



**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**



**UPLA**  
UNIVERSIDAD PERUANA LOS ANDES

1

# 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.



**UPLA**  
UNIVERSIDAD PERUANA LOS ANDES

# 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



**UPLA**  
UNIVERSIDAD PERUANA LOS ANDES

## 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,





## 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 presento un diseño basado en la norma ISO 27001 en cual se acomoda a las necesidades de la Corte Superior de Justicia de Piura.



# HIPÓTESIS

## Hipotesis 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

## Hipotesis 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



**UPLA**  
UNIVERSIDAD PERUANA LOS ANDES



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

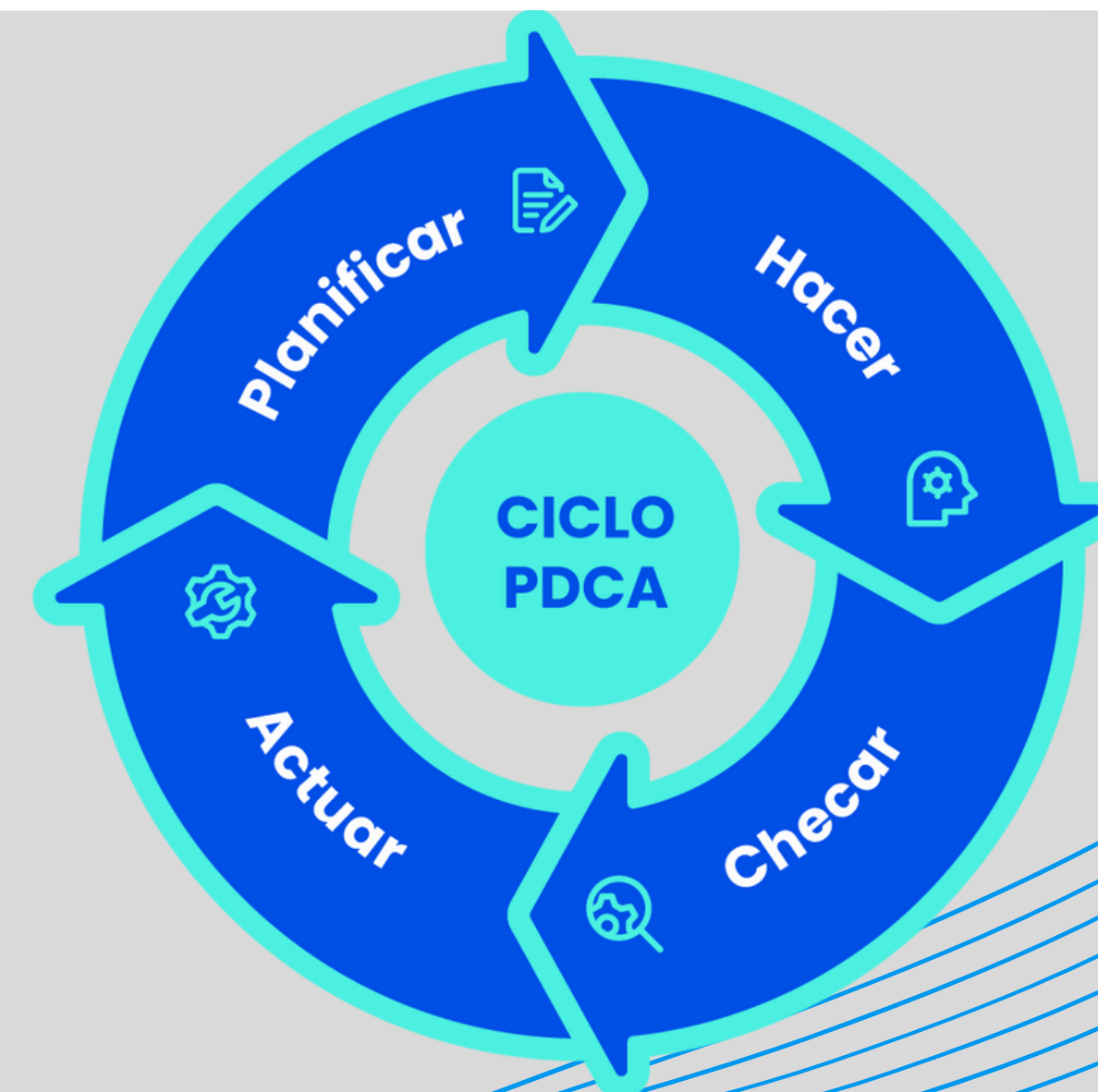
Explicativo

## 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.



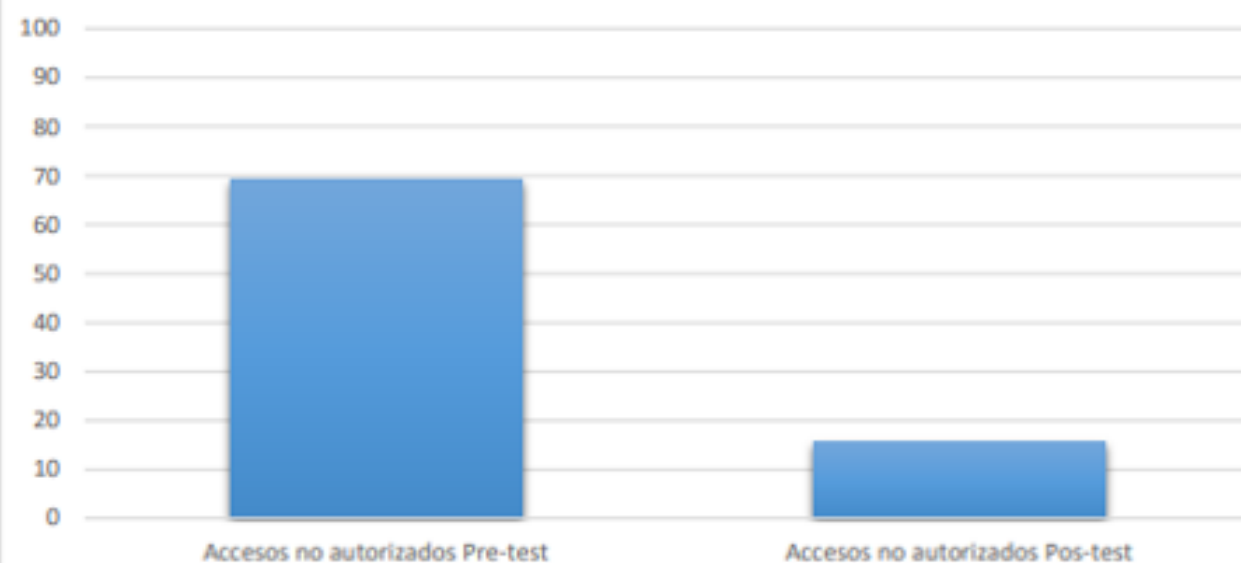
**UPLA**  
UNIVERSIDAD PERUANA LOS ANDES

## 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 Posttest

## Porcentaje total de Accesos No Autorizados a la información



## Pruebas de normalidad

	Kolmogorov-Smirnov <sup>a</sup>			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
DIFERENCIA	,141	20	,200 <sup>*</sup>	,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	Suma de rangos
POST_TEST - PRE_TEST	Rangos negativos	20 <sup>a</sup>	10,50	210,00
	Rangos positivos	0 <sup>b</sup>	,00	,00
	Empates	0 <sup>c</sup>		
	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<sup>a</sup>

	POST_TEST - PRE_TEST
Z	-3,922 <sup>b</sup>
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

## Porcentaje total de Información Modificada sin Autorización

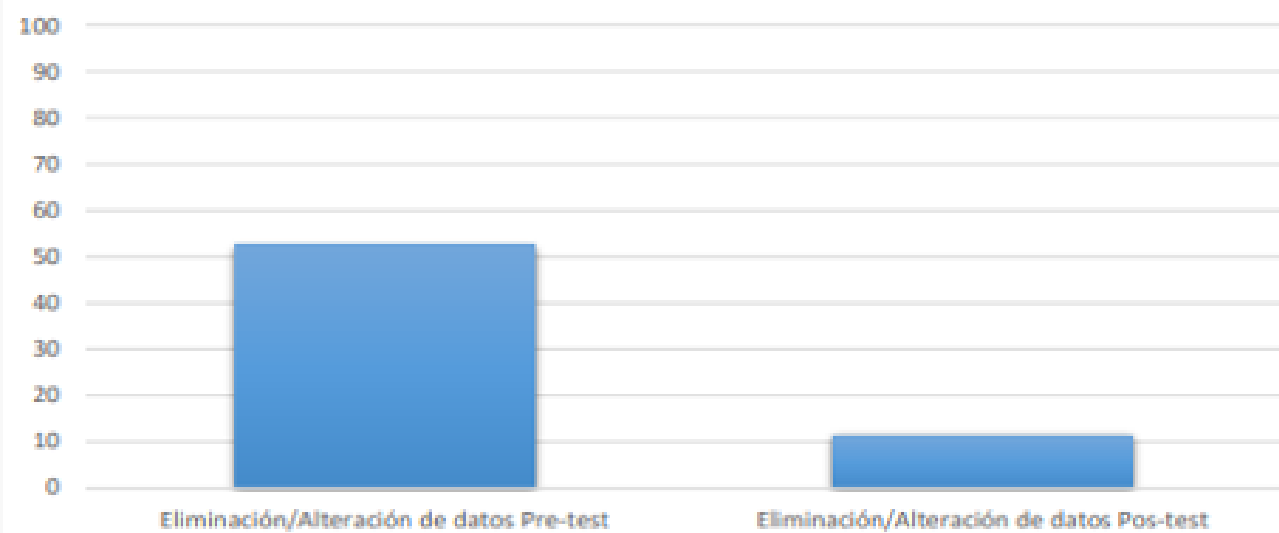


Figura 6. Histograma del PreTest y PostTest de Modificación de información

## Pruebas de normalidad

	Kolmogorov-Smirnov <sup>a</sup>			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
DIFERENCIA	,128	20	,200 <sup>*</sup>	,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

## Rangos

		N	Rango promedio	Suma de rangos
POSTEST - PRETEST	Rangos negativos	20 <sup>a</sup>	10,50	210,00
	Rangos positivos	0 <sup>b</sup>	,00	,00
	Empates	0 <sup>c</sup>		
	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<sup>a</sup>

	POSTEST - PRETEST
Z	-3,924 <sup>b</sup>
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

**Porcentaje total de Inaccesibilidad inmediata a la Información**

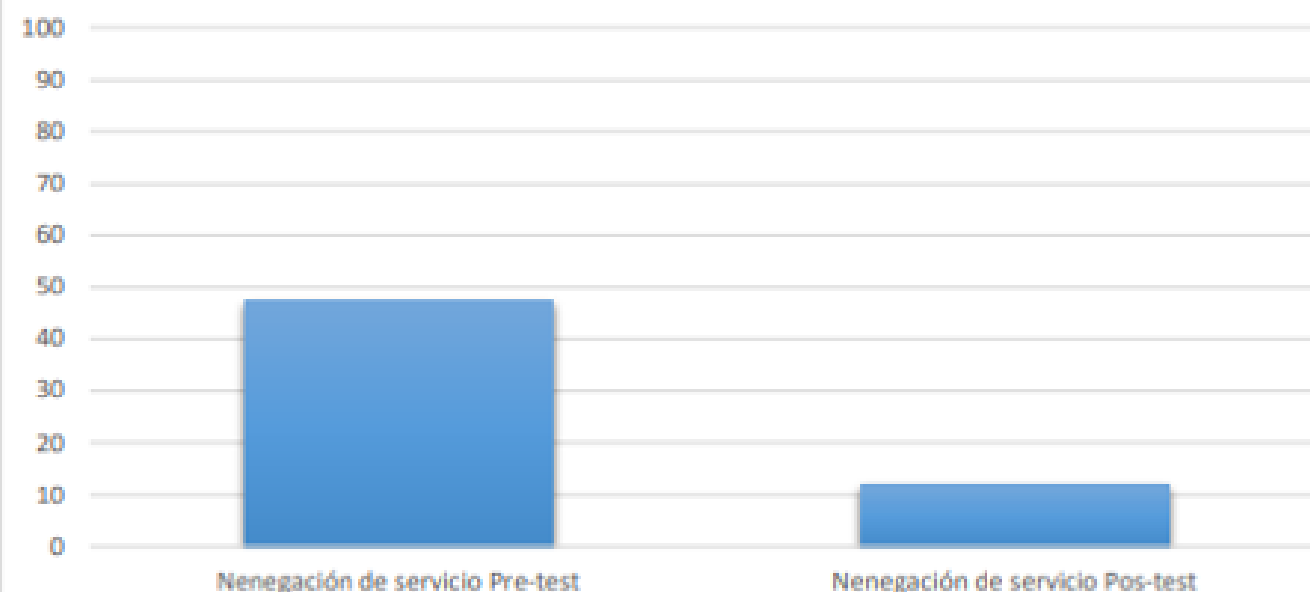


Figura 8. Histograma del PreTest y PosTest de Inaccesibilidad de información

**Pruebas de normalidad**

	Kolmogorov-Smirnov <sup>a</sup>			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
DIFERENCIA	,114	20	,200 <sup>a</sup>	,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 <sup>a</sup>	10,50	210,00
	Rangos positivos	0 <sup>b</sup>	,00	,00
	Empates	0 <sup>c</sup>		
	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<sup>a</sup>**

	POSTEST - PRETEST
Z	-3,921 <sup>b</sup>
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
<b>PROBLEMA GENERAL:</b> ¿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?	<b>OBJETIVO GENERAL:</b> 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	<b>HIPÓTESIS GENERAL:</b> 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	<b>VARIABLE I</b>  SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO 27001:2022          <b>VARIABLE II</b>  INVULNERABILIDAD	<b>MÉTODO DE INVESTIGACIÓN:</b>  Método deductivo  <b>TIPO DE INVESTIGACIÓN:</b>  Aplicada  <b>ALCANCE DE LA INVESTIGACIÓN:</b>  Explicativa  <b>DISEÑO DE LA INVESTIGACIÓN:</b>  pre experimental  <b>POBLACIÓN:</b>  17 oficinas administrativas  <b>MUESTRA:</b>  3 oficinas administrativas  <b>TECNICAS DE ENTREVISTA</b> Entrevista, encuesta, Fichaje
<b>PROBLEMA ESPECÍFICO</b> ¿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?	<b>OBJETIVOS ESPECÍFICOS</b> 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.	<b>HIPÓTESIS ESPECÍFICO</b> 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



**UPLA**  
UNIVERSIDAD PERUANA LOS ANDES

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.