



FACULTAD DE INGENIERÍA



ESCUELA DE INGENIERÍA
DE
SISTEMAS Y COMPUTACIÓN



PROYECTO DE INVESTIGACIÓN:

**SISTEMA DE GESTIÓN DE SEGURIDAD DE LA
INFORMACIÓN BASADO EN LA NORMA ISO 27001:2022
PARA LA INVULNERABILIDAD DEL HOSPITAL CARRIÓN**

PRESENTADO POR:

Bach. ROMERO CARHUAS, Andy Charles

Líneas de investigación: Ingeniería e Infraestructura

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO DE SISTEMAS Y COMPUTACIÓN

HUANCAYO - PERÚ

2024

CONTENIDO

- 1. EL PROBLEMA DE INVESTIGACIÓN**
- 2. MARCO TEÓRICO**
- 3. METODOLOGÍA**
- 4. RESULTADOS**
- 5. DISCUSIÓN DE RESULTADOS**
- 6. CONCLUSIONES Y RECOMENDACIONES**



PROBLEMA DE INVESTIGACIÓN

DESCRIPCIÓN DE LA REALIDAD PROBLEMÁTICA



La seguridad de la información es un aspecto crítico en cualquier organización, especialmente en instituciones de salud donde se maneja una gran cantidad de datos sensibles como registro de pacientes, datos del personal, registros financieros. El área administrativa del Hospital Docente Quirúrgico Daniel Alcides Carrión de Huancayo enfrenta serios desafíos en la gestión de la seguridad de la información ya que no llevan controles de accesos, usan sistemas desfasados, no tienen políticas de manejo de datos, lo cual afecta la confidencialidad, integridad y disponibilidad de datos críticos.



FORMULACIÓN DEL PROBLEMA



Problema General:

¿De qué manera influye el sistema de gestión de seguridad de la información basado en la norma ISO 27001:2022 para la invulnerabilidad del hospital Carrión?

Problemas Específicos:

¿De qué manera influye el sistema de gestión de seguridad de la información basado en la norma ISO 27001:2022 en la confidencialidad del hospital Carrión?

¿De qué manera influye el sistema de gestión de seguridad de la información basado en la norma ISO 27001:2022 en la Integridad del hospital Carrión?

¿De qué manera influye el sistema de gestión de seguridad de la información basado en la norma ISO 27001:2022 en la disponibilidad del hospital Carrión?

OBJETIVOS

Objetivo General:

Determinar la influencia de la implementación de un sistema de gestión de seguridad de la información basado en la norma ISO 27001:2022 mejora la invulnerabilidad del Hospital Carrión.

Objetivos Específicos:

Determinar la influencia de la implementación de un sistema de gestión de seguridad de la información basado en la norma ISO 27001:2022 fortalece la confidencialidad del Hospital Carrión

Determinar la influencia de la implementación de un sistema de gestión de seguridad de la información basado en la norma ISO 27001:2022 mejora la integridad del Hospital Carrión

Determinar la influencia de la implementación de un sistema de gestión de seguridad de la información basado en la norma ISO 27001:2022 aumenta la disponibilidad del Hospital Carrión



MARCO TEÓRICO

ANTECEDENTES INTERNACIONALES



Guerra Aleman, 2020). En la tesis “PLAN DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA EP-EMAPA-A CON LA NORMA ISO/IEC27001:2013” PONTIFICA UNIVERSIDAD CATÓLICA DEL ECUADOR, Aborda la siguiente problemática. En la actualidad las empresas, se encuentran expuestas a fraudes y robos de información La información que maneja la EP-EMAPA-A, es sensible y, por lo tanto, es resguardada, de ahí que las normas ISO 27001 El objetivo general de este estudio, se centra en: Desarrollar un plan de gestión de seguridad de la información para la EP-EMAPA-A con la norma ISO/IEC 27001:2013 para el centro de la base de datos, pues su finalidad es generar una cultura de manejo de información tanto en administradores como en usuarios,



MARCO TEÓRICO



ANTECEDENTES NACIONALES

(Castro Hidalgo, 2020) En la tesis “Diseño de un sistema de gestión de seguridad de la información para la Corte Superior de Justicia de Piura, mediante la normativa ISO/IEC 27001”. Aborda el problema de que en la Corte Superior de Piura (CSJP) existe gran diversidad de información importante y confidencial que debe ser protegida de un amplio rango de amenazas tanto de orden fortuito (incendios, inundaciones) así como de orden premeditado, tal como estafa, espionaje, conspiración, vandalismo etc, Teniendo como objetivo salvaguardar la información -Este trabajo de tesis presenta un diseño basado en la norma ISO 27001 en cual se acomoda a las necesidades de la Corte Superior de Justicia de Piura.

HIPÓTESIS

Hipótesis General:

La implementación de un sistema de gestión de seguridad de la información basado en la norma ISO 27001:2022 influye positivamente en la invulnerabilidad del Hospital Carrión

Hipótesis Específicos:

La implementación de un sistema de gestión de seguridad de la información basado en la norma ISO 27001:2022 fortalece la confidencialidad en el Hospital Carrión

La implementación de un sistema de gestión de seguridad de la información basado en la norma ISO 27001:2022 mejora la integridad en el Hospital Carrión

La implementación de un sistema de gestión de seguridad de la información basado en la norma ISO 27001:2022 aumenta la disponibilidad en el Hospital Carrión

OPERACIONALIZACIÓN DE VARIABLES

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO
27001:2022 PARA LA INVULNERABILIDAD DEL HOSPITAL CARRIÓN



UPLA
UNIVERSIDAD PERUANA LOS ANDES

VARIABLES	DIMENSIONES	INDICADORES	DESCRIPCIÓN	TÉCNICA	INSTRUMENTO	UNIDAD O MEDIDA
VARIABLE I SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO 27001:2022	Política de Seguridad de la Información	<ul style="list-style-type: none"> Porcentaje de empleados capacitados en la política de seguridad. 	Determinar el porcentaje de empleados capacitados en la política de seguridad.	Entrevista	Cuestionario	% de empleados capacitados
	Gestión de Activos	<ul style="list-style-type: none"> Porcentaje de activos clasificados. 	Determinar porcentaje de activos clasificados.	Entrevista	Cuestionario	% de activos clasificados
	Control de Acceso	<ul style="list-style-type: none"> Porcentaje de sistemas con controles de acceso implementados 	Determinar porcentaje de controles de acceso implementados	Encuestas	Cuestionario	% de sistemas con control
	Seguridad Física y del Entorno	<ul style="list-style-type: none"> Porcentaje de áreas con control de acceso físico 	Determinar porcentaje de áreas con control de acceso físico	Encuestas	Cuestionario	% de áreas con control
	Cumplimiento	<ul style="list-style-type: none"> Porcentaje de cumplimiento con requisitos legales 	Determinar porcentaje de cumplimiento con requisitos legales	Fichaje	Ficha de Observación	% de cumplimiento
VARIABLE II INVULNERABILIDAD	Confidencialidad	<ul style="list-style-type: none"> Porcentaje total de accesos no autorizados a la información 	Determinar el Porcentaje total de accesos no autorizados a la información	Fichaje	Ficha de Observación	% de accesos no autorizados
	Integridad	<ul style="list-style-type: none"> Porcentaje total de información modificada sin autorización 	Determinar porcentaje total de información modificada sin autorización	Fichaje	Ficha de Observación	% de información modificada
	Disponibilidad	<ul style="list-style-type: none"> Porcentaje total de inaccesibilidad de la información 	Determinar porcentaje total de inaccesibilidad de la información	Fichaje	Ficha de Observación	% de inaccesibilidad

METODOLÓGICA

MÉTODO DE INVESTIGACIÓN

Deductivo

TIPO DE INVESTIGACIÓN

Aplicada

ALCANCE DE LA INVESTIGACIÓN

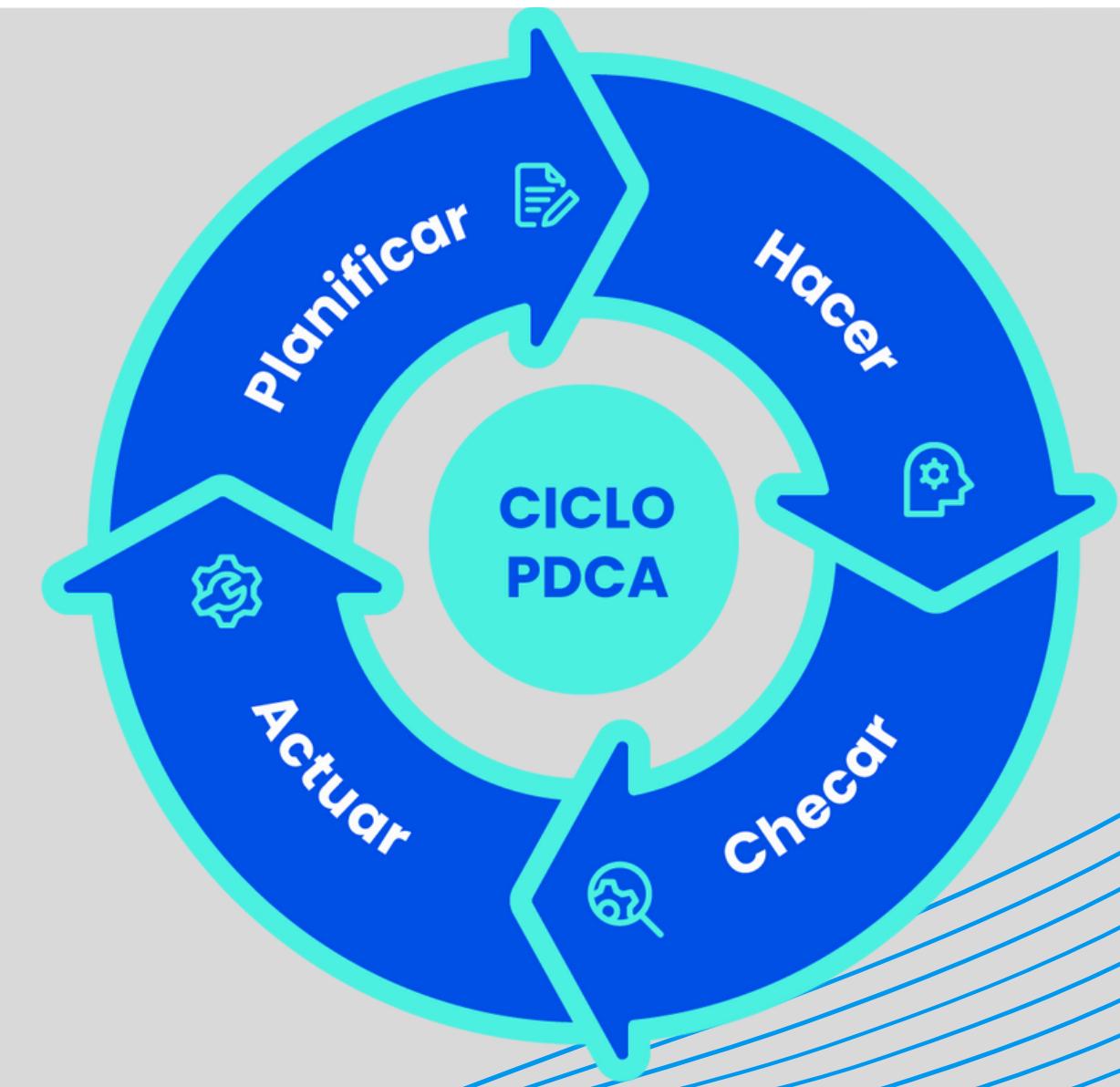
Explicativo

DISEÑO DE INVESTIGACIÓN

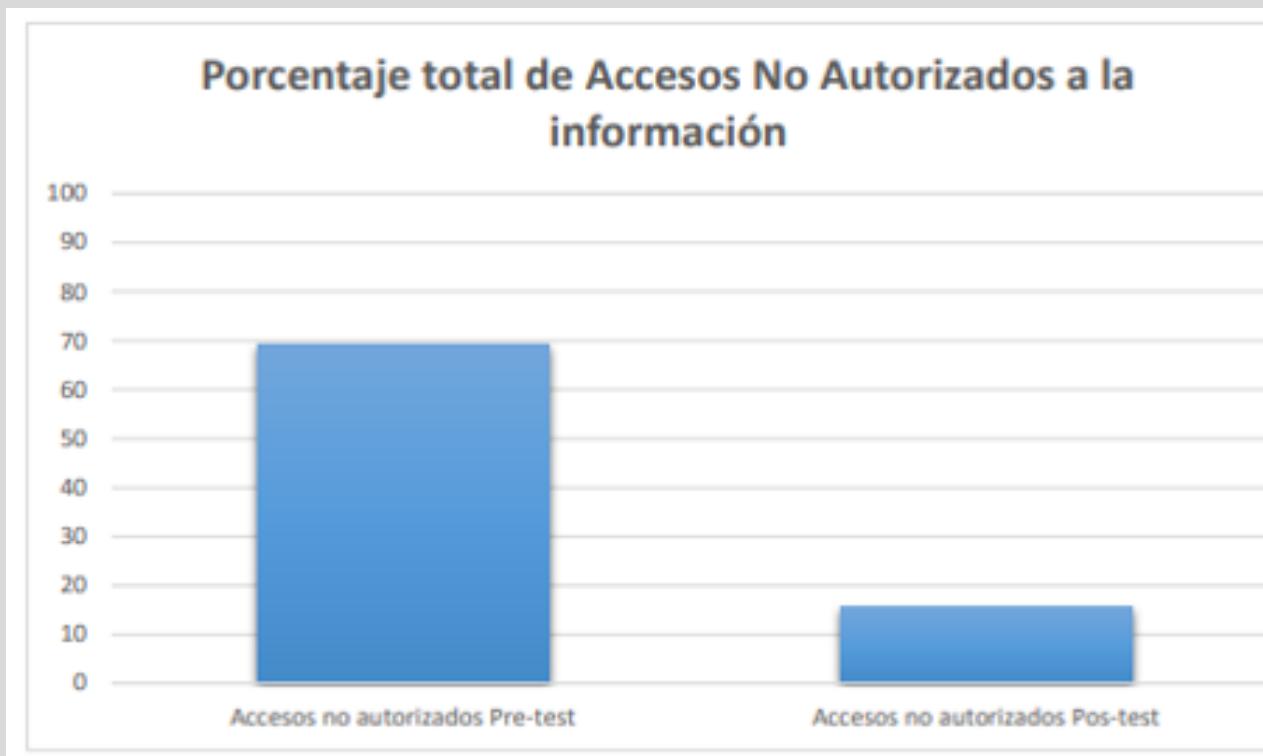
Pre-experimental

CICLO PDCA O CICLO DEMING

es una estrategia de mejora continua de la calidad de las empresas a través de una metodología de resolución de problemas utilizado en los sistemas de gestión, compuesto de cuatro puntos básicos y cuyo fin último es la calidad.



RESULTADOS CONFIDENCIALIDAD



Estadísticos descriptivos					
	N	Mínimo	Máximo	Media	Desv. Desviación
PRE_TEST	20	45	83	68,85	12,991
POST_TEST	20	0	30	15,40	8,165
N válido (por lista)	20				

Figura 3: Estadísticos descriptivos del indicador de Accesos No Autorizados a la información con el PreTest y Postest

Pruebas de normalidad						
	Kolmogorov-Smirnov ^a		Shapiro-Wilk			
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
DIFERENCIA	,141	20	,200 ^b	,959	20	,533

*. Esto es un límite inferior de la significación verdadera.
a. Corrección de significación de Lilliefors

Figura 9: Prueba Shapiro-Wilk para Accesos no autorizados a la información

Rangos			
		N	Rango promedio
POST_TEST - PRE_TEST	Rangos negativos	20 ^a	10,50
	Rangos positivos	0 ^b	,00
	Empates	0 ^c	
	Total	20	

a. POST_TEST < PRE_TEST
b. POST_TEST > PRE_TEST
c. POST_TEST = PRE_TEST

Figura 12. Pruebas de rangos con signo de Wilcoxon de la primera hipótesis

Estadísticos de prueba^a	
Z	-3,922 ^b
Sig. asintótica(bilateral)	,000

a. Prueba de rangos con signo de Wilcoxon
b. Se basa en rangos positivos.

Figura 13. Significancia asintótica de la primera hipótesis

RESULTADOS DE INTEGRIDAD



Estadísticos descriptivos					
	N	Mínimo	Máximo	Media	Desv. Desviación
PRETEST	20	40	70	52,60	8,708
POSTEST	20	0	22	11,40	7,287
N válido (por lista)	20				

Figura 5. Estadísticos descriptivos del indicador de Información Modificada sin Autorización con el PreTest y PostTest

Pruebas de normalidad						
	Kolmogorov-Smirnov ^a		Shapiro-Wilk			
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
DIFERENCIA	,128	20	,200*	,950	20	,372

*. Esto es un límite inferior de la significación verdadera.
a. Corrección de significación de Lilliefors

Figuras 10. Prueba Shapiro-Wilk para Información Modificada sin Autorización

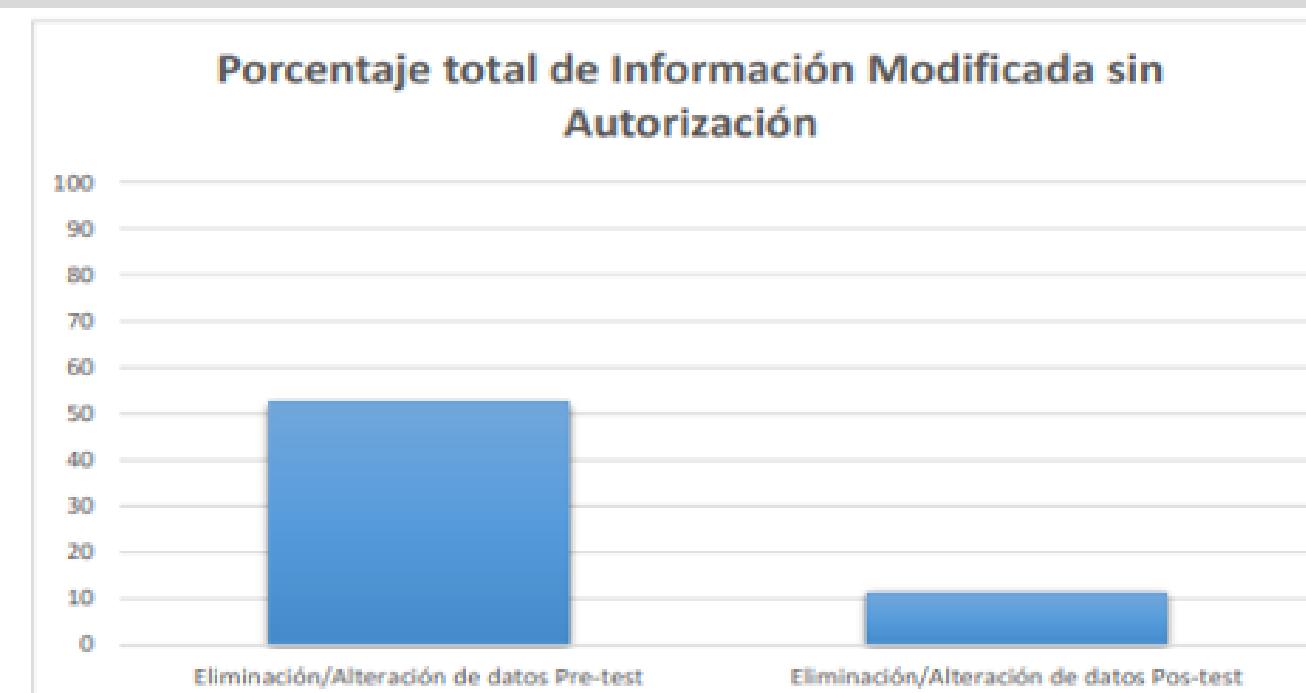


Figura 6. Histograma del PreTest y PostTest de Modificación de información

		Rangos	N	Rango promedio	Suma de rangos
POSTEST - PRETEST	Rangos negativos	20 ^a		10,50	210,00
	Rangos positivos	0 ^b		,00	,00
	Empates	0 ^c			
	Total	20			

a. POSTEST < PRETEST
b. POSTEST > PRETEST
c. POSTEST = PRETEST

Figura 14. Prueba de rangos con signo de Wilcoxon de la segunda hipótesis con

Estadísticos de prueba ^a	
POSTEST - PRETEST	
Z	-3,924 ^b
Sig. asintótica(bilateral)	,000

a. Prueba de rangos con signo de Wilcoxon
b. Se basa en rangos positivos.

Figura 15. Significancia asintótica de la segunda hipótesis

RESULTADOS DISPONIBILIDAD



Estadísticos descriptivos					
	N	Mínimo	Máximo	Media	Desv. Desviación
PRETEST	20	30	75	47,15	12,419
POSTEST	20	0	29	11,95	9,795
N válido (por lista)	20				

Figura 7. Estadísticos descriptivos del indicador de Inaccesibilidad a la información

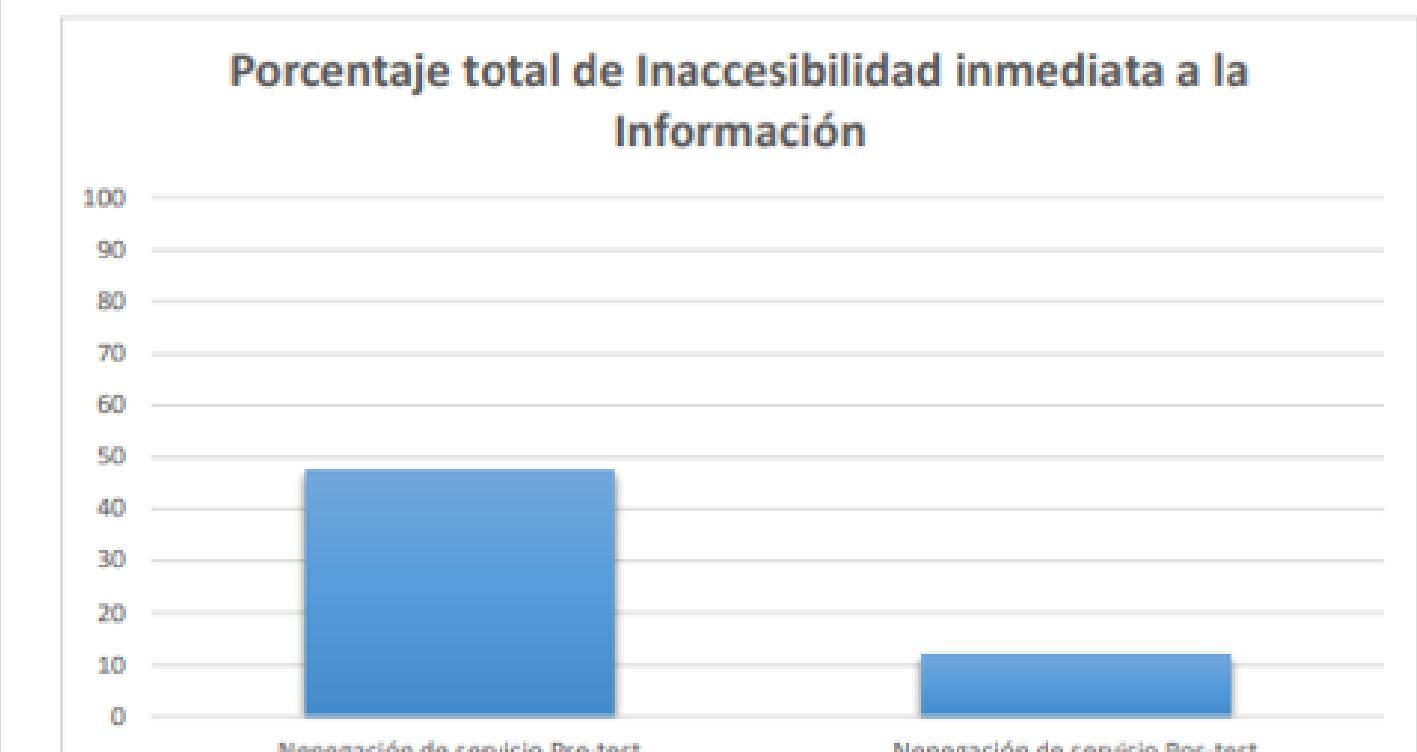


Figura 8. Histograma del PreTest y PosTest de Inaccesibilidad de información

Pruebas de normalidad						
Kolmogorov-Smirnov ^a			Shapiro-Wilk			
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
DIFERENCIA	,114	20	,200 ^b	,966	20	,660

a. Corrección de significación de Lilliefors

Figura 11. Prueba Shapiro-Wilk para Inaccesibilidad Inmediata a la Información

Rangos				
		N	Rango promedio	Suma de rangos
POSTEST - PRETEST	Rangos negativos	20 ^a	10,50	210,00
	Rangos positivos	0 ^b	.00	.00
	Empates	0 ^c		
	Total	20		

a. POSTEST < PRETEST
b. POSTEST > PRETEST
c. POSTEST = PRETEST

Figura 16. Pruebas de rangos con signo de Wilcoxon de la tercera hipótesis

Estadísticos de prueba ^a	
	POSTEST - PRETEST
Z	-3,921 ^b
Sig. asintótica(bilateral)	,000

a. Prueba de rangos con signo de Wilcoxon
b. Se basa en rangos positivos.

Figura 17. Significancia asintótica de la tercera hipótesis

Fuente: Elaboración propia

MATRIZ DE CONSISTENCIA

"Sistema de gestión de seguridad de la información basado en la norma ISO 27001:2022 para la invulnerabilidad del hospital Carrión"



PROBLEMAS	OBJETIVOS	HIPÓTESIS	VARIABLES	METODOLOGÍA
PROBLEMA GENERAL: ¿De qué manera influye el sistema de gestión de seguridad de la información basado en la norma ISO 27001:2022 para la invulnerabilidad del Hospital Carrión?	OBJETIVO GENERAL: Determinar la influencia de la implementación de un sistema de gestión de seguridad de la información basado en la norma ISO 27001:2022 mejora la invulnerabilidad del Hospital Carrión	HIPÓTESIS GENERAL: La implementación de un sistema de gestión de seguridad de la información basado en la norma ISO 27001:2022 influye positivamente en la invulnerabilidad del Hospital Carrión	VARIABLE I SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO 27001:2022	MÉTODO DE INVESTIGACIÓN: Método deductivo TIPO DE INVESTIGACIÓN: Aplicada ALCANCE DE LA INVESTIGACIÓN: Explicativa DISEÑO DE LA INVESTIGACIÓN: pre experimental POBLACIÓN: 17 oficinas administrativas MUESTRA: 3 oficinas administrativas TECNICAS DE ENTREVISTA Entrevista, encuesta, Fichaje
PROBLEMA ESPECÍFICO ¿De qué manera influye el sistema de gestión de seguridad de la información basado en la norma ISO 27001:2022 en la confidencialidad del Hospital Carrión?	OBJETIVOS ESPECÍFICOS Determinar la influencia de la implementación de un sistema de gestión de seguridad de la información basado en la norma ISO 27001:2022 fortalece la confidencialidad del Hospital Carrión.	HIPÓTESIS ESPECÍFICO La implementación de un sistema de gestión de seguridad de la información basado en la norma ISO 27001:2022 fortalece la confidencialidad en el Hospital Carrión.		
¿De qué manera influye el sistema de gestión de seguridad de la información basado en la norma ISO 27001:2022 en la Integridad del Hospital Carrión?	Determinar la influencia de la implementación de un sistema de gestión de seguridad de la información basado en la norma ISO 27001:2022 mejora la integridad del Hospital Carrión.	La implementación de un sistema de gestión de seguridad de la información basado en la norma ISO 27001:2022 mejora la integridad en el Hospital Carrión.		
¿De qué manera influye el sistema de gestión de seguridad de la información basado en la norma ISO 27001:2022 en la disponibilidad del Hospital Carrión?	Determinar la influencia de la implementación de un sistema de gestión de seguridad de la información basado en la norma ISO 27001:2022 aumenta la disponibilidad del Hospital Carrión.	La implementación de un sistema de gestión de seguridad de la información basado en la norma ISO 27001:2022 aumenta la disponibilidad en el Hospital Carrión.		

DISCUSIONES RESUELTAS



Finalmente, Paredes y Voto (2021) desarrollaron un marco de trabajo de protección de la información para el control de accesos de usuarios, enfocado y guiado en la normativa ISO/IEC 27001:2022, en empresas de teletrabajo. Su estudio reveló una disminución significativa del 65.40% al 37.10% en la falta de disponibilidad de la información, representando un mejoramiento del 28.3% tras la implementación.

En otro estudio, Risco (2021) examinó el desarrollo de un sistema de gestión resguardo de la información conforme a la directriz ISO 27001:2022 en una entidad enfocada en la construcción. La implementación de dicho sistema resultó en una mejora del 41.20% en la integridad de la información de la entidad.

CONCLUSIONES Y RECOMENDACIONES



Se sugiere la adaptación integral de la directriz ISO/27001:2022 en la totalidad de las funciones de las instituciones del sector público hospitalario. Obtener la certificación internacional a través de esta norma no solo asegura la conformidad con estándares reconocidos a nivel mundial, sino que también genera una mayor confianza en la protección de los activos de la institución

Se recomienda llevar a cabo una investigación exhaustiva no solo sobre la norma ISO 27001, sino también sobre otras normativas y estándares relacionados, como la NTP/ISO 27001 específicamente adaptada para instituciones públicas del estado peruano.