y debidamente formalizado.
Indicador numérico: Manejo de inventario: 80% (nivel intermedio)

10. ¿La dirección del hospital revisa constantemente los temas de seguridad de la información? **Figura 24.**

Seguridad de la informacion



Interpretación:

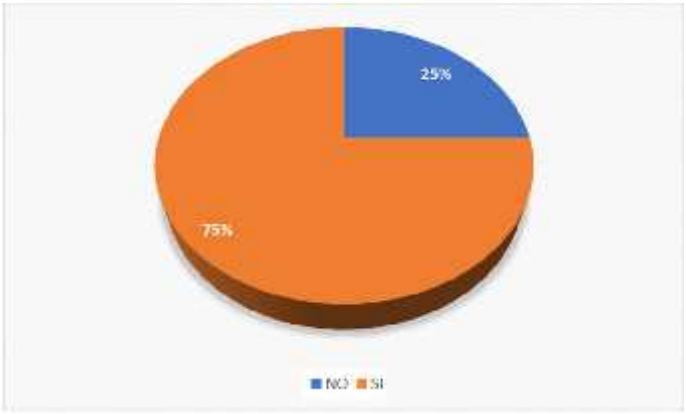
Dominio ISO/IEC 27001. Clausula Liderazgo

Los resultados muestran un bajo nivel de compromiso de la alta dirección con la seguridad de la información: el 90% de los directivos no realizan revisiones continuas y el 10% si lo realiza.. Esta situación constituye un incumplimiento significativo de la Cláusula 5 (Gestión) de ISO/IEC 27001:2022 y de los controles organizacionales de ISO/IEC 27002:2022, que requieren una participación activa de la dirección en la definición, seguimiento y mejora del SGSI. La falta de gobernanza es un factor de riesgo crítico que puede comprometer la eficacia de las políticas de seguridad y la protección de los activos de información del hospital.

11.- ¿Están identificados y registrados los activos de información (sistemas, datos, equipos)?

Figura 25.

Activos de Informacion



Dominio ISO/IEC 27001. Controles organizacionales

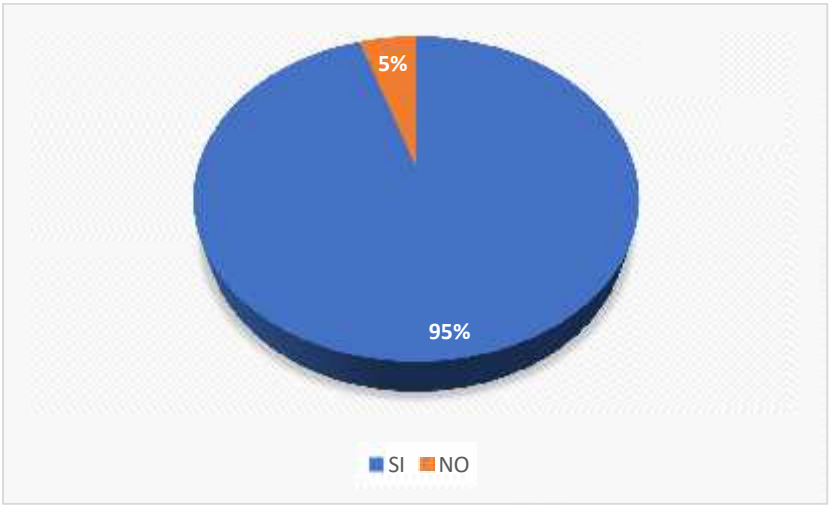
Control específico: Inventario de activos

El Ítem evaluado cumple con la norma ISO/IEC 27002:2022 control 5.9 “Activos”, perteneciente a los controles organizacionales del SGSI. El resultado muestra que el 75% de los activos de información están identificados y registrados, lo que indica un cumplimiento parcial del control. Sin embargo, el 25% que no se registra es una diferencia significativa porque los activos no inventariables no pueden protegerse adecuadamente ni tomarse en cuenta en el análisis de riesgos, comprometiendo así la confidencialidad, integridad y disponibilidad de la información institucional.

12.- ¿Está protegida la información almacenada en las computadoras portátiles?

Figura 26.

Almacenamiento en portátiles



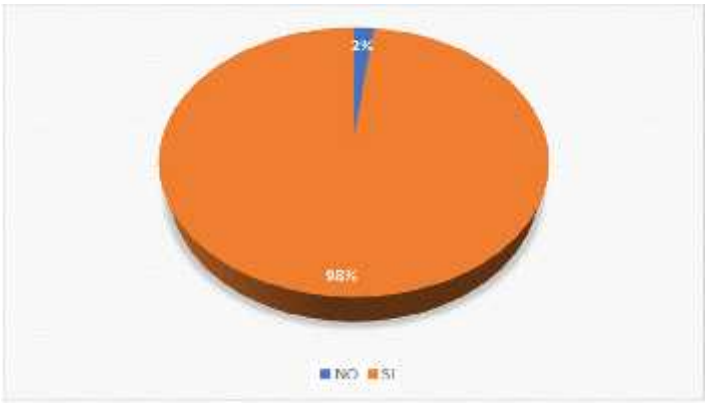
Dominio principal: Controles tecnológicos. En ISO 27001:2022, estos controles forman parte del Anexo A — Controles de seguridad de la información.

El resultado muestra un nivel crítico de vulnerabilidad en la protección de la información almacenada en dispositivos portátiles. El hecho de que el 95% de las computadoras portátiles no cuenten con mecanismos de seguridad adecuados indica una falta de cumplimiento de los controles especificados en ISO/IEC 27002:2022, especialmente aquellos relacionados con los dispositivos del usuario final y la protección de activos fuera de las instalaciones. Mientras que el 5% si cuenta. Esta situación expone a la organización a un alto riesgo de pérdida, robo o acceso no autorizado a información sensible, comprometiendo la confidencialidad, integridad y disponibilidad de los datos institucionales.

13.-¿Los empleados reciben capacitación en seguridad de la información?

Figura 27.

Capacitación en seguridad de la Informacion



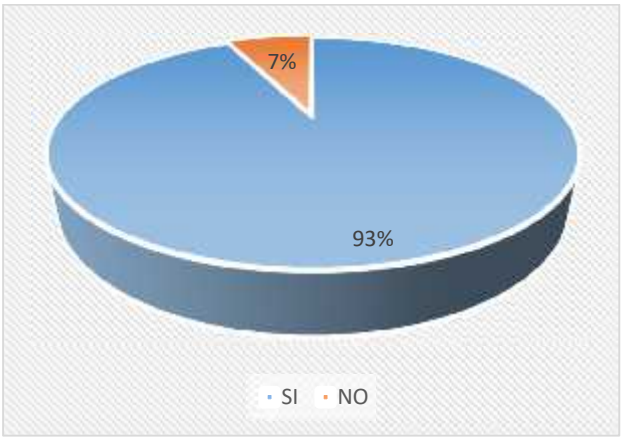
Dominio Gestión de recursos humanos / Seguridad relacionada con las personas (Controles de personas — ISO 27002:2022)

El ítem relacionado con la capacitación en seguridad de la información está relacionado con la cláusula 7 (Soporte) de ISO/IEC 27001:2022 y la cláusula 6.3 de control de ISO/IEC 27002:2022. punto correspondiente a la sensibilización, educación y formación del personal. El resultado obtenido (98% sin capacitación) indica una brecha crítica en la gestión de seguridad de la información, ya que la falta de capacitación aumenta el riesgo de incidentes derivados del factor humano e indica un bajo nivel de madurez del sistema de seguridad institucional.

14.- ¿Existe control de acceso a áreas sensibles (archivos clínicos, farmacias)?

Figura 28

. Acceso a áreas sensibles



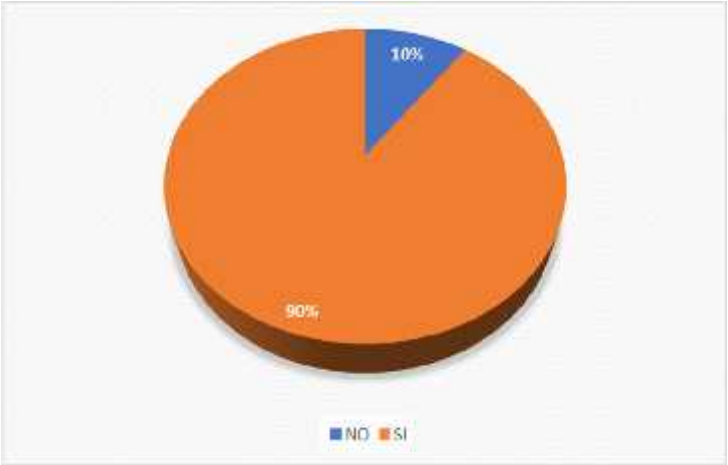
Dominio: Controles físicos. Categoría: Seguridad física y ambiental

Los resultados muestran que el 93% de los empleados percibe la existencia de controles de acceso a áreas sensibles como archivos clínicos y farmacias, lo que indica un nivel adecuado de implementación de control físico según ISO/IEC 27002:2022. Sin embargo, el 7% restante indica que no existe dicho control, lo que crea una brecha de seguridad importante ya que en estas áreas se almacena información confidencial y activos importantes. Según la norma, todas las áreas sensibles deben contar con mecanismos de contención y monitoreo, por lo que el incumplimiento parcial aumenta el riesgo de acceso no autorizado, pérdida de información o robo de medicamentos.

15.- ¿Cada usuario tiene credenciales individuales para acceder a los sistemas?

Figura 29.

Credenciales para acceder al sistema



Dominio, indicador e interpretación normativa. Categoría: Controles tecnológicos

El resultado indica un cumplimiento parcial de los controles de gestión de identidad definidos en ISO/IEC 27001:2022 e ISO/IEC 27002:2022. Mientras que el 90% de los usuarios tiene credenciales individuales para acceder a los sistemas institucionales, un 10% sin dichas credenciales indica una debilidad significativa en el control de acceso. Tal situación impide una trazabilidad adecuada de las actividades, aumenta el riesgo de acceso no autorizado y es contraria a las buenas prácticas internacionales de seguridad de la información, que estipulan que cada persona que accede a los sistemas de información debe tener una identidad única y autenticada.

16.- ¿Se utilizan sistemas antivirus o antimalware?

Figura 30.

Sistemas Antivirus

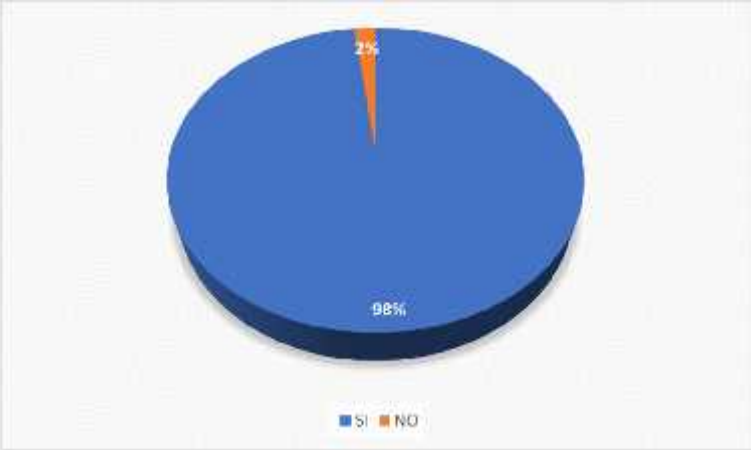
Dominio: Controles tecnológicos. Control específico: Protección contra malware

Los controles relacionados con el uso de sistemas antivirus o antimalware cumplen con el área de control tecnológico de la norma ISO/IEC 27002:2022, específicamente el control 8.7 “Protección contra software malicioso”. El resultado obtenido (95% de realización) muestra un alto nivel de protección en la mayoría de los equipos; Sin embargo, la presencia de un 5% sin protección es una vulnerabilidad importante que puede comprometer la seguridad de toda la infraestructura tecnológica. Por lo tanto, se considera un cumplimiento parcial de un control que requiere acciones correctivas para alcanzar la cobertura total según lo especificado en la norma.

17.- ¿Se realizan copias de seguridad de los datos periódicamente?

Figura 31.

Copias de Seguridad



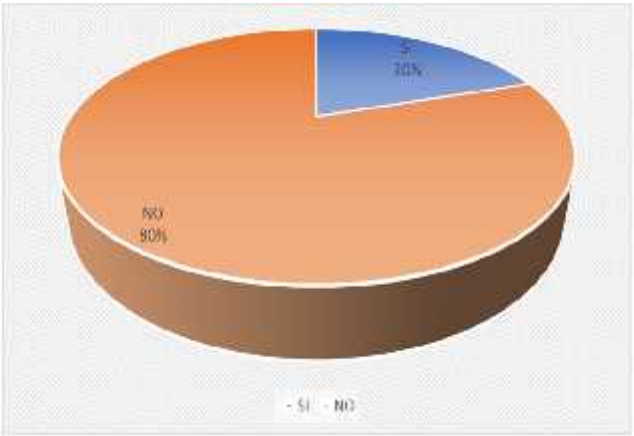
Dominio: Controles tecnológicos. Control específico: Copias de seguridad (Backup)

El control de respaldos muestra un alto nivel de cumplimiento (98%), lo que indica que la organización implementa mecanismos que garantizan la disponibilidad y recuperación de la información. Sin embargo, un desajuste del 2% es una vulnerabilidad importante, ya que la falta de copias de seguridad de algunos activos puede provocar una pérdida permanente de datos, interrupciones del servicio e impactos en la continuidad del negocio. Según ISO/IEC 27002:2022 (Control 8.13), todas las copias deben realizarse, probarse y almacenarse de forma segura periódicamente, por lo que se recomiendan acciones correctivas para lograr su total cumplimiento.

18.- ¿Existe un procedimiento para reportar incidentes de seguridad?

Figura 32.

Incidentes de Seguridad



Dominio: Controles organizacionales — Gestión de incidentes

El alto porcentaje de respuestas negativas (80%) indica que la organización carece de un procedimiento formal de notificación de incidentes o que el personal no está adecuadamente informado al respecto. Mientras que el 20% dice que si. Esto significa incumplimiento de los controles de gestión de incidentes establecidos en ISO/IEC 27002:2022 y limita las capacidades institucionales para detectar, responder y mitigar incidentes de seguridad de la información.

19.- ¿Se realizan pruebas de conmutación por error o recuperación ante desastres?

Figura 33.

Recuperación ante desastres

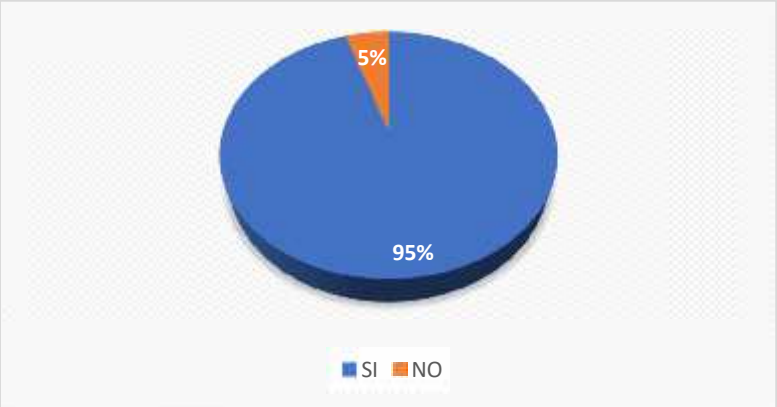
Dominio (Control de la norma). ISO/IEC 27002:2022 — Controles organizacionales

El hecho de que el 90% de los encuestados indique que no se realizan pruebas de conmutación por error o recuperación ante desastres indica un bajo nivel de madurez en la preparación de las TIC para la continuidad del negocio. Según ISO/IEC 27002:2022 control 5.30, las organizaciones deben planificar, implementar y probar periódicamente mecanismos de recuperación para garantizar la disponibilidad de los servicios críticos. La ausencia de estos controles aumenta significativamente el riesgo operativo y amenaza la resiliencia de las instituciones en caso de incidentes o desastres tecnológicos.

20.- ¿Se toman acciones correctivas después del incidente?

Figura 34.

Acciones correctivas



Dominio (Área de la norma). ISO/IEC 27001:2022 — Cláusula 10: Mejora

Control organizacional

El alto porcentaje de respuestas afirmativas (95%) indica que la organización toma acciones correctivas después de incidentes de seguridad de la información que cumplen con los requisitos de mejora continua de ISO/IEC 27001:2022 y los controles de gestión de incidentes de ISO/IEC 27002:2022. Sin embargo, la existencia de respuestas negativas 5%, revela brechas en la estandarización de procesos, comunicación o documentación que pueden comprometer la efectividad del SGSI y la capacidad de prevenir incidentes repetidos.

b) Caracterizar el modelo de buenas prácticas para gestionar la seguridad de información en hospitales nivel II.

El modelo de buenas prácticas de gestión de seguridad de la información en hospitales de Nivel II se basa en la adopción de un sistema de gestión de seguridad de la información (SGSI) alineado con las normas ISO/IEC 27001 e ISO/IEC 27002. Su propósito es proteger la confidencialidad, integridad y disponibilidad de la información clínica, administrativa y tecnológica, teniendo en cuenta la naturaleza crítica de la atención médica y la sensibilidad de los datos de los pacientes. Este modelo se caracteriza por un enfoque sistemático basado en la gestión de riesgos que permite la identificación, análisis y tratamiento de amenazas y vulnerabilidades relacionadas con

los sistemas de información hospitalarios. Esto incluye la definición de políticas de seguridad, controles organizativos, técnicos y físicos, así como procedimientos de control de acceso, continuidad del negocio, protección de datos personales y respuesta a incidentes de seguridad. El modelo también incorpora buenas prácticas descritas en ISO/IEC 27002 como guía para la implementación de medidas de control específicas como seguridad del personal, control de activos, criptografía, seguridad de redes, seguridad en el desarrollo y mantenimiento de sistemas y gestión de proveedores. Se adapta al contexto de los hospitales de nivel II donde los recursos son limitados, pero también muy dependientes de las tecnologías de tratamiento médico. Finalmente, se caracteriza por un enfoque de mejora continúa utilizando el ciclo PHVA (Planificar-Hacer-Verificar-Actuar), que permite evaluar periódicamente la efectividad de los controles implementados, fortalecer la cultura de seguridad de la información de los trabajadores de la salud y garantizar la resiliencia institucional frente a ciber amenazas y fallas operativas.

IMPLEMENTACIÓN

El SGSI es un modelo estructurado preventivo que se utiliza para garantizar que el centro de cómputo del Hospital La Caleta sea capaz de reconocer, asumir, gestionar y reducir los riesgos de seguridad de la información de manera eficiente y organizada.

Las normas ISO/IEC 27001 e ISO/IEC 27002 definen los objetivos y medidas de control para la implementación de un sistema de gestión de seguridad de la información (SGSI), que tiene como objetivo proteger la confidencialidad, integridad y disponibilidad de la información. La versión actual (ISO/IEC 27001:2022 e ISO/IEC 27002:2022) organiza los controles en 4 dominios principales que conforman los objetivos de seguridad específicos.

1. Controles organizacionales

Objetivo: Establecer gobernanza, políticas y procesos para gestionar la seguridad de la información. Incluya objetivos específicos como:

- Definir políticas de seguridad de la información.

- Asignar roles y responsabilidades
- Gestión de riesgos de seguridad de la información.
- Contabilidad de activos y uso aceptable.
- Clasificación de la información
- Seguridad en las relaciones con proveedores
- Seguridad mientras trabaja de forma remota
- Sensibilización y formación del personal.
- Manejo de incidentes de seguridad
- Continuidad del negocio
- Cumplimiento de la ley y la legislación.
- Protección de datos personales
- Gestión del cambio
- Seguridad del proyecto
- Prevención de la fuga de información.

2. Control personal

Objetivo: Reducir los riesgos relacionados con el factor humano.

Objetivos específicos:

- Antes de la aprobación del empleo (verificación básica)
- Condiciones de trabajo seguras
- Formación y sensibilización continua.
- Responsabilidad del usuario
- Procedimientos disciplinarios
- Seguridad en caso de cambio o cese de empleo
- Acuerdos de confidencialidad y no divulgación

3. Control físico

Finalidad: Proteger locales, equipos e infraestructuras de accesos físicos no autorizados o daños.

Objetivos específicos:

- Seguridad perimetral de objetos
- Control de acceso físico

- Protección de áreas seguras (salas de servidores, archivos clínicos, etc.)
- Protección contra peligros ambientales (incendio, inundación, daños eléctricos)
- Seguridad del equipo
- Eliminación segura de activos
- Limpiar mesas y mamparas.
- Proteger dispositivos fuera de la organización

4. Control tecnológico

Finalidad: proteger sistemas, redes y datos mediante medidas técnicas.
Objetivos específicos:

- Control de acceso lógico (usuarios y privilegios)
- Autenticación segura
- Gestión de identidad
- Protección contra malware
- Copias de seguridad
- Registro y monitoreo de eventos
- Seguridad de la red
- Criptografía y cifrado de información.
- Seguridad en el desarrollo de software.
- Gestión de vulnerabilidades
- Protección de aplicaciones y bases de datos
- Seguridad en los servicios en la nube
- Filtrado web y de correo electrónico
- Prevención de intrusiones
- Protección de la información en tránsito

El sistema propuesto para la gestión de la seguridad consta de las siguientes etapas:
El alcance,
la definición de las políticas SGSI,
la gestión de riesgos,
la declaración de aplicación y
la implementación de procedimientos y controles son todos temas importantes.

DEFINICION DEL ALCANCE

Es importante destacar que las mismas serán creadas siguiendo los dominios y controles de la ISO/IEC 27001 e ISO/IEC 27002

Será necesario definir el alcance en función de las características de la institución, considerando factores importantes como activos, organización, recursos, etc.

Después de definir el alcance, el director del hospital la Caleta, con el apoyo del jefe del departamento de Estadística e Informática y tecnología, será responsable de hacerlo.

El Hospital La Caleta define el SGSI como los servicios y sistemas que manejan información sobre los procesos cotidianos de la institución.

Para facilitar la comprensión de los procesos que incluye el alcance, se enumeran los siguientes servicios:

- Mantenimiento preventivo del equipamiento físico y de los sistemas que se manejan: Se llevarán a cabo revisiones regulares de ciertos componentes de hardware y software con el objetivo de garantizar un desempeño fiable tanto de equipos como sistemas y garantizar que los datos almacenados sean infalibles.
- Gestión de recursos humanos: Los empleados deben comprometerse a proteger la información. Se establecerán responsabilidades de gestión y estándares para asegurar la seguridad de recursos e información durante el periodo laboral, además de la fase posterior, de terminación o de cambio de empleo.
- Gestión de activos: la gestión de los activos propiedad del Hospital La Caleta es sin duda uno de los aspectos más cruciales. Se establecerán normas que describan las responsabilidades y regulan su uso adecuado, sin duda después de realizar una gestión completa de riesgos y vulnerabilidades potenciales.
- Acceso controlado. La verificación de identidad de un funcionario es necesaria para que tenga acceso a un recurso físico o lógico específico, manteniendo la confidencialidad e integridad de la información.

- Gestionar tanto las operaciones como las comunicaciones. Se definirán herramientas procedimientos para garantizar el correcto funcionamiento y operación de los mismos, así como para garantizar la disponibilidad de la información y evitar que la institución se arriesgue a detener sus procesos.

Es importante mencionar que la dirección del Hospital La Caleta está a cargo de definir el alcance, y el departamento de TICS brindará soporte y apoyo en los servicios y procesos mencionados anteriormente.

POLITICAS DE SEGURIDAD DEL SGSI

La siguiente política de seguridad para la implementación del Sistema de Gestión de Seguridad de la Información cubre la mayoría de las necesidades de gestión de seguridad de la información:

“Promover prácticas que aseguren la continuidad de las funciones del centro de cómputo del Hospital La Caleta mediante un Sistema de Gestión de Seguridad de la Información basado en un control preventivo y enfocado en lograr un nivel adecuado de integridad, confidencialidad y disponibilidad de la información institucional relevante”.

Objetivos:
Se han establecido metas para garantizar el cumplimiento de la política mencionada:

- Establecer controles para proteger la seguridad de la información.
- Realizar un plan para controlar y administrar los riesgos de la información.
- Establecer una solución para administrar la seguridad de la información.
- Monitore el SGSI para asegurarse de que se procese correctamente la información.

GESTIÓN DE RIESGOS

Es crucial analizar y evaluar el impacto de los riesgos para la institución teniendo en cuenta las posibles repercusiones en los procesos que se llevan a cabo, especialmente si se maneja información crucial.

Este proceso tiene como objetivo determinar si un riesgo específico es aceptable o, por el contrario, encontrar y aplicar el tratamiento adecuado para reducirlo.

Se trata de un enfoque cualitativo en el que se analizan los activos de la institución y se identifican las amenazas asociadas con ellos, así como su probabilidad de ocurrencia. A partir de esta información, se detallan las vulnerabilidades que podrían llevar a la ejecución o materialización de las amenazas.

Aquí hay un esquema de la metodología a utilizar: Ver Figura 11.

Figura 11

Metodología para la gestión de riesgos

Nota*: Elaboración propia*

Se ha establecido una metodología para llevar a cabo el análisis y evaluación de riesgos para completar este apartado.

IDENTIFICACIÓN DE ACTIVOS:

Todos los activos de la institución tienen un valor significativo porque contienen o manipulan información, por lo que es necesario protegerlos adecuadamente.

Después de identificar todos los activos, se evalúan para gestionar aquellos que se consideran "más importantes" o de "mayor relevancia" para el desarrollo de las actividades del Hospital La Caleta, basándose en el grado de impacto en la confidencialidad, integridad y disponibilidad de la información.

Una vez que se han identificado los activos considerados de "mayor importancia", se identifican tanto las amenazas como las vulnerabilidades, lo que determina el nivel de impacto en los activos de la institución.

Posteriormente, se realiza una evaluación y determinación de la probabilidad real de ocurrencia de la amenaza, considerando las consecuencias o los efectos que tendría en caso de materializarse, lo cual representa un riesgo para la confidencialidad, integridad y disponibilidad de la información.

Finalmente, el valor del riesgo se calcula dividiendo el valor del activo por el valor de la probabilidad de amenaza.

INVENTARIOS DE ACTIVOS INFORMÁTICOS:

El análisis y la gestión de riesgos de los activos que participan en los procesos de la Institución son uno de los pasos importantes para la implementación del SGSI.
Se asignó un código a cada activo identificado, ya sea físico, software o sistema de información. Ver tabla 12 y tabla 13

Tabla 12

Códigos

Abreviaturas o códigos	*Significado*
SIS	*Activo de tipo de sistema de información*
SW	*Activo de Tipo Software*
AF	*Activo de tipo físico ubicado dentro de la Institucion*

Tabla 13

Identificación de Activos Informáticos

Id	Activo	Características
AF-01	Servidor de archivos	Cantidad: 4 Marca: DELL Procesador: Xeon Memoria:128 Gb Disco duro:1 TB Cantidad: 195

AF-02	Computadoras	Marca: HP Procesador: Intel Core i5 Memoria:8 RAM Disco duro: 1 TB
AF-03	Switch	22
AF-04	Reuter	2
AF-05	Central Telefónico IP	1
AF-06	Central Telefónica KX-TD 1232 A/D	1
AF-07	Impresora Multifuncional/Copiadora	102
SIS-01	Sis Gedo (Sistema de tramite documentario)	El SISGEDO es un sistema informático que lleva a cabo diversas etapas de gestión documental, incluyendo la recepción, registro, clasificación, derivación, atención y archivamiento de documentos que provienen de las unidades orgánicas del Gobierno Regional Áncash y los que ingresan a la Entidad.
SIS-02	SIAF	Sistema Integrado de Administración Financiera
SIS-03	SIGA	Sistema Integrado de Gestión Administrativa
SIS-04	SISGALENOS	Sistemas de Gestión Hospitalaria
SW-01	Correo institucional	Outlook
SW-02	Cuentas de usuarios	Cuentas de Usuarios en el servidor del sistema Operativo Windows Server 2016
SIS-05	PLH	Software de Planillas
SIS-06	HIS ver-3.04-2007	Sistema de Información
SIS-07	TEMPUS	Sistema de Control de Asistencia
SIS-08	SINADEF	Sistema de Información de Defunción

SIS-09	CNV	Sistema de registro de certificado de nacido vivo

Nota: Elaborado por: Investigador

Se evalúa cada uno de los activos en un rango de 1 a 5 en función del nivel de confidencialidad, disponibilidad e integridad que brindan para el aseguramiento de la información para identificar los riesgos. Ver Tabla 14.

Tabla 14

Identificación de riesgos

Activo	Confidencialidad	Disponibilidad	Integridad	Total
Servidor de archivos	4	4	3	4
Computadoras	3	3	2	3
Switch	4	4	2	3
Router	4	3	3	3
Central	4	4	4	4
Telefónico IP				
Central Telefónica A/D	4	3	4	4
Impresora Multifuncional	4	3	3	3
SisGedo (Sistema de tramite documentario)	4	3	3	3
SIAF	3	4	4	4
SIGA	4	4	4	4
SISGALENOS	4	3	2	3
Correo institucional	3	3	3	3
Cuentas de usuarios	3	2	3	3
PLH	4	4	4	4
HIS ver-3.04-2007	4	3	4	4
TEMPUS	4	4	3	4

SINADEF	4	2	4	3
CNV	4	3	4	3

Nota: Elaborado por el Investigador

Se utiliza la tabla anterior para identificar los activos cuyo valor es superior o igual a 3.Ver tabla 15.

Tabla 15

Activos de mayor importancia

Activo	Total
Servidor de archivos	4
Computadoras	3
Switch	3
Router	3
Central Telefónico IP	4
Central Telefónica A/D	4
Impresora Multifuncional/copiadora	3
SisGedo (Sistema de tramite documentario)	3
SIAF	4
SIGA	4
SISGALENOS	3
Correo institucional	3
Cuentas de usuarios	3
PLH	4
HIS ver-3.04-2007	4
TEMPUS	4
SINADEF	3
CNV	3

Nota: Elaborado por: Investigador

Tabla 16

Calificación de los Activos, Amenazas y Vulnerabilidades del Hospital La caleta

Activo	Amenazas	Vulnerabilidades	Valoración del activo (1 al 5)	Probabilidad de ocurrencia de la amenaza (1-5)	Total Riesgo
Servidor de archivos	Cambiar la Información	Seguridad inexistente	4	3	12
	Robo de Datos	Cifrado débil o inexistente			
	Caídas de Tensión	Fuente de poder quemada			
	Temperaturas Extremas	Recalentamiento del chipset de video o microprocesador			
Computadoras	virus	Falta mantenimiento preventivo			
		Falta de capacidad de control de red			
	Malware	Utilización inadecuada de Internet			
		Los usuarios no reciben suficiente educación sobre técnicas de ataques informáticos.	4	3	12
	Phishing	Falta de herramientas contra el engaño			
	Servicio denegado	Falta de seguimiento de los enrutadores y firewall			
	Recalentar	Los cambios en el suministro eléctrico			
Switch	Bajo desempeño				

Router	Conexión con interrupciones	Falta de mantenimiento preventivo	3	3	9
	Recalentar	Los cambios en el suministro eléctrico			
	Bajo desempeño	Falta de Mantenimiento preventivo	3	3	9
	Conexión con interrupciones	La ubicación incorrecta del dispositivo			
Central Telefónico IP	Perdida de conectividad	Mal manejo de la central telefónica	4	3	12
Central Telefónica A/D	Perdida de conectividad	Mal manejo de la central telefónica	4	3	12
Impresora Multifuncional	Daños en los cartuchos	Falta de mantenimiento preventivo	3	4	12
	Daño en los cabezales				
	Atascamiento de papel	carga de papel incorrecta			
		Papel no adecuado			
SisGedo (Sistema de tramite documentario)	Perdida de información	La falta de medidas de seguridad	3	3	9
		Falta de medidas para controlar el acceso			
SIAF	Perdida de Información	La falta de medidas de seguridad	4	3	12
		Falta de medidas para controlar el acceso			
SIGA	Perdida de Información	La falta de medidas de seguridad			

		Falta de medidas para controlar el acceso	4	3	12
SISGALENOS	Perdidas de Información	La falta de medidas de seguridad Falta de medidas para controlar el acceso	4	3	12
Correo institucional	Eliminación o modificación de correos	La falta de medidas de seguridad Falta de medidas para controlar el acceso	4	3	12
Cuentas de usuarios	Eliminación o modificación de cuentas	La falta de medidas de seguridad Falta de medidas para controlar el acceso	4	3	12
PLH	Eliminación o Perdida de información	La falta de medidas de seguridad	4	3	12
HIS ver-3.04-2007	Perdidas de Información	Falta de medidas para controlar el acceso	4	3	12
TEMPUS	Perdidas de Información	Falta de medidas para controlar el acceso	4	3	12
SINADEF	Perdidas de Información	Falta de medidas para controlar el acceso	4	3	12
CNV	Perdidas de Información	Falta de medidas para controlar el acceso	4	3	12

Nota: Elaborado por el Investigador

c). Determinar la influencia del Modelo de las buenas prácticas en la gestión de la seguridad y el riesgo en el Hospital nivel II, la Caleta de Chimbote

Es la base del estudio, pues su propósito es evaluar específicamente el impacto que tendría la implementación de un modelo estructurado de seguridad de la información en un ambiente hospitalario real. En los hospitales secundarios, donde los servicios de atención especializada se combinan con limitaciones presupuestarias y tecnológicas,

la información clínica y administrativa es un activo crítico, cuya protección es esencial para garantizar la continuidad de la atención y la seguridad del paciente.

Este objetivo permite analizar si la aplicación de buenas prácticas -especialmente aquellas basadas en estándares internacionales como ISO/IEC 27001 e ISO/IEC 27002- ayuda a mejorar los procesos de identificación, evaluación y tratamiento de riesgos relacionados con los sistemas de información hospitalarios. También permite medir cambios en la capacidad institucional para prevenir incidentes como pérdida de datos, acceso no autorizado, cortes del sistema o violaciones de la confidencialidad de la información médica, situaciones que pueden afectar directamente la calidad de la atención médica. Además, centrarse en el "impacto" implica un análisis comparativo, normalmente utilizando un diseño pre-test-post-test o de intervención diagnóstica, que permita ver mejoras tangibles en la gestión de la seguridad antes y después de aplicar el modelo. Esto incluye aspectos organizativos, tecnológicos y humanos como la existencia de políticas formales, procedimientos de control de acceso, capacitación del personal, gestión de incidentes y continuidad del negocio. En el contexto del Hospital La Caleta Chimbote, donde la transformación digital del sector salud avanza paulatinamente, este análisis cobra mayor relevancia para fortalecer la resiliencia de las instituciones frente a amenazas internas y externas.

Finalmente, este objetivo específico proporciona evidencia científica sobre la viabilidad y efectividad de implementar modelos de seguridad de la información en hospitales públicos de nivel II, contribuyendo no solo a la protección de datos sensibles de los pacientes, sino también a la mejora de la gestión de riesgos institucionales, la toma de decisiones y el cumplimiento de la normativa aplicable. Por lo tanto, su desarrollo respalda la relevancia del modelo propuesto y su posible replicabilidad en otras instituciones de salud con características similares, constituyéndose como un componente clave para modernizar la gestión hospitalaria y garantizar servicios seguros, confiables y sostenibles.

CAPITULO IV

RESULTADOS Y DISCUSIÓN

En el estudio actual, los hallazgos recopilados se han ordenado de acuerdo con los objetivos específicos establecidos, lo que facilita la identificación estructurada de las conclusiones alcanzadas en el Hospital Nivel II La Caleta.

1.- Resultados en relación al objetivo específico: Conocer la seguridad de la información en el Hospital Nivel II La Caleta de Chimbote

Los hallazgos del diagnóstico indican que la seguridad de la información en el Hospital La Caleta presenta un estado de madurez que se sitúa entre bajo y medio. Durante el año 2024, se registraron un total de 145 incidentes de seguridad, siendo más frecuentes las infecciones por malware (32. 4%), la pérdida o corrupción de datos (16. 5%) y los accesos no autorizados (13. 7%).

Igualmente, se constató que un 55. 5% de los dispositivos informáticos presentan problemas técnicos recurrentes, el 100% no tiene antivirus actualizado y un número considerable de equipos no dispone de políticas de respaldo automático, lo que aumenta el riesgo de pérdida de información crítica.

Con respecto a la disponibilidad de los sistemas esenciales, se observaron tiempos de inactividad significativos en módulos fundamentales como historias clínicas (24 horas) y laboratorio (35 horas), lo que genera un impacto considerable en la continuidad del servicio en el hospital.

Estos hallazgos permiten inferir que la institución enfrenta notables debilidades en la gestión de la seguridad de la información, particularmente en lo que concierne a los controles técnicos, la gestión de incidentes y la cultura organizacional.

Enfoque Estadístico
1. Resultados del Objetivo Específico 1
Conocer la seguridad de la información en el Hospital La Caleta

Tabla 17

Incidentes de seguridad de la información registrados en el año 2024

Tipo de incidente	Frecuencia (n)	Porcentaje (%)
Infecciones por malware/virus	50	32.4
Pérdida o corrupción de información	24	16.5
Accesos no autorizados	20	13.7
Fallas de disponibilidad	15	10.3
Otros (errores/configuración)	36	24.8
Total	145	100%

Nota. Datos obtenidos del diagnóstico institucional.

Análisis estadístico:

Se observa que el 32.4% de los incidentes corresponde a malware, constituyendo la principal amenaza. Asimismo, los incidentes relacionados con factores humanos (errores y configuración) representan un 24.8%, evidenciando debilidades en la capacitación del personal.

Tabla 18

Estado de la infraestructura tecnológica

Indicador	Valor
Equipos con fallas técnicas	100
Porcentaje de equipos con fallas	55.5%
Equipos sin antivirus actualizado	180
Equipos sin respaldo automático	120
Equipos con sistemas obsoletos	30

Nota. Elaboración propia.

Análisis estadístico:

Más del 50% de los equipos presentan fallas, lo cual representa un riesgo alto. El hecho de que el 100% no cuente con antivirus actualizado evidencia una vulnerabilidad crítica en la seguridad tecnológica.

2. Resultados en relación con el objetivo específico: caracterizar el modelo de buenas prácticas para gestionar la seguridad de informacion en hospitales nivel II , la caleta Chimbote.

A través del examen de la situación vigente y la evaluación de estándares internacionales, se pudo delinear un modelo de prácticas adecuadas fundamentado en enfoques como ISO/IEC 27001, el cual combinas políticas, procedimientos y controles dirigidos a preservar la confidencialidad, integridad y accesibilidad de la información.

El modelo sugerido incluye elementos esenciales como:

- Establecimiento de políticas para la seguridad de la información
- Control de acceso y manejo de identidades
- Evaluación de riesgos y manejo de vulnerabilidades
- Aplicación de medidas técnicas (protección antivirus, respaldos, supervisión)
- Formación y sensibilización del personal
- Estrategias de continuidad operativa

Además, se constató que las áreas evaluadas muestran distintos grados de cumplimiento, destacando un bajo nivel en las políticas de seguridad y concienciación del personal, mientras que el manejo de accesos y incidentes presenta un nivel medio.

Esto facilitó la creación de un modelo adaptado al ámbito hospitalario, con el objetivo de reforzar la gestión integral de la seguridad de la información.

2. Resultados del Objetivo Específico 2

Caracterizar el modelo de buenas prácticas

Tabla 19

Nivel de cumplimiento de dimensiones de seguridad

Dimensión evaluada	Nivel de cumplimiento
Políticas de seguridad	Bajo
Gestión de accesos	Medio
Gestión de incidentes	Medio
Continuidad del negocio	Alto
Concienciación del personal	Bajo

Nota. Evaluación basada en diagnóstico institucional.

Análisis estadístico:

Se evidencia una distribución heterogénea, predominando niveles bajos y medios, lo que indica un nivel de madurez insuficiente. Las dimensiones más críticas son políticas de seguridad y concienciación.

3*. Resultados relacionados con el objetivo específico: Determinar la influencia del modelo de buenas prácticas en la gestión de la seguridad y el riesgos en el Hospital II , la Caleta Chimbote.*

Los hallazgos muestran que la adopción de un modelo de buenas prácticas tiene un impacto considerable en la optimización de la gestión de la seguridad de la información.

Se concluyó que la ejecución del modelo posibilita:

- Disminuir la frecuencia de incidentes de seguridad
- Administración de riesgos a través de la detección y el tratamiento oportuno de las vulnerabilidades
- Reforzar la protección de datos sensibles y los controles de acceso
- Aumentar la disponibilidad de sistemas críticos
- Fomentar una cultura organizativa centrada en la seguridad

Además, se evidencia que la formalización de los procesos y la integración de estándares internacionales tiene un efecto positivo en la calidad de las decisiones y en la continuidad de operaciones del hospital.

Por lo tanto, se verifica que el modelo de buenas prácticas tiene un efecto beneficioso en la gestión de la seguridad de la información, permitiendo reducir riesgos y mejorar el desempeño de los sistemas informáticos en el Hospital La Caleta

3. Resultados del Objetivo Específico 3: Influencia del modelo de buenas prácticas

Análisis Estadístico

Variable independiente: Modelo de buenas prácticas
Variable dependiente: Seguridad de la información

Los resultados muestran que el hospital presenta un nivel de madurez bajo en seguridad de la información, evidenciado por la alta incidencia de malware (32.4%) y la ausencia de controles básicos como antivirus actualizado. En este contexto, el modelo de buenas prácticas propuesto actúa como un mecanismo estructural que permite reducir vulnerabilidades, mejorar la gestión del riesgo y garantizar la continuidad operativa.

CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

1. Falta de un Sistema de Gestión de Seguridad de la Información (SGSI)

   El análisis cuantitativo demostró que el Hospital La Caleta *no ha implementado un Sistema de Gestión de Seguridad de la Información (SGSI) de acuerdo con la norma ISO/IEC 27001.* Esto se evidencia en la falta de políticas de seguridad de la información que son reconocidas por el 80% del personal. Esta circunstancia restringe la habilidad de la institución para salvaguardar la confidencialidad, integridad y disponibilidad de la información clínica y administrativa.

2. Mala administración de riesgos en la seguridad de la información.

   Se determina que la organización muestra *un nivel preocupante de desarrollo en la gestión de riesgos*, puesto que el 95% de los encuestados indica que no se utilizan metodologías para la identificación, análisis y tratamiento de riesgos. Esta vulnerabilidad aumenta la posibilidad de eventos de seguridad que podrían comprometer la continuidad de las operaciones del hospital.

3. Falta de preparación adecuada para manejar incidentes y fallos en los sistemas.

   Los hallazgos indican que el 95% del personal reporta que *no se realizan simulacros de caídas de sistemas*, lo que pone de manifiesto la ausencia de planes de contingencia y de continuidad del negocio. Esta situación viola las directrices establecidas en el Anexo A. 17 de la ISO/IEC 27001 y pone a la institución en riesgo de sufrir interrupciones críticas en el servicio de salud.

4. Controles operativos que han sido aplicados de manera incompleta y sin un formato uniforme.

   Aunque hay acciones efectivas como el control de acceso al Centro de Datos (90%), el mantenimiento preventivo de los equipos (87%) y el monitoreo de los sistemas (70%), *estos controles no están incorporados en un marco*

normativo oficial, lo que restringe su eficacia y durabilidad a lo largo del tiempo.

5. Administración de activos e inventarios con un grado de madurez intermedio.
   El manejo de los inventarios tecnológicos logra un 80%, lo que muestra progresos en la administración de activos; no obstante, la ausencia de una organización de la información y de encargados formales impide cumplir completamente con los requerimientos del Anexo A. 8 de la norma ISO/IEC 27001.

6. Importancia de reforzar la cultura organizacional en la seguridad de la información.
   Aunque el 80% del personal está informado sobre sus responsabilidades en el uso de los recursos tecnológicos, persiste un 20% que no tiene claridad sobre dichas obligaciones. Esto evidencia la necesidad de implementar programas estructurados de *sensibilización y formación que estén en línea con las buenas prácticas* establecidas por la norma.

.

5.2 RECOMENDACIONES

1. *Establecer un Sistema de Administración de Seguridad de la Información fundamentado en la norma ISO/IEC 27001.*

   Se sugiere crear e introducir gradualmente un Sistema de Gestión de Seguridad de la Información (SGSI) que contemple políticas de seguridad, metas, funciones y responsabilidades, con el apoyo claro de la alta dirección del Hospital La Caleta, garantizando su conformidad con la regulación del sector salud.

2. *Desarrollar y establecer de manera formal la administración de riesgos relacionados con la seguridad de la información.*

   Se sugiere utilizar un enfoque formal para la gestión de riesgos (como ISO/IEC 27005 o similar), que facilite la identificación, análisis, evaluación y manejo de los riesgos relacionados con los activos de información esenciales del hospital, dando prioridad a los sistemas clínicos y administrativos.

3. *Desarrollar y evaluar estrategias para la continuidad del negocio y la recuperación en caso de desastres*.

   Es esencial elaborar un Plan de Continuidad del Negocio (BCP) y un Plan de Recuperación ante Desastres (DRP), así como llevar a cabo ejercicios regulares de fallo de sistemas, de acuerdo con las directrices del Anexo A. 17 de la norma ISO/IEC 27001.

4. *Registrar y establecer de manera formal los controles de seguridad actuales.*

   Se sugiere uniformar y registrar los controles vigentes relacionados con el acceso, mantenimiento, supervisión y seguridad de las comunicaciones, incorporándolos al Sistema de Gestión de Seguridad de la Información (SGSI) para asegurar su seguimiento, progreso continuo y auditoría.

5. *Reforzar la administración de activos y de inventarios de información.*

   Se recomienda llevar a cabo un inventario completo de los activos de información, que abarque hardware, software, datos y servicios. Esto debe incluir la designación de responsables y la clasificación de la información de

acuerdo a su nivel de importancia, conforme al Anexo A. 8 de la norma ISO/IEC 27001.

6. *Establecer un programa continuo de formación y sensibilización.*
   Se sugiere implementar programas de capacitación continua en seguridad de la información para todo el personal, con el propósito de reducir la brecha de conocimiento detectada y mejorar la cultura de seguridad en la institución.

7. *Definir indicadores de rendimiento y promover la mejora constante.*
   Se sugiere establecer indicadores clave de rendimiento en seguridad de la información (KPIs) que faciliten la evaluación frecuente del grado de cumplimiento del SGSI y respalden la elaboración de decisiones estratégicas, alineándose con el ciclo de mejora continua PDCA propuesto por la norma ISO/IEC 27001.

I. REFERENCIAS BIBLIOGRAFICA

Alcántara Flores, J. C. (2015). *Guía de implementación de la seguridad basado en la norma ISO/IEC 27001, para apoyar la seguridad en los sistemas informáticos de la Comisaría del Norte P.N.P. en la ciudad de Chiclayo*.
[Tesis de pregrado, Universidad Católica Santo Toribio de Mogrovejo].
http://investigacion.usat.edu.pe/handle/usat/539

Almanza Ruiz, L. C., & Caldera Álvarez, V. L. (2023). *Buenas prácticas en la seguridad del paciente en el servicio de urgencia: ESE Camú Prado, Cereté, septiembre 2021–2022* (Trabajo de especialización). Universidad de Córdoba, Facultad de Ciencias de la Salud

Álvarez, G., Pérez, P. (2004). *Seguridad de la información para empresas y particulares.* (1era Ed) Mc Graw-Hill/interamericana de España, S. A. U.

Alavi, M., & Leidner, D. E. (2022). *Knowledge management and information systems: Conceptual foundations and research issues.* Springer.

Aguirre, J. R. (2006*). Libro electrónico de seguridad de la información y criptografía.* Universidad Politécnica de Madrid.

Aguilera, J., & Ramos, M. (2023). *Gestión de la seguridad de la información y ciberseguridad organizacional.* Alfaomega.

Aguilera, P. (2011*). Redes seguras* (seguridad de la información). Madrid, España: Editex.

Arenas Leaño, A. M. (2025). *Implementación de un sistema HIS para optimizar procesos hospitalarios en una clínica privada de la ciudad de Lima, Perú* (Tesis de posgrado, Universidad Privada del Norte).

Baldera Bravo, A. J. (2025). *Modelo de gestión de seguridad de la información basado en un enfoque de gestión de riesgos para el sector de salud privado de Chiclayo* (Tesis de posgrado, Universidad Nacional Pedro Ruiz Gallo).

Beynon-Davies, P. (2015). *Sistemas de información: Introducción a la informática en las organizaciones.* Editorial Reverté.

Cabello Roca, P. E. (2022*). Implementación de sistemas de gestión de seguridad de la información (SGSI), de servicios de TI (ITSM) y firma electrónica* (Trabajo de suficiencia profesional para optar el título de Ingeniero Informático). Pontificia Universidad Católica del Perú.

Calderón Sánchez, J. (2019). *Seguridad de la información y la gestión de riesgos en los trabajadores de la DIGERE del Ministerio de Educación, 2018* [Tesis de licenciatura, Universidad César Vallejo].

Calder, A. (2022). IT *governance: An international guide to data security and ISO 27001/ISO 27002* (7th ed.). Kogan Page.

Carr, J. J. (2022*). Introduction to biomedical equipment technology*. Editorial
Carranza, J., & Gómez, H. (2017). *Sistema de gestión de seguridad de la información basado en la norma ISO 27001 para el Hospital Nivel II La Caleta* [Tesis de maestría, Universidad Privada San Pedro].

Correa Sánchez, J. J. (2020). *Manual de buenas prácticas en seguridad de la información para entornos hospitalarios* [Trabajo de grado de pregrado, Universidad EIA].

Costas, J. (2011). *Seguridad y alta disponibilidad*. RA-MA Editorial.

Chiquito Manrique, C. D. (2023). *Implementación de políticas de seguridad en la infraestructura tecnológica del Hospital Básico Jipijapa mediante un appliance Fortinet 80E* [Proyecto de titulación de maestría, Universidad Estatal del Sur de Manabí, Instituto de Posgrado].

Enríquez, A. A. (2018). *Modelo de gestión de seguridad de la información para instituciones de salud, basado en las normas ISO 27799:2008, ISO/IEC 27005:2008 e*

ISO/IEC 27002:2013 aplicadas a la clínica médica fértil [Tesis de grado, Universidad Técnica del Norte]. Repositorio Institucional de la Universidad Técnica del Norte. https://repositorio.utn.edu.ec/handle/123456789/857

Faliero, J. C. (2023). *Infosecurity, seguridad informática, ciberseguridad & hacking: To hack and not to jail*. Ad Hoc. https://www.amazon.com.mx/INFOSECURITY-SEGURIDAD-INFORM%C3%81TICA-CIBERSEGURIDAD-HACKING/dp/9877452669

Falcon Fernández, J. A. (2021). *Propuesta de implementación de un sistema de gestión de seguridad de la información basado en la norma ISO 27001 para una empresa de telecomunicaciones* (Trabajo de investigación de licenciatura). Universidad Nacional José Faustino Sánchez Carrión, Huacho, Perú.

Fernández Caso, D. R. (2024). *Diseño de un sistema de gestión de seguridad de la información en el proceso de emisión de certificados médicos de aptitud: Caso Clínica IPC Salud* [Tesis de pregrado, Universidad Nacional Mayor de San Marcos].

García, A. (2024). *Ciberseguridad y ciberataques: retos del mundo digital*. Editorial.

Gupta, S., Kapoor, M., & Debnath, S. K. (2025). *Artificial intelligence-enabled security for healthcare systems: Safeguarding patient data and improving services*. Springer. https://doi.org/10.1007/978-3-031-82810-2

Gómez, A. (2006). *Seguridad de la información*. Ra-Ma.

Guevara, R. A. (2017). *Sistema de gestión de seguridad de la información basado en la norma ISO 27001 para el departamento de tecnologías de la información y comunicación del distrito 18D01 de educación* [Tesis de grado, Universidad Técnica de Ambato].

http://repositorio.uta.edu.ec/bitstream/123456789/26932/1/Investigacion_t1339si.pdf

Grubb, S. (2021). *How cybersecurity really works: A hands-on guide for anyone trying to secure their wired world*. No Starch Press.

Herrera Velásquez, M. H. (2025). *Sistema de gestión para la seguridad de la información y la confidencialidad de la información en el Hospital II-1 Moyobamba* (Tesis de posgrado). Universidad Nacional de San Martín.

Hernández-Sampieri, R., & Mendoza, C. (2022). *Metodología de la investigación: Las rutas cuantitativa, cualitativa y mixta*. McGraw-Hill Education.

Herzmann, D. P., Lashkari, A. H., & Parizadeh, M. (2024). *Understanding cybersecurity management in healthcare: Challenges, strategies and trends*. Springer. https://doi.org/10.1007/978-3-031-68034-2

García-Moliner, G., Pérez, J., & Torres, A. (2023). Security governance and international standards adoption: Impacts on organizational resilience. *Journal of Information Security and Applications, 69*, 103345.

Gómez, R., & Luna, M. (2022). *Gestión de proyectos: Buenas prácticas para equipos efectivos*. Editorial Universitaria. https://www.editorialuniversitaria.edu/libro/gestion-buenas-practicas

Guzmán, G. (2017). *Metodología para la seguridad de tecnologías de información y comunicación en la Clínica Ortega* [Tesis de maestría, Universidad Nacional del Centro del Perú]. Huancayo, Perú.

IBM Security. (2022). *X-Force Threat Intelligence Index 2022*. https://secure-iss.com/wp-content/uploads/2022/11/X-Force-Threat-Intelligence-Index-2022-Full-Report.pdf

ISACA. (2019). *COBIT® 2019 framework: Governance and management objectives*. Information Systems Audit and Control Association. https://www.isaca.org/resources/cobit

ISACA. (2023). *COBIT 2019: Governance and management objectives*. ISACA.

Instituto Nacional de Estadística e Informática (INEI). (2001). *Guía práctica para el desarrollo de planes de contingencia de los sistemas de información*. Talleres Gráficos del INEI.

International Organization for Standardization. (2022). *ISO/IEC 27002:2022: Information security, cybersecurity and privacy protection—Information security controls*. https://www.iso.org/standard/75652.html

International Organization for Standardization. (2022). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. ISO.

International Organization for Standardization & International Electrotechnical Commission. (2022). *ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls*. ISO.

Izquierdo Cabrera, J. (2021). *Modelo basado en la gestión de seguridad de la información para contribuir en los procesos de las farmacias de los hospitales II-I en la región Amazonas* (Tesis de maestría). Universidad Católica Santo Toribio de Mogrovejo, Chiclayo, Perú.

Kerzner, H. (2023). *Project management best practices* (5th ed.). Wiley. https://www.oreilly.com/library/view/project-management-best/9781394179206/

Remolina, L. C. (2019). *Diseño de un modelo de seguridad de la información a una empresa en su sistema de monitoreo del área de tecnología* [Trabajo de grado, Universidad Cooperativa de Colombia].

Roa, J. F. (2013). *Seguridad de la información* (1.ª ed.). McGraw-Hill/Interamericana de España, S. L.

Romero, M. I., Figueroa, G. L., & Área de Innovación y Desarrollo, S. Ll. (2018). *Introducción a la seguridad de la información y el análisis de vulnerabilidades* (1.ª ed.).

Sánchez, E., & Rebolledo, F. (2017). *Diseño de un modelo de gestión de la seguridad de la información en el área de talento humano de la secretaría de educación* [Tesis de grado, Institución Universitaria Politécnico Grancolombiano].

Stallings, W. (2023). *Network security essentials: Applications and standards*. Pearson Education.

Martínez. (2024). *Conceptos fundamentales de la seguridad y el riesgo*.

Mercado Rojas, J. E. (2016). *Modelo de gestión de seguridad de la información para el e-gobierno*.
http://catalogo.sisbib.unmsm.edu.pe/uhtbin/cgisirsi/?ps=kAuvpBt0C7/00/178200059/9

Molano, R. (2017). *Proyecto de investigación estrategia para implementar un sistema de gestión de la seguridad de la información basada en la norma ISO 27001 en el área de TI para la empresa Market Mix*.

MARKETmix. (s. f.). *Investigación/proyecto de investigación: estrategia para implementar SGSI según la norma ISO 27001 en el área de TI de la empresa MARKETmix* [Documento PDF].

Monteiro, S. C., & Cruz-Correia, R. J. (2022). *FHIR based interoperability of medical devices*.

Whitman, M. E., & Mattord, H. J. (2022). *Principles of information security* (7th ed.). Cengage Learning.

National Institute of Standards and Technology. (2024). *Framework for improving critical infrastructure cybersecurity (NIST CSF 2.0).*

Nicho Gómez, M. N. (2024). *Modelo de gestión de riesgos para mejorar la seguridad de la información en los procesos de emergencia en el sector salud pública de la región Lambayeque* [Tesis de maestría, Universidad Católica Santo Toribio de Mogrovejo].

Peltier, T. R. (2023). *Information security policies, procedures, and standards*. Auerbach Publications.

Pérez, J. (2024). *Ciberseguridad en un mundo digital: amenazas y estrategias*. Sin editorial.

Reyes Araujo, D. G. (2023). *Modelo de buenas prácticas para la calidad de atención del personal de enfermería del Instituto Nefro urológico del Norte, Chiclayo* [Tesis de maestría, Universidad Señor de Sipán].

Sharp, R. (2024). *Introduction to cybersecurity: A multidisciplinary challenge*. Springer. https://link.springer.com/book/10.1007/978-3-031-41463-3

Rodríguez, A. (2023). *Seguridad y amenazas en el ciberespacio*.

Rosero Córdoba, J. E. (2024). *Recomendar las mejores prácticas en el sector salud basadas en frameworks de ciberseguridad aplicables a hospitales del sector público en Colombia* [Trabajo de especialización, Universidad Nacional Abierta y a Distancia].

Ross, R. A. (2024). *Managing information security risk: Threats, vulnerabilities, and resilience*. Springer.

Sharma, D. P., Lashkari, A. H., & Parizadeh, M. (2024). *Understanding cybersecurity management in healthcare: Challenges, strategies and trends*. Springer. https://doi.org/10.1007/978-3-031-68034-2

Sánchez Marín, R. V. (2024). *Implementación de un sistema de gestión de información y eventos de seguridad para la detección de amenazas en una entidad pública del sector salud* [Investigación de posgrado]. Universidad Nacional Tecnológica de Lima Sur.

Sierra, D., & Cadena, M. (2017). *Modelo de un sistema de gestión de la seguridad de la información (SGSI) aplicada a entidades bancarias*. Investigación de Ingeniería, Universidad Distrital Francisco José de Caldas, Bogotá, Colombia.

Siesquen Sandoval, P. (2022). *Desarrollo de un modelo de gestión de incidentes de TI basado en estándares de buenas prácticas para mejorar el servicio de TI en las direcciones regionales de salud del Perú* [Tesis de pregrado, Universidad Señor de Sipán].

Valverde, S. (2025). *Fundamentos de seguridad informática para todos*.

Vaca, P. (2019). *Modelo de gestión de seguridad lógica de la información en la protección de los datos sensibles de los distritos de educación del Ecuador* (Tesis de maestría, Universidad Técnica de Ambato, Ecuador).

Vega Valqui, C. (2025). *Sistema de gestión de seguridad de la información, basado en normas ISO, para mejorar la seguridad de la información en la Gerencia Regional de Salud Lambayeque* (Tesis de pregrado). Universidad Nacional Pedro Ruiz Gallo.

Vieites, Á. G. (2013). *Auditoría de seguridad de la información*. Ediciones de la U.

Villegas Rivera, C. A. (2022). *Modelo de gestión de riesgos de TI que contribuye en la protección de los activos de información en hospitales de nivel II-1 de la región Amazonas* (Tesis de maestría). Universidad Católica Santo Toribio de Mogrovejo.

Villanueva Espinoza, E. (2021). *Implementación de un sistema informático para mejorar la atención de pacientes en los servicios de emergencia y hospitalización del Hospital Carlos Lanfranco La Hoz* (Tesis de titulación profesional). Universidad Tecnológica del Perú.

Von Solms, R., & Van Niekerk, J. (2022). *Information security governance*. Springer.
Whitman, M. E., & Mattord, H. J. (2022). *Principles of information security* (7th ed.). Cengage Learning.

Whitman, M. E., & Mattord, H. J. (2022). *Gestión de la seguridad de la información* (Módulo 3). Cengage Learning. https://wcruzy.pe/sdli/04gestion.pdf
William Stallings (2024) *Computer Security: Principles and Practice*

Yang, M. B. H. Yap, & H. Ohno-Machado (Eds.), *MEDINFO 2021: One World, One Health – Global Partnership for Digital Innovation* (pp. 123–129). IOS Press. https://www.researchgate.net/publication/361144212_FHIR_Based_Interoperability_of_Medical_Devices.

,

.

ANEXO N°01

ENCUESTA

La finalidad de este cuestionario es determinar el grado de seguridad de la información que se presenta en la entidad.

INSTRUCCIONES; Examina detenidamente las afirmaciones antes de contestar a las propuestas que se presentan.

Nro	Pregunta	Alternativa	
		SI	NO
1	¿Existen políticas actuales de seguridad para la gestión de la información?		
2	¿Están establecidas responsabilidades para los empleados en cuanto al uso adecuado de los recursos?		
3	¿Existe alguna forma de controlar el acceso no autorizado del personal para proteger los sistemas y equipamiento de la institución?		
4	¿Los equipos de la institución reciben mantenimiento regular?		
5	¿Se han llevado a cabo simulacros de caídas de los sistemas que controlan?		
6	¿Se monitorean los sistemas de información que administran?		
7	¿Se implementa gestión de riesgos en relación con la seguridad de la información?		
8	¿Qué medidas de seguridad se implementan en los sistemas de información y comunicación?		
9	¿Qué medidas de seguridad se implementan en los sistemas de información y comunicación?		
10	¿La dirección del hospital revisa constantemente los temas de seguridad de la información		
11	¿Están identificados y registrados los activos de información (sistemas, datos, equipos)?		

12	¿Está protegida la información almacenada en las computadoras portátiles?		
13	¿Los empleados reciben capacitación en seguridad de la información?		
14	¿Existe control de acceso a áreas sensibles (archivos clínicos, farmacias)?		
15	¿Cada usuario tiene credenciales individuales para acceder a los sistemas?		
16	¿Se utilizan sistemas antivirus o antimalware?		
17	¿Se realizan copias de seguridad de los datos periódicamente?		
18	¿Existe un procedimiento para reportar incidentes de seguridad?		
19	¿Se realizan pruebas de conmutación por error o recuperación ante desastres?		
20	¿Se toman acciones correctivas después del incidente?		