UNIVERSIDAD NACIONAL DE CAÑETE

FACULTAD DE INGENIERÍA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Sistema con Tecnología Blockchain para la Gestión de la Seguridad de la Información en una Institución Privada, Callao, 2022

TESIS PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS

AUTOR:

Bach. Mariano Anthony Cardenas Quispe

orcid.org/0000-0003-3033-7846

ASESOR:

Mg. Alex Abelardo Pacheco Pumaleque

orcid.org/0000-0001-9721-0730

Firmado digitalmente por: PACHECO PUMALEQUE ALEX ABELARDO
Motivo: En señal de conformidad
Fecha: 30/07/2025 16:50:12-0500

CO ASESOR:

Ph. D. Dulio Oseda Gago

orcid.org/0000-0002-3136-6094

Firmado digitalmente por: OSEDA GAGO DULIO
Motivo: Soy el autor del documento
Fecha: 01/08/2025 13:24:20-0500

LÍNEA DE INVESTIGACIÓN

Plataforma TIC

San Vicente de Cañete, Perú, 2024

Firma de los Jurados

FIRMA DIGITAL

Firmado digitalmente por: ALMIDON ORTIZ CARLOS ALCIDES
Motivo: Soy el autor del documento
Fecha: 31/07/2025 16:33:54-0500

Dr. Carlos Alcides Almidón Ortiz
Presidente
Jurado Evaluador
Facultad de Ingeniería

Firmado digitalmente por: ASTO HUAMAN Leonidas FAU 20491363402 soft
Motivo: Doy V° B°
Fecha: 31/07/2025 13:10:07-0500

M. Sc. Leonidas Asto Huamán
Secretario
Jurado Evaluador
Facultad de Ingeniería

FIRMA DIGITAL

Firmado digitalmente por: DURAN CARHUAMACA AMANDA FIR 20114878 hard
Motivo: Soy el autor del documento
Fecha: 31/07/2025 17:33:40-0500

Mg. Amanda Durán Carhuamaca
Vocal
Jurado Evaluador
Facultad de Ingeniería

Acta de Sustentación

UNIVERSIDAD NACIONAL DE CAÑETE

Código: F-M01.03.04-GT-003 Fecha de Aprobación: 16-10-2023	Versión: 04

FACULTAD DE INGENIERÍA

ACTA DE SUSTENTACIÓN DE TESIS PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS

En la ciudad de Cañete, en la Unidad de Investigación de la Facultad de Ingeniería, siendo las 3:00 p.m. horas del día 29 de agosto del 2024, se reunió el Jurado Evaluador y el asesor, designados por decreto N° 071-2024-UIFI/FI/UNDC

Presidente(a): Dr. Carlos Alcides Almidón Ortiz
Secretario (a): M.Sc. Leonidas Asto Huaman
Vocal: Mg. Amanda Durán Carhuamaca

Asesor: Mg. Alex Abelardo Pacheco Pumaleque

Para el acto de sustentación de la tesis titulada: **Sistema con tecnología blockchain para la gestión de la seguridad de la información en una institución privada, Callao, 2022;** presentada por el Bachiller **Mariano Anthony Cardenas Quispe** para optar al Título profesional de Ingeniería de Sistemas.

Después de concluido el acto de sustentación y luego de que el sustentante dio respuesta a las preguntas respectivas, el Jurado Evaluador calificó la sustentación o defensa de la investigación según los siguientes criterios, y promediando las notas del jurado se obtuvo:

Tesista: Mariano Anthony Cardenas Quispe

Criterio	Desaprobado (menor de 14)	Regular (14-15)	Bueno (16-17)	Muy bueno (18-19)	Excelente (20)	Puntaje
Claridad de la exposición		14				14
Dominio del tema		14				14
Visión holística del trabajo		14				14
Promedio						14

Para obtener la nota final de todo el proceso de investigación, conforme al artículo 100° del Reglamento General de Investigación de la Universidad Nacional de Cañete aprobado mediante Resolución Nº 180-2023-UNDC/CO, se procedió a calcular la nota final:

Tesista	Nota del Informe (40%)	Nota de Sustentación (60%)	Nota Final
Mariano Anthony Cardenas Quispe	16	14	15

F-M01.03.04-GT-003 Toda copia de este documento, sea del entorno virtual o del documento original en físico es considerada "copia no controlada".

Y, establece como calificación FINAL: 15 (quince)

- Aprobado, con nota Regular ([X]), Bueno ( ), Muy Bueno ( ), Excelente ( )
- Desaprobado ( )

Por tanto, el graduado se encuentra expedito(s) ([X]), impedido(s) ( ) para realizar los trámites que corresponden a la obtención del Título Profesional de Ingeniero de Sistemas.

Siendo las 4:00 p.m., se dio por terminado el acto de sustentación.

M.Sc. Leonidas Asto Huaman **Secretario**	Dr. Carlos Alcides Almidón Ortiz **Presidente**	Mg. Amanda Durán Carhuamaca **Vocal**	Mg. Alex Abelardo Pacheco Pumaleque **Asesor**

F-M01.03.04-GT-003 Toda copia de este documento, sea del entorno virtual o del documento original en físico es considerada "copia no controlada".

Dedicatoria

Dedicado con profundo agradecimiento a Dios, por ser mi guía constante en cada paso de este camino; a mis padres y mi familia, cuyo amor incondicional y apoyo inquebrantable han sido mi roca y fortaleza; a mis amistades, por estar siempre presentes y brindarme momentos de alegría y consuelo; a todos los que de una manera u otra han aportado a mi crecimiento personal y profesional; también al Mg. Alex Pacheco, cuya recomendación y motivación para investigar sobre blockchain han sido la chispa que dio comienzo a la realización de esta investigación. A todos, sin excepción, mi eterna gratitud.

Agradecimiento

En primer lugar, agradezco a Dios por todo.

Mi gratitud infinita hacia mi madre y mi padre, cuyo amor, sacrificio y apoyo incondicional han sido el faro que ha iluminado mi camino. Su entrega incansable y su apoyo constante han sido más que suficientes para guiarme y sostenerme en cada etapa de mi vida.

Extiendo mi agradecimiento a toda mi familia, cuya presencia y apoyo, tanto directo como indirecto, han sido pilares fundamentales en mi vida. Su fe inquebrantable en mis capacidades ha sido una fuente constante de fuerza y motivación.

A la Universidad Nacional de Cañete, un profundo reconocimiento. A través de sus docentes, personal administrativo, autoridades, talleres, programas de apoyo social e investigación, infraestructura y recursos, ha proporcionado un entorno académico de excelencia que me ha permitido desarrollarme como profesional. Cada lección aprendida en sus aulas y cada desafío enfrentado han sido esenciales en mi formación.

Mi gratitud especial al Mg. Alex Pacheco y al Dr. Dulio Oseda, cuya guía y apoyo en la realización de esta investigación han sido fundamentales.

Agradezco también a quienes brindaron valiosos aportes que hicieron mejorar la presente investigación.

Mi reconocimiento a los docentes, instructores y escuelas que han sido parte de mi educación desde mis primeros años. Cada uno de ellos ha contribuido a sembrar las semillas del conocimiento y la curiosidad que me han llevado a este punto.

A mis amistades, gracias por ser el soporte emocional, por las risas compartidas y los momentos de desahogo. Su amistad es uno de los tesoros más grandes que llevo conmigo.

Agradezco a cada persona, conocida o desconocida, que ha extendido su solidaridad y apoyo en los momentos en que más lo necesité. Su generosidad y bondad han sido un regalo invaluable en mi vida.

Por último, pero no menos importante, me agradezco a mí mismo por el compromiso, la perseverancia y la dedicación invertidos en la realización de esta tesis y la obtención de mi título profesional.

Índice

Firma de los Jurados 2
Acta de Sustentación 3
Dedicatoria 5
Agradecimiento 6
Índice 7
Índice de Figuras 10
Índice de Tablas 11
Resumen 12
Abstract 13
Capítulo I: Introducción 14
1.1. Planteamiento del Problema 14
1.2. Formulación del Problema 15
1.2.1. Problema General 15
1.2.2. Problemas Específicos 15
1.3. Objetivos 15
1.3.1. Objetivo General 15
1.3.2. Objetivos Específicos 15
1.4. Justificación 15
1.4.1. Justificación Teórica 15
1.4.2. Justificación Practica 16
1.4.3. Justificación Metodológica 16
1.5. Delimitación de la Investigación 16
1.5.1. Delimitación Teórica 16
1.5.2. Delimitación Temporal 16
1.5.3. Delimitación Espacial 16
Capitulo II: Marco Teórico 17
2.1. Antecedentes de Investigación 17
2.1.1. Artículos Científicos 17
2.1.2. Tesis Nacionales e Internacionales 19
2.2. Bases Teóricas 22
2.2.1. Variable Independiente 22
2.2.2. Variable Dependiente 24
2.3. Definición de Términos Básicos 26

Capitulo III: Hipótesis y Variables 27
3.1. Hipótesis 27
3.1.1. Hipótesis General 27
3.1.2. Hipótesis Especifica 27
3.2. Definición Conceptual de Variables 27
3.2.1. Variable Independiente: Sistema con Tecnología Blockchain 27
3.2.2. Variable Dependiente: Gestión de la Seguridad de la Información 27
3.3. Operacionalización de Variables (Definición Operacional) 28
Capitulo IV: Metodología 31
4.1. Enfoque de la Investigación 31
4.2. Tipo de Investigación 31
4.3. Nivel de Investigación 31
4.4. Método de Investigación 31
4.5. Diseño de Investigación 31
4.6. Población, Muestra y Muestreo 32
4.6.1. Población 32
4.6.2. Muestra 32
4.6.3. Muestreo 32
4.7. Técnicas e Instrumentos de Recolección de Datos 32
4.8. Técnicas Estadísticas de Análisis de Datos 33
4.9. Consideraciones Eticas 33
Capitulo V: Resultados 34
5.1. Resultados Descriptivos 34
5.1.1. Primera Dimensión: Disponibilidad de la Información 34
5.1.2. Segunda Dimensión: Integridad de la Información 36
5.1.3. Tercera Dimensión: Confidencialidad de la Información 38
5.2. Resultados Inferenciales 40
5.2.1. Primera Dimensión: Disponibilidad de la Información 40
5.2.2. Segunda Dimensión: Integridad de la información 42
5.2.3. Tercera Dimensión: Confidencialidad de la Información 44
Capítulo VI: Discusión 47
6.1. Discusión de la Primera Dimensión: Disponibilidad de la Información 47
6.1.1. Resultados Descriptivos 47
6.1.2. Resultados Inferenciales 47
6.2. Discusión de la Segunda Dimensión: Integridad de la Información 47

6.2.1. Resultados Descriptivos 47
6.2.2. Resultados Inferenciales 47
6.3. Discusión de la Tercera Dimensión: Confidencialidad de la Información 48
6.3.1. Resultados Descriptivos 48
6.3.2. Resultados Inferenciales 48
Capítulo VII: Conclusiones 49
Capitulo VIII: Recomendaciones 50
Referencias 51
Anexos 56
Anexo 01: Matriz de Consistencia 56
Anexo 02: Instrumento de Recolección de Datos 58
Anexo 03: Certificado de Validez de Contenido (Juicio de Expertos) 59
Anexo 04: Certificado de Validez de Contenido (Juicio de Expertos) 62
Anexo 05: Base de Datos de los Indicadores (Instrumento de Recolección de Datos) 64
Anexo 06: Autorización de la Institución para Realizar la Investigación 66
Anexo 07: Desarrollo de la Solución Tecnológica 67
Anexo 08: Constancia de Similitud 80
Anexo 09: Autorización de Publicación en el Repositorio Institucional de la UNDC 81
Anexo 10: Articulo Científico 83

Índice de Figuras

Figura 1. Comparación de promedios del indicador PACD 36
Figura 2. Comparación de promedios del indicador PACI 38
Figura 3. Comparación de promedios del indicador PACEC 40

Índice de Tablas

Tabla I. 28
Tabla II. 29
Tabla III. 29
Tabla IV. 30
Tabla V. 34
Tabla VI. 35
Tabla VII. 36
Tabla VIII. 37
Tabla IX. 38
Tabla X. 39
Tabla XI. 41
Tabla XII. 41
Tabla XIII. 42
Tabla XIV. 42
Tabla XV. 43
Tabla XVI. 43
Tabla XVII. 44
Tabla XVIII. 45
Tabla XIX. 46

Resumen

En esta tesis, el objetivo principal fue determinar el impacto de un sistema basado en tecnología blockchain en la gestión de la seguridad de la información en una institución privada del Callao durante el año 2022. La investigación busco abordar el problema de la falta de protección de la información en los certificados emitidos por la institución. Se empleó una metodología cuantitativa de tipo aplicada, con un nivel explicativo, utilizando el método hipotético-deductivo y un diseño pre-experimental. La población y muestra de estudio consistió en 24 certificados de publicación. Los datos recopilados fueron procesados utilizando el software Microsoft Excel 365 de 64 bits y IBM SPSS Statistics v.21. Los resultados mostraron mejoras significativas en los tres indicadores evaluados: primero, el indicador PACD evidenció una mejora en la disponibilidad de los certificados del 66.67% en el pre test al 100% en el post test, demostrando un impacto positivo en la disponibilidad de la información; segundo, el indicador PACI mostró una mejora en la integridad de los certificados del 50% en el pre test al 100% en el post test, indicando una mejora en la integridad de la información; y tercero, el indicador PACEC reflejó una mejora en la confidencialidad de los certificados del 26.14% en el pre test al 92.05% en el post test, demostrando un impacto positivo en la confidencialidad de la información. En conclusión, el sistema basado en tecnología blockchain tuvo un efecto positivo en la gestión de la seguridad de la información en la institución privada estudiada en el Callao en el año 2022.

Palabras claves – Blockchain, Disponibilidad, Integridad, Confidencialidad, Certificados

Abstract

In this thesis, the main objective was to determine the impact of a system based on blockchain technology in the management of information security in a private institution in Callao in the year 2022. The research sought to address the problem of the lack of information protection in the certificates issued by the institution. An applied quantitative methodology was used, with an explanatory level, using the hypothetical-deductive method and a pre-experimental design. The study population and sample consisted of 24 publication certificates. The data collected were processed using Microsoft Excel 365 64-bit software and IBM SPSS Statistics v.21. The results showed significant improvements in the three indicators evaluated: first, the PACD indicator showed an improvement in certificate availability from 66 67% in the pre-test to 100% in the post-test, demonstrating a positive effect on information availability; second, the PACI indicator showed an improvement in certificate integrity from 50% in the pre-test to 100% in the post-test, demonstrating an improvement in information integrity; and third, the PACEC indicator reflected an improvement in certificate confidentiality from 26.14% in the pre-test to 92.05% in the post-test, demonstrating a positive effect on information confidentiality. In conclusion, the system based on blockchain technology had a positive impact on information security management in the private institution studied in Callao in 2022.

Keywords - Blockchain, Availability, Integrity, Confidentiality, Certificates

Capítulo I: Introducción

1.1. Planteamiento del Problema

En el contexto contemporáneo, la seguridad de la información implica la protección integral de los datos y los sistemas informáticos frente a diversas amenazas, tales como el acceso no autorizado o la divulgación no deseada de información confidencial, las cuales pueden desencadenar su alteración o destrucción [1]. Sin embargo, los sistemas de información enfrentan constantes amenazas de ciberataques y fraudes, lo que, sumado a la demora en la verificación de datos, conlleva a un funcionamiento empresarial lento y resultados deficientes; en este sentido, la tecnología blockchain surge como una solución, al proporcionar una confianza sólida respaldada por una alta seguridad y una mayor eficiencia operativa [2].

A escala internacional, la incertidumbre es un desafío, ya que los entornos son cada vez más ambiguos y volátiles, y en una sociedad con demanda digital, las organizaciones usan tecnología expuesta a este entorno, resaltando la necesidad de optimizar la confianza [3]. En Colombia, la digitalización de los servicios públicos conlleva el riesgo de vulnerar la información, afectando su integridad y confidencialidad, lo que impulsa al gobierno a implementar medidas para mitigar estos riesgos [4].

En el contexto nacional, se destaca que en el año 2019, Pomas y Vargas señalaron que el Perú es considerado el país más vulnerable frente a ataques cibernéticos [5]. En adición, en el año 2023, se evidencia un aumento de 150% en fraudes en línea y robo de información mediante aplicaciones [6]. En la provincia constitucional del Callao, se identifica la falta de adherencia a políticas de seguridad de la información en algunas instituciones, subrayando la urgencia de promover la adopción generalizada de estas políticas para proteger los datos [7], [8].

En una institución privada del Callao, los certificados de publicación de artículos científicos presentan serias deficiencias de seguridad. Estos certificados, gestionados por el área de TI y el presidente del directorio, carecen de políticas de protección adecuadas, lo que ha generado diversos problemas. Actualmente, la integridad de los documentos solo cumple en un 50%, debido a errores recurrentes como nombres incorrectos y datos faltantes. La disponibilidad, evaluada en un 66.67%, se ha visto afectada, ya que algunos certificados no se encuentran disponibles cuando se requieren. Además, la confidencialidad es alarmantemente baja, con un 26.14%, ya que los certificados se comparten en una carpeta general en la nube, lo que expone la información a accesos no autorizados y posibles modificaciones.

1.2. Formulación del Problema

1.2.1. Problema General

¿Cuál es el efecto de un sistema con tecnología blockchain en la gestión de la seguridad de la información en una Institución Privada, Callao, 2022?

1.2.2. Problemas Específicos

- **PE1:** ¿Cuál es el efecto de un sistema con tecnología blockchain en la disponibilidad de la información de la gestión de la seguridad de la información en una institución privada, Callao, 2022?
- **PE2:** ¿Cuál es el efecto de un sistema con tecnología blockchain en la integridad de la información de la gestión de la seguridad de la información en una institución privada, Callao, 2022?
- **PE3:** ¿Cuál es el efecto de un sistema con tecnología blockchain en la confidencialidad de la información de la gestión de la seguridad de la información en una institución privada, Callao, 2022?

1.3. Objetivos

1.3.1. Objetivo General

Determinar el efecto de un Sistema con tecnología blockchain en la gestión de la seguridad de la información en una institución privada, Callao, 2022.

1.3.2. Objetivos Específicos

- **OE1:** Evaluar el efecto de un sistema con tecnología blockchain en la disponibilidad de la información de la gestión de la seguridad de la información en una institución privada, Callao, 2022.
- **OE2:** Determinar el efecto de un sistema con tecnología blockchain en la integridad de la información de la gestión de la seguridad de la información en una institución privada, Callao, 2022.
- **OE3:** Determinar el efecto de un sistema con tecnología blockchain en la confidencialidad de la información de la gestión de la seguridad de la información en una institución privada, Callao, 2022.

1.4. Justificación

1.4.1. Justificación Teórica

El imperativo de proteger los datos de los certificados emitidos posiciona a la tecnología blockchain como una excelente candidata. En los últimos años, ha demostrado su potencial en áreas de digitalización, seguridad y trazabilidad [9]. Sus características distintivas, que incluyen mayor seguridad, anonimato, capacidad de operar de igual a igual y trazabilidad, la convierten en una opción relevante para abordar los desafíos de la seguridad de la información [10].

1.4.2. Justificación Practica

La tecnología blockchain ha ganado popularidad recientemente por su capacidad innovadora de facilitar transacciones seguras y eficientes [11]. Su aplicación en la protección de la información de certificados podría prevenir el riesgo de adulteraciones y perdidas a largo plazo.

1.4.3. Justificación Metodológica

El marco de trabajo SCRUM [12] fue seleccionado para este proyecto debido a su capacidad para facilitar la adaptación al cambio, fomentar la colaboración y priorizar la entrega continua de valor al usuario.

1.5. Delimitación de la Investigación

1.5.1. Delimitación Teórica

En el presente estudio, se abordan dos variables: la variable independiente "Sistema con tecnología blockchain" se distingue por su reconocida transparencia e inmutabilidad en el registro de datos, que son cruciales en entornos donde se requieren mecanismos de seguridad que prevengan la falsificación de la información [13]; y la variable dependiente “Gestión de la Seguridad de la información” abarca una serie de medidas proactivas y correctivas ideadas para resguardar la información personal o valiosa de individuos u organizaciones, con el propósito de evitar su acceso y uso no autorizado [14].

1.5.2. Delimitación Temporal

Este estudio se enfoca en datos recogidos de la institución privada desde el año 2021 hasta agosto de 2022. La implementación de la solución propuesta se llevó a cabo en enero de 2024, seguida por una evaluación inmediata para analizar los resultados obtenidos.

1.5.3. Delimitación Espacial

Esta investigación se realiza en una Institución Privada ubicada en la provincia constitucional del Callao, Región del Callo, Perú.

Capítulo II: Marco Teórico

2.1. Antecedentes de Investigación

2.1.1. Artículos Científicos

En el contexto global, [15] de acuerdo con su estudio académico publicado en la revista IEEE en el año 2024, de título "Enhancing Cloud-Based Inventory Management: A Hybrid Blockchain Approach With Generative Adversarial Network and Elliptic Curve Diffie Helman Techniques", tienen el objetivo central de proponer un enfoque híbrido que combine tecnologías avanzadas, como blockchain, Técnicas de Identificación por Radiofrecuencia (RFID), preprocesamiento basado en Redes Generativas Adversariales (GNA) y técnicas criptográficas de Elliptic Curve Diffie-Hellman (ECDH), con el fin de fortalecer las medidas de seguridad en un sistema de inventario basados en la nube. El método aplicado integra la captura de datos mediante RFID y el procesamiento de datos utilizando GNA para garantizar la calidad de los datos recopilados; además, la generación de claves seguras se realiza a través de ECDH, y el almacenamiento seguro de datos se gestiona mediante la tecnología blockchain; en ese sentido; así mismo, la implementación se realizó en Python y se evaluó utilizando un conjunto de datos RFID de acceso público, finalmente, la evaluación comparó la eficiencia de este enfoque con métodos contemporáneos de seguridad mediante varias métricas de rendimiento. Los resultados indicaron mejoras significativas en los tiempos de cifrado, descifrado y generación de claves, superando a técnicas de seguridad avanzadas; también el enfoque híbrido mostró altas tasas de rendimiento y confidencialidad de datos a través de diferentes volúmenes de datos, demostrando su eficacia en la mejora de la seguridad de los datos. En conclusión, el estudio validó que el enfoque híbrido mejora significativamente la seguridad y la eficiencia de los sistemas de gestión de inventarios basados en la nube; además, la integración de tecnologías avanzadas, como blockchain y ECDH, contribuye de manera significativa a la protección de datos, optimizando la gestión de inventario de manera transparente y en tiempo real. Este trabajo aporta a la investigación en seguridad de la información mediante la combinación de tecnologías emergentes para abordar las vulnerabilidades en la gestión de información.

También, [16] según su escrito científico titulado "Integrity and Privacy-Aware, Patient-Centric Health Record Access Control Framework Using a Blockchain", publicado en la revista Applied Sciences en el año 2023, tienen el propósito de crear un sistema gestionado con tecnología blockchain para mejorar la seguridad y la privacidad de la información de salud. La metodología se basó en una revisión detallada de literatura sobre la aplicación de la tecnología

blockchain en la gestión de registros de salud, con especial atención en la privacidad y la integridad de los datos; continuando, se realizó un análisis comparativo entre varias plataformas blockchain, tales como Ethereum, Hyperledger Fabric y ConsenSys Codefi, evaluando aspectos críticos como el soporte de lenguajes de programación, tipos de blockchain, algoritmos de consenso y herramientas de desarrollo, donde Hyperledger Fabric fue seleccionado por su superioridad en términos de seguridad, rendimiento y escalabilidad. En los resultados, se muestra que Hyperledger Fabric fue implementado exitosamente en un entorno virtual de ORACLE VM VirtualBox, donde se desarrolló y desplegó un contrato inteligente, donde, este contrato está diseñado para gestionar operaciones clave como la creación, lectura, actualización, eliminación y asignación de permisos de acceso a los registros; también, las pruebas realizadas confirmaron la funcionalidad, seguridad y escalabilidad del sistema, asegurando que cumple con los requisitos establecidos para el proyecto. Se concluyo, que el sistema desarrollado confirmó que Hyperledger Fabric es una plataforma adecuada para la gestión de registros médicos con un alto nivel de seguridad; además, se destacó la personalización y eficiencia del sistema, permitiendo a los pacientes una gestión efectiva del acceso a su información personal de salud en un entorno de blockchain autorizado con políticas de seguridad claras y robustas. Este antecedente demuestra la viabilidad de aplicar la tecnología blockchain en un enfoque de privacidad y seguridad de los datos.

Así también, [17] conforme a su artículo titulado “Security and Privacy for Mobile IoT Applications Using Blockchain”, publicado en la revista Sensors en el año 2021. Su objetivo principal es desarrollar y validar una arquitectura que use blockchain y tecnologías complementarias para mejorar la privacidad y seguridad en aplicaciones de IoT, centrada en anonimización y control de datos por el usuario. La metodología empleada fue diseñar una arquitectura integrando blockchain con tecnologías como MQTT y Storj para potenciar la administración de la confidencialidad y la protección en aplicaciones IoT, después la arquitectura fue evaluada mediante pruebas experimentales para verificar su eficacia y viabilidad. Los resultados demostraron que la arquitectura propuesta es efectiva en mejorar la protección y el secreto de las aplicaciones IoT, proporcionando anonimato del usuario y privacidad controlada por el usuario gracias a las características de blockchain. En conclusión, la arquitectura propuesta aborda de manera eficiente los problemas de seguridad y privacidad en aplicaciones IoT móviles; además, esta solución robusta protege la identidad del usuario y asegura la confidencialidad de los datos, extendiendo sus beneficios no solo a aplicaciones IoT

móviles, sino también a otras aplicaciones IoT. Este antecedente evidencia que la aplicación de blockchain junto con tecnologías como MQTT y Storj tiene la capacidad de mejorar la privacidad y seguridad en aplicaciones IoT.

Por último, [18] en su trabajo científico publicado en 2020 en la revista Applied Sciences, titulado "Blockchain Implementation to Verify Archives Integrity on Cilegon E-Archive", buscan desarrollar un prototipo para el sistema Cilegon E-Archive (CEA) que integre tecnologías de IPFS y blockchain para mejorar la seguridad, disponibilidad y autenticidad de los archivos. Se emplea una metodología de desarrollo de sistemas que incluyó la integración del Sistema de Archivos Interplanetario (IPFS) y la red privada Ethereum, para construir una aplicación descentralizada (DApp) que facilita la interacción de los usuarios con el sistema CEA, gestionada a través de un contrato inteligente. En los resultados, el prototipo desarrollado resolvió problemas de punto único de fallo, baja disponibilidad de datos y dificultades para verificar la autenticidad de los archivos en el sistema CEA anterior, al mejorar significativamente la seguridad del sistema en términos de confidencialidad, integridad y disponibilidad de los datos, en otras palabras, los archivos se distribuyen de manera más segura y se almacenan hashes en blockchain para garantizar su integridad y prevenir falsificaciones. En conclusión, los autores mencionan que la integración de IPFS y Ethereum en el sistema CEA condujo a mejoras significativas en la gestión de archivos, asegurando alta disponibilidad y resistencia a alteraciones no autorizadas, es decir, este enfoque descentralizado proporciona una solución robusta para los desafíos enfrentados por los sistemas de archivos centralizados, especialmente en entornos gubernamentales donde la seguridad y la exactitud de los datos son críticas. Este antecedente ilustra el uso práctico de blockchain para mejorar la seguridad en la gestión de archivos, demostrando cómo la descentralización y la inmutabilidad del blockchain pueden abordar problemas clave como la integridad, la disponibilidad y la autenticidad de la información.

2.1.2. Tesis Nacionales e Internacionales

En el contexto internacional, en al año 2023, [19] en su tesis con título “Improving the Security and Reliability of Application Systems with Blockchain Technology”, tiene como meta principal aumentar la seguridad y la credibilidad del sistema de votación electrónica (sistema E-voting) y el sistema de registro de auditoría utilizando blockchain y tecnologías relacionadas. Se desarrolla una metodología que incorpora la tecnología blockchain utilizando la plataforma Hyperledger Fabric en dos sistemas; en el Sistema de Votación se emplea dos blockchains

(DBE-Voting), una privada y otra pública, para gestionar los datos de votación, donde, la privacidad de los votantes se mantiene a través de la blockchain privada, mientras que la blockchain pública facilita la verificación transparente de los resultados electorales; además se utilizan firmas de anillo enlazables para autenticar a los votantes y prevenir la reutilización de votos, asegurando así la integridad del proceso electoral; paralelamente, en el Sistema de Registro de Auditoría se aplica la tecnología blockchain que aborda la integridad de los datos y reduce la dependencia de sistemas de registro centralizados, susceptibles a manipulaciones; este sistema implementa un modelo en el que tanto los registradores como los auditores se consideran potencialmente no confiables y utiliza múltiples nodos para garantizar la seguridad de los datos registrados, donde los registros se almacenan en el Sistema de Archivos Interplanetario (IPFS, por sus siglas en inglés), aprovechando su estructura descentralizada, mientras que las pruebas de integridad se mantienen en la blockchain como tokens no fungibles subordinados (sub-NFTs), facilitando un sistema robusto y seguro para la gestión de auditorías. En los resultados, en primer lugar, el sistema de voto electrónico con doble blockchain puede manejar hasta 29 transacciones por segundo con un tamaño de bloque de 512 KB, además, el análisis de seguridad confirmó que el sistema es capaz de cumplir con los cinco requisitos principales para la votación electrónica de manera simultánea; en segundo lugar, el sistema de registro de auditoria basado en blockchain demostró ser capaz de tolerar una cierta cantidad de nodos maliciosos, protegiendo la integridad de los datos, además, el método de prueba de integridad propuesto logró ahorrar aproximadamente el 50% del espacio de almacenamiento en comparación con otros sistemas basados en blockchain. En conclusión, la incorporación de tecnología blockchain en sistemas de votación electrónica y sistemas de registro de auditoría puede mejorar significativamente su seguridad y confiabilidad. Este antecedente muestra que la tecnología blockchain mejora la seguridad y eficiencia en sistemas de votación electrónica y auditorías.

En el mismo escenario, [20] en el año 2022, en su tesis de título "Blockchain Based Solution for Electronic Health Record Integrity", se propuso la implementación de un sistema de recopilación de datos médicos mediante la tecnología blockchain para asegurar la seguridad y precisión de la información. La metodología aplicada incluyó la selección de la plataforma blockchain Algorand sobre otras alternativas. El desarrollo de la propuesta se dividió en tres partes: primero, se diseñó y desarrolló una aplicación web que integraba el despliegue de Algorand SDK y Algorand API, además de establecer la conexión con la base de datos, en segundo lugar, se llevó a cabo el despliegue de la plataforma blockchain de Algorand, y

finalmente, se realizó el despliegue de la base de datos y se configuró el almacenamiento. La propuesta se implementó en un equipo con un procesador AMD Ryzen 5 3600, 16 GB de memoria RAM, sistema operativo Windows 10 y red Algorand Testnet; posteriormente, se evaluó el prototipo procesando encuestas de 10 preguntas con 4 alternativas cada una, manteniendo un tamaño constante de 39 bytes; además, durante el desarrollo del proyecto, se emplearon diversas tecnologías, entre las que destacan: React.js para el frontend, Spring Boot / Java para el backend, Apache Tomcat para el servidor, PostgreSQL para la base de datos y Algorand Testnet para la blockchain; también, se utilizaron tecnologías complementarias como Pgcrypt para la criptografía en PostgreSQL, TEAL como lenguaje de contrato inteligente de Algorand, Algorand API para la conectividad entre Algorand y la aplicación, y Algorand Standard Asset para el mecanismo de token de seguridad. Los resultados obtenidos de la tesis muestran un tiempo promedio de análisis de aproximadamente 0.18841 segundos (equivalente a 188.41 milisegundos) y un uso promedio de memoria de alrededor de 84.10 megabytes para las funciones evaluadas. Es importante señalar que estos tiempos no incluyen el tiempo requerido para la formación de la cadena. Los autores concluyeron que su sistema de encuestas médicas basado en blockchain, utilizando Algorand y TEAL, ofrece una eficaz prevención de la falsificación de datos, asegurando la integridad de las respuestas y manteniendo la confidencialidad mediante el almacenamiento cifrado y hasheado de los datos de los pacientes. Este antecedente demuestra que el uso de Algorand en la gestión de registros puede asegurar la integridad y confidencialidad de los datos mediante el cifrado y hashado.

En el contexto nacional, [21] en su estudio del año 2023, tiene el objetivo principal de simular un modelo de tecnología blockchain para asegurar la protección de la información en el proceso de admisión de una universidad pública en Perú. La metodología empleada combina un diseño pre-experimental, aplicado, de investigación mixta y un enfoque cuantitativo de alcance explicativo. La población de estudio son escenarios de fraude de seguridad de la información, utilizando una muestra que comprende siete escenarios específicos en el proceso de admisión. Para la recolección de datos se emplea la simulación, utilizando como instrumento un software blockchain desarrollado mediante una metodología propia dividida en tres fases: análisis del proceso de negocio, elaboración del modelo blockchain y proceso de simulación del modelo. Los resultados indican una aceptación del 88.57% en el indicador contable, destacando las características de transparencia y registro histórico que proporciona la tecnología blockchain. En el modelo propuesto se identifican 17 nodos, garantizando un escenario eficiente gracias al

factor distribuido de la blockchain. Se destacan tres nodos validadores como requisito esencial para asegurar la transparencia, la integridad y la distribución de copias originales de la blockchain, asegurando que un mismo nodo no monopolice la autoridad sobre la veracidad de una transacción. Finalmente, se logra un 100% en confidencialidad, integridad y disponibilidad. En conclusión, la implementación de la tecnología blockchain influye de manera positiva y significativa en la seguridad de la información en el proceso de admisión de la universidad, demostrando el amplio potencial que tiene el uso de esta tecnología en la protección de la información. El antecedente demuestra que la tecnología blockchain puede significativamente mejorar la seguridad y transparencia en procesos de admisión universitaria, asegurando confidencialidad, integridad y disponibilidad de la información.

En ese sentido, [22] de acuerdo con su estudio realizado en el año 2022, buscan evaluar la eficacia de la arquitectura blockchain MA-ABS específicamente diseñada para la gestión de historias clínicas electrónicas en Perú. La investigación, de carácter tecnológico y cuantitativo, adopta un diseño experimental y cuasi experimental aplicado a un grupo único. La población de estudio abarca 17 arquitecturas blockchain diferentes que se encuentran en el mercado, seleccionando la arquitectura MA-ABS para la muestra. La técnica de recolección de datos empleada es la observación, utilizando como herramienta la ficha de observación. Los resultados indican que no hubo pérdida de información, logrando un cumplimiento del 100% en los indicadores de privacidad y control de acceso para la seguridad de los datos. En conclusión, los resultados del estudio confirman que la arquitectura blockchain MA-ABS cumple de manera efectiva con los estándares de privacidad y seguridad, logrando una efectividad total en las pruebas de control de acceso y privacidad de las historias clínicas de los pacientes, sin incidencias de filtraciones de información. El antecedente demuestra que la arquitectura blockchain MA-ABS es altamente efectiva para gestionar historias clínicas electrónicas, garantizando privacidad y control de acceso sin pérdida de información.

2.2. Bases Teóricas

2.2.1. Variable Independiente

A. Definición

La tecnología blockchain es un sistema que mantiene un registro de transacciones distribuidas entre múltiples computadoras interconectadas en una red peer-to-peer, lo que posibilita la creación de un entorno descentralizado donde los datos no están bajo el control de

ninguna organización externa [23]. Blockchain, también conocida como libro mayor distribuido, es una tecnología diseñada para revolucionar la gestión de datos, procesos comerciales y transacciones [24]. Introducida por primera vez en 2008 por Nakamoto, blockchain fue concebida como el primer libro mayor descentralizado que permite a cualquiera escribir en la base de datos sin estar sujeto a un único organismo controlador; sin embargo, aunque hay diversas cadenas de bloques activas, alcanzar la interoperabilidad entre ellas sigue siendo un desafío, a menos que se recurra a un tercero confiable [25]. Aunque enfrenta desafíos en cuanto a la interoperabilidad, el blockchain ha captado una gran atención tanto en el ámbito académico como en el industrial debido a sus características únicas, tales como la confiabilidad, la seguridad, la descentralización y la integridad de los datos [26].

B. Dimensiones

En el marco de esta investigación actual, no se aplicó la medición de la variable independiente mediante dimensiones.

C. Indicadores

En el marco de esta investigación actual, no se aplicó la medición de la variable independiente mediante indicadores.

D. Teorías

Blockchain Publica

Las Blockchains públicas son fundamentales en la tecnología debido a su naturaleza abierta y descentralizada, que permite a cualquier persona acceder a las transacciones sin restricciones ni necesidad de permisos, facilitando así una contabilidad distribuida y la verificación de registros actuales y pasados [27]. Estas Blockchains están diseñadas para ser transparentes y participativas, utilizando algoritmos como la prueba de trabajo (PoW) para permitir la participación de cualquier individuo en la cadena de bloques, garantizando así la visibilidad completa de todas las transacciones para todos los participantes y evitando el control por parte de usuarios o entidades específicas [28].

Blockchain Privada

En las blockchains privadas, los participantes deben solicitar permiso para unirse a la red, y todas las transacciones están disponibles mediante el acceso proporcionado únicamente por los participantes autorizados [28]. Estas blockchains operan con características de acceso limitado, facilitando transacciones solo con el permiso del administrador del sistema y

desarrollando plataformas que destacan por su alta privacidad, eficiencia, rapidez en las transacciones, mejor escalabilidad y mayor velocidad [27].

Blockchain Hibrida

Las cadenas de bloques híbridas son una combinación de cadenas de bloques públicas y privadas, se requieren para un mejor control y la consecución de objetivos más elevados [27]**.** Es decir, estas blockchains exhiben flexibilidad al ofrecer la opción de seleccionar qué datos se compartirán con el público y cuáles se mantendrán en privado [28].

2.2.2. Variable Dependiente

A. Definición

La gestión de la seguridad de la información implica la implementación de acciones preventivas y estratégicas llevadas a cabo por las entidades para proteger sus activos y asegurar la continuidad de las operaciones, utilizando como herramienta clave el estándar ISO/IEC 27001 para el desarrollo y mantenimiento de un sistema efectivo a nivel organizacional que mitigue los riesgos de ataques y violaciones de datos [29]. Este enfoque resalta la necesidad de abordar no solo los aspectos técnicos de la seguridad sino también la dimensión humana, reconociendo que numerosos incidentes de seguridad provienen de vulnerabilidades humanas; mediante esta estrategia holística, se busca reforzar la defensa contra amenazas de índole técnica y humana, mejorando así la efectividad del sistema de gestión de seguridad de la información [30].

B. Dimensiones

La seguridad de la información enfrenta el desafío de salvaguardar la Confidencialidad, Integridad y Disponibilidad (CIA por sus siglas en ingles) de los sistemas de información de una organización ante diversas amenazas y ataques [30]. Por lo tanto, este estudio examinará las dimensiones de Disponibilidad, Integridad y Confidencialidad dentro del marco de la variable dependiente Gestión de la Seguridad de la Información.

Confidencialidad significa salvaguardar los datos tanto de posibles filtraciones no autorizadas como de divulgaciones deliberadas, siendo sinónimo de privacidad [31]. En otras palabras, la confidencialidad asegura que solo las entidades autorizadas, ya sean personas, organizaciones o sistemas, tengan acceso a la información, impidiendo que aquellos sin permiso puedan verla o usarla.

Integridad se enfoca en asegurar la exactitud y la coherencia (validez) de los datos [32]. Es decir, la integridad implica que los datos no se hayan alterado desde su almacenamiento o actualización, realizados por un agente autorizado, y que al ser consultados, estos datos sean exactos y válidos.

Disponibilidad se refiere a la propiedad que tiene la información de estar accesible y utilizable por los usuarios autorizados cuando sea necesario [33]. De igual manera, la disponibilidad se refiere a las acciones de prevenir interrupciones y mantener el sistema accesible en todo momento o durante los períodos de tiempo requeridos.

C. Indicadores

Porcentaje Acumulado de Certificados Disponibles: Es el método de medición que permite comparar conjuntos de datos calculando la proporción de la frecuencia acumulada en cada intervalo, además, este porcentaje se obtiene dividiendo la frecuencia acumulada por el total de observaciones y multiplicando por 100 [34]. Además representa documentos que son accesibles y están listos para ser utilizados por los usuarios autorizados en el momento en que se necesiten, midiendo así la disponibilidad de la información [33].

Porcentaje Acumulado de Certificados Íntegros: Es el método de medición que permite comparar conjuntos de datos calculando la proporción de la frecuencia acumulada en cada intervalo, además, este porcentaje se obtiene dividiendo la frecuencia acumulada por el total de observaciones y multiplicando por 100 [34]. Además representa documentos que presentan la exactitud y la coherencia (validez) de los datos [32], midiendo así la integridad de la información.

Porcentaje Acumulado de Certificados Entregados Correctamente: Es el método de medición que permite comparar conjuntos de datos calculando la proporción de la frecuencia acumulada en cada intervalo, además, este porcentaje se obtiene dividiendo la frecuencia acumulada por el total de observaciones y multiplicando por 100 [34]. Además representa el proceso de mantener la privacidad de los documentos [31], midiendo así la confidencialidad de la información.

D. Teorías

La norma ISO/IEC 27001 especifica los lineamientos para establecer y operar un Sistema de Gestión de Seguridad de la Información (SGSI) en organizaciones, enfocándose en la implementación de controles efectivos para la protección de los activos informativos y el

fortalecimiento de la confianza entre los interesados; originada de un código de prácticas británico de 1989, que evolucionó al BS7799, esta normativa promueve la integración de prácticas de seguridad óptimas en la administración de servicios, facilitando la optimización de los costos operativos, la administración efectiva de riesgos y la mitigación de la vulnerabilidad a amenazas [35].

2.3. Definición de Términos Básicos

Nodo: Un dispositivo informático, que puede ser desde un equipo personal hasta una computadora de gran capacidad, desempeña un papel crucial en una red al utilizar un protocolo común para verificar la autenticidad de las transacciones [36].

Bloque: Constituye un registro público que incluye varias transacciones confirmadas, las cuales se duplican en todos los nodos que forman parte de una cadena de bloques [37].

Hash: Según lo descrito por Casma Injante y Irigoyen Villacorta (2020), el Hash funciona como una especie de "huella dactilar" al convertir datos en cadenas alfanuméricas de longitud fija mediante una función matemática [36].

Consenso: Representan los pilares esenciales de cualquier blockchain, ya que dictan las normativas sobre quién y mediante qué procedimiento se formará un bloque nuevo en la blockchain [37].

Red P2P: En una red donde los dispositivos se interconectan directamente, prescindiendo de un servidor central y aprovechando la capacidad distribuida para determinar la ruta óptima entre los nodos, facilitando así la comunicación entre pares de manera eficiente [36].

Libro mayor distribuido: Un libro mayor distribuido es un registro que rastrea transacciones, similar a la contabilidad tradicional, y se denomina distribuido porque cada participante mantiene una copia actualizada, asegurando que todos compartan la misma información de manera uniforme [37].

Contratos inteligentes: De acuerdo con, Wasim Ahmad et al., en el año 2021, explican que los contratos inteligentes son programas autónomos en blockchain que automatizan procesos comerciales eliminando intermediarios; operan con reglas predefinidas que se codifican para asegurar la confianza entre las partes [36].

Certificado: Es un documento que atestigua y confirma la veracidad de un hecho [38].

Capítulo III: Hipótesis y Variables

3.1. Hipótesis

3.1.1. Hipótesis General

El sistema con tecnología blockchain tiene un efecto significativo en la gestión de la seguridad de la información en una institución privada, Callao, 2022.

3.1.2. Hipótesis Específica

- **HE1:** El sistema con tecnología blockchain tiene un efecto significativo en la disponibilidad de la información de la gestión de la seguridad de la información en una institución privada, Callao, 2022.
- **HE2:** El sistema con tecnología blockchain tiene un efecto significativo en la integridad de la información de la gestión de la seguridad de la información en una institución privada, Callao, 2022.
- **HE3:** El sistema con tecnología blockchain tiene un efecto significativo en la confidencialidad de la información de la gestión de la seguridad de la información en una institución privada, Callao, 2022.

3.2. Definición Conceptual de Variables

3.2.1. Variable Independiente: Sistema con Tecnología Blockchain

Es un sistema web que tiene integrada la tecnología blockchain. Con esta tecnología, los datos encriptados se almacenan en una estructura llamada bloque, el cual se relaciona con otros bloques predecesores, formando así una cadena de bloques [39]. Esto permite que los datos sean seguros, confiables e inmutables, ofreciendo una nueva alternativa para almacenar y operar la información.

3.2.2. Variable Dependiente: Gestión de la Seguridad de la Información

La gestión de la seguridad de la información se define como el reconocimiento, protección y regulación del acceso a los datos en todas sus formas, desde documentos impresos y digitales hasta comunicaciones transmitidas y verbales, para prevenir daños y garantizar su confidencialidad, autenticidad, integridad y disponibilidad [40]. Es decir, se debe proteger la información en todas sus formas, tanto virtuales como impresas, como en el caso de los certificados de publicación que contienen información crítica que valida la

autenticidad y credibilidad de publicaciones científicas, requiriendo así medidas robustas de seguridad para asegurar su disponibilidad, integridad y confidencialidad.

3.3. Operacionalización de Variables (Definición Operacional)

Tabla I.

VARIABLES, DIMENSIONES, INDICADORES, DEFINICIONES

Variable Dependiente	Dimensiones	Indicadores	Definición
Gestión de la seguridad de la información	Disponibilidad de la información	Porcentaje Acumulado de certificados disponibles	Es el método de medición que permite comparar conjuntos de datos calculando la proporción de la frecuencia acumulada en cada intervalo, además, este porcentaje se obtiene dividiendo la frecuencia acumulada por el total de observaciones y multiplicando por 100 [34]. Además representa documentos que son accesibles y están listos para ser utilizados por los usuarios autorizados en el momento en que se necesiten, midiendo así la disponibilidad de la información [33].
	Integridad de la información	Porcentaje Acumulado de certificados íntegros	Es el método de medición que permite comparar conjuntos de datos calculando la proporción de la frecuencia acumulada en cada intervalo, además, este porcentaje se obtiene dividiendo la frecuencia acumulada por el total de observaciones y multiplicando por 100 [34]. Además representa documentos que presentan la exactitud y la coherencia (validez) de los datos [32], midiendo así la integridad de la información.
	Confidencialidad de la información	Porcentaje Acumulado de certificados entregados correctamente	Es el método de medición que permite comparar conjuntos de datos calculando la proporción de la frecuencia acumulada en cada intervalo, además, este porcentaje se obtiene dividiendo la frecuencia acumulada por el total de observaciones y multiplicando por 100 [34]. Además representa el proceso de mantener la privacidad de los documentos [31], midiendo así la confidencialidad de la información.

Tabla II.

TABLA DE INDICADORES

Fórmulas	Definición
$\mathbf{PACD} = \frac{\mathbf{FACE}}{\mathbf{TRCD}} \mathbf{x\ 100}$	PACD: Porcentaje Acumulado de Certificados Disponibles
	FACE: Frecuencia Acumulada de Certificados Encontrados
	TRCD: Total Requerido de Certificados Disponibles
$\mathbf{PACI} = \frac{\mathbf{FACICC}}{\mathbf{TRCI}} \mathbf{x\ 100}$	PACI: Porcentaje Acumulado de Certificados Íntegros
	FACIC: Frecuencia Acumulada de Certificados con Información Completa y Correcta
	TRCI: Total Requerido de Certificados Íntegros
$\mathbf{PACEC} = \frac{\mathbf{FACCEC}}{\mathbf{TRECC}} \mathbf{x\ 100}$	PACEC: Porcentaje Acumulado de Certificados Entregados Correctamente
	FACCEC: Frecuencia Acumulada de Certificados Confidenciales Entregados Correctamente
	TRECC: Total requerido de Entregas Confidenciales de Certificados

Tabla III.

ESCALA VALORATIVA APLICADA EN LA INVESTIGACIÓN

	Aplicado	Definición
Escala valorativa	Razón	Las escalas racionales, asimismo conocidas como escalas de cocientes, integran los atributos de las escalas ordinales y de intervalo, incluyendo un valor cero absoluto que representa la ausencia de la característica medida, lo que posibilita realizar comparaciones tanto proporcionales como cuantitativas, por ejemplo, al medir los gastos de transporte de un trabajador que pueden ser nulos o al determinar la antigüedad de un empleado recién ingresado, y aunque la unidad de medida en estas escalas es arbitraria, se pueden comparar tanto los intervalos como los valores asignados, siendo fundamentales en mediciones como el peso, la longitud, la masa y el valor monetario, donde las razones son aplicables [41].

Tabla IV.

INSTRUMENTO DE RECOLECCIÓN DE DATOS APLICADO EN LA INVESTIGACIÓN

	Aplicado	Definición
Instrumento de recolección de datos	Fichaje	Es un procedimiento efectivo, y de acuerdo con Hernandez y Duana en el año 2020, esta técnica se describe como el grupo de acciones enfocadas en recoger datos relevantes para solucionar problemas de interés, por lo cual el fichaje permitió reunir y almacenar información crucial para el estudio, además este instrumento, facilita la organización de las ideas [42].

Capítulo IV: Metodología

4.1. Enfoque de la Investigación

El enfoque cuantitativo, basado en la inducción probabilística del positivismo lógico, se distingue por su medición rigurosa, objetiva y controlada, lo que permite al indagador hacer inferencias que trascienden los datos obtenidos mediante un proceso confirmatorio inferencial deductivo, orientado a obtener resultados utilizando datos sólidos y repetibles [43]. Por tal motivo, en esta tesis se aplica el enfoque cuantitativo para llegar a conclusiones claras y verificables.

4.2. Tipo de Investigación

La investigación de tipo aplicada combina el uso práctico del conocimiento con una investigación meticulosa, buscando así generar nuevos conocimientos [44]. Esta tesis es de tipo aplicada, ya que desarrolla una solución para salvaguardar los datos de una organización.

4.3. Nivel de Investigación

Este trabajo de investigación se ubica en un nivel explicativo. Este nivel se dedica a descubrir las relaciones de causa y efecto; por lo tanto, más allá de simplemente presentar o examinar un problema, su objetivo es identificar las razones subyacentes que lo originan [44].

4.4. Método de Investigación

El método hipotético-deductivo se distingue por su objetivo de ampliar el conocimiento mediante la obtención de resultados universales y la formulación de leyes científicas que explican las causas de los fenómenos, lo cual facilita tanto la predicción como el control de dichos fenómenos [44]. En este estudio se aplicará el método de investigación hipotético-deductivo.

4.5. Diseño de Investigación

Esta investigación adopta un diseño pre-experimental, tal como lo indica [45] , donde la Variable Independiente (VI) se establece en un único nivel correspondiente al grupo de experimentación. Además, es necesario que la variable dependiente se evalúe con una herramienta específica en dos momentos distintos: antes de la intervención (pre-test) y después de esta (post-test).

Según lo explicado en el párrafo anterior, se describe a continuación:

$$G \rightarrow T_1 - X - T_2$$

Donde:

T1: Pre-test; **T2:** Post-test

X: Intervención de la VI; **G:** Grupo de estudio

4.6. Población, Muestra y Muestreo

4.6.1. Población

Según Hernández y Mendoza en el año 2018, sostienen que la población en una investigación puede incluir no solo personas, sino cualquier elemento cuantificable, permitiendo así derivar una muestra que facilite un análisis completo de la población y evaluar cómo esta es influenciada por la variable en estudio [21]. La población objeto de este estudio está constituida por un total de 24 certificados de publicación. Estos certificados están directamente relacionados con los artículos que han sido publicados en tres ediciones diferentes de una revista científica perteneciente a una institución privada, específicamente los contenidos en el Volumen 1 (Números 1 y 2) y el Volumen 2 (Número 3).

4.6.2. Muestra

Según Cifuentes et al. y Asencio et al., ambos citados en [46], coinciden en que cuando el número de sujetos en una población es menor a cincuenta, esta población puede considerarse una representación completa de la muestra, debido a que las características de la población se equiparan directamente con las de la muestra. Debido a que la cantidad de la población de estudio es menor de cincuenta, se elegirá el total de la población de estudio.

4.6.3. Muestreo

El muestreo se define como la práctica estadística en la que se eligen elementos de una población mediante una técnica específica, con el propósito de llegar a conclusiones limitadas a la muestra o adquirir conocimientos sobre la población observada para realizar una inferencia estadística general [47]. El muestreo en este estudio es de tipo no probabilístico por conveniencia. Dichas muestras, también conocidas como accidentales, se seleccionan porque los elementos están espacial, temporal o administrativamente accesibles para el investigador que realiza la recolección de datos [47]. En este estudio se emplea el muestreo no probabilístico basado en conveniencia.

4.7. Técnicas e Instrumentos de Recolección de Datos

El procedimiento denominado fichaje, consiste en recopilar y obtener datos relevantes mientras se investiga el tema de estudio, donde cada dato recolectado contiene información de valor único e intrínseco [48]. El recurso denominado Ficha de Registro se emplea para

documentar los datos importantes de las fuentes que se consultan, las cuales deben ser diseñadas de manera que resulten simples y de fácil llenado, asegurando así un proceso eficiente y claro para el usuario [48]. En este trabajo de investigación, se aplica la técnica fichaje e instrumento ficha de registro para la recolección de datos.

4.8. Técnicas Estadísticas de Análisis de Datos

Para obtener información estadística, se emplea la ficha de registro. Durante este proceso, los datos fueron registrados utilizando el software Microsoft® Excel® para Microsoft 365 MSO de 64 bits. Después de completada la recolección de datos, se procede a su procesamiento y análisis utilizando el software IBM SPSS versión 21. Tras obtener los resultados, se lleva a cabo su análisis e interpretación.

4.9. Consideraciones Éticas

El proyecto se desarrolló siguiendo los principios éticos de respeto hacia la institución privada que forma parte del estudio de esta tesis. Se ha garantizado una comunicación completa y transparente, informando detalladamente a la institución sobre los alcances de su participación. Asimismo, se ha enfocado en mantener la confidencialidad total de los datos recopilados, asegurando que no se divulguen de manera no autorizada. Además, se ha mantenido un compromiso absoluto con la integridad académica, evitando cualquier forma de plagio.

Capítulo V: Resultados

En este capítulo se presentarán primero los resultados descriptivos y luego los resultados inferenciales. Estos resultados se obtuvieron tanto antes como después de la implementación de la solución propuesta.

5.1. Resultados Descriptivos

5.1.1. Primera Dimensión: Disponibilidad de la Información

A. Primer Indicador: Porcentaje Acumulado de Certificados Disponibles

La Tabla V presenta los datos recopilados del indicador PACD (Porcentaje Acumulado de Certificados Disponibles) durante las mediciones de preprueba y postprueba, en las cuales se llevaron a cabo un total de 24 evaluaciones. Se observa una mejora progresiva en la disponibilidad de la información a partir del séptimo certificado en la prueba posterior. En consecuencia, se observa que la solución propuesta está contribuyendo de manera significativa a la mejora de la disponibilidad de la información.

Tabla V.

PACD: PREPRUEBA Y POSTPRUEBA

PACD	**Porcentaje Acumulado de certificados disponibles**	
	PACD Preprueba	PACD Postprueba
1	4.17%	4.17%
2	8.33%	8.33%
3	12.50%	12.50%
4	16.67%	16.67%
5	20.83%	20.83%
6	25.00%	25.00%
7	25.00%	29.17%
8	29.17%	33.33%
9	33.33%	37.50%
10	37.50%	41.67%
11	41.67%	45.83%
12	41.67%	50.00%
13	41.67%	54.17%
14	41.67%	58.33%
15	41.67%	62.50%
16	41.67%	66.67%
17	41.67%	70.83%
18	41.67%	75.00%
19	45.83%	79.17%
20	50.00%	83.33%
21	54.17%	87.50%
22	58.33%	91.67%

23	62.50%	95.83%
24	66.67%	100.00%

Así mismo, la tabla VI revela que el porcentaje mínimo de certificados emitidos fue de 4.17%, lo que indica que al menos esa proporción del total previsto fue efectivamente emitida en ambas fases. Se observa una notable diferencia en los valores máximos, dado que durante la preprueba la disponibilidad máxima alcanzó el 66.67%, mientras que en la postprueba se logró la totalidad, es decir, el 100%. Asimismo, el promedio en la postprueba superó al de la preprueba, registrando un 52.08% frente a un 36.81%. Estos datos sugieren que la intervención realizada contribuye a una optimización significativa en la disponibilidad de los certificados.

Tabla VI.

REGISTROS DESCRIPTIVOS DEL PACD

	N	Mínimo	Máximo	Media	Desviación Estándar
PACD – Preprueba	24	4.17	66.67	36.81	16.47
PACD – Postprueba	24	4.17	100.00	52.08	29.46

En ese sentido, la Figura 1 presenta una comparación entre los promedios de las fases de preprueba y postprueba, revelando que el promedio del PACD en la evaluación posterior alcanza el 52.08%, superior al 36.81% observado en la evaluación previa. Este incremento sugiere una mejora en el proceso de accesibilidad de certificados. No obstante, la Tabla VI muestra que la desviación estándar en la postprueba es de 29.46, notablemente más alta que la desviación estándar de 16.47 registrada en la preprueba. Esta mayor variabilidad en el porcentaje acumulado de certificados disponibles no implica necesariamente una inconsistencia en el proceso de emisión, sino que refleja la naturaleza acumulativa de los datos, donde cada certificado disponible contribuye de manera incremental al porcentaje total acumulado. La variabilidad ampliada en la evaluación posterior es influenciada por el aumento en la cantidad de certificados disponibles, lo que resulta en una contribución más heterogénea al porcentaje acumulado.

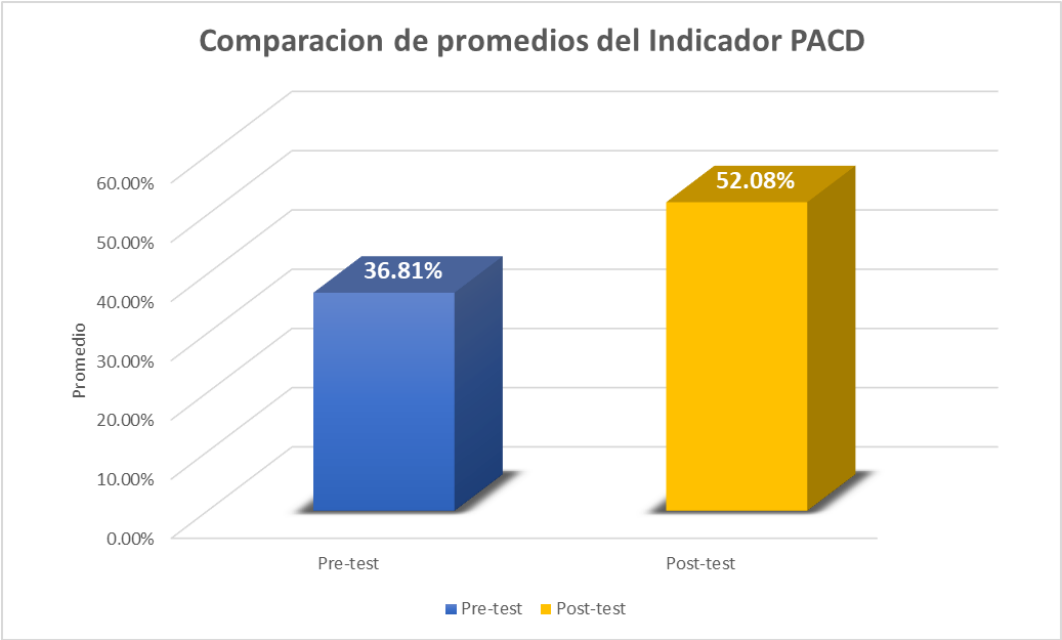


Fig. 1. Comparación de promedios del indicador PACD

5.1.2. Segunda Dimensión: Integridad de la Información

A. Segundo Indicador: Porcentaje Acumulado de Certificados Íntegros

La Tabla VII presenta los datos recopilados del indicador PACI (Porcentaje Acumulado de Certificados Íntegros) durante las mediciones de preprueba y postprueba, en las cuales se llevaron a cabo un total de 24 evaluaciones. Se observa una mejora progresiva en la integridad de la información a partir del sexto certificado en la prueba posterior. En consecuencia, se observa que la solución propuesta está contribuyendo de manera significativa a la mejora de la integridad de la información.

Tabla VII.

PACI: PREPRUEBA Y POSTPRUEBA

PACI	**Porcentaje Acumulado de certificados íntegros**	
	PACI Preprueba	PACI Postprueba
1	4.17%	4.17%
2	8.33%	8.33%
3	12.50%	12.50%
4	16.67%	16.67%
5	20.83%	20.83%
6	20.83%	25.00%
7	20.83%	29.17%
8	20.83%	33.33%
9	20.83%	37.50%
10	20.83%	41.67%

11	25.00%	45.83%
12	25.00%	50.00%
13	25.00%	54.17%
14	25.00%	58.33%
15	25.00%	62.50%
16	25.00%	66.67%
17	25.00%	70.83%
18	25.00%	75.00%
19	29.17%	79.17%
20	33.33%	83.33%
21	37.50%	87.50%
22	41.67%	91.67%
23	45.83%	95.83%
24	50.00%	100.00%

Así mismo, la tabla VIII revela que el porcentaje mínimo de certificados íntegros fue de 4.17%, lo que indica que al menos esa proporción del total previsto presentaba integridad en ambas fases. Se observa una notable diferencia en los valores máximos, dado que durante la preprueba la integridad máxima alcanzó el 50%, mientras que en la postprueba se logró la totalidad, es decir, el 100%. Asimismo, el promedio en la postprueba superó al promedio de la preprueba, registrando un 52.08% frente a un 25.17%. Estos datos sugieren que la intervención realizada contribuye a una optimización significativa en la integridad de los certificados.

Tabla VIII.

REGISTROS DESCRIPTIVOS DEL PACI

	N	Mínimo	Máximo	Media	Desviación Estándar
PACI – Preprueba	24	4.17	50.00	25.17	10.67
PACI – Postprueba	24	4.17	100.00	52.08	29.46

En ese sentido, la Figura 2 presenta una comparación entre los promedios de las fases de preprueba y postprueba, revelando que el promedio del PACI en la evaluación posterior alcanza el 52.08%, superior al 25.17% observado en la evaluación previa. Este incremento sugiere una mejora en las características de integridad de certificados. No obstante, la Tabla VIII muestra que la desviación estándar en la postprueba es de 29.46, notablemente más alta que la desviación estándar de 10.67 registrada en la preprueba. Esta mayor variabilidad en el porcentaje acumulado de certificados íntegros no implica necesariamente una inconsistencia en el proceso de verificación de integridad, sino que refleja la naturaleza acumulativa de los datos, donde cada certificado con propiedades de integridad contribuye de manera incremental al

porcentaje total acumulado. La variabilidad ampliada en la evaluación posterior es influenciada por el aumento en la cantidad de certificados íntegros, lo que resulta en una contribución más heterogénea al porcentaje acumulado.

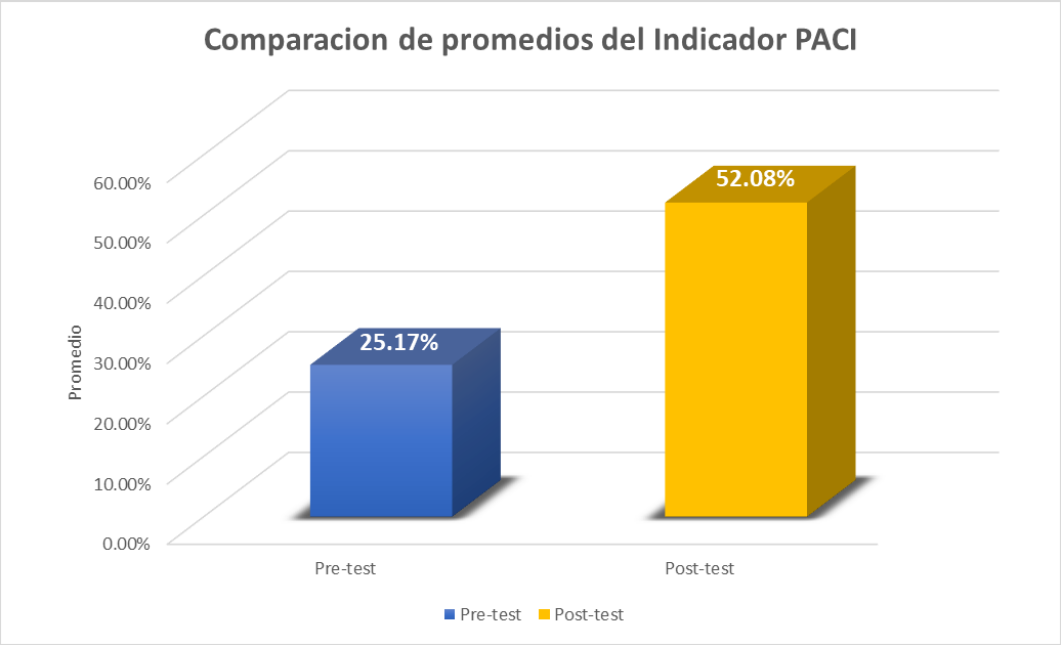


Fig. 2. Comparación de promedios del indicador PACI

5.1.3. Tercera Dimensión: Confidencialidad de la Información

A. Tercer Indicador: Porcentaje Acumulado de Certificados Entregados Correctamente

La Tabla IX presenta los datos recopilados del indicador PACEC (Porcentaje Acumulado de Certificados Entregados Correctamente) durante las mediciones de preprueba y postprueba, en las cuales se llevaron a cabo un total de 24 evaluaciones. Se observa una mejora progresiva en la confidencialidad de la información a partir del primer certificado en la prueba posterior. En consecuencia, se observa que la solución propuesta está contribuyendo de manera significativa a la mejora de la confidencialidad de la información.

Tabla IX.

PACEC: PREPRUEBA Y POSTPRUEBA

PACEC	**Porcentaje Acumulado de certificados entregados correctamente**	
	PACEC Preprueba	PACEC Postprueba
1	0.00%	4.55%
2	0.00%	9.09%
3	0.00%	13.64%
4	0.00%	17.05%

5	0.00%	19.32%
6	0.00%	23.86%
7	0.00%	28.41%
8	0.00%	32.95%
9	0.00%	37.50%
10	0.00%	39.77%
11	0.00%	40.91%
12	0.00%	43.18%
13	0.00%	47.73%
14	0.00%	51.14%
15	0.00%	55.68%
16	0.00%	61.36%
17	0.00%	64.77%
18	0.00%	65.91%
19	4.55%	70.45%
20	9.09%	75.00%
21	14.77%	80.68%
22	19.32%	85.23%
23	25.00%	90.91%
24	26.14%	92.05%

Así mismo, la tabla X revela que el porcentaje mínimo de certificados entregados correctamente fue de 0 % en la etapa preprueba y 4.55% en la etapa postprueba. Se observa una notable diferencia en los valores máximos, dado que durante la preprueba la confidencialidad máxima alcanzó el 26.14%, mientras que en la postprueba se logró el 92.05%. Asimismo, el promedio en la postprueba superó al de la preprueba, registrando un 47.96% frente a un 4.12%. Estos datos sugieren que la intervención realizada contribuye a una optimización significativa en la confidencialidad de los certificados.

Tabla X.

REGISTROS DESCRIPTIVOS DEL PACEC

	N	Mínimo	Máximo	Media	Desviación Estándar
PACEC – Preprueba	24	0	26.14	4.12	8.33
PACEC – Postprueba	24	4.55	92.05	47.96	26.48

En ese sentido, la Figura 3 presenta una comparación entre los promedios de las fases de preprueba y postprueba, revelando que el promedio del PACEC en la evaluación posterior alcanza el 47.96%, superior al 4.12% observado en la evaluación previa. Este incremento sugiere una mejora en las características de la confidencialidad de certificados. No obstante, la Tabla X muestra que la desviación estándar en la postprueba es de 26.48, notablemente más alta

que la desviación estándar de 8.33 registrada en la preprueba. Esta mayor variabilidad en el porcentaje acumulado de certificados entregados correctamente no implica necesariamente una inconsistencia en el proceso de la emisión confidencial, sino que refleja la naturaleza acumulativa de los datos, donde cada certificado entregado correctamente contribuye de manera incremental al porcentaje total acumulado. La variabilidad ampliada en la evaluación posterior es influenciada por el aumento en la cantidad de certificados entregados confidencialmente, lo que resulta en una contribución más heterogénea al porcentaje acumulado.

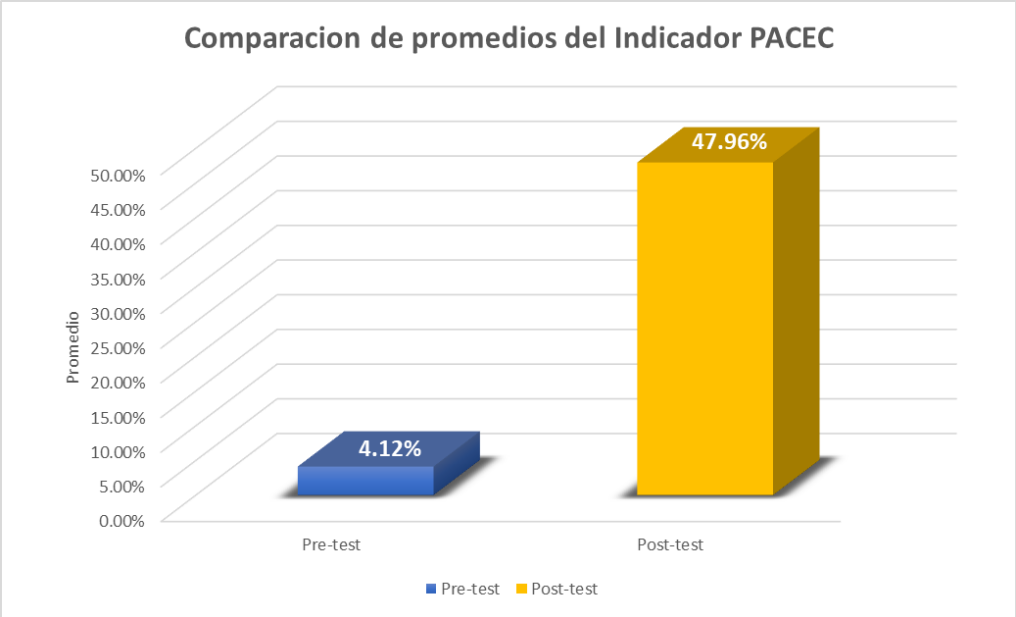


Fig. 3. Comparación de promedios del indicador PACEC

5.2. Resultados Inferenciales

5.2.1. Primera Dimensión: Disponibilidad de la Información

A. Primer Indicador: Porcentaje Acumulado de Certificados Disponibles

Prueba de normalidad:

Hernández et al. (2014) mencionan que para conjuntos de datos de hasta 50 elementos se recomienda la utilización de la prueba de Shapiro-Wilk, como se cita en [49]. Además, de acuerdo con J. Arias y M. Covinos, un valor de significancia (Sig.) superior a al valor de 0.05 indica una distribución normal de los datos, mientras que un valor de (Sig.) inferior al valor de 0.05 sugiere una distribución no normal, según se menciona en [50].

A continuación se redacta las hipótesis de la prueba de normalidad del indicador PACD:

- **Hipótesis nula (Ho):** La distribución de los datos del indicador PACD es normal.

- **Hipótesis Alterna (H1):** La distribución de los datos del indicador PACD **no** es normal.

Tabla XI.

PRUEBA DE NORMALIDAD DEL INDICADOR PACD

	Shapiro-Wilk		
	Estadístico	gl	Sig.
PACD – Pre-test	,957	24	,373
PACD – Post-test	,959	24	,416

Los hallazgos obtenidos después de aplicar el test Shapiro-Wilk para determinar la normalidad al indicador PACD se detallan en la Tabla XI. Para los datos del pre-test, se encontró un nivel de significancia 0.373, mientras que para el post-test, este valor fue de 0.416. Considerando que ambos indicadores de significación superan el umbral de 0.05, no se dispone de la evidencia necesaria para descartar la hipótesis nula. En resumen, la hipótesis nula no se descarta.

Prueba de hipótesis:

Los datos correspondientes al indicador PACD se muestran distribuidos normalmente. Así, para la realización del test de hipótesis, se aplicará la prueba t de Student. Este enfoque se fundamenta en la observación de [50], quien señala que para datos que presentan una distribución normal se aplica la prueba de t de Student.

A continuación se redacta las hipótesis del indicador PACD:

- **Hipótesis nula (Ho):** El sistema con tecnología blockchain **no** tiene un efecto significativo en la disponibilidad de la información de certificados de la gestión de la seguridad de la información en una institución Privada, Callao, 2022.
- **Hipótesis alterna (H1):** El sistema con tecnología blockchain tiene un efecto significativo en la disponibilidad de la información de la gestión de la seguridad de la información en una institución Privada, Callao, 2022.

Tabla XII.

ESTADÍSTICOS DE MUESTRAS RELACIONADAS

		Media	N	Desviación típ.	Error típ. de la media
Par 1	PACD – Pre test	36,8067	24	16,46962	3,36185
	PACD – Post test	52,0833	24	29,46262	6,01403

Tabla XIII.

PRUEBA DE MUESTRAS RELACIONADAS

		Diferencias relacionadas							
					95% Intervalo de confianza para la diferencia				
		Media	Desviación típ.	Error típ. de la media	Inferior	Superior	t	gl	Sig. (bilateral)
Par 1	PACD Pre test – PACD Post test	-15,27667	14,25800	2,91040	-21,29729	-9,25604	-5,249	23	,000

En la Tabla XIII se exponen los hallazgos del test de t de Student para el indicador PACD. Se documentó un índice de significación de 0.000, notablemente menor al límite establecido de 0.05. En consecuencia, se rechaza la hipótesis de nula y se admite la hipótesis alternativa. Esto indica que los promedios recopilados pre y post-test, utilizando la ficha de registro, difieren significativamente.

5.2.2. Segunda Dimensión: Integridad de la información

A. Segundo Indicador: Porcentaje Acumulado de Certificados Íntegros

Prueba de normalidad:

Hernández et al. (2014) mencionan que para conjuntos de datos de hasta 50 elementos se recomienda la utilización de la prueba de Shapiro-Wilk, como se cita en [49]. Además, de acuerdo con J. Arias y M. Covinos, un valor de significancia (Sig.) superior a al valor de 0.05 indica una distribución normal de los datos, mientras que un valor de (Sig.) inferior al valor de 0.05 sugiere una distribución no normal, según se menciona en [50].

A continuación se redacta las hipótesis de la prueba de normalidad del indicador PACI:

- **Hipótesis nula (Ho):** La distribución de los datos del indicador PACI es normal.
- **Hipótesis Alterna (H1):** La distribución de los datos del indicador PACI **no** es normal.

Tabla XIV.

PRUEBA DE NORMALIDAD DEL INDICADOR PACI

	Shapiro-Wilk		
	Estadístico	gl	Sig.
PACI – Pre test	,922	24	,063
PACI – Post test	,959	24	,416

Los hallazgos obtenidos después de aplicar el test Shapiro-Wilk para determinar la normalidad al indicador PACI se detallan en la Tabla XIV. Para los datos del pre-test, se encontró un nivel de significancia 0.063, mientras que para el post-test, este valor fue de 0.416. Considerando que ambos indicadores de significación superan el umbral de 0.05, no se dispone de la evidencia necesaria para descartar la hipótesis nula. En resumen, la hipótesis nula no se descarta.

Prueba de hipótesis:

Los datos correspondientes al indicador PACI se muestran distribuidos normalmente. Así, para la realización del test de hipótesis, se aplicará la prueba t de Student. Este enfoque se fundamenta en la observación de [50], quien señala que para datos que presentan una distribución normal se aplica la prueba de t de Student.

A continuación se redacta las hipótesis del indicador PACI:

- **Hipótesis nula (Ho):** El sistema con tecnología blockchain **no** tiene un efecto significativo en la integridad de la información de certificados de la gestión de la seguridad de la información en una institución Privada, Callao, 2022.
- **Hipótesis alterna (H1):** El sistema con tecnología blockchain tiene un efecto significativo en la integridad de la información de la gestión de la seguridad de la información en una institución Privada, Callao, 2022.

Tabla XV.

ESTADÍSTICOS DE MUESTRAS RELACIONADAS

		Media	N	Desviación típ.	Error típ. de la media
Par 1	PACI Pre test	25,1729	24	10,67471	2,17897
	PACI Post test	52,0833	24	29,46262	6,01403

Tabla XVI.

PRUEBA DE MUESTRAS RELACIONADAS

		Diferencias relacionadas							
		Media	Desviación típ.	Error típ. de la media	95% Intervalo de confianza para la diferencia		t	gl	Sig. (bilateral)
					Inferior	Superior			
Par 1	PACI Pre test – PACI Post test	-26,91042	20,15051	4,11321	-35,41923	-18,40160	-6,542	23	,000

La Tabla XVI presenta los resultados del test de t de Student para el indicador PACI. Se documentó un índice de significación de 0.000, notablemente menor al límite establecido de 0.05. En consecuencia, se rechaza la hipótesis de nula y se admite la hipótesis alternativa. Esto indica que los promedios recopilados pre y post-test, utilizando la ficha de registro, difieren significativamente.

5.2.3. Tercera Dimensión: Confidencialidad de la Información

A. Tercer Indicador: Porcentaje Acumulado de Certificados Entregados Correctamente

Prueba de normalidad:

Hernández et al. (2014) mencionan que para conjuntos de datos de hasta 50 elementos se recomienda la utilización de la prueba de Shapiro-Wilk, como se cita en [49]. Además, de acuerdo con J. Arias y M. Covinos, un valor de significancia (Sig.) superior a al valor de 0.05 indica una distribución normal de los datos, mientras que un valor de (Sig.) inferior al valor de 0.05 sugiere una distribución no normal, según se menciona en [50].

A continuación se redacta las hipótesis de la prueba de normalidad del indicador PACEC:

- **Hipótesis nula (Ho):** La distribución de los datos del indicador PACEC es normal.
- **Hipótesis Alterna (H1):** La distribución de los datos del indicador PACEC **no** es normal.

Tabla XVII.

PRUEBA DE NORMALIDAD DEL INDICADOR PACEC

	Shapiro-Wilk		
	Estadístico	gl	Sig.
PACEC – Pre test	,562	24	,000
PACEC – Post test	,964	24	,516

Los hallazgos obtenidos después de aplicar el test Shapiro-Wilk para determinar la normalidad al indicador PACEC se detallan en la Tabla XVII. Para los datos del pre-test, se encontró un nivel de significancia 0.000, mientras que para el post-test, este valor fue de 0.516. El valor de significancia obtenido para la evaluación previa (pre-test) es inferior al umbral de 0.05, lo que conduce a rechazar la hipótesis nula para los datos de la evaluación previa (pre-test); en contraste, el valor de significancia correspondiente a la evaluación posterior (post-test)

supera el límite de 0.05, lo que significa que la hipótesis nula no se rechaza para los datos de la evaluación posterior (post-test).

Prueba de hipótesis:

Para el análisis del tercer indicador PACEC se identificó que los datos correspondientes al pre-test no seguían una distribución normal, en contraste con los datos del post-test que sí se ajustaban a dicha distribución. Esta constatación llevó a optar por la prueba de Wilcoxon para realizar la prueba de hipótesis. Según [51], la técnica estadística denominada t de Student, una prueba paramétrica, es apropiada para la comparación de dos grupos cuyas variables cuantitativas continuas se distribuyen normalmente; sin embargo, para datos relacionados que carecen de normalidad, se prefieren las pruebas no paramétricas, como la de Wilcoxon. Los autores subrayan que la aplicación de pruebas paramétricas requiere que ambos conjuntos de datos exhiban una distribución normal; por lo tanto, ante la falta de normalidad en el pre-test, se eligió el uso de la prueba no paramétrica de Wilcoxon.

A continuación se redacta las hipótesis del indicador PACEC:

- **Hipótesis nula (Ho):** El sistema con tecnología blockchain **no** tiene un efecto significativo en la confidencialidad de la información de certificados de la gestión de la seguridad de la información en una institución Privada, Callao, 2022.
- **Hipótesis alterna (H1):** El sistema con tecnología blockchain tiene un efecto significativo en la confidencialidad de la información de la gestión de la seguridad de la información en una institución Privada, Callao, 2022.

Tabla XVIII.

PRUEBA DE RANGO DE SIGNOS DE WILCOXON

		N	Rango promedio	Suma de rangos
PACEC Post test – PACEC Pre test	Rangos negativos	0[a]	,00	,00
	Rangos positivos	24[b]	12,50	300,00
	Empates	0[c]		
	Total	24		

a. PACEC Post test < PACEC Pre test

b. PACEC Post test > PACEC Pre test

c. PACEC Post test = PACEC Pre test

Tabla XIX.

ESTADISTICO DE CONTRASTE

	Prueba de rangos con signo de Wilcoxon	
	Z	Sig. asintót. (bilateral)
PACEC Post test – PACEC Pre test	-4,293[b]	,000

a. Prueba de los rangos con signo de Wilcoxon

b. Basado en los rangos negativos.

La Tabla XVIII muestra los hallazgos del test de rango con signos de Wilcoxon. Se nota que el total de rangos negativos alcanza 0.00 mientras que el total de rangos positivos asciende a 300.00. Esta diferencia en los rangos indica que existen más diferencias positivas, lo que sugiere que los valores obtenidos en el post-test superan a los del pre-test. Asimismo, la Tabla XIX exhibe el valor estadístico de la prueba de rango con signo de Wilcoxon: un valor Z de -4.293 y un índice de significancia de 0.000, que resulta ser inferior al umbral de 0.05. El resultado obtenido indica el rechazo de la hipótesis nula y la aceptación de la hipótesis alterna.

Capítulo VI: Discusión

Se realizo un análisis de los resultados alcanzados en la presente investigación, obtenidos mediante los indicadores del porcentaje acumulado de: certificados disponibles, certificados íntegros y certificados entregados correctamente.

6.1. Discusión de la Primera Dimensión: Disponibilidad de la Información

6.1.1. Resultados Descriptivos

Los datos recopilados mediante el indicador PACD, muestran en el pre-test, que el PACD alcanza un máximo del 66.67%, mientras que en el post-test asciende al 100%, lo que refleja que la aplicación integrada con tecnología blockchain mejora en un 33.33% la disponibilidad de la información de certificados. Así mismo, [52] mencionan que el uso de la tecnología blockchain permite mejorar en un 45% la disponibilidad de la información.

6.1.2. Resultados Inferenciales

Los datos recopilados del indicador PACD evidencian que poseen características de una repartición normal, y mediante el método estadístico denominado prueba de t de student, validan que se rechaza la hipótesis nula, es decir que El sistema con tecnología blockchain tiene un efecto significativo en la disponibilidad de la información de la gestión de la seguridad de la información en una institución Privada, Callao, 2022. Del mismo modo [52], mencionan que la aplicación de la tecnología blockchain en su propuesta tecnológica garantiza la disponibilidad de la información para los pacientes y médicos.

6.2. Discusión de la Segunda Dimensión: Integridad de la Información

6.2.1. Resultados Descriptivos

Los datos recopilados mediante el indicador PACI, muestran en el pre-test, que el PACI alcanza un máximo del 50%, mientras que en el post-test asciende al 100%, lo que refleja que la aplicación integrada con tecnología blockchain mejora en un 50% la integridad de la información de certificados. Así mismo, [52] mencionan que el uso de la tecnología blockchain disminuye en un 50% el riesgo de alteraciones no autorizadas y duplicidad de datos en los registros médicos.

6.2.2. Resultados Inferenciales

Los datos recopilados del indicador PACI evidencian que poseen características de una repartición normal, y mediante el método estadístico denominado prueba de t de student, validan

que se rechaza la hipótesis nula, es decir que El sistema con tecnología blockchain tiene un efecto significativo en la integridad de la información de la gestión de la seguridad de la información en una institución Privada, Callao, 2022. Del mismo modo [52], mencionan que la aplicación de la tecnología blockchain en su propuesta tecnológica mejora la integridad y consistencia de la información.

6.3. Discusión de la Tercera Dimensión: Confidencialidad de la Información

6.3.1. Resultados Descriptivos

Los datos recopilados mediante el indicador PACEC, muestran en el pre-test, el PACEC alcanza un máximo del 26.14%, mientras que en el post-test asciende al 92.05%, lo que refleja que la aplicación integrada con tecnología blockchain mejora en un 65.91% la confidencialidad de la información de certificados. Así mismo, [52] mencionan que el uso de la tecnología blockchain disminuye en un 20% el riesgo de que terceros accedan a la información.

6.3.2. Resultados Inferenciales

Los datos recopilados del indicador PACEC evidencian que los datos del pre-test no poseen características una repartición normal, mientras que los datos del post-test si poseen características de una repartición normal, y mediante el método estadístico denominado test los rangos con signo de Wilcoxon, validan que se rechaza la hipótesis nula, es decir que El sistema con tecnología blockchain tiene un efecto significativo en la confidencialidad de la información de la gestión de la seguridad de la información en una institución Privada, Callao, 2022. Del mismo modo [52], mencionan que la aplicación de la tecnología blockchain en su propuesta tecnológica mejora la confidencialidad de la información.

Capítulo VII: Conclusiones

1. En primer lugar, se concluye que la solución propuesta de sistema con tecnología blockchain tiene un efecto positivo en la disponibilidad de la información de certificados de la gestión de la seguridad de la información en una institución Privada, Callao, 2022, ya que el indicador PACD demostró una mejora del 33.33% en la disponibilidad de la información de certificados.
2. En segundo lugar, se concluye que la solución propuesta de sistema con tecnología blockchain tiene un efecto positivo en la integridad de la información de certificados de la gestión de la seguridad de la información en una institución Privada, Callao, 2022, ya que el indicador PACI demostró una mejora del 50% en la integridad de la información de certificados.
3. En Tercer lugar, se concluye que la solución propuesta de sistema con tecnología blockchain tiene un efecto positivo en la confidencialidad de la información de certificados de la gestión de la seguridad de la información en una institución Privada, Callao, 2022, ya que el indicador PACI demostró una mejora del 65.91% en la confidencialidad de la información de certificados.
4. Por lo tanto, se concluye que el sistema con tecnología blockchain afecta positivamente la gestión de la seguridad de la información en una institución Privada, Callao, 2022, dado que los indicadores demuestran mejoras en las dimensiones de disponibilidad, integridad y confidencialidad.

Capitulo VIII: Recomendaciones

Tras obtener resultados positivos en la investigación presente, es aconsejable tomar en cuenta las recomendaciones a continuación:

1. En primer lugar, diseñar estrategias para la expansión del sistema de blockchain, con el fin de que éste pueda evolucionar junto con el desarrollo de la entidad y garantizar su viabilidad y eficacia en el futuro.
2. En segundo lugar, explorar la viabilidad de integrar tecnologías avanzadas como la inteligencia artificial y el aprendizaje automático para anticipar necesidades y optimizar los mecanismos de protección de datos.
3. En tercer lugar, dadas las mejorías constatadas, se aconseja perpetuar y extender el uso de la tecnología de cadena de bloques a diferentes segmentos de la administración de datos.
4. En cuarto lugar, profundizar en el estudio sobre la transferibilidad de estos resultados a otras organizaciones o escenarios, incluyendo distintas áreas geográficas o sectores económicos, para ampliar el alcance de las ventajas ofrecidas por la blockchain.

Referencias

[1] Cloudflare, "¿Qué es la seguridad de la información?" Accessed: Apr. 14, 2024. [Online]. Available: https://www.cloudflare.com/es-es/learning/security/what-is-information-security/

[2] IBM, "¿Qué es la tecnología blockchain? - IBM Blockchain." Accessed: Apr. 27, 2024. [Online]. Available: https://www.ibm.com/es-es/topics/blockchain

[3] J. Cano, "Gobierno y gestión de la seguridad y la ciberseguridad. Una agenda complementaria a los estándares vigentes y las buenas prácticas | Global Strategy," Global Strategy Report. Accessed: Apr. 14, 2024. [Online]. Available: https://global-strategy.org/gobierno-y-gestion-de-la-seguridad-y-la-ciberseguridad-una-agenda-complementaria-a-los-estandares-vigentes-y-las-buenas-practicas/

[4] E. A. Ramírez-Camargo and M. A. Rinconc-Pinzon, "La importancia de la seguridad de la información en el sector público en Colombia.," *RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação*, vol. 2022, no. 46, pp. 97–99, Jun. 2022, doi: 10.17013/RISTI.46.87-99.

[5] S. Bustamante-García, M. Á. Valles-Coral, I. E. Cuellar-Rodríguez, and D. Lévano-Rodríguez, "Políticas basadas en la ISO 27001:2013 y su influencia en la gestión de seguridad de la información en municipalidades de Perú," *Enfoque UTE*, vol. 12, no. 2, pp. 69–79, Apr. 2021, doi: 10.29019/ENFOQUEUTE.743.

[6] J. Veliz-Delgado, "Ciberdelincuencia e Inteligencia Artificial en Perú 2023 | RPP Noticias," RPP. Accessed: Apr. 19, 2024. [Online]. Available: https://rpp.pe/tecnologia/mas-tecnologia/ciberdelincuencia-e-inteligencia-artificial-en-peru-2023-noticia-1508418

[7] M. P. Delgado-Baltazar and J. H. Valverde-Huamani, "Sistema de seguridad de la información para optimizar los servidores web en la oficina de tecnología de información y comunicación de la Facultad de Ingeniería Industrial y de Sistemas de la Universidad Nacional del Callao 2022," Universidad Nacional de Callao, 2023. Accessed: Apr. 19, 2024. [Online]. Available: http://repositorio.unac.edu.pe/handle/20.500.12952/8534

[8] C. Rodríguez-Gutiérrez, "Propuesta de implementación de un sistema de gestión de seguridad de la información aplicando la Norma ISO 27001:2013 para una institución del Estado en la Provincia Constitucional de Callao - 2021," Universidad Tecnologica del Perú, 2021. Accessed: Apr. 19, 2024. [Online]. Available: http://repositorio.utp.edu.pe/handle/20.500.12867/5101

[9] P. Babilonia-Martel and H. E. N. Carretero-Gonzales, "El uso de la tecnología blockchain para desarrollar una cadena logística sostenible en el transporte marítimo internacional: caso peruano," Universidad de Lima, 2022. Accessed: Apr. 28, 2024. [Online]. Available: https://repositorio.ulima.edu.pe/handle/20.500.12724/17182

[10] H. D. Zubaydi, P. Varga, and S. Molnár, "Leveraging Blockchain Technology for Ensuring Security and Privacy Aspects in Internet of Things: A Systematic Literature Review," *Sensors*, vol. 23, no. 2, p. 788, Jan. 2023, doi: 10.3390/S23020788.

[11] T. Ahram, A. Sargolzaei, S. Sargolzaei, J. Daniels, and B. Amaba, "Blockchain technology innovations," *2017 IEEE Technology and Engineering Management Society Conference, TEMSCON 2017*, no. 2016, pp. 137–141, 2017, doi: 10.1109/TEMSCON.2017.7998367.

[12] K. Schwaber and Sutherland. Jeff, “Guía de Scrum,” SCRUM GUIDES. Accessed: Jan. 22, 2025. [Online]. Available: https://scrumguides.org/scrum-guide.html#purpose-of-the-scrum-guide

[13] P. A. Villa-Sánchez, J. Gutiérrez-Obando, and A. M. López-Echeverry, “Elementos de Seguridad para Gestión Documental con Blockchain,” *Entre Ciencia e Ingeniería*, vol. 17, no. 34, pp. 36–42, Nov. 2023, doi: 10.31908/19098367.2667.

[14] Ministerio Público Fiscalía de la Nación, “¿Qué es la seguridad de la información? - Orientación,” Plataforma digital única del Estado Peruano. Accessed: Apr. 29, 2024. [Online]. Available: https://www.gob.pe/23391-que-es-la-seguridad-de-la-informacion

[15] R. R. Irshad *et al.*, “Enhancing Cloud-Based Inventory Management: A Hybrid Blockchain Approach With Generative Adversarial Network and Elliptic Curve Diffie Helman Techniques,” *IEEE*, vol. 12, pp. 25917–25932, 2024, doi: 10.1109/ACCESS.2024.3367445.

[16] R. A. Abutaleb, S. S. Alqahtany, and T. A. Syed, “Integrity and Privacy-Aware, Patient-Centric Health Record Access Control Framework Using a Blockchain,” *Applied Sciences 2023*, vol. 13, no. 2, p. 1028, Jan. 2023, doi: 10.3390/APP13021028.

[17] K. Carvalho and J. Granjal, “Security and Privacy for Mobile IoT Applications Using Blockchain,” *Sensors*, vol. 21, no. 17, p. 5931, Sep. 2021, doi: 10.3390/S21175931.

[18] I. Permatasari, M. Essaid, H. Kim, and H. Ju, “Blockchain Implementation to Verify Archives Integrity on Cilegon E-Archive,” *Applied Sciences*, vol. 10, no. 7, p. 2621, Apr. 2020, doi: 10.3390/APP10072621.

[19] Z. Liu, “Improving the security and reliability of application systems with blockchain technology,” The Hong Kong Polytechnic University, 2023. Accessed: May 03, 2024. [Online]. Available: https://theses.lib.polyu.edu.hk/handle/200/12549

[20] K. Çelik, “Blockchain based solution for electronic health record integrity,” Middle East Technical University, 2022. Accessed: May 04, 2024. [Online]. Available: https://open.metu.edu.tr/handle/11511/99487

[21] O. A. Gutierrez-Baracco and J. A. Lujan-Alfaro, “Simulación de un modelo de tecnología blockchain para garantizar la seguridad de la información del proceso de admisión de una universidad pública del Perú,” Universidad Tecnológica del Perú, 2023. Accessed: May 03, 2024. [Online]. Available: http://repositorio.utp.edu.pe/handle/20.500.12867/8240

[22] F. D. Martínez-Montenegro, “Evaluación de arquitectura blockchain ma-abs para la gestión de historias clínicas electrónicas peruanas,” Universidad Señor de Sipán, 2022. Accessed: May 03, 2024. [Online]. Available: http://repositorio.uss.edu.pe//handle/20.500.12802/9219

[23] R. Raimundo and A. Rosário, “Blockchain System in the Higher Education,” *Eur J Investig Health Psychol Educ*, vol. 11, no. 1, pp. 276–293, Mar. 2021, doi: 10.3390/EJIHPE11010021.

[24] L. Koh, A. Dolgui, and J. Sarkis, “Blockchain in transport and logistics – paradigms and transitions,” *Int J Prod Res*, vol. 58, no. 7, pp. 2054–2062, Apr. 2020, doi: 10.1080/00207543.2020.1736428.

[25] P. Lafourcade and M. Lombard-Platet, “About blockchain interoperability,” *Inf Process Lett*, vol. 161, p. 105976, Sep. 2020, doi: 10.1016/J.IPL.2020.105976.

[26] M. Alshamsi, M. Al-Emran, and K. Shaalan, “A Systematic Review on Blockchain Adoption,” *Applied Sciences*, vol. 12, no. 9, p. 4245, Apr. 2022, doi: 10.3390/APP12094245.

[27] P. Paul, P. S. Aithal, R. Saavedra, and S. Ghosh, “Blockchain Technology and Its Types—A Short Review,” Dec. 2021, Accessed: May 06, 2024. [Online]. Available: https://papers.ssrn.com/abstract=4050933

[28] I. Abu-elezz, A. Hassan, A. Nazeemudeen, M. Househ, and A. Abd-alrazaq, “The benefits and threats of blockchain technology in healthcare: A scoping review,” *Int J Med Inform*, vol. 142, no. February, p. 104246, 2020, doi: 10.1016/j.ijmedinf.2020.104246.

[29] M. Mirtsch, J. Kinne, and K. Blind, “Exploring the Adoption of the International Information Security Management System Standard ISO/IEC 27001: A Web Mining-Based Analysis,” *IEEE*, vol. 68, no. 1, pp. 87–100, Feb. 2021, doi: 10.1109/TEM.2020.2977815.

[30] K. Khando, S. Gao, S. M. Islam, and A. Salman, “Enhancing employees information security awareness in private and public organisations: A systematic literature review,” *Comput Secur*, vol. 106, p. 102267, Jul. 2021, doi: 10.1016/J.COSE.2021.102267.

[31] G. A. Kaissis, M. R. Makowski, D. Rückert, and R. F. Braren, “Secure, privacy-preserving and federated machine learning in medical imaging,” *Nat Mach Intell*, vol. 2, no. 6, pp. 305–311, Jun. 2020, doi: 10.1038/s42256-020-0186-1.

[32] D. M. El-Din, A. E. Hassanien, and E. E. Hassanien, “Information Integrity for Multi-sensors Data Fusion in Smart Mobility,” *Studies in Computational Intelligence*, vol. 846, pp. 99–121, 2020, doi: 10.1007/978-3-030-24513-9_6.

[33] K. J. Altamirano-de-la-Borda, “La seguridad de la información en la administración pública,” in *Construyendo un mundo inteligente para la sostenibilidad. Actas del III Congreso Internacional de Ingeniería de Sistemas*, Lima: Universidad de Lima, Nov. 2021. Accessed: May 10, 2024. [Online]. Available: https://repositorio.ulima.edu.pe/handle/20.500.12724/13917

[34] Statistics Canada, “Statistics: Power from Data! Analytical graphing: Cumulative percentage,” Statistics Canada. Accessed: Jan. 29, 2024. [Online]. Available: https://www150.statcan.gc.ca/n1/edu/power-pouvoir/ch10/5214864-eng.htm

[35] M. W. Aji-Bawono, M. Amin-Soetomo, and T. Apriatin, “Analysis correlation of the Implementation Framework COBIT 5, ITIL V3 and ISO 27001 for ISO 10002 Customer satisfaction,” *ACMIT Proceedings*, vol. 7, no. 1, pp. 31–46, Jul. 2020, doi: 10.33555/ACMIT.V7I1.105.

[36] C. E. Remolina-Medina, “Beneficios y limitaciones del Blockchain en contratos inteligentes en el sector salud. Una revisión de la literatura,” *Revista Científica Anfibios*, vol. 5, no. 2, pp. 57–71, 2022, doi: 10.37979/afb.2022v5n2.113.

[37] C. R. Sánchez, “Blockchain: Funcionamiento y pertinencia en sectores públicos y privados,” *Interconectando Saberes*, vol. 7, no. 14, pp. 169–178, 2022, doi: 10.25009/IS.V0I14.2734.

[38] Real Academia Española, “certificación | Definición | Diccionario de la lengua española | RAE - ASALE,” Real Academia Española. Accessed: Oct. 11, 2024. [Online]. Available: https://dle.rae.es/certificaci%C3%B3n

[39] L. Rosero-Correa, M. Morales-Morales, and S. Morales-Cardoso, “Registro de títulos académicos mediante una aplicación basada en Blockchain y Smart Contracts,” *Cátedra*, vol. 3, no. 2, pp. 73–98, 2020, doi: 10.29166/catedra.v3i2.2200.

[40] W. A. Apaza-Chávez, “Propuesta de un plan de seguridad de la información para incrementar la fiabilidad de datos en una financiera,” *Innovación Y Software*, vol. 2, no. 2, pp. 27–43, 2021, [Online]. Available: https://revistas.ulasalle.edu.pe/innosoft/article/view/39

[41] J. Coronado Padilla, “Escalas de medición,” *Paradigmas: Una Revista Disciplinar de Investigación*, vol. 2, no. 2, pp. 104–125, 2007, Accessed: May 15, 2024. [Online]. Available: https://dialnet.unirioja.es/servlet/articulo?codigo=4942056

[42] F. J. Callupe-Mendoza and S. Perez-Romero, “Sistema Help desk para la gestión de incidencias en el área de TI de la empresa comunal Ecosem, Morococha 2023,” Universidad Cesar Vallejo, 2023. Accessed: May 15, 2024. [Online]. Available: https://repositorio.ucv.edu.pe/handle/20.500.12692/129854

[43] R. Ochoa, N. Nava, and D. Fusil, “Comprensión epistemológica del tesista sobre investigaciones cuantitativas, cualitativas y mixtas,” *Orbis: revista de Ciencias Humanas*, vol. 15, no. 45, pp. 13–22, 2020, Accessed: May 17, 2024. [Online]. Available: https://dialnet.unirioja.es/servlet/articulo?codigo=7407375

[44] C. D. de-la-Cruz-Galvan, “Aplicación móvil para emisión de información en tiempo real del servicio de transporte en la Universidad Nacional de Cañete, 2023. Almidón Ortiz, Carlos Alcides,” Universidad Nacional de Cañete, Cañete, 2023. Accessed: May 17, 2024. [Online]. Available: https://repositorio.undc.edu.pe/handle/123456789/108

[45] C. Ramos-Galarza, “Diseños De Investigaciónex Perimental,” *CienciAmérica*, vol. 10, no. 1, 2021, [Online]. Available: https://dialnet.unirioja.es/servlet/articulo?codigo=7890336

[46] J. C. Medrano-Cabello, “Sistema de información para mejorar la gestión documentaria de la carpeta pedagógica de una institución educativa pública, Lima - 2023,” Universidad Cesar Vallejo, 2024. Accessed: May 17, 2024. [Online]. Available: https://hdl.handle.net/20.500.12692/134752

[47] L. J. Reales-Chacón, G. E. Robalino-Morales, A. C. Peñafiel-Luna, J. H. Cárdenas-Medina, and P. F. Cantuña-Vallejo, “El Muestreo Intencional No Probabilístico como herramienta de la investigación científica en carreras de Ciencias de la Salud.,” *Universidad y Sociedad*, vol. 14, no. S5, pp. 681-691., Oct. 2022, Accessed: May 17, 2024. [Online]. Available: https://rus.ucf.edu.cu/index.php/rus/article/view/3338

[48] J. G. Leon-Luque, “Business intelligence basado en Hefesto para la toma de decisiones del departamento de marketing en Favo S.A.C.,” Universidad Cesar Vallejo, 2023. Accessed: May 20, 2024. [Online]. Available: https://repositorio.ucv.edu.pe/handle/20.500.12692/120426

[49] P. A. Quiroz-Soriano and A. E. Quiroz-Soriano, “Sistema web para el proceso de reserva de espacios deportivos en la empresa Agrícola Tercer Mundo S.A., Cañete, 2023,” 2023. Accessed: Feb. 03, 2024. [Online]. Available: https://repositorio.undc.edu.pe/items/5258066a-b7b6-4ca5-9a14-1f5f1aa3946a

[50] C. P. Reyna-Vizcarra and R. C. Sanchez-Ramos, “Software con tecnologia qr geolocalizada para el control de asistencias del personal de la empresa mts group restaurantes peruanos s.a.c. cañete,2023,” 2023. Accessed: Feb. 03, 2024. [Online]. Available: https://repositorio.undc.edu.pe/items/ca27f31c-31c5-4334-ab2f-8ad97ef39d0e

[51] E. Flores-Ruiz, M. G. Miranda-Novales, M. Á. Villasís-Keever, E. Flores-Ruiz, M. G. Miranda-Novales, and M. Á. Villasís-Keever, “El protocolo de investigación VI: cómo elegir la prueba estadística adecuada. Estadística inferencial,” *Rev Alerg Mex*, vol. 64, no. 3, pp. 364–370, Jul. 2017, doi: 10.29262/RAM.V64I3.304.

[52] A. Martinez Cervantes and C. A. Molina Charaja, “Arquitectura Tecnológica para la Gestión del Historial Médico usando Blockchain en el Sector Privado de Salud,” Universidad Peruana de Ciencias Aplicadas, 2021. Accessed: May 22, 2024. [Online]. Available: https://repositorioacademico.upc.edu.pe/handle/10757/655796

Anexos

Anexo 01: Matriz de Consistencia

Sistema con Tecnología Blockchain para la Gestión de la Seguridad de la Información en una Institución Privada, Callao, 2022

PROBLEMA	OBJETIVO	HIPÓTESIS	VARIABLES Y DIMENSIONES	METODOLOGÍA
Problema General	**Objetivo General**	**Hipótesis General**	**Variable independiente**	**Tipo de investigación:** Aplicada **Enfoque de investigación:** Cuantitativo **Nivel de investigación:** Explicativo **Método de investigación:** Hipotético-deductivo **Diseño de investigación:** Preexperimental **Población y Muestra:** **Población:** 24 certificados de publicación, contenidos en el Volumen 1 (Números 1 y 2) y el Volumen 2 (Número 3) **Muestra:** 24 certificados de publicación, contenidos en el Volumen 1 (Números 1 y 2) y el Volumen 2 (Número 3) **Muestreo:** No probabilístico por conveniencia **Técnicas e instrumentos de recolección de datos** **Técnica:** Fichaje **Instrumentos:** Ficha de registro
¿Cuál es el efecto de un sistema con tecnología blockchain en la gestión de la seguridad de la información en una institución privada, Callao, 2022?	Determinar el efecto de un Sistema con tecnología blockchain en la gestión de la seguridad de la información en una institución privada, Callao, 2022.	El sistema con tecnología blockchain tiene un efecto significativo en la gestión de la seguridad de la información en una institución privada, Callao, 2022.	Sistema con Tecnología Blockchain	
Problemas específicos	**Objetivos Específicos**	**Hipótesis Específicos**	**Variable dependiente**	
a) ¿Cuál es el efecto de un sistema con tecnología blockchain en la disponibilidad de la información de la gestión de la seguridad de la información en una institución privada, Callao, 2022? **b)** ¿Cuál es el efecto de un sistema con tecnología blockchain en la integridad de la información de la gestión de la seguridad de la información en una institución privada, Callao, 2022? **c)** ¿Cuál es el efecto de un sistema con tecnología blockchain en la confidencialidad de la información de la gestión de la seguridad de la información en una institución privada, Callao, 2022?	**a)** Evaluar el efecto de un sistema con tecnología blockchain en la disponibilidad de la información de la gestión de la seguridad de la información en una institución privada, Callao, 2022. **b)** Determinar el efecto de un sistema con tecnología blockchain en la integridad de la información de la gestión de la seguridad de la información en una institución privada, Callao, 2022. **c)** Determinar el efecto de un sistema con tecnología blockchain en la confidencialidad de la información de la gestión de la seguridad de la información en una institución privada, Callao, 2022.	**a)** El sistema con tecnología blockchain tiene un efecto significativo en la disponibilidad de la información de la gestión de la seguridad de la información en una institución privada, Callao, 2022. **b)** El sistema con tecnología blockchain tiene un efecto significativo en la integridad de la información de la gestión de la seguridad de la información en una institución privada, Callao, 2022. **c)** El sistema con tecnología blockchain tiene un efecto significativo en la confidencialidad de la información de la gestión de la seguridad de la información en una institución privada, Callao, 2022.	Gestión de la Seguridad de la Información **Dimensiones:** 1. Disponibilidad 2. Integridad 3. Confidencialidad **Indicadores:** 1. Porcentaje Acumulado de Certificados Disponibles 2. Porcentaje Acumulado de Certificados Íntegros 3. Porcentaje Acumulado de Certificados Entregados Correctamente	

Operacionalización de variables

VARIABLE	DIMENSIONES	INDICADORES	FORMULA	Escala valorativa	Técnica/ Instrumento
Gestión de la Seguridad de la Información	Disponibilidad de la información	Porcentaje Acumulado de Certificados Disponibles	$valor = \frac{Frecuencia\ Acumulada\ de\ Certificados\ encontrados}{Total\ requerido\ de\ Certificados\ Disponibles} \times 100$	Razón	Fichaje / Ficha de registro
	Integridad de la información	Porcentaje Acumulado de Certificados Íntegros	$valor = \frac{Frecuencia\ Acumulada\ de\ Certificados\ con\ informacion\ completa\ y\ correcta}{Total\ requerido\ de\ certificados\ integros} X\ 100$		
	Confidencialidad de la información	Porcentaje Acumulado de Certificados Entregados Correctamente	$valor = \frac{Frecuencia\ Acumulada\ de\ Certificados\ confidenciales\ entregados\ correctamete}{Total\ requerido\ de\ Entregas\ Confidenciales\ de\ Certificados} X\ 100$		

Anexo 02: Instrumento de Recolección de Datos

Ficha de Registro			
Investigador		Tipo de prueba	
Organización investigada			
Indicador utilizado			
Fecha de inicio		Fecha de culminación	
Variable 1			
Variable 2			

Fórmula $Valor = \frac{Variable\ 1 \times 100}{\text{Variable 2}}$

ITEM	FECHA	VARIABLE 1	VARIABLE 2	VALOR %

Anexo 03: Certificado de Validez de Contenido (Juicio de Expertos)

Ficha de validación N° 1

FICHAS DE VALIDACIÓN

INFORME DE OPINIÓN DEL JUICIO DE EXPERTO

DATOS GENERALES

1.1. Título de la Investigación: Sistema con Tecnología Blockchain para la Gestión de la Seguridad de la Información en una Institucion Privada, Callao, 2022

1.2. Nombre de los instrumentos: Ficha de registro

ASPECTOS DE VALIDACIÓN

Indicadores	Criterios	Deficiente				Baja				Regular				Buena				Muy bueno			
		0	6	11	16	21	26	31	36	41	46	51	56	61	66	71	76	81	86	91	96
		5	10	15	20	25	30	35	40	45	50	55	60	65	70	75	80	85	90	95	100
1. Claridad	Está formulado con lenguaje apropiado																	X			
2. Objetividad	Está expresado en conductas observables																X				
3. Actualidad	Adecuado al avance de la ciencia pedagógica																X				
4. Organización	Existe una organización lógica.																	X			
5. Suficiencia	Comprende los aspectos en cantidad y calidad																X				
6. Intencionalidad	Adecuado para valorar los instrumentos de investigación																	X			
7. Consistencia	Basado en aspectos teóricos científicos																	X			
8. Coherencia	Entre los índices, indicadores																X				
9. Metodología	La estrategia responde al propósito del diagnóstico.																	X			
10. Pertinencia	Es útil y adecuado para la investigación																	X			

PROMEDIO DE VALORACIÓN: 83.0

OPINIÓN DE APLICABILIDAD: a) Deficiente b) Baja c) Regular d) Buena e) Muy buena

Nombres y Apellidos:	Wilson Ricardo Marin Verastegui	**DNI N°**	45801046
Dirección domiciliaria:	Independencia, Lima	**Teléfono/Celular:**	951 705 579
Grado Académico:	Magíster		
Mención:	Gestión de Tecnologías de Información		



Firma

Lugar y fecha: Independencia, 28 de junio del 2022

Ficha de validación N° 2

FICHAS DE VALIDACIÓN

INFORME DE OPINIÓN DEL JUICIO DE EXPERTO

DATOS GENERALES

1.1. **Título de la Investigación:** Sistema con Tecnología Blockchain para la Gestión de la Seguridad de la Información en una Institucion Privada, Callao, 2022

1.2. **Nombre de los instrumentos:** Ficha de registro

ASPECTOS DE VALIDACIÓN

Indicadores	Criterios	Deficiente				Baja				Regular				Buena				Muy bueno			
		0	6	11	16	21	26	31	36	41	46	51	56	61	66	71	76	81	86	91	96
		5	10	15	20	25	30	35	40	45	50	55	60	65	70	75	80	85	90	95	100
1. Claridad	Está formulado con lenguaje apropiado																	X			
2. Objetividad	Está expresado en conductas observables																	X			
3. Actualidad	Adecuado al avance de la ciencia pedagógica																	X			
4. Organización	Existe una organización lógica.																	X			
5. Suficiencia	Comprende los aspectos en cantidad y calidad																X				
6. Intencionalidad	Adecuado para valorar los instrumentos de investigación																	X			
7. Consistencia	Basado en aspectos teóricos científicos																X				
8. Coherencia	Entre los índices, indicadores																X				
9. Metodología	La estrategia responde al propósito del diagnóstico.																	X			
10. Pertinencia	Es útil y adecuado para la investigación																	X			

PROMEDIO DE VALORACIÓN: 83.5

OPINIÓN DE APLICABILIDAD: a) Deficiente b) Baja c) Regular d) Buena e) Muy buena

Nombres y Apellidos:	Ivan Robles Fernandez	**DNI N°**	40960211
Dirección domiciliaria:	San Juan de Miraflores, Lima	**Teléfono/Celular:**	997 634 204
Grado Académico:	Magister		
Mención:	En Direccion de Tecnologias de Informacion		

Firma

Lugar y fecha: San Juan de Miraflores, 22 de Junio del 2022

Ficha de validación N° 3

FICHAS DE VALIDACIÓN

INFORME DE OPINIÓN DEL JUICIO DE EXPERTO

DATOS GENERALES

1.1. **Título de la Investigación:** Sistema con Tecnología Blockchain para la Gestión de la Seguridad de la Información en una Institucion Privada, Callao, 2022

1.2. **Nombre de los instrumentos:** Ficha de registro

ASPECTOS DE VALIDACIÓN

Indicadores	Criterios	Deficiente				Baja				Regular				Buena				Muy bueno			
		0	6	11	16	21	26	31	36	41	46	51	56	61	66	71	76	81	86	91	96
		5	10	15	20	25	30	35	40	45	50	55	60	65	70	75	80	85	90	95	100
1. Claridad	Está formulado con lenguaje apropiado																	X			
2. Objetividad	Está expresado en conductas observables																	X			
3. Actualidad	Adecuado al avance de la ciencia pedagógica																X				
4. Organización	Existe una organización lógica.																	X			
5. Suficiencia	Comprende los aspectos en cantidad y calidad																	X			
6. Intencionalidad	Adecuado para valorar los instrumentos de investigación																	X			
7. Consistencia	Basado en aspectos teóricos científicos																X				
8. Coherencia	Entre los índices, indicadores																	X			
9. Metodología	La estrategia responde al propósito del diagnóstico.																X				
10. Pertinencia	Es útil y adecuado para la investigación																	X			

PROMEDIO DE VALORACIÓN: 83.5

OPINIÓN DE APLICABILIDAD: a) Deficiente b) Baja c) Regular d) Buena e) Muy buena

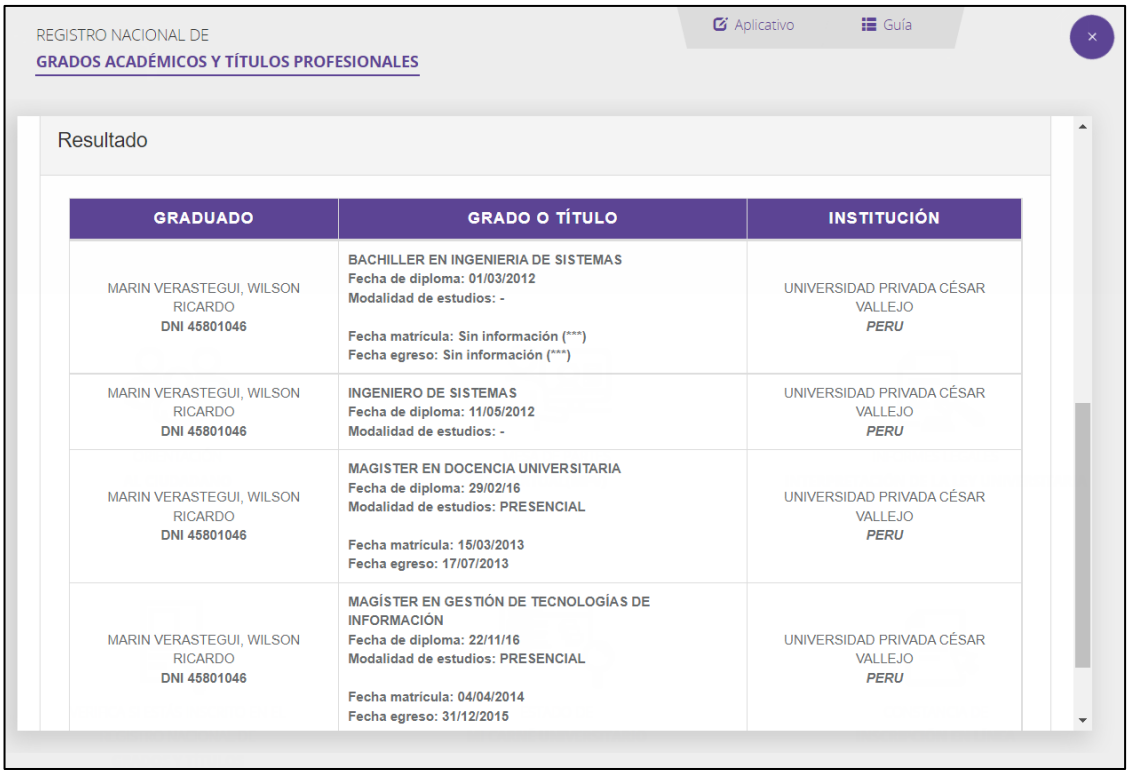
Nombres y Apellidos:	Abraham Rafael Saenz Apari	**DNI N°**	10454966
Dirección domiciliaria:	Los Olivos, Lima	**Teléfono/Celular:**	991 882 305
Grado Académico:	Magister		
Mención:	Administracion Estrategica de Empresas		

Firma

Lugar y fecha: Los Olivos, 24 de Junio del 2022

Anexo 04: Certificado de Validez de Contenido (Juicio de Expertos)

Experto N° 1



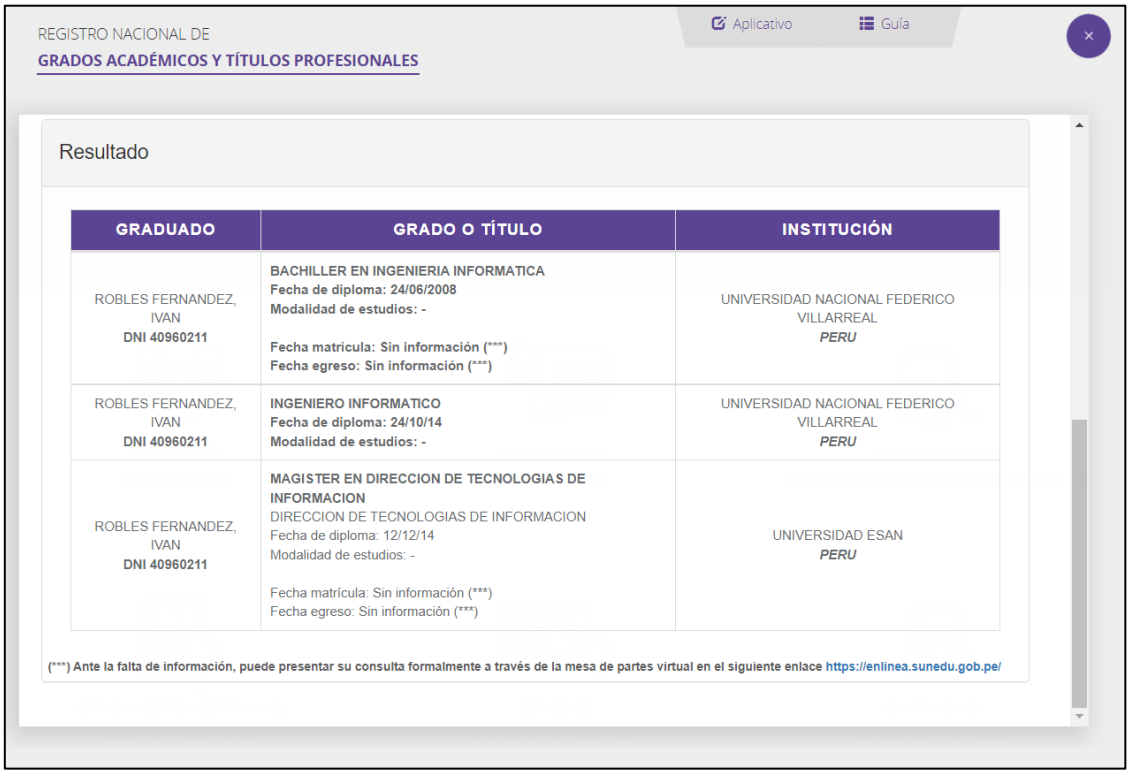
REGISTRO NACIONAL DE
GRADOS ACADÉMICOS Y TÍTULOS PROFESIONALES

Aplicativo Guía

Resultado

GRADUADO	GRADO O TÍTULO	INSTITUCIÓN
MARIN VERASTEGUI, WILSON RICARDO **DNI 45801046**	**BACHILLER EN INGENIERIA DE SISTEMAS** **Fecha de diploma: 01/03/2012** **Modalidad de estudios: -** **Fecha matrícula: Sin información (***)** **Fecha egreso: Sin información (***)**	UNIVERSIDAD PRIVADA CÉSAR VALLEJO ***PERU***
MARIN VERASTEGUI, WILSON RICARDO **DNI 45801046**	**INGENIERO DE SISTEMAS** **Fecha de diploma: 11/05/2012** **Modalidad de estudios: -**	UNIVERSIDAD PRIVADA CÉSAR VALLEJO ***PERU***
MARIN VERASTEGUI, WILSON RICARDO **DNI 45801046**	**MAGISTER EN DOCENCIA UNIVERSITARIA** **Fecha de diploma: 29/02/16** **Modalidad de estudios: PRESENCIAL** **Fecha matrícula: 15/03/2013** **Fecha egreso: 17/07/2013**	UNIVERSIDAD PRIVADA CÉSAR VALLEJO ***PERU***
MARIN VERASTEGUI, WILSON RICARDO **DNI 45801046**	**MAGÍSTER EN GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN** **Fecha de diploma: 22/11/16** **Modalidad de estudios: PRESENCIAL** **Fecha matrícula: 04/04/2014** **Fecha egreso: 31/12/2015**	UNIVERSIDAD PRIVADA CÉSAR VALLEJO ***PERU***

Experto N° 2



REGISTRO NACIONAL DE
GRADOS ACADÉMICOS Y TÍTULOS PROFESIONALES

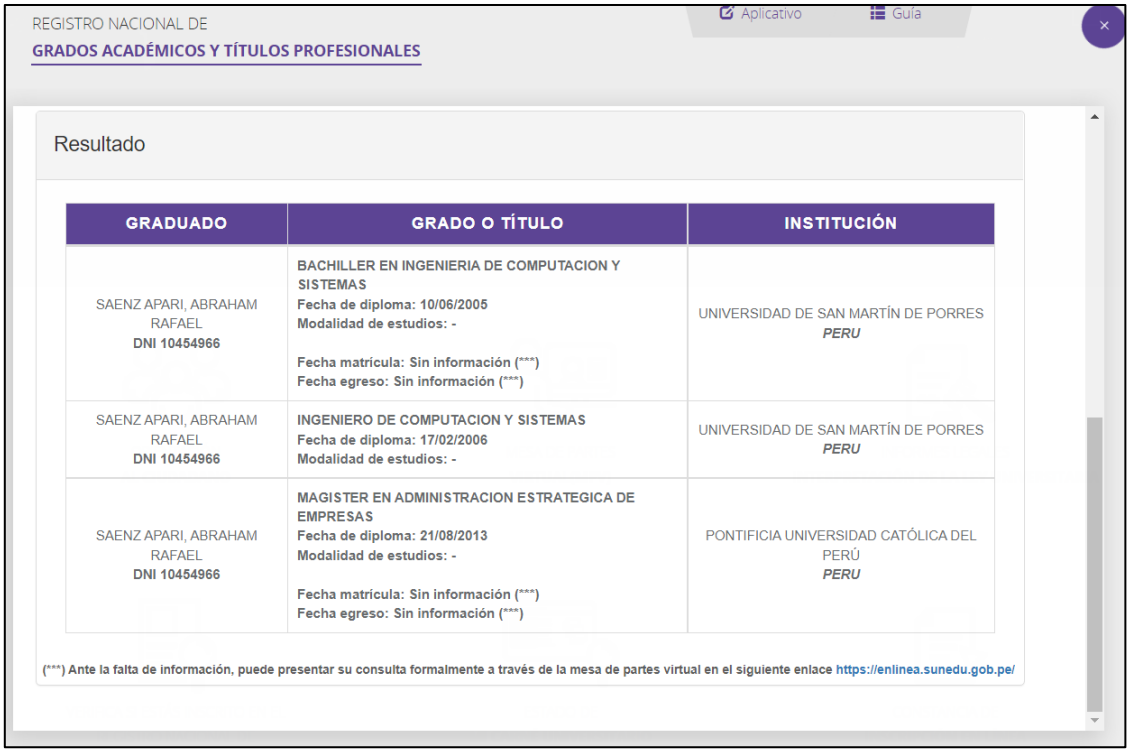
Aplicativo Guía

Resultado

GRADUADO	GRADO O TÍTULO	INSTITUCIÓN
ROBLES FERNANDEZ, IVAN **DNI 40960211**	**BACHILLER EN INGENIERIA INFORMATICA** **Fecha de diploma: 24/06/2008** **Modalidad de estudios: -** **Fecha matrícula: Sin información (***)** **Fecha egreso: Sin información (***)**	UNIVERSIDAD NACIONAL FEDERICO VILLARREAL ***PERU***
ROBLES FERNANDEZ, IVAN **DNI 40960211**	**INGENIERO INFORMATICO** **Fecha de diploma: 24/10/14** **Modalidad de estudios: -**	UNIVERSIDAD NACIONAL FEDERICO VILLARREAL ***PERU***
ROBLES FERNANDEZ, IVAN **DNI 40960211**	**MAGISTER EN DIRECCION DE TECNOLOGIAS DE INFORMACION** DIRECCION DE TECNOLOGIAS DE INFORMACION Fecha de diploma: 12/12/14 Modalidad de estudios: - Fecha matrícula: Sin información (***) Fecha egreso: Sin información (***)	UNIVERSIDAD ESAN ***PERU***

(***) Ante la falta de información, puede presentar su consulta formalmente a través de la mesa de partes virtual en el siguiente enlace https://enlinea.sunedu.gob.pe/

Experto N° 3



REGISTRO NACIONAL DE
GRADOS ACADÉMICOS Y TÍTULOS PROFESIONALES

Aplicativo Guía

Resultado

GRADUADO	GRADO O TÍTULO	INSTITUCIÓN
SAENZ APARI, ABRAHAM RAFAEL **DNI 10454966**	**BACHILLER EN INGENIERIA DE COMPUTACION Y SISTEMAS** **Fecha de diploma: 10/06/2005** **Modalidad de estudios: -** **Fecha matrícula: Sin información (***)** **Fecha egreso: Sin información (***)**	UNIVERSIDAD DE SAN MARTÍN DE PORRES ***PERU***
SAENZ APARI, ABRAHAM RAFAEL **DNI 10454966**	**INGENIERO DE COMPUTACION Y SISTEMAS** **Fecha de diploma: 17/02/2006** **Modalidad de estudios: -**	UNIVERSIDAD DE SAN MARTÍN DE PORRES ***PERU***
SAENZ APARI, ABRAHAM RAFAEL **DNI 10454966**	**MAGISTER EN ADMINISTRACION ESTRATEGICA DE EMPRESAS** **Fecha de diploma: 21/08/2013** **Modalidad de estudios: -** **Fecha matrícula: Sin información (***)** **Fecha egreso: Sin información (***)**	PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ ***PERU***

(***) Ante la falta de información, puede presentar su consulta formalmente a través de la mesa de partes virtual en el siguiente enlace https://enlinea.sunedu.gob.pe/

Anexo 05: Base de Datos de los Indicadores (Instrumento de Recolección de Datos)

PRE - TEST

Ficha de Registro			
Investigador	Mariano Anthony Cardenas Quispe	**Tipo de Prueba**	Pre Test
Organización Investigada	Institucion Privada		
Indicador Utilizado	Porcentaje Acumulado de Certificados Disponibles		
Fecha de Inicio	26/12/2023	**Fecha de culminacion**	7/01/2024
Variable 1	Frecuencia Acumulada de Certificados Encontrados		
Variable 2	Total Requerido de Certificados Disponibles		
Fórmula $Valor = \frac{Variable\ 1 \times 100}{\text{Variable 2}}$			

Item	Fecha	Variable 1	Variable 2	Valor
V.1 N.1 - Articulo 1	7/01/2024	1	24	4.17
V.1 N.1 - Articulo 2	7/01/2024	2	24	8.33
V.1 N.1 - Articulo 3	7/01/2024	3	24	12.50
V.1 N.1 - Articulo 4	7/01/2024	4	24	16.67
V.1 N.1 - Articulo 5	7/01/2024	5	24	20.83
V.1 N.1 - Articulo 6	7/01/2024	6	24	25.00
V.1 N.1 - Articulo 7	7/01/2024	6	24	25.00
V.1 N.1 - Articulo 8	7/01/2024	7	24	29.17
V.1 N.1 - Articulo 9	7/01/2024	8	24	33.33
V.1 N.1 - Articulo 10	7/01/2024	9	24	37.50
V.1 N.1 - Articulo 11	7/01/2024	10	24	41.67
V.1 N.2 - Articulo 1	7/01/2024	10	24	41.67
V.1 N.2 - Articulo 2	7/01/2024	10	24	41.67
V.1 N.2 - Articulo 3	7/01/2024	10	24	41.67
V.1 N.2 - Articulo 4	7/01/2024	10	24	41.67
V.1 N.2 - Articulo 5	7/01/2024	10	24	41.67
V.1 N.2 - Articulo 6	7/01/2024	10	24	41.67
V.1 N.2 - Articulo 7	7/01/2024	10	24	41.67
V.2 N.3 - Articulo 1	7/01/2024	11	24	45.83
V.2 N.3 - Articulo 2	7/01/2024	12	24	50.00
V.2 N.3 - Articulo 3	7/01/2024	13	24	54.17
V.2 N.3 - Articulo 4	7/01/2024	14	24	58.33
V.2 N.3 - Articulo 5	7/01/2024	15	24	62.50
V.2 N.3 - Articulo 6	7/01/2024	16	24	66.67

Ficha de Registro			
Investigador	Mariano Anthony Cardenas Quispe	**Tipo de Prueba**	Pre Test
Organización Investigada	Institucion Privada		
Indicador Utilizado	Porcentaje Acumulado de Certificados Íntegros		
Fecha de Inicio	26/12/2023	**Fecha de culminacion**	7/01/2024
Variable 1	Frecuencia Acumulada de Certificados con informacion completa y correcta		
Variable 2	Total Requerido de Certificados Integros		
Fórmula $Valor = \frac{Variable\ 1 \times 100}{\text{Variable 2}}$			

Item	Fecha	Variable 1	Variable 2	Valor
V.1 N.1 - Articulo 1	7/01/2024	1	24	4.17
V.1 N.1 - Articulo 2	7/01/2024	2	24	8.33
V.1 N.1 - Articulo 3	7/01/2024	3	24	12.50
V.1 N.1 - Articulo 4	7/01/2024	4	24	16.67
V.1 N.1 - Articulo 5	7/01/2024	5	24	20.83
V.1 N.1 - Articulo 6	7/01/2024	5	24	20.83
V.1 N.1 - Articulo 7	7/01/2024	5	24	20.83
V.1 N.1 - Articulo 8	7/01/2024	5	24	20.83
V.1 N.1 - Articulo 9	7/01/2024	5	24	20.83
V.1 N.1 - Articulo 10	7/01/2024	5	24	20.83
V.1 N.1 - Articulo 11	7/01/2024	6	24	25.00
V.1 N.2 - Articulo 1	7/01/2024	6	24	25.00
V.1 N.2 - Articulo 2	7/01/2024	6	24	25.00
V.1 N.2 - Articulo 3	7/01/2024	6	24	25.00
V.1 N.2 - Articulo 4	7/01/2024	6	24	25.00
V.1 N.2 - Articulo 5	7/01/2024	6	24	25.00
V.1 N.2 - Articulo 6	7/01/2024	6	24	25.00
V.1 N.2 - Articulo 7	7/01/2024	6	24	25.00
V.2 N.3 - Articulo 1	7/01/2024	7	24	29.17
V.2 N.3 - Articulo 2	7/01/2024	8	24	33.33
V.2 N.3 - Articulo 3	7/01/2024	9	24	37.50
V.2 N.3 - Articulo 4	7/01/2024	10	24	41.67
V.2 N.3 - Articulo 5	7/01/2024	11	24	45.83
V.2 N.3 - Articulo 6	7/01/2024	12	24	50.00

Ficha de Registro			
Investigador	Mariano Anthony Cardenas Quispe	**Tipo de Prueba**	Pre Test
Organización Investigada	Institucion Privada		
Indicador Utilizado	Porcentaje de certificados entregados correctamente		
Fecha de Inicio	26/12/2023	**Fecha de culminacion**	7/01/2024
Variable 1	Frecuencia Acumulada de Certificados confidenciales entregados correctamente		
Variable 2	Total Requerido de Entregas Confidenciales de Certificados		
Fórmula $Valor = \frac{Variable\ 1 \times 100}{\text{Variable 2}}$			

Item	Fecha	Variable 1	Variable 2	Valor
V.1 N.1 - Articulo 1	7/01/2024	0	88	0.00
V.1 N.1 - Articulo 2	7/01/2024	0	88	0.00
V.1 N.1 - Articulo 3	7/01/2024	0	88	0.00
V.1 N.1 - Articulo 4	7/01/2024	0	88	0.00
V.1 N.1 - Articulo 5	7/01/2024	0	88	0.00
V.1 N.1 - Articulo 6	7/01/2024	0	88	0.00
V.1 N.1 - Articulo 7	7/01/2024	0	88	0.00
V.1 N.1 - Articulo 8	7/01/2024	0	88	0.00
V.1 N.1 - Articulo 9	7/01/2024	0	88	0.00
V.1 N.1 - Articulo 10	7/01/2024	0	88	0.00
V.1 N.1 - Articulo 11	7/01/2024	0	88	0.00
V.1 N.2 - Articulo 1	7/01/2024	0	88	0.00
V.1 N.2 - Articulo 2	7/01/2024	0	88	0.00
V.1 N.2 - Articulo 3	7/01/2024	0	88	0.00
V.1 N.2 - Articulo 4	7/01/2024	0	88	0.00
V.1 N.2 - Articulo 5	7/01/2024	0	88	0.00
V.1 N.2 - Articulo 6	7/01/2024	0	88	0.00
V.1 N.2 - Articulo 7	7/01/2024	0	88	0.00
V.2 N.3 - Articulo 1	7/01/2024	4	88	4.55
V.2 N.3 - Articulo 2	7/01/2024	8	88	9.09
V.2 N.3 - Articulo 3	7/01/2024	13	88	14.77
V.2 N.3 - Articulo 4	7/01/2024	17	88	19.32
V.2 N.3 - Articulo 5	7/01/2024	22	88	25.00
V.2 N.3 - Articulo 6	7/01/2024	23	88	26.14

POST – TEST

Ficha de Registro			
Investigador	Mariano Anthony Cardenas Quispe	**Tipo de Prueba**	Post-test
Organización Investigada	Institucion Privada		
Indicador Utilizado	Porcentaje Acumulado de Certificados Disponibles		
Fecha de Inicio	28/01/2024	**Fecha de culminacion**	29/01/2024
Variable 1	Frecuencia Acumulada de Certificados Encontrados		
Variable 2	Total Requerido de Certificados Disponibles		

Fórmula $Valor = \frac{Variable\ 1 \times 100}{\text{Variable 2}}$

Item	Fecha	Variable 1	Variable 2	Valor
V.1 N.1 - Articulo 1	29/01/2024	1	24	4.17
V.1 N.1 - Articulo 2	29/01/2024	2	24	8.33
V.1 N.1 - Articulo 3	29/01/2024	3	24	12.50
V.1 N.1 - Articulo 4	29/01/2024	4	24	16.67
V.1 N.1 - Articulo 5	29/01/2024	5	24	20.83
V.1 N.1 - Articulo 6	29/01/2024	6	24	25.00
V.1 N.1 - Articulo 7	29/01/2024	7	24	29.17
V.1 N.1 - Articulo 8	29/01/2024	8	24	33.33
V.1 N.1 - Articulo 9	29/01/2024	9	24	37.50
V.1 N.1 - Articulo 10	29/01/2024	10	24	41.67
V.1 N.1 - Articulo 11	29/01/2024	11	24	45.83
V.1 N.2 - Articulo 1	29/01/2024	12	24	50.00
V.1 N.2 - Articulo 2	29/01/2024	13	24	54.17
V.1 N.2 - Articulo 3	29/01/2024	14	24	58.33
V.1 N.2 - Articulo 4	29/01/2024	15	24	62.50
V.1 N.2 - Articulo 5	29/01/2024	16	24	66.67
V.1 N.2 - Articulo 6	29/01/2024	17	24	70.83
V.1 N.2 - Articulo 7	29/01/2024	18	24	75.00
V.2 N.3 - Articulo 1	29/01/2024	19	24	79.17
V.2 N.3 - Articulo 2	29/01/2024	20	24	83.33
V.2 N.3 - Articulo 3	29/01/2024	21	24	87.50
V.2 N.3 - Articulo 4	29/01/2024	22	24	91.67
V.2 N.3 - Articulo 5	29/01/2024	23	24	95.83
V.2 N.3 - Articulo 6	29/01/2024	24	24	100.00

Ficha de Registro			
Investigador	Mariano Anthony Cardenas Quispe	**Tipo de Prueba**	Post-test
Organización Investigada	Institucion Privada		
Indicador Utilizado	Porcentaje Acumulado de Certificados Íntegros		
Fecha de Inicio	28/01/2024	**Fecha de culminacion**	29/01/2024
Variable 1	Frecuencia Acumulada de Certificados con informacion completa y correcta		
Variable 2	Total Requerido de Certificados Integros		

Fórmula $Valor = \frac{Variable\ 1 \times 100}{\text{Variable 2}}$

Item	Fecha	Variable 1	Variable 2	Valor
V.1 N.1 - Articulo 1	29/01/2024	1	24	4.17
V.1 N.1 - Articulo 2	29/01/2024	2	24	8.33
V.1 N.1 - Articulo 3	29/01/2024	3	24	12.50
V.1 N.1 - Articulo 4	29/01/2024	4	24	16.67
V.1 N.1 - Articulo 5	29/01/2024	5	24	20.83
V.1 N.1 - Articulo 6	29/01/2024	6	24	25.00
V.1 N.1 - Articulo 7	29/01/2024	7	24	29.17
V.1 N.1 - Articulo 8	29/01/2024	8	24	33.33
V.1 N.1 - Articulo 9	29/01/2024	9	24	37.50
V.1 N.1 - Articulo 10	29/01/2024	10	24	41.67
V.1 N.1 - Articulo 11	29/01/2024	11	24	45.83
V.1 N.2 - Articulo 1	29/01/2024	12	24	50.00
V.1 N.2 - Articulo 2	29/01/2024	13	24	54.17
V.1 N.2 - Articulo 3	29/01/2024	14	24	58.33
V.1 N.2 - Articulo 4	29/01/2024	15	24	62.50
V.1 N.2 - Articulo 5	29/01/2024	16	24	66.67
V.1 N.2 - Articulo 6	29/01/2024	17	24	70.83
V.1 N.2 - Articulo 7	29/01/2024	18	24	75.00
V.2 N.3 - Articulo 1	29/01/2024	19	24	79.17
V.2 N.3 - Articulo 2	29/01/2024	20	24	83.33
V.2 N.3 - Articulo 3	29/01/2024	21	24	87.50
V.2 N.3 - Articulo 4	29/01/2024	22	24	91.67
V.2 N.3 - Articulo 5	29/01/2024	23	24	95.83
V.2 N.3 - Articulo 6	29/01/2024	24	24	100.00

Ficha de Registro			
Investigador	Mariano Anthony Cardenas Quispe	**Tipo de Prueba**	Post-test
Organización Investigada	Institucion Privada		
Indicador Utilizado	Porcentaje de certificados entregados		
Fecha de Inicio	28/01/2024	**Fecha de culminacion**	29/01/2024
Variable 1	Frecuencia Acumulada de Certificados confidenciales entregados correctamente		
Variable 2	Total Requerido de Entregas Confidenciales de Certificados		

Fórmula $Valor = \frac{Variable\ 1 \times 100}{\text{Variable 2}}$

Item	Fecha	Variable 1	Variable 2	Valor
V.1 N.1 - Articulo 1	29/01/2024	4	88	4.55
V.1 N.1 - Articulo 2	29/01/2024	8	88	9.09
V.1 N.1 - Articulo 3	29/01/2024	12	88	13.64
V.1 N.1 - Articulo 4	29/01/2024	15	88	17.05
V.1 N.1 - Articulo 5	29/01/2024	17	88	19.32
V.1 N.1 - Articulo 6	29/01/2024	21	88	23.86
V.1 N.1 - Articulo 7	29/01/2024	25	88	28.41
V.1 N.1 - Articulo 8	29/01/2024	29	88	32.95
V.1 N.1 - Articulo 9	29/01/2024	33	88	37.50
V.1 N.1 - Articulo 10	29/01/2024	35	88	39.77
V.1 N.1 - Articulo 11	29/01/2024	36	88	40.91
V.1 N.2 - Articulo 1	29/01/2024	38	88	43.18
V.1 N.2 - Articulo 2	29/01/2024	42	88	47.73
V.1 N.2 - Articulo 3	29/01/2024	45	88	51.14
V.1 N.2 - Articulo 4	29/01/2024	49	88	55.68
V.1 N.2 - Articulo 5	29/01/2024	54	88	61.36
V.1 N.2 - Articulo 6	29/01/2024	57	88	64.77
V.1 N.2 - Articulo 7	29/01/2024	58	88	65.91
V.2 N.3 - Articulo 1	29/01/2024	62	88	70.45
V.2 N.3 - Articulo 2	29/01/2024	66	88	75.00
V.2 N.3 - Articulo 3	29/01/2024	71	88	80.68
V.2 N.3 - Articulo 4	29/01/2024	75	88	85.23
V.2 N.3 - Articulo 5	29/01/2024	80	88	90.91
V.2 N.3 - Articulo 6	29/01/2024	81	88	92.05

Anexo 06: Autorización de la Institución para Realizar la Investigación

Por razones de confidencialidad y a solicitud de la empresa participante, su nombre se mantiene en el anonimato a lo largo de este estudio

Anexo 07: Desarrollo de la Solución Tecnológica

Desarrollo mediante la metodología ágil SCRUM del sistema con tecnología blockchain.

1. Roles en el Proyecto

Product Owner	Jefe del área de TI de la Institución Privada
Scrum Master	Mariano Anthony Cardenas Quispe
Equipo de Desarrollo	Mariano Anthony Cardenas Quispe

2. Historias de Usuario

En esta sección se describen las funcionalidades del sistema desde la perspectiva del usuario, donde se incluye información sobre la prioridad, el riesgo y los criterios de validación.

ID	**HU01**	
Nombre: Verificar la Autenticidad del Certificado		**Rol:** Usuario
Prioridad: Alto	**Riesgo:** Bajo	
Descripción: El usuario podrá verificar la autenticidad de un certificado utilizando el hash único del certificado.		
Validación: 1. El sistema debe permitir ingresar el hash del certificado. 2. El sistema debe mostrar si el certificado es válido o no. 3. El sistema debe mostrar la información del certificado si es válido (datos del certificado). 4. El sistema debe ser accesible públicamente sin necesidad de iniciar sesión.		

ID	**HU02**	
Nombre: Registrar Nuevos Certificados		**Rol:** Participante
Prioridad: Alto	**Riesgo:** Medio	
Descripción: El participante con el rol registro podrá registrar nuevos certificados en el sistema con la información del certificado de publicación de articulo.		

Validación: 1. El sistema debe permitir el ingreso de la información del certificado de publicación. 2. El sistema debe generar un hash único para cada certificado. 3. El sistema debe almacenar el certificado en la blockchain. 4. Solo participantes autenticados con rol de registro pueden registrar certificados.

ID	**HU03**
Nombre: Firmar los Certificados	**Rol:** Participante
Prioridad: Medio	**Riesgo:** Alto
Descripción: El participante con rol firmar podrá firmar certificados para asegurar su integridad y validez.	
Validación: 1. El sistema debe permitir firmar un certificado por cada participante autorizado. 2. Cada certificado debe poder ser firmado por múltiples participantes autorizados. 3. El sistema debe registrar quién firmó cada certificado y en qué fecha. 4. El sistema debe permitir verificar la validez de las firmas digitales. 5. Solo usuarios autenticados con roles de firma específicos pueden firmar los certificados.	

ID	**HU04**
Nombre: Notificación por Correo Electrónico	**Rol:** Usuario
Prioridad: Bajo	**Riesgo:** Bajo
Descripción: El usuario recibirá una notificación por correo electrónico cuando su certificado esté registrado o disponible para descargar, con un enlace para acceder al mismo.	
Validación: 1. El sistema debe enviar un correo electrónico al usuario cuando se registra su certificado. 2. El correo electrónico debe contener el hash del certificado y el identificador único. 3. El correo electrónico debe notificar cuando el certificado este firmado por todos los participantes con rol de firma. 4. El usuario debe poder acceder al certificado con el hash único.	

ID	**HU05**
Nombre: Interfaz Web Intuitiva	**Rol:** Usuario - Participante
Prioridad: Medio	**Riesgo:** Medio
Descripción: El participante/usuario podrá acceder a una interfaz web intuitiva y fácil de usar para interactuar con el sistema, buscar certificados e información relacionada.	
Validación: **1.** La interfaz debe ser fácil de navegar y comprender. **2.** La interfaz debe tener un diseño atractivo y profesional.	

3. Requerimientos Funcionales

En esta sección se describen las funciones específicas que el sistema debe realizar.

- **RF01:** El sistema debe permitir a los usuarios verificar la autenticidad de los certificados utilizando el hash único.
- **RF02:** El sistema debe permitir a los participantes con el rol de "registrador" registrar nuevos certificados con la información del certificado de publicación del artículo.
- **RF03:** El sistema debe permitir a los participantes autorizados firmar certificados digitalmente.
- **RF04:** El sistema debe enviar notificaciones por correo electrónico al usuario cuando su certificado esté registrado o disponible para descargar, con un enlace para acceder al mismo.
- **RF05:** El sistema debe proporcionar una interfaz web intuitiva para la interacción, búsqueda de certificados e información relacionada.
- **RF06:** El sistema debe implementar una función de roles para restringir el acceso a ciertas funcionalidades, como el registro de nuevos certificados.

4. Requerimientos No Funcionales

En esta sección se describen las características de calidad del sistema, como la seguridad, la escalabilidad y la eficiencia.

- **RNF01:** El sistema debe ser seguro y proteger la información contra accesos no autorizados.
- **RNF02:** El sistema debe ser escalable para manejar un número creciente de certificados.
- **RNF03:** El sistema debe ser eficiente y responder rápidamente a las solicitudes.
- **RNF04:** La interfaz web debe ser usable e intuitiva.
- **RNF05:** El sistema debe ser compatible con los navegadores web modernos.

5. Product Backlog

En esta sección, se compone de las Historias de Usuario y su relación con los Requerimientos Funcionales.

Historias de Usuario	Nombre	Prioridad	RF Relacionados
HU01	Verificar la Autenticidad del Certificado	Alta	RF01, RF05
HU02	Registrar Nuevos Certificados	Alta	RF02, RF05, RF06
HU03	Firmar los Certificados	Media	RF03, RF06
HU04	Notificación por Correo Electrónico	Baja	RF04
HU05	Interfaz Web Intuitiva	Media	RF05

6. Plan de SPRINTS

El Plan de Sprints define la duración, los objetivos, las Historias de Usuario a abordar y las tareas a realizar en cada Sprint.

Sprint	Duración	Objetivo	HU	Tareas
00	03 semanas	Desarrollar la base del sistema con tecnología blockchain.	-	• Diseñar e implementar la estructura de la blockchain para el almacenamiento de certificados, incluyendo la lógica para la generación de hashes únicos y la estructura de datos para la información de los certificados. • Desarrollar e implementar contratos inteligentes para la gestión de certificados, incluyendo scripts para su funcionamiento y un script de consenso bizantino. • Configurar la red blockchain interna de Docker, incluyendo nodos y mecanismos de consenso. • Configurar el entorno de desarrollo utilizando Python y Docker. • Implementar el modulo que define roles a los participantes
01	01 semana	Implementar el registro, verificación de certificados y la interfaz web.	HU01, HU02, HU05	• Desarrollar la interfaz para registrar nuevos certificados e implementar la lógica para la verificación de certificados. • Integrar el sistema con la blockchain e implementar la lógica para la autorización de usuarios con el rol de "registrador". Desarrollar la interfaz

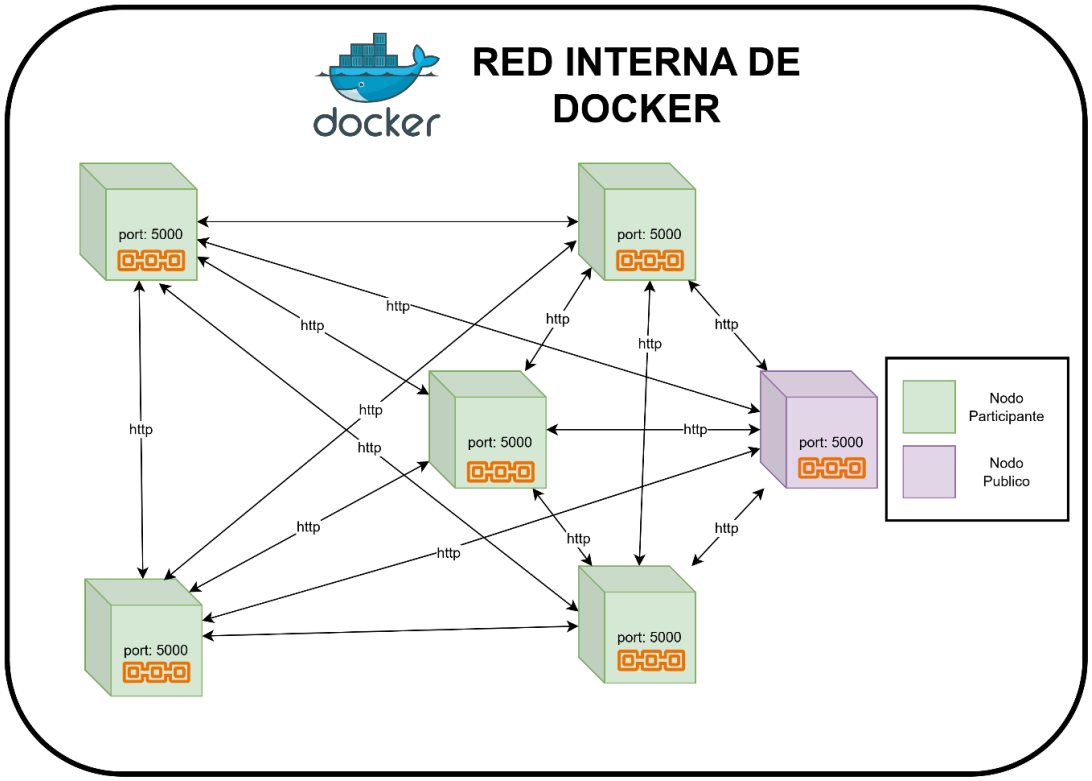
				web con las funcionalidades de registro.
02	01 semana	Implementar la firma de certificados y la interfaz web.	HU03, HU05	• Implementar la funcionalidad para firmar certificados. • Desarrollar la interfaz web con las funcionalidades de firma.
03	01 semana	Implementar las notificaciones por correo electrónico.	HU04	• Configurar el sistema de notificaciones. • Desarrollar la lógica para enviar notificaciones. • Personalizar las notificaciones con la información del certificado.

7. Desarrollo de Sprint

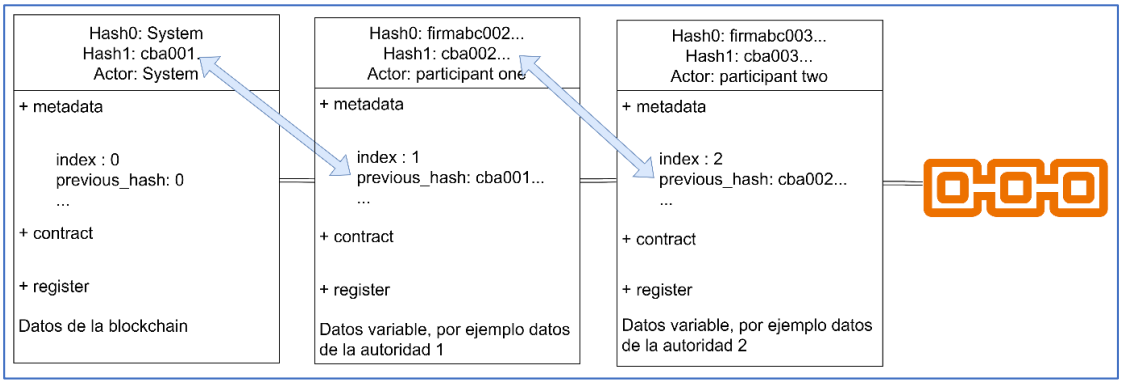
7.1. Sprint 0

En este sprint se desarrolla la base del sistema con tecnología blockchain, incluyendo la estructura de la blockchain, los contratos inteligentes, la red interna de Docker y el entorno de desarrollo.

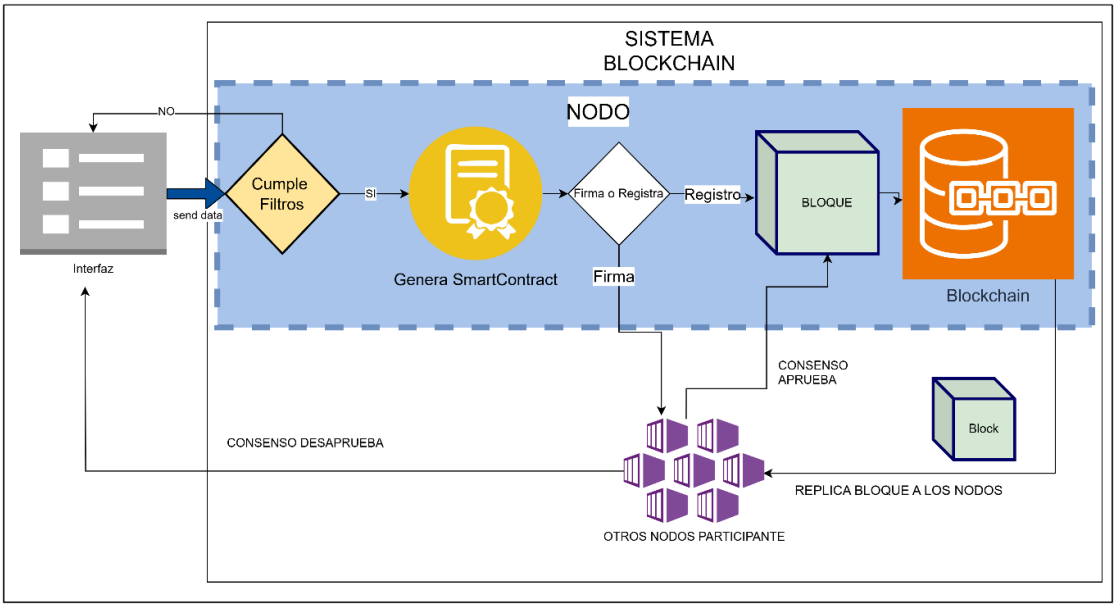
7.1.1. Arquitectura del sistema blockchain hibrido: En la siguiente imagen se muestra la arquitectura del sistema blockchain hibrido, que podrá estar compuesto hasta por 5 nodos privados, y un nodo público para las consultas y verificación. se usa contenedores Docker y su red privada para ejecutar la red blockchain entre nodos, como se puede observar en el grafico a continuación:



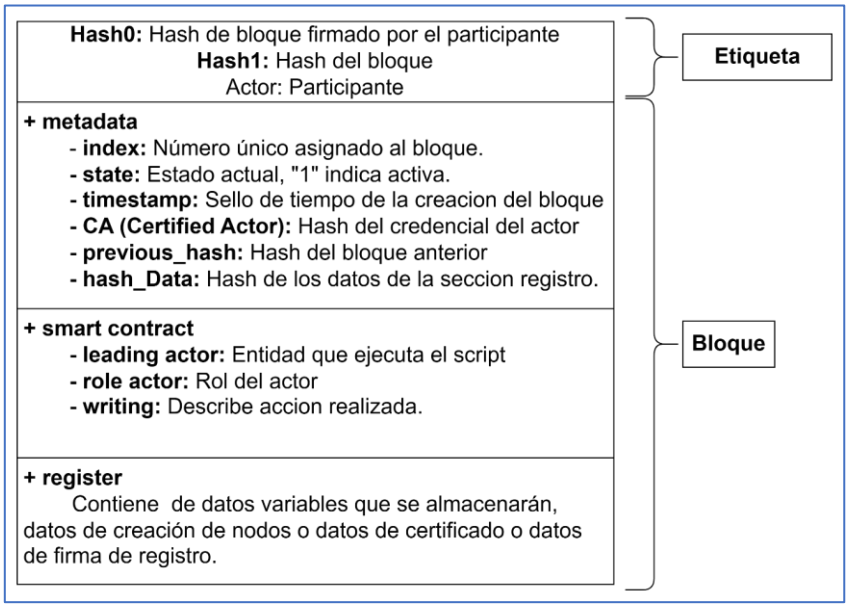
7.1.2. ***Almacenamiento en cadena de bloques:*** Cada registro se almacenará en un bloque, y cada bloque estará vinculado al bloque anterior, formando una cadena inmutable e integra.



7.1.3. ***Diseño del sistema blockchain:*** El sistema está compuesto por una red blockchain privada con hasta 5 nodos participantes y un nodo público que permite la verificación. Este nodo público ofrece una interfaz de usuario con funciones de registro y firma. Cada operación, ya sea de registro o firma, pasa por filtros y un script de Smart Contract antes de crear un bloque. Para firmar el contenido del bloque, se emplea un consenso bizantino. Finalmente, el bloque se replica en todos los nodos participantes para asegurar la descentralización del sistema.



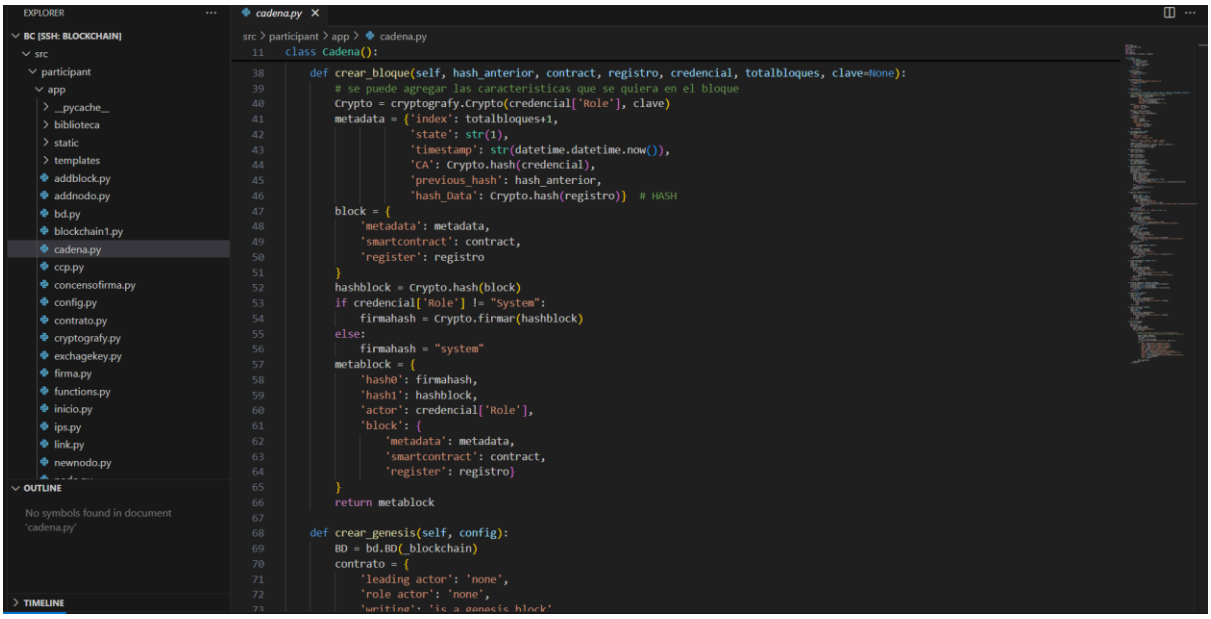
7.1.4. ***Estructura de datos del bloque en el sistema blockchain***: Los bloques que componen la cadena de bloque, tendrán una estructura personalizada, como se muestra en la siguiente imagen.



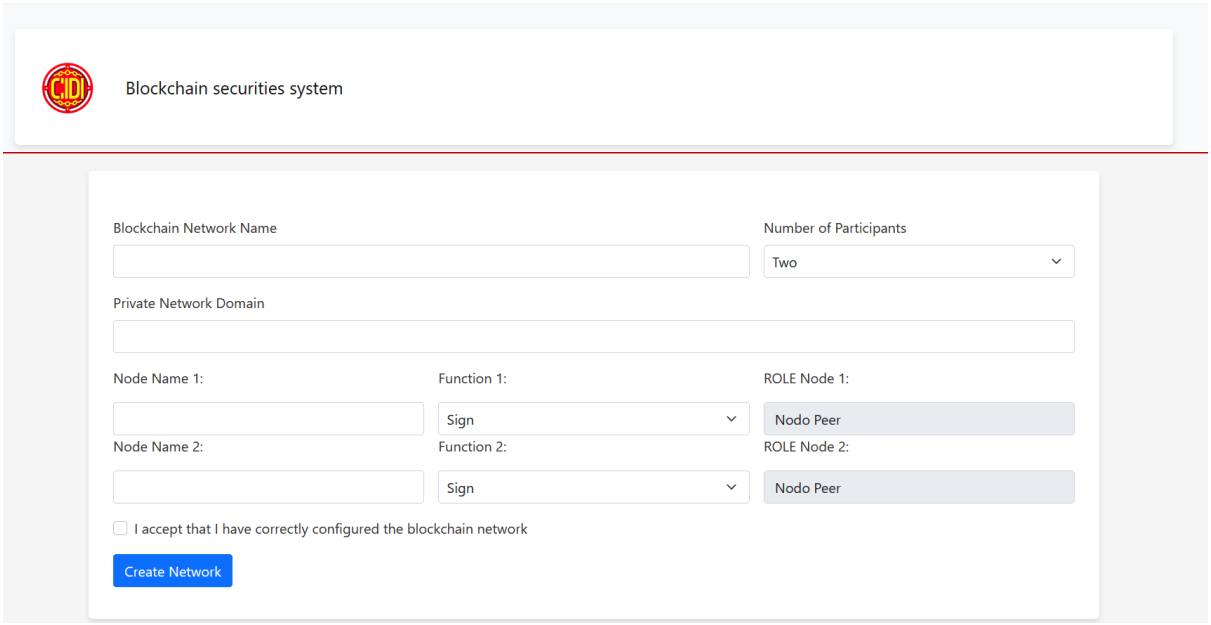
7.1.5. ***Red interna Docker realizada:*** Se presenta el despliegue del entorno blockchain compuesto por contenedores Docker, que muestran los nodos participantes de la red blockchain, como se puede observar la red interna de Docker, en la imagen a continuación:


```
"ConfigFrom": {
    "Network": ""
},
"ConfigOnly": false,
"Containers": {
    "062dc94d3637fddc088e249bf152e0f1a73766ffbac2f959bf1fcf98a7ec0278": {
        "Name": "node-test2",
        "EndpointID": "04cf6399e3df369fa3b22c8ca14c4e524d27d1ef67582057471ab0b20b0ac8da",
        "MacAddress": "02:42:ac:11:00:03",
        "IPv4Address": "172.17.0.3/16",
        "IPv6Address": ""
    },
    "1abf14b4026620fd7210e9fa5c96fb5c78f048232c91c139d8f682e041876616": {
        "Name": "node-test5",
        "EndpointID": "bb6ed7780dcfcc0bf0c54ec39163a22b19f0d8b863fd5b83fd2dfe2cc336d016",
        "MacAddress": "02:42:ac:11:00:06",
        "IPv4Address": "172.17.0.6/16",
        "IPv6Address": ""
    },
    "c7d436f9624f63a4f1c2d59a91a6c5be004d5fde1d2df7af982c324c78e8d8b1": {
        "Name": "node-test3",
        "EndpointID": "c4e512f6ac66cff9caf65263beabdb01401f9ba352e25e1dff8cf83079e0bac2",
        "MacAddress": "02:42:ac:11:00:04",
        "IPv4Address": "172.17.0.4/16",
        "IPv6Address": ""
    },
    "d434fea3d7abecd8cb05fb8a91b35cd3bfb3ea39d752ea6efde3da5ed8b0eee4": {
        "Name": "node-test1",
        "EndpointID": "6cbfa4ccbc9866a456f0b9d5e84f87f626c09f56eb09d6588e35338bae82681b",
        "MacAddress": "02:42:ac:11:00:02",
        "IPv4Address": "172.17.0.2/16",
        "IPv6Address": ""
    },
    "e1c03d62587154b4134fdd30eade7f9733005e1906225b6562a05be0a3fc6816": {
        "Name": "node-test4",
        "EndpointID": "6ff68e974a4484e13f55b6f0396520f65feb45a556cd8dc4872ff0c7ad928e25",
        "MacAddress": "02:42:ac:11:00:05",
        "IPv4Address": "172.17.0.5/16",
        "IPv6Address": ""
    }
},
```

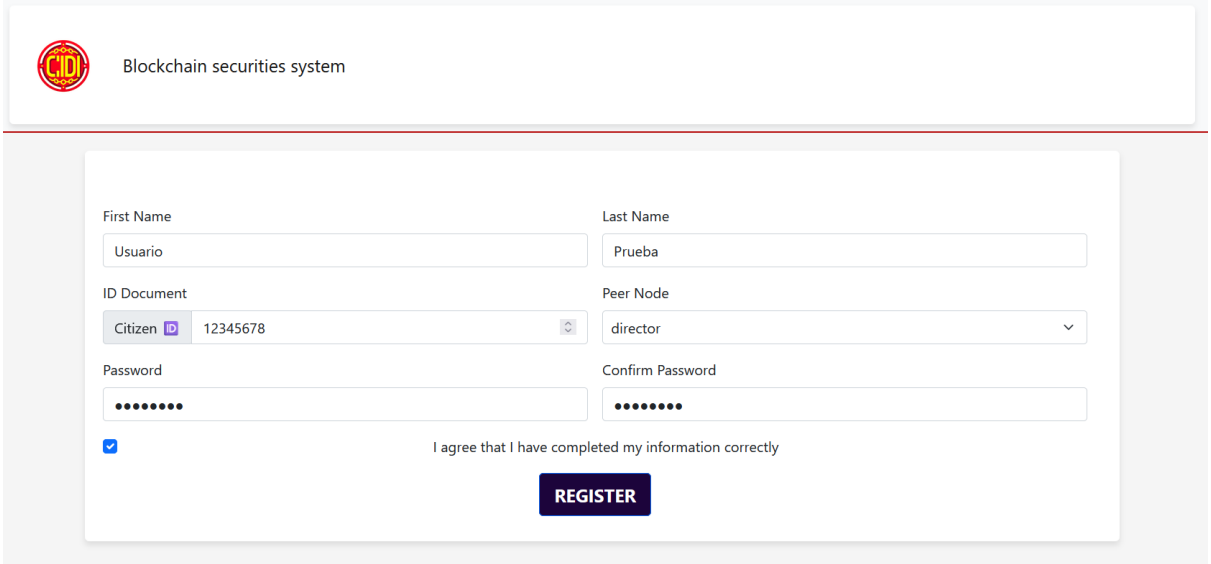
7.1.6. Extracto del código del sistema blockchain: En la imagen a continuación, se presenta el código fuente del sistema blockchain y sus archivos.



7.1.7. Interfaz de configuración de inicio del sistema blockchain: En la imagen a continuación se muestra la interfaz inicial al instanciar el sistema blockchain.



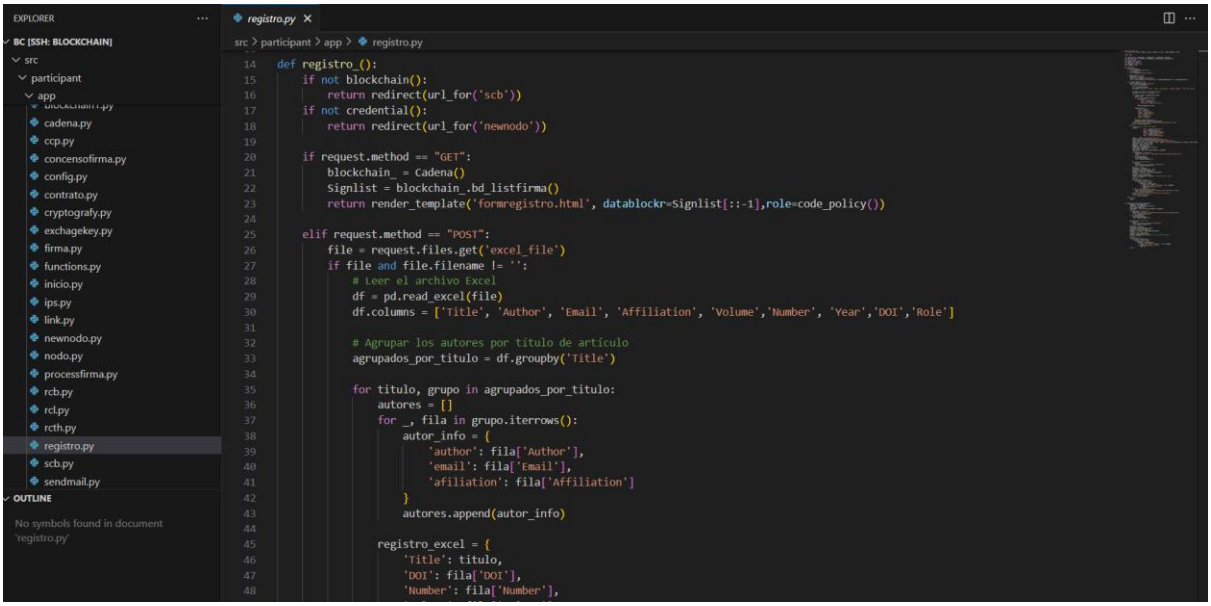
7.1.8. Interfaz de registro del nodo: En la imagen a continuación se muestra la interfaz del registro del usuario en el nodo a participar en la blockchain.



7.2. Sprint 01

En este sprint, se implementan las funcionalidades de registro y verificación de certificados, así como la interfaz web.

7.2.1. ***Código fuente de la función registro en el sistema:*** A continuación, se muestra la imagen que contiene el código fuente correspondiente a la función de registro en el sistema.



```
def registro_():
    if not blockchain():
        return redirect(url_for('scb'))
    if not credential():
        return redirect(url_for('newnodo'))

    if request.method == "GET":
        blockchain_ = Cadena()
        Signlist = blockchain_.bd_listfirma()
        return render_template('formregistro.html', datablockr=Signlist[::-1],role=code_policy())

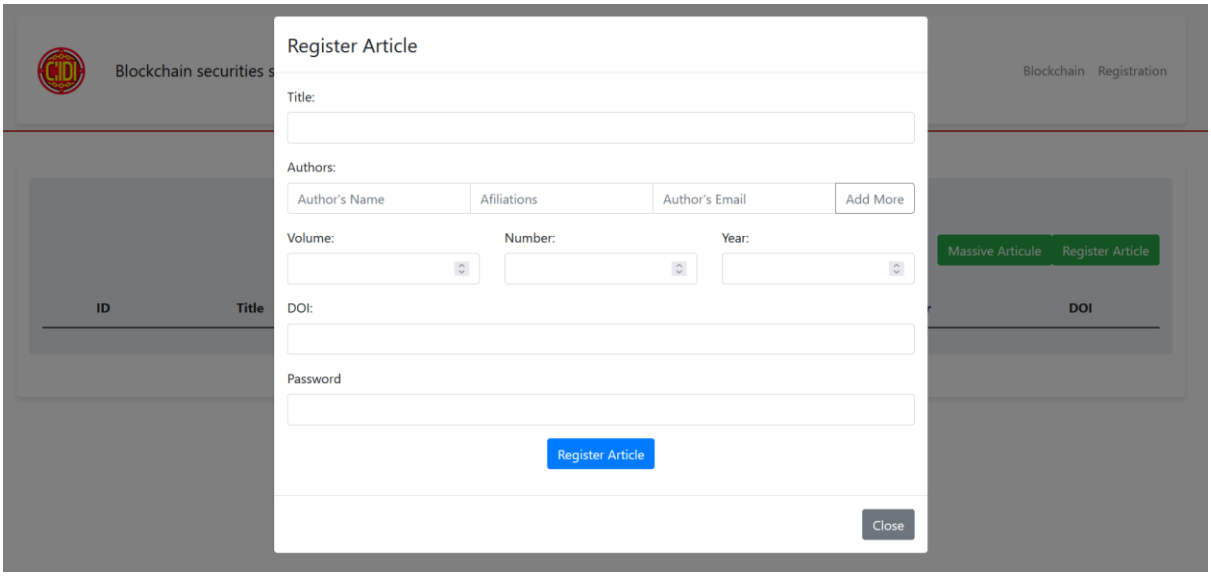
    elif request.method == "POST":
        file = request.files.get('excel_file')
        if file and file.filename != '':
            # Leer el archivo Excel
            df = pd.read_excel(file)
            df.columns = ['Title', 'Author', 'Email', 'Affiliation', 'Volume','Number', 'Year','DOI','Role']

            # Agrupar los autores por título de artículo
            agrupados_por_titulo = df.groupby('Title')

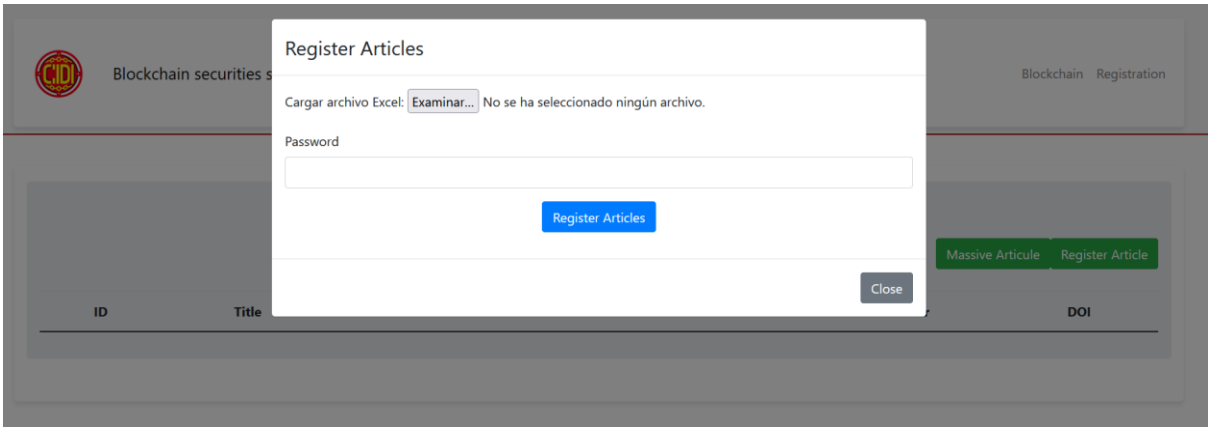
            for titulo, grupo in agrupados_por_titulo:
                autores = []
                for _, fila in grupo.iterrows():
                    autor_info = {
                        'author': fila['Author'],
                        'email': fila['Email'],
                        'afiliation': fila['Affiliation']
                    }
                    autores.append(autor_info)

                registro_excel = {
                    'Title': titulo,
                    'DOI': fila['DOI'],
                    'Number': fila['Number'],
```

7.2.2. **Interfaz de la función registro en el sistema blockchain**: A continuación se muestra las imágenes correspondientes al método registro

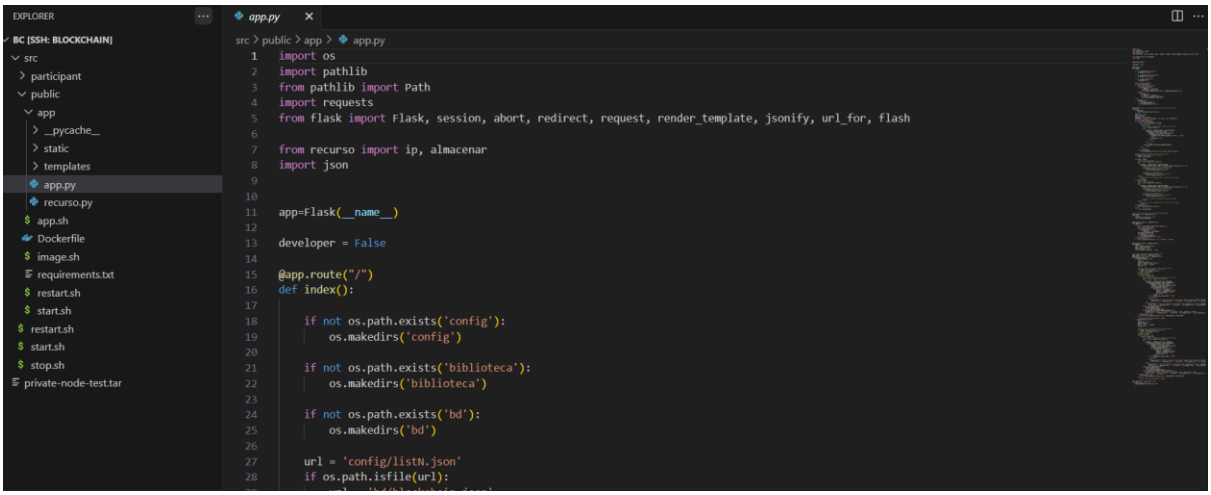


Nota: Interfaz de registro diseñada para permitir el registro de un certificado de publicación.



Nota: Interfaz de registro diseñada para permitir el registro masivo de certificados de publicación.

7.2.3. Código fuente de la función del nodo público en el sistema: A continuación, se muestra la imagen que contiene el código fuente correspondiente a la función de nodo público, para la verificación de certificados en el sistema.



7.2.4. **Interfaz del nodo público en el sistema blockchain**: A continuación, se presentan la imagen correspondiente al nodo público, que incluye la funcionalidad de verificación de los certificados de publicación



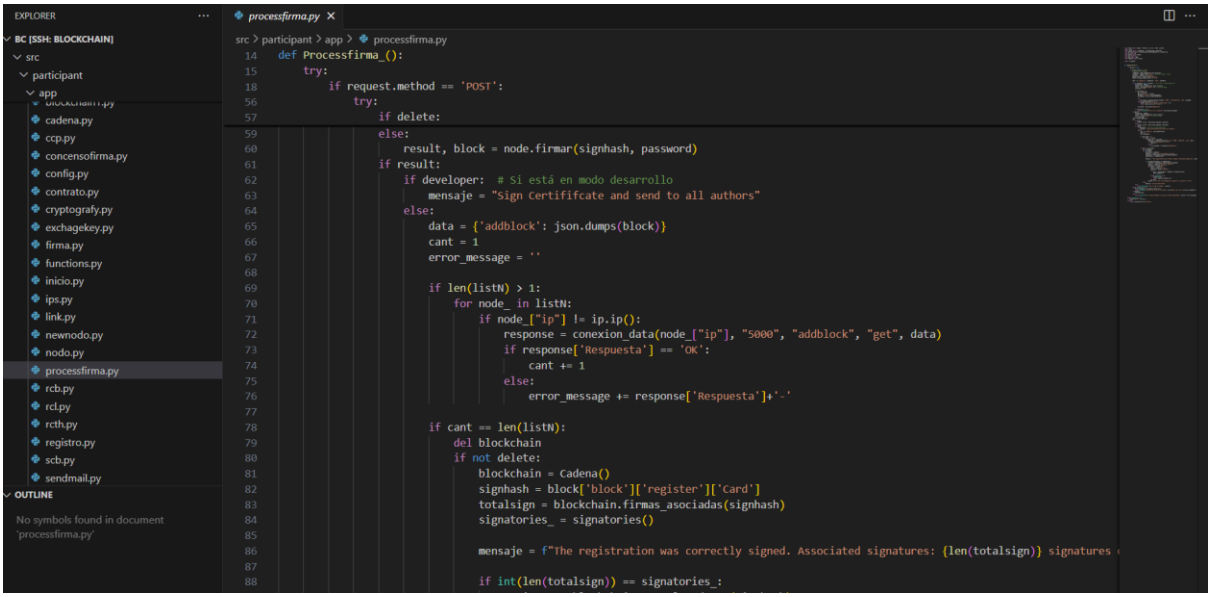
7.3. Sprint 02

En este sprint se implementa la funcionalidad de firma de certificados y su interfaz web.

7.3.1. ***Código fuente de la función firma en el sistema***: A continuación se muestra las imágenes correspondientes al método firmar.

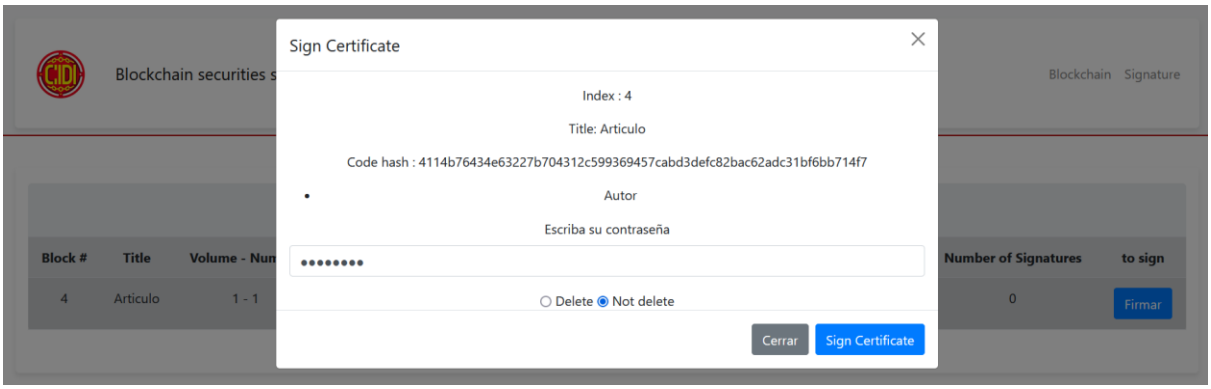


Nota: Código fuente para cargar la interfaz del método firmar.



Nota: Código fuente para procesar la firma en el sistema.

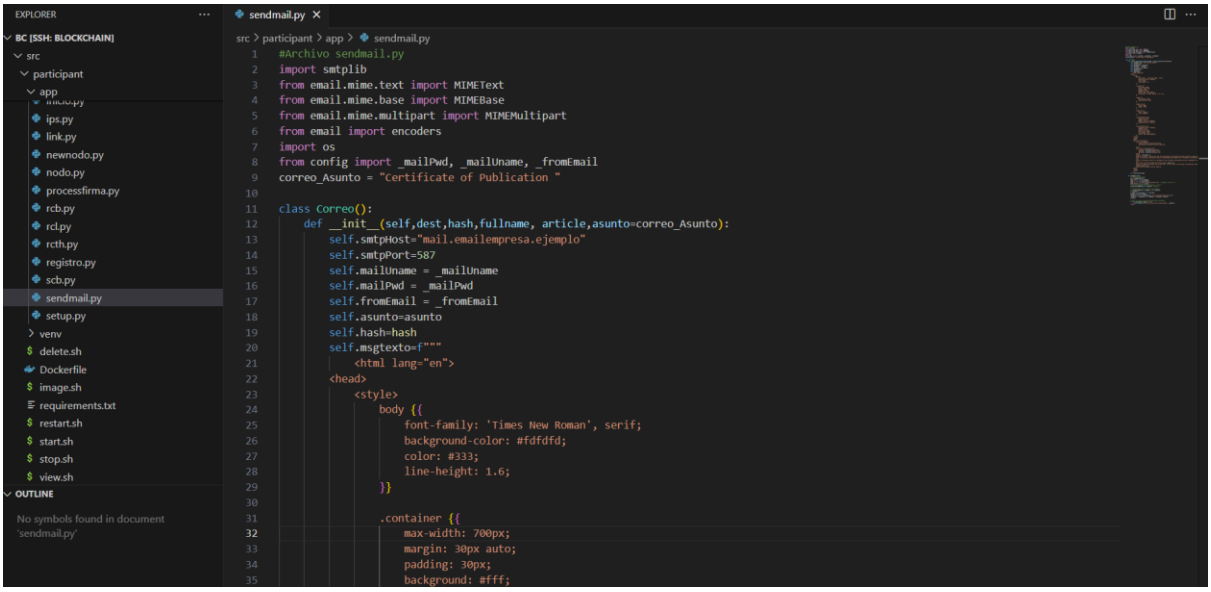
7.3.2. **Interfaz de la función firmar en el sistema blockchain**: A continuación se muestra la imagen correspondiente al método firmar.



7.4. Sprint 03

En este sprint se implementa el sistema de notificaciones por correo electrónico para informar a los usuarios sobre el estado de sus certificados.

7.4.1. ***Código fuente de la función notificación de correo electrónico en el sistema:*** A continuación, se muestra la imagen que contiene el código fuente correspondiente a la función de notificación de correo electrónico del sistema.



7.4.2. **Correo electrónico de notificación:** A continuación, en la imagen se muestra a modo de ejemplo la plantilla del correo electrónico configurado que ha sido enviado vía correo electrónico.



Anexo 08: Constancia de Similitud

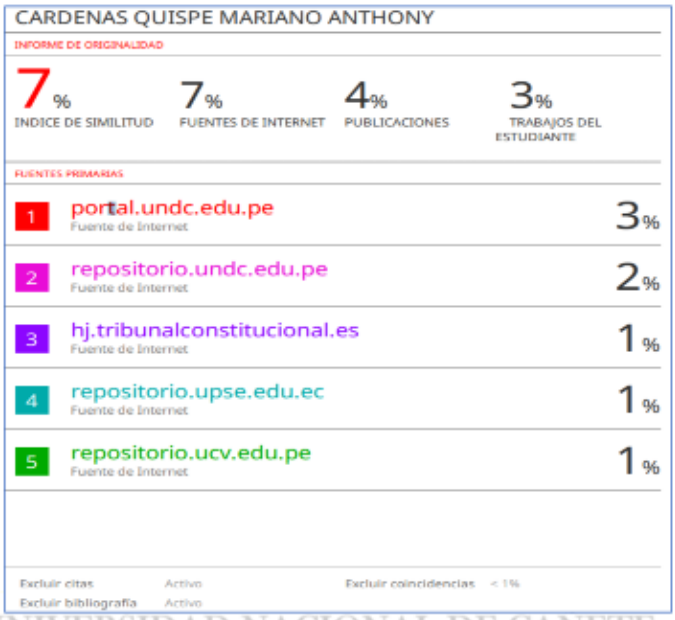
UNIVERSIDAD NACIONAL DE CAÑETE
Ley de Creación N° 29488
FACULTAD DE INGENIERÍA
UNIDAD DE INVESTIGACION DE LA FACULTAD DE INGENIERIA
"Año del Bicentenario, de la Consolidación de nuestra Independencia
Y de la conmemoración de las heroicas batallas de Junín y Ayacucho"

San Vicente de Cañete, 26 de agosto del 2024

CONSTANCIA DE SIMILITUD DE INFORME FINAL DE TESIS N° 020-2024

Título del Trabajo de Investigación: "Sistema con Tecnología Blockchain para la Gestión de la Seguridad de la Información en una Institución Privada, Callao, 2022"

Autor(es): Mariano Anthony Cárdenas Quispe



CARDENAS QUISPE MARIANO ANTHONY

INFORME DE ORIGINALIDAD

7%	7%	4%	3%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	portal.undc.edu.pe Fuente de Internet	3%
2	repositorio.undc.edu.pe Fuente de Internet	2%
3	hj.tribunalconstitucional.es Fuente de Internet	1%
4	repositorio.upse.edu.ec Fuente de Internet	1%
5	repositorio.ucv.edu.pe Fuente de Internet	1%

Excluir citas Activo
Excluir bibliografía Activo
Excluir coincidencias < 1%

UNIVERSIDAD NACIONAL DE CAÑETE

Por lo tanto, se otorga esta constancia a solicitud del interesado(a) para los fines que estime conveniente.

FIRMA DIGITAL
Firmado digitalmente por: DURAN CARHUAMACA AMANDA FIR 20114878 hard
Motivo: Soy el autor del documento
Fecha: 26/08/2024 18:48:18-0500

Mg. Amanda Durán Carhuamaca
(e) Directora de la Unidad de Investigación
Facultad de Ingeniería – UNDC

Anexo 09: Autorización de Publicación en el Repositorio Institucional de la UNDC

UNIVERSIDAD NACIONAL DE CAÑETE

AUTORIZACIÓN DE PUBLICACIÓN EN EL REPOSITORIO INSTITUCIONAL DE LA UNDC

I INFORMACIÓN DEL DOCUMENTO

1.1 Título del documento:

Sistema con Tecnología Blockchain para la Gestión de la Seguridad de la Información en una Institución Privada, Callao, 2022

1.2 Descripción (Seleccionar)

Tesis de Pregrado	X	Libro	
Tesis de Maestría		Capítulo de libro	
Tesis de Doctorado		Monografía	
Trabajo de Investigación		Artículo	
Tesis de Segunda Especialidad		Conferencia	
Trabajo de Suficiencia Profesional		Programa informativo	
Trabajo académico		Datos	

1.3 Autores del documento

Apellidos completos	Nombres completos	Correo electrónico	DNI	ORCID
Cardenas Quispe	Mariano Anthony	1773830690@undc.edu.pe	73830690	https://orcid.org/0000-0003-3033-7846

1.4 Asesor (es)

Apellidos completos	Nombres completos	Correo electrónico	DNI	ORCID
Alex Abelardo	Pacheco Pumaleque	apacheco@undc.edu.pe	41651279	https://orcid.org/0000-0001-9721-0730
Dulio	Oseda Gago	doseda@undc.edu.pe	20044737	https://orcid.org/0000-0002-3136-6094

1.5 Centro de Investigación

Facultad	Facultad de ingeniería
Escuela Profesional	Escuela profesional de Ingeniería de Sistemas

I. ORIGINALIDAD DEL TRABAJO PRESENTADO

Con la presentación de esta ficha, el(los) autor(es) señalan expresamente que la obra es original, ya que sus contenidos son producto de su directa contribución intelectual. Se reconoce también que todos los datos y las referencias a materiales ya publicados están debidamente identificados con su respectivo crédito e incluidos en las notas bibliográficas y en las citas que se destacan como tal,

Toda copia de este documento, sea del entorno virtual o del documento original en físico es considerada "copia no controlada".

III. AUTORIZACIÓN DEL TRABAJO PRESENTADO

3.1 Por medio del presente documento, afirmo y garantizo(amos) ser el (los) legítimo (s), titular(es) de todos los derechos de propiedad intelectual sobre los entregables, las obras, los contenidos, los productos y/o las creaciones en general (en adelante, los "Contenidos" que serán incluidos en el Repositorio Institucional de la Universidad Nacional de Cañete (en adelante, la "Universidad").

3.2 Autorizo a la Universidad a publicar los Contenidos en el Repositorio Institucional de la Universidad y, en consecuencia, en el Repositorio Nacional Digital de Ciencia, Tecnología e Innovación de Acceso Abierto, sobre la base de lo establecido en la Ley N° 30035, sus normas reglamentarias, modificatorias, sustitutorias y conexas, y de acuerdo con las políticas de acceso abierto que la Universidad aplique en relación con su Repositorio Institucional. Autorizo expresamente toda consulta y uso de los Contenidos, por parte de cualquier persona, por el tiempo de duración de los derechos patrimoniales de autor y derechos conexos, a título gratuito y a nivel mundial.

3.3 En consecuencia, la Universidad tendrá la posibilidad de divulgar y difundir los Contenidos, de manera total o parcial, sin limitación alguna y sin derecho a pago de contraprestación, remuneración ni regalía alguna a favor mío; en los medios, canales y plataformas que la Universidad y/o el Estado de la República del Perú determinen, a nivel mundial, sin restricción geográfica alguna y de manera indefinida, pudiendo crear y/o extraer los metadatos sobre los Contenidos, e incluir los Contenidos en los índices y buscadores que estimen necesarios para promover su difusión.

Firma	26/05/2025 Fecha

IV: PUBLICACIÓN DIFERIDA

Este ítem solo es de interés para los autores que han decidido la publicación diferida de sus documentos. Caso contrario, obviar este apartado.

Autorización	Motivo (marcar)		Firma
Solicito la publicación diferida del documento depositado en el repositorio, por 12 meses. (indicar el tiempo que solicita)	Exclusividad de revista, editor		
	Por patente		
	Secreto o seguridad nacional		
	Por otras razones		

Cualquier motivo utilizado, el solicitante debe acreditar con documento su pedido (subir junto con la autorización la evidencia que sustenta su solicitud).

Toda copia de este documento, sea del entorno virtual o del documento original en físico es considerada "copia no controlada".

Anexo 10: Articulo Científico

Sistema con Tecnología Blockchain para la Gestión de la Seguridad de la Información en una Institución Privada, Callao, 2022

Cardenas-Quispe, Mariano Anthony
1773830690@undc.edu.pe
Ingeniería de sistemas, Facultad de ingeniería, Universidad Nacional de Cañete

***Abstract*— This thesis determined the impact of a blockchain-based system on information security management in a private institution in Callao in 2022. The research addressed the lack of protection in the certificates issued. An applied quantitative methodology was used, with an explanatory approach, hypothetico-deductive method and pre-experimental design. The sample consisted of 24 certificates. The data were processed using Microsoft Excel 365 64-bit and IBM SPSS Statistics v.21. The results showed significant improvements: the PACD indicator improved certificate availability from 66.67% in the pre-test to 100% in the post-test; the PACI indicator improved certificate integrity from 50% to 100%; and the PACEC indicator improved confidentiality from 26.14% to 92.05%. In conclusion, the blockchain system had a positive impact on the information security management of the studied institution.**

Keywords — Blockchain, Availability, Integrity, Confidentiality, Certificates

I. Introducción

En el contexto contemporáneo, la seguridad de la información implica la protección integral de los datos y los sistemas informáticos frente a diversas amenazas, tales como el acceso no autorizado o la divulgación no deseada de información confidencial, las cuales pueden desencadenar su alteración o destrucción [1]. Sin embargo, los sistemas de información enfrentan constantes amenazas de ciberataques y fraudes, lo que, sumado a la demora en la verificación de datos, conlleva a un funcionamiento empresarial lento y resultados deficientes; en este sentido, la tecnología blockchain surge como una solución, al proporcionar una confianza sólida respaldada por una alta seguridad y una mayor eficiencia operativa [2].

A escala internacional, la incertidumbre es un desafío, ya que los entornos son cada vez más ambiguos y volátiles, y en una sociedad con demanda digital, las organizaciones usan tecnología expuesta a este entorno, resaltando la necesidad de optimizar la confianza [3]. En Colombia, la digitalización de los servicios públicos conlleva el riesgo de vulnerar la información, afectando su integridad y confidencialidad, lo que impulsa al gobierno a implementar medidas para mitigar estos riesgos [4].

En el contexto nacional, se destaca que en el año 2019, Pomas y Vargas señalaron que el Perú es considerado el país más vulnerable frente a ataques cibernéticos, según su investigación [5]. En adición, en el año 2023, se evidencia un aumento de 150% en fraudes en línea y robo de información mediante aplicaciones [6].

En la provincia constitucional del Callao, se identifica la falta de adherencia a políticas de seguridad de la información en algunas instituciones, subrayando la urgencia de promover la adopción generalizada de estas políticas para proteger los datos [7], [8].

En una institución privada ubicada en la Provincia Constitucional del Callao, se edita una revista científica que emite certificados de publicación para los artículos científicos que publica, así como certificados de revisión por pares ciegos. Sin embargo, se ha observado que esta institución no ha implementado políticas de protección de la información asociada a estos certificados. Esta carencia de medidas de seguridad aumenta el riesgo de que la información no esté disponible cuando sea requerida, pueda perder su integridad o ser expuesta sin autorización.

A. Formulación del problema

Problema general

¿Cuál es el efecto de un sistema con tecnología blockchain en la gestión de la seguridad de la información en una Institución Privada, Callao, 2022?

B. Problemas específicos

¿Cuál es el efecto de un sistema con tecnología blockchain en la disponibilidad de la información de certificados de la gestión de la seguridad de la información en una institución Privada, Callao, 2022?

¿Cuál es el efecto de un sistema con tecnología blockchain en la integridad de la información de certificados de la gestión de la seguridad de la información en una institución Privada, Callao, 2022?

¿Cuál es el efecto de un sistema con tecnología blockchain en la confidencialidad de la información de certificados de la gestión de la seguridad de la información en una institución Privada, Callao, 2022?

C. Objetivos Objetivo general

Determinar el efecto de un Sistema con tecnología blockchain en la gestión de la seguridad de la información en una institución Privada, Callao, 2022.

D. Objetivos específicos

Evaluar el efecto de un sistema con tecnología blockchain en la disponibilidad de la información de certificados de la gestión de la seguridad de la información en una institución Privada, Callao, 2022.
Determinar el efecto de un sistema con tecnología blockchain en la integridad de la información de certificados de la gestión de la seguridad de la información en una institución Privada, Callao, 2022.
Determinar el efecto de un sistema con tecnología blockchain en la confidencialidad de la información de certificados de la gestión de la seguridad de la información en una institución Privada, Callao, 2022.

E. Marco Conceptual

Blockchain: La tecnología blockchain es un sistema que mantiene un registro de transacciones distribuidas entre múltiples computadoras interconectadas en una red peer-to-peer, lo que posibilita la creación de un entorno descentralizado donde los datos no están bajo el control de ninguna organización externa [9]. Blockchain, también conocida como libro mayor distribuido, es una tecnología diseñada para revolucionar la gestión de datos, procesos comerciales y transacciones [10]. Introducida por primera vez en 2008 por Nakamoto, blockchain fue concebida como el primer libro mayor descentralizado que permite a cualquiera escribir en la base de datos sin estar sujeto a un único organismo controlador; sin embargo, aunque hay diversas cadenas de bloques activas, alcanzar la interoperabilidad entre ellas sigue siendo un desafío, a menos que se recurra a un tercero confiable [11]. Aunque enfrenta desafíos en cuanto a la interoperabilidad, el blockchain ha captado una gran atención tanto en el ámbito académico como en el industrial debido a sus características únicas, tales como la confiabilidad, la seguridad, la descentralización y la integridad de los datos [12].

II. Teorías relacionadas

Blockchain Publica: Las Blockchains públicas son fundamentales en la tecnología debido a su naturaleza abierta y descentralizada, que permite a cualquier persona acceder a las transacciones sin restricciones ni necesidad de permisos, facilitando así una contabilidad distribuida y la verificación de registros actuales y pasados [13]. Por otro lado, estas Blockchains están diseñadas para ser transparentes y participativas, utilizando algoritmos como la prueba de trabajo (PoW) para permitir la participación de cualquier individuo en la cadena de bloques, garantizando así la visibilidad completa de todas las transacciones para todos los participantes y evitando el control por parte de usuarios o entidades específicas [14].

Blockchain Privada: En las blockchains privadas, los participantes deben solicitar permiso para unirse a la red, y todas las transacciones están disponibles mediante el acceso proporcionado únicamente por los participantes autorizados [14]. Estas blockchains operan con características de acceso limitado, facilitando transacciones solo con el permiso del administrador del sistema y desarrollando plataformas que destacan por su alta privacidad, eficiencia, rapidez en las transacciones, mejor escalabilidad y mayor velocidad [13].

Blockchain Hibrida: Las cadenas de bloques híbridas son una combinación de cadenas de bloques públicas y privadas, se requieren para un mejor control y la consecución de objetivos más elevados [13]. Es decir, estas blockchains exhiben flexibilidad al ofrecer la opción de seleccionar qué datos se compartirán con el público y cuáles se mantendrán en privado [14].

III. Metodología

A. Enfoque de la investigación

El enfoque cuantitativo, basado en la inducción probabilística del positivismo lógico, se distingue por su medición rigurosa, objetiva y controlada, lo que permite al indagador hacer inferencias que trascienden los datos obtenidos mediante un proceso confirmatorio inferencial deductivo, orientado a obtener resultados utilizando datos sólidos y repetibles [15]. Por tal motivo, en esta tesis se aplica el enfoque cuantitativo para llegar a conclusiones claras y verificables.

B. Tipo de investigación

La investigación de tipo aplicada combina el uso práctico del conocimiento con una investigación meticulosa, buscando así generar nuevos conocimientos [16]. Esta tesis es de tipo aplicada, ya que desarrolla una solución para salvaguardar los datos de una organización.

C. Nivel de investigación

Este trabajo de investigación se ubica en un nivel explicativo. Este nivel se dedica a descubrir las relaciones de causa y efecto; por lo tanto, más allá de simplemente presentar o examinar un problema, su objetivo es identificar las razones subyacentes que lo originan [16].

D. Método de investigación

El método hipotético-deductivo se distingue por su objetivo de ampliar el conocimiento mediante la obtención de resultados universales y la formulación de leyes científicas que explican las causas de los fenómenos, lo cual facilita tanto la predicción como el control de dichos fenómenos [16]. En este estudio se aplicará el método de investigación hipotético-deductivo.

E. Diseño de investigación

Esta investigación adopta un diseño pre-experimental, tal como lo indica [17] , donde la Variable Independiente (VI) se establece en un único nivel correspondiente al grupo de experimentación. Además, es necesario que la variable dependiente se evalúe con una herramienta específica en dos momentos distintos: antes de la intervención (pre-test) y después de esta (post-test).

F. Población, muestra y muestreo

Población

Según Hernández y Mendoza en el año 2018, sostienen que la población en una investigación puede incluir no solo personas, sino cualquier elemento cuantificable, permitiendo así derivar una muestra que facilite un análisis completo de la población y evaluar cómo esta es influenciada por la variable en estudio [18]. La población objeto de este estudio está constituida por un total de 24 certificados de publicación. Estos certificados están directamente relacionados con los artículos que han sido publicados en tres ediciones diferentes de una revista científica perteneciente a una institución privada, específicamente los contenidos en el Volumen 1 (Números 1 y 2) y el Volumen 2 (Número 3).

Muestra

Según Cifuentes et al. (2022) y Asencio et al. (2017) coinciden en que cuando el número de sujetos en una población es menor a cincuenta, esta población puede considerarse una representación completa de la muestra, debido a que las características de la población se equiparan directamente con las de la muestra [19]. Debido a que la cantidad de la población de estudio es menor de cincuenta, se elegirá el total de la población de estudio.

Muestreo

El muestreo se define como la práctica estadística en la que se eligen elementos de una población mediante una técnica específica, con el propósito de llegar a conclusiones limitadas a la muestra o adquirir conocimientos sobre la población observada para realizar una inferencia estadística general [20]. El muestreo en este estudio es de tipo no probabilístico por conveniencia. Dichas muestras, también conocidas como accidentales, se seleccionan porque los elementos están espacial, temporal o administrativamente accesibles para el investigador que realiza la recolección de datos [20]. En esta investigación se aplicará el muestreo no probabilístico por conveniencia.

G. Técnicas e instrumentos de recolección de datos

La técnica denominada fichaje, consiste en recopilar y obtener datos relevantes mientras se investiga el tema de estudio, donde cada dato recolectado contiene información de valor único e intrínseco [21]. El instrumento denominado Ficha de Registro se emplea para documentar los datos importantes de las fuentes que se consultan, las cuales deben ser diseñadas de manera que resulten simples y de fácil llenado, asegurando así un proceso eficiente y claro para el usuario [21]. En este trabajo de investigación, se aplica la técnica fichaje e instrumento ficha de registro para la recolección de datos.

H. Técnicas estadísticas de análisis de datos

Para la recolección de datos, se emplea la ficha de registro. Durante este proceso, los datos fueron registrados utilizando el software Microsoft® Excel® para Microsoft 365 MSO de 64 bits. Después de completada la recolección de datos, se procede a su procesamiento y análisis utilizando el software IBM SPSS versión 21. Tras obtener los resultados, se lleva a cabo su análisis e interpretación.

I. Consideraciones éticas

El proyecto se desarrolló siguiendo los principios éticos de respeto hacia la institución privada que forma parte del estudio de esta tesis. Se ha garantizado una comunicación completa y transparente, informando detalladamente a la institución sobre los alcances de su participación. Asimismo, se ha enfocado en mantener la confidencialidad total de los datos recopilados, asegurando que no se divulguen de manera no autorizada. Además, se ha mantenido un compromiso absoluto con la integridad académica, evitando cualquier forma de plagio.

IV. **Resultados**

En este capítulo se presentarán primero los resultados descriptivos y luego los resultados inferenciales. Estos resultados se obtuvieron tanto antes como después de la implementación de la solución propuesta.

Resultados descriptivos

Primera Dimensión: Disponibilidad de la información

Primer indicador: Porcentaje Acumulado de certificados disponibles

La Tabla I presenta los datos recopilados del indicador PACD (Porcentaje Acumulado de Certificados Disponibles) durante las mediciones de preprueba y postprueba, en las cuales se llevaron a cabo un total de 24 evaluaciones. Se observa una mejora progresiva en la disponibilidad de la información a partir del séptimo certificado en la prueba posterior. En consecuencia, se observa que la solución propuesta está contribuyendo de manera significativa a la mejora de la disponibilidad de la información.

Tabla I.
PACD: PREPRUEBA Y POSTPRUEBA

PACD	**Porcentaje Acumulado de certificados disponibles**	
	PACD Preprueba	PACD Postprueba
1	4.17%	4.17%
2	8.33%	8.33%
3	12.50%	12.50%
4	16.67%	16.67%
5	20.83%	20.83%
6	25.00%	25.00%
7	25.00%	29.17%
8	29.17%	33.33%
9	33.33%	37.50%
10	37.50%	41.67%
11	41.67%	45.83%
12	41.67%	50.00%
13	41.67%	54.17%
14	41.67%	58.33%
15	41.67%	62.50%
16	41.67%	66.67%
17	41.67%	70.83%
18	41.67%	75.00%
19	45.83%	79.17%

20	50.00%	83.33%
21	54.17%	87.50%
22	58.33%	91.67%
23	62.50%	95.83%
24	66.67%	100.00%

Asi mismo, la tabla II revela que el porcentaje mínimo de certificados emitidos fue de 4.17%, lo que indica que al menos esa proporción del total previsto fue efectivamente emitida en ambas fases. Se observa una notable diferencia en los valores máximos, dado que durante la preprueba la disponibilidad máxima alcanzó el 66.67%, mientras que en la postprueba se logró la totalidad, es decir, el 100%. Asimismo, el promedio en la postprueba superó al de la preprueba, registrando un 52.08% frente a un 36.81%. Estos datos sugieren que la intervención realizada contribuye a una optimización significativa en la disponibilidad de los certificados.

TABLA II.
MEDIDAS DESCRIPTIVAS DEL PACD

	N	Mínimo	Máximo	Media	Desviación Estándar
PACD – Preprueba	24	4.17	66.67	36.81	16.47
PACD – Postprueba	24	4.17	100.00	52.08	29.46

En ese sentido, la Figura 1 presenta una comparación entre los promedios de las fases de preprueba y postprueba, revelando que el promedio del PACD en la evaluación posterior alcanza el 52.08%, superior al 36.81% observado en la evaluación previa. Este incremento sugiere una mejora en el proceso de emisión de certificados. No obstante, la Tabla II muestra que la desviación estándar en la postprueba es de 29.46, notablemente más alta que la desviación estándar de 16.47 registrada en la preprueba. Esta mayor variabilidad en el porcentaje acumulado de certificados disponibles no implica necesariamente una inconsistencia en el proceso de emisión, sino que refleja la naturaleza acumulativa de los datos, donde cada certificado emitido contribuye de manera incremental al porcentaje total acumulado. La variabilidad ampliada en la evaluación posterior es influenciada por el aumento en la cantidad de certificados emitidos, lo que resulta en una contribución más heterogénea al porcentaje acumulado.

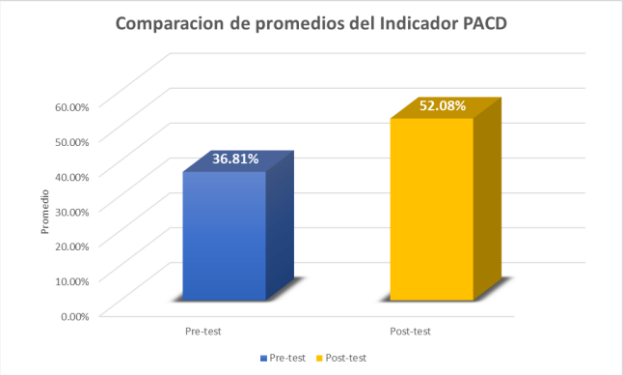


Fig. 1. Comparación de promedios del indicador PACD

Segunda Dimensión: Integridad de la información

Segundo indicador: Porcentaje acumulado de certificados íntegros

La Tabla III presenta los datos recopilados del indicador PACI (Porcentaje Acumulado de Certificados Íntegros) durante las mediciones de preprueba y postprueba, en las cuales se llevaron a cabo un total de 24 evaluaciones. Se observa una mejora progresiva en la integridad de la información a partir del sexto certificado en la prueba posterior. En consecuencia, se observa que la solución propuesta está contribuyendo de manera significativa a la mejora de la integridad de la información.

Tabla III.
PACI: PREPRUEBA Y POSTPRUEBA

PACI	**Porcentaje Acumulado de certificados íntegros**	
	PACI Preprueba	PACI Postprueba
1	4.17%	4.17%
2	8.33%	8.33%
3	12.50%	12.50%
4	16.67%	16.67%
5	20.83%	20.83%
6	20.83%	25.00%
7	20.83%	29.17%
8	20.83%	33.33%
9	20.83%	37.50%
10	20.83%	41.67%
11	25.00%	45.83%
12	25.00%	50.00%
13	25.00%	54.17%
14	25.00%	58.33%
15	25.00%	62.50%
16	25.00%	66.67%
17	25.00%	70.83%
18	25.00%	75.00%
19	29.17%	79.17%
20	33.33%	83.33%
21	37.50%	87.50%
22	41.67%	91.67%
23	45.83%	95.83%
24	50.00%	100.00%

Asi mismo, la tabla IV revela que el porcentaje mínimo de certificados íntegros fue de 4.17%, lo que indica que al menos esa proporción del total previsto presentaba integridad en ambas fases. Se observa una notable diferencia en los valores máximos, dado que durante la preprueba la integridad máxima alcanzó el 50%, mientras que en la postprueba se logró la totalidad, es decir, el 100%. Asimismo, el promedio en la postprueba superó al de la preprueba, registrando un 52.08% frente a un 25.17%. Estos datos sugieren que la intervención realizada contribuye a una optimización significativa en la integridad de los certificados.

Tabla IVIII.
MEDIDAS DESCRIPTIVAS DEL PACI

	N	Mínimo	Máximo	Media	Desviación Estándar
PACI – Preprueba	24	4.17	50.00	25.17	10.67
PACI – Postprueba	24	4.17	100.00	52.08	29.46

En ese sentido, la Figura 2 presenta una comparación entre los promedios de las fases de preprueba y postprueba, revelando que el promedio del PACI en la evaluación posterior alcanza el 52.08%, superior al 25.17% observado en la evaluación previa. Este incremento sugiere una mejora en las características de integridad de certificados. No obstante, la Tabla IV muestra que la desviación estándar en la postprueba es de 29.46, notablemente más alta que la desviación estándar de 10.67 registrada en la preprueba. Esta mayor variabilidad en el porcentaje acumulado de certificados íntegros no implica necesariamente una inconsistencia en el proceso de verificación de integridad, sino que refleja la naturaleza acumulativa de los datos, donde cada certificado con propiedades de integridad contribuye de manera incremental al porcentaje total acumulado. La variabilidad ampliada en la evaluación posterior es influenciada por el aumento en la cantidad de certificados íntegros, lo que resulta en una contribución más heterogénea al porcentaje acumulado.

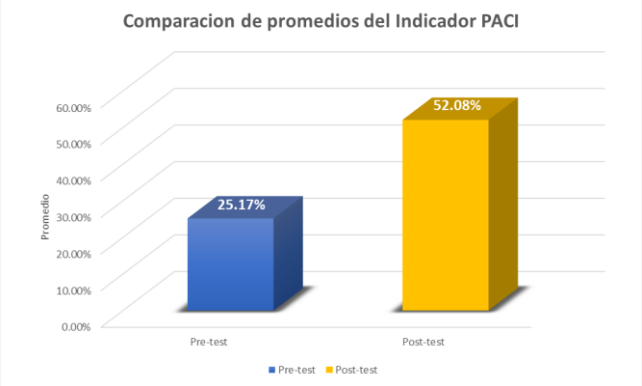


Fig. 2. Comparación de promedios del indicador PACI

Tercera Dimensión: Confidencialidad de la información

Tercer indicador: Porcentaje acumulado de certificados entregados correctamente

La Tabla V presenta los datos recopilados del indicador PACEC (Porcentaje Acumulado de Certificados Entregados Correctamente) durante las mediciones de preprueba y postprueba, en las cuales se llevaron a cabo un total de 24 evaluaciones. Se observa una mejora progresiva en la confidencialidad de la información a partir del primer certificado en la prueba posterior. En consecuencia, se observa que la solución propuesta está contribuyendo de manera significativa a la mejora de la confidencialidad de la información.

Tabla V.
PACEC: PREPRUEBA Y POSTPRUEBA

PACEC	**Porcentaje Acumulado de certificados entregados correctamente**	
	PACEC Preprueba	PACEC Postprueba
1	0.00%	4.55%
2	0.00%	9.09%
3	0.00%	13.64%
4	0.00%	17.05%
5	0.00%	19.32%
6	0.00%	23.86%
7	0.00%	28.41%
8	0.00%	32.95%
9	0.00%	37.50%
10	0.00%	39.77%
11	0.00%	40.91%
12	0.00%	43.18%
13	0.00%	47.73%
14	0.00%	51.14%
15	0.00%	55.68%
16	0.00%	61.36%
17	0.00%	64.77%
18	0.00%	65.91%
19	4.55%	70.45%
20	9.09%	75.00%
21	14.77%	80.68%
22	19.32%	85.23%
23	25.00%	90.91%
24	26.14%	92.05%

Asi mismo, la tabla VI revela que el porcentaje mínimo de certificados entregados correctamente fue de 0 % en la etapa preprueba y 4.55% en la etapa postprueba. Se observa una notable diferencia en los valores máximos, dado que durante la preprueba la confidencialidad máxima alcanzó el 26.14%, mientras que en la postprueba se logró el 92.05%. Asimismo, el promedio en la postprueba superó al de la preprueba, registrando un 47.96% frente a un 4.12%. Estos datos sugieren que la intervención realizada contribuye a una optimización significativa en la confidencialidad de los certificados.

Tabla VI.
MEDIDAS DESCRIPTIVAS DEL PACEC

	N	Mínimo	Máximo	Media	Desviación Estándar
PACEC – Preprueba	24	0	26.14	4.12	8.33
PACEC – Postprueba	24	4.55	92.05	47.96	26.48

En ese sentido, la Figura 3 presenta una comparación entre los promedios de las fases de preprueba y postprueba, revelando que el promedio del PACEC en la evaluación posterior alcanza el 47.96%, superior al 4.12% observado en la evaluación previa. Este incremento sugiere una mejora en las características de integridad de certificados. No obstante, la Tabla VI muestra que la desviación estándar en la postprueba es de 26.48, notablemente más alta que la desviación estándar de 8.33 registrada en la preprueba. Esta mayor variabilidad en el porcentaje acumulado de certificados íntegros no implica necesariamente una inconsistencia en el proceso de verificación de integridad, sino que refleja la naturaleza acumulativa de los datos, donde cada certificado con propiedades de integridad contribuye de manera incremental al porcentaje total acumulado. La variabilidad ampliada en la evaluación posterior es influenciada por el aumento en la cantidad de certificados íntegros, lo que resulta en una contribución más heterogénea al porcentaje acumulado.

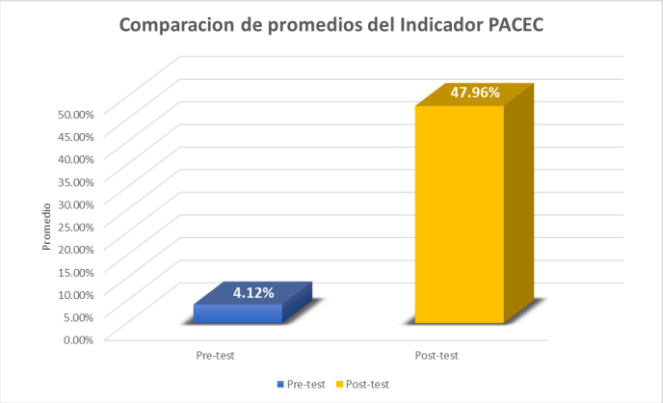


Fig. 3. Comparación de promedios del indicador PACEC

Resultados inferenciales

Primera Dimensión: Disponibilidad de la información

Primer indicador: Porcentaje Acumulado de certificados disponibles

Prueba de normalidad:

Hernández et al. (2014) mencionan que para conjuntos de datos de hasta 50 elementos se recomienda la utilización de la prueba de Shapiro-Wilk, como se cita en [22]. Además, de acuerdo con J. Arias y M. Covinos, un valor de significancia (Sig.) superior a al valor de 0.05 indica una distribución normal de los datos, mientras que un valor de (Sig.) inferior al valor de 0.05 sugiere una distribución no normal, según se menciona en [23].

A continuación se redacta las hipótesis de la prueba de normalidad del indicador PACD:

- **Hipótesis nula (Ho):** La distribución de los datos del indicador PACD es normal.
- **Hipótesis Alterna (H1):** La distribución de los datos del indicador PACD **no** es normal.

Tabla VII.

PRUEBA DE NORMALIDAD DEL INDICADOR PACD

	Shapiro-Wilk		
	Estadístico	gl	Sig.
PACD – Pre-test	,957	24	,373
PACD – Post-test	,959	24	,416

Los hallazgos obtenidos después de aplicar la prueba de normalidad de Shapiro-Wilk al indicador PACD se detallan en la Tabla VII. Para los datos del pre-test, se encontró un nivel de significancia 0.373, mientras que para el post-test, este valor fue de 0.416. Considerando que ambos indicadores de significación superan el umbral de 0.05, no se dispone de la evidencia necesaria para descartar la hipótesis nula. En resumen, la hipótesis nula no se descarta.

Prueba de hipótesis:

Los datos correspondientes al indicador PACD exhiben una distribución normal. Por lo tanto, para la prueba de hipótesis, se aplicará la prueba t de Student. Este enfoque se fundamenta en la observación de [23], quien señala que para datos que presentan una distribución normal se aplica la prueba de t de Student.

A continuación se redacta las hipótesis del indicador PACD:

- **Hipótesis nula (Ho):** El sistema con tecnología blockchain **no** mejora significativamente la disponibilidad de la información de certificados de la gestión de la seguridad de la información en una institución Privada, Callao, 2022.
- **Hipótesis alterna (H1):** El sistema con tecnología blockchain mejora significativamente la disponibilidad de la información de certificados de la gestión de la seguridad de la información en una institución Privada, Callao, 2022.

Tabla IVIII.

ESTADÍSTICOS DE MUESTRAS RELACIONADAS

		Media	N	Desviación típ.	Error típ. de la media
Par 1	PACD – Pretest	36,8067	24	16,46962	3,36185
	PACD – Posttest	52,0833	24	29,46262	6,01403

Tabla IX.

PRUEBA DE MUESTRAS RELACIONADAS

		Diferencias relacionadas					t	gl	Sig. (bilateral)
		Media	Desviación típ.	Error típ. de la media	95% Intervalo de confianza para la diferencia Inferior	Superior			
Par 1	PACD Pre test – PACD Post test	-15,27667	14,25800	2,91040	-21,29729	-9,25604	-5,249	23	,000

En la Tabla IX se exponen los hallazgos del test de t de Student para el indicador PACD. Se documentó un índice de significación de 0.000, notablemente menor al límite establecido de 0.05. En consecuencia, se rechaza la hipótesis de nula y se admite la hipótesis alternativa. Esto indica que los promedios recopilados pre y post-test, utilizando la ficha de registro, difieren significativamente.

Segunda Dimensión: Integridad de la información

Segundo indicador: Porcentaje acumulado de certificados íntegros

Prueba de normalidad:

Hernández et al. (2014) mencionan que para conjuntos de datos de hasta 50 elementos se recomienda la utilización de la prueba de Shapiro-Wilk, como se cita en [22]. Además, de acuerdo con J. Arias y M. Covinos, un valor de significancia (Sig.) superior a al valor de 0.05 indica una distribución normal de los datos, mientras que un valor de (Sig.) inferior al valor de 0.05 sugiere una distribución no normal, según se menciona en [23].

A continuación se redacta las hipótesis de la prueba de normalidad del indicador PACI:

- **Hipótesis nula (Ho):** La distribución de los datos

del indicador PACI es normal.

- **Hipótesis Alterna (H1):** La distribución de los datos del indicador PACI **no** es normal.

Tabla X.
PRUEBA DE NORMALIDAD DEL INDICADOR PACI

	Shapiro-Wilk		
	Estadístico	gl	Sig.
PACI – Pre test	,922	24	,063
PACI – Post test	,959	24	,416

Los hallazgos obtenidos después de aplicar la prueba de normalidad de Shapiro-Wilk al indicador PACI se detallan en la Tabla X. Para los datos del pre-test, se encontró un nivel de significancia 0.063, mientras que para el post-test, este valor fue de 0.416. Considerando que ambos indicadores de significación superan el umbral de 0.05, no se dispone de la evidencia necesaria para descartar la hipótesis nula. En resumen, la hipótesis nula no se descarta.

Prueba de hipótesis:

Los datos correspondientes al indicador PACI exhiben una distribución normal. Por lo tanto, para la prueba de hipótesis, se aplicará la prueba t de Student. Este enfoque se fundamenta en la observación de [23], quien señala que para datos que presentan una distribución normal se aplica la prueba de t de Student.

A continuación se redacta las hipótesis del indicador PACI:

- **Hipótesis nula (Ho):** El sistema con tecnología blockchain **no** mejora significativamente la integridad de la información de certificados de la gestión de la seguridad de la información en una institución Privada, Callao, 2022.
- **Hipótesis alterna (H1):** El sistema con tecnología blockchain mejora significativamente la integridad de la información de certificados de la gestión de la seguridad de la información en una institución Privada, Callao, 2022.

Tabla XI.
ESTADÍSTICOS DE MUESTRAS RELACIONADAS

		Media	N	Desviación típ.	Error típ. de la media
Par 1	PACI Pre test	25,172924		10,67471	2,17897
	PACI Post test	52,083324		29,46262	6,01403

Tabla XII.
PRUEBA DE MUESTRAS RELACIONADAS

		Diferencias relacionadas							
		Media	Desviación típ.	Error típ. de la media	95% Intervalo de confianza para la diferencia		t	gl	Sig. (bilateral)
					Inferior	Superior			
Par 1	PACI Pre test – PACI Post test	-26,91042	20,15051	4,11321	-35,41923	-18,40160	-6,542	23	,000

En la Tabla XII se exponen los hallazgos del test de t de Student para el indicador PACI. Se documentó un índice de significación de 0.000, notablemente menor al límite establecido de 0.05. En consecuencia, se rechaza la hipótesis de nula y se admite la hipótesis alternativa. Esto indica que los promedios recopilados pre y post-test, utilizando la ficha de registro, difieren significativamente.

Tercera Dimensión: Confidencialidad de la información

Tercer indicador: Porcentaje acumulado de certificados entregados correctamente

Prueba de normalidad:

Hernández et al. (2014) mencionan que para conjuntos de datos de hasta 50 elementos se recomienda la utilización de la prueba de Shapiro-Wilk, como se cita en [22]. Además, de acuerdo con J. Arias y M. Covinos, un valor de significancia (Sig.) superior a al valor de 0.05 indica una distribución normal de los datos, mientras que un valor de (Sig.) inferior al valor de 0.05 sugiere una distribución no normal, según se menciona en [23].

A continuación se redacta las hipótesis de la prueba de normalidad del indicador PACEC:

- **Hipótesis nula (Ho):** La distribución de los datos del indicador PACEC es normal.
- **Hipótesis Alterna (H1):** La distribución de los datos del indicador PACEC **no** es normal.

Tabla XIII.
PRUEBA DE NORMALIDAD DEL INDICADOR PACEC

	Shapiro-Wilk		
	Estadístico	gl	Sig.
PACEC – Pre test	,562	24	,000
PACEC – Post test	,964	24	,516

Los hallazgos obtenidos después de aplicar la prueba de normalidad de Shapiro-Wilk al indicador PACEC se detallan en la Tabla XIII. Para los datos del pre-test, se encontró un nivel de significancia 0.000, mientras que para el post-test, este valor fue de 0.516. El valor de significancia obtenido para el pre-test es inferior al umbral de 0.05, lo que conduce a rechazar la hipótesis nula para los datos de la evaluación previa (pre test). En contraste, el valor de significancia correspondiente al post test supera el límite de 0.05, lo que significa que la hipótesis nula no se rechaza para los datos de la evaluación posterior (post-test).

Prueba de hipótesis:

Para el análisis del tercer indicador PACEC se identificó que los datos correspondientes al pre-test no seguían una

distribución normal, en contraste con los datos del post-test que sí se ajustaban a dicha distribución. Esta constatación llevó a optar por la prueba de Wilcoxon para realizar la prueba de hipótesis. Según [24], la técnica estadística denominada t de Student, una prueba paramétrica, es apropiada para la comparación de dos grupos cuyas variables cuantitativas continuas se distribuyen normalmente; sin embargo, para datos relacionados que carecen de normalidad, se prefieren las pruebas no paramétricas, como la de Wilcoxon. Los autores subrayan que la aplicación de pruebas paramétricas requiere que ambos conjuntos de datos exhiban una distribución normal; por lo tanto, ante la falta de normalidad en el pre-test, se eligió el uso de la prueba no paramétrica de Wilcoxon.

A continuación se redacta las hipótesis del indicador PACEC:

- **Hipótesis nula (Ho):** El sistema con tecnología blockchain **no** mejora significativamente la confidencialidad de la información de certificados de la gestión de la seguridad de la información en una institución Privada, Callao, 2022.
- **Hipótesis alterna (H1):** El sistema con tecnología blockchain mejora significativamente la confidencialidad de la información de certificados de la gestión de la seguridad de la información en una institución Privada, Callao, 2022.

Tabla XIV.
PRUEBA DE RANGO DE SIGNOS DE WILCOXON

		N	Rango promedio	Suma de rangos
PACEC Post test – PACEC Pre test	Rangos negativos	0[a]	,00	,00
	Rangos positivos	24[b]	12,50	300,00
	Empates	0[c]		
	Total	24		

a. PACEC Post test < PACEC Pre test

b. PACEC Post test > PACEC Pre test

c. PACEC Post test = PACEC Pre test

Tabla XV.
ESTADISTICO DE CONTRASTE

	Prueba de rangos con signo de Wilcoxon	
	Z	Sig. asintót. (bilateral)
PACEC Post test – PACEC Pre-test	-4,293[b]	,000

a. Prueba de los rangos con signo de Wilcoxon

b. Basado en los rangos negativos.

La Tabla XIV muestra los hallazgos del test de rango con signos de Wilcoxon. Se nota que el total de rangos negativos alcanza 0.00 mientras que el total de rangos positivos asciende a 300.00. Esta diferencia en los rangos indica que existen más diferencias positivas, lo que sugiere que los valores obtenidos en el post test superan a los del pre test. Asimismo, la Tabla XV exhibe el valor estadístico de la prueba de rango con signo de Wilcoxon: un valor Z de -4.293 y un índice de significacia de 0.000, que resulta ser inferior al umbral de 0.05. El resultado obtenido indica el rechazo de la hipótesis nula y la aceptación de la hipótesis alterna.

V. Discusión

Se realizo un análisis de los resultados alcanzados en la presente investigación, obtenidos mediante los indicadores del porcentaje acumulado de: certificados disponibles, certificados íntegros y certificados entregados correctamente.

Discusión de la primera dimensión: Disponibilidad de la Información

Resultados descriptivos

Los datos recopilados mediante el indicador PACD, muestran en el pre-test, el PACD alcanza un máximo del 66.67%, mientras que en el post-test asciende al 100%, lo que refleja que la aplicación integrada con tecnología blockchain mejora en un 33.33% la disponibilidad de la información de certificados. Así mismo, [25] mencionan que el uso de la tecnología blockchain permite mejorar en un 45% la disponibilidad de la información.

Resultados Inferenciales

Los datos recopilados del indicador PACD evidencian que poseen características de una repartición normal, y mediante el método estadístico denominado prueba de t de student, validan que se rechaza la hipótesis nula, es decir que el sistema con tecnología blockchain mejora significativamente la disponibilidad de la información de certificados de la gestión de la seguridad de la información en una institución Privada, Callao, 2022. Del mismo modo [25], mencionan que la aplicación de la tecnología blockchain en su propuesta tecnológica garantiza la disponibilidad de la información para los pacientes y médicos.

Discusión de la segunda dimensión: Integridad de la Información

Resultados descriptivos

Los datos recopilados mediante el indicador PACI, muestran en el pre-test, el PACI alcanza un máximo del 50%, mientras que en el post-test asciende al 100%, lo que refleja que la aplicación integrada con tecnología blockchain mejora en un 50% la integridad de la información de certificados. Así mismo, [25] mencionan que el uso de la tecnología blockchain disminuye en un 50% el riesgo de alteraciones no autorizadas y duplicidad de datos en los registros médicos.

Resultados Inferenciales

Los datos recopilados del indicador PACI evidencian que poseen características de una repartición normal, y mediante el método estadístico denominado prueba de t de student, validan que se rechaza la hipótesis nula, es decir que el sistema con tecnología blockchain mejora significativamente la integridad de la información de certificados de la gestión de la seguridad de la información en una institución Privada,

Callao, 2022. Del mismo modo [25], mencionan que la aplicación de la tecnología blockchain en su propuesta tecnológica mejora la integridad y consistencia de la información.

Discusión de la tercera dimensión: Confidencialidad de la Información

Resultados descriptivos

Los datos recopilados mediante el indicador PACEC, muestran en el pre-test, el PACEC alcanza un máximo del 26.14%, mientras que en el post-test asciende al 92.05%, lo que refleja que la aplicación integrada con tecnología blockchain mejora en un 65.91% la confidencialidad de la información de certificados. Así mismo, [25] mencionan que el uso de la tecnología blockchain disminuye en un 20% el riesgo de que terceros accedan a la información.

Resultados Inferenciales

Los datos recopilados del indicador PACEC evidencian que poseen características de una repartición normal, y mediante el método estadístico denominado prueba de t de student, validan que se rechaza la hipótesis nula, es decir que el sistema con tecnología blockchain mejora significativamente la confidencialidad de la información de certificados de la gestión de la seguridad de la información en una institución Privada, Callao, 2022. Del mismo modo [25], mencionan que la aplicación de la tecnología blockchain en su propuesta tecnológica mejora la confidencialidad de la información.

VI. Conclusiones

Según los resultados de este trabajo científico, se llegan a las siguientes conclusiones:

En primer lugar, se concluye que la solución propuesta de sistema con tecnología blockchain tiene un efecto positivo en la disponibilidad de la información de certificados de la gestión de la seguridad de la información en una institución Privada, Callao, 2022, ya que el indicador PACD demostró una mejora del 33.33% en la disponibilidad de la información de certificados.

En segundo lugar, se concluye que la solución propuesta de sistema con tecnología blockchain tiene un efecto positivo en la integridad de la información de certificados de la gestión de la seguridad de la información en una institución Privada, Callao, 2022, ya que el indicador PACI demostró una mejora del 50% en la integridad de la información de certificados.

En Tercer lugar, se concluye que la solución propuesta de sistema con tecnología blockchain tiene un efecto positivo en la confidencialidad de la información de certificados de la gestión de la seguridad de la información en una institución Privada, Callao, 2022, ya que el indicador PACI demostró una mejora del 65.91% en la confidencialidad de la información de certificados.

Por lo tanto, se concluye que el sistema con tecnología blockchain afecta positivamente la gestión de la seguridad de la información en una institución Privada, Callao, 2022, dado que los indicadores demuestran mejoras en las dimensiones de disponibilidad, integridad y confidencialidad.

VII. Recomendaciones

Tras obtener resultados positivos en la investigación presente, es aconsejable tomar en cuenta las recomendaciones a continuación:

En primer lugar, diseñar estrategias para la expansión del sistema de blockchain, con el fin de que éste pueda evolucionar junto con el desarrollo de la entidad y garantizar su viabilidad y eficacia en el futuro.

En segundo lugar, explorar la viabilidad de integrar tecnologías avanzadas como la inteligencia artificial y el aprendizaje automático para anticipar necesidades y optimizar los mecanismos de protección de datos.

En tercer lugar, dadas las mejorías constatadas, se aconseja perpetuar y extender el uso de la tecnología de cadena de bloques a diferentes segmentos de la administración de datos.

En cuarto lugar, profundizar en el estudio sobre la transferibilidad de estos resultados a otras organizaciones o escenarios, incluyendo distintas áreas geográficas o sectores económicos, para ampliar el alcance de las ventajas ofrecidas por la blockchain.

VIII. Referencias

[1] Cloudflare, "¿Qué es la seguridad de la información?" Accessed: Apr. 14, 2024. [Online]. Available: https://www.cloudflare.com/es-es/learning/security/what-is-information-security/

[2] IBM, "¿Qué es la tecnología blockchain? - IBM Blockchain." Accessed: Apr. 27, 2024. [Online]. Available: https://www.ibm.com/es-es/topics/blockchain

[3] J. Cano, "Gobierno y gestión de la seguridad y la ciberseguridad. Una agenda complementaria a los estándares vigentes y las buenas prácticas | Global Strategy," Global Strategy Report. Accessed: Apr. 14, 2024. [Online]. Available: https://global-strategy.org/gobierno-y-gestion-de-la-seguridad-y-la-ciberseguridad-una-agenda-complementaria-a-los-estandares-vigentes-y-las-buenas-practicas/

[4] E. A. Ramírez-Camargo and M. A. Rinconc-Pinzon, "La importancia de la seguridad de la información en el sector público en Colombia.," *RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação*, vol. 2022, no. 46, pp. 97–99, Jun. 2022, doi: 10.17013/RISTI.46.87-99.

[5] S. Bustamante-García, M. Á. Valles-Coral, I. E. Cuellar-Rodríguez, and D. Lévano-Rodríguez, "Políticas basadas en la ISO 27001:2013 y su influencia en la gestión de seguridad de la información en municipalidades de Perú," *Enfoque UTE*, vol. 12, no. 2, pp. 69–79, Apr.

2021, doi: 10.29019/ENFOQUEUTE.743.
[6] J. Veliz-Delgado, “Ciberdelincuencia e Inteligencia Artificial en Perú 2023 | RPP Noticias,” RPP. Accessed: Apr. 19, 2024. [Online]. Available: https://rpp.pe/tecnologia/mas-tecnologia/ciberdelincuencia-e-inteligencia-artificial-en-peru-2023-noticia-1508418
[7] M. P. Delgado-Baltazar and J. H. Valverde-Huamani, “Sistema de seguridad de la información para optimizar los servidores web en la oficina de tecnología de información y comunicación de la Facultad de Ingeniería Industrial y de Sistemas de la Universidad Nacional del Callao 2022,” Universidad Nacional de Callao, 2023. Accessed: Apr. 19, 2024. [Online]. Available: http://repositorio.unac.edu.pe/handle/20.500.12952/8534
[8] C. Rodríguez-Gutiérrez, “Propuesta de implementación de un sistema de gestión de seguridad de la información aplicando la Norma ISO 27001:2013 para una institución del Estado en la Provincia Constitucional de Callao - 2021,” Universidad Tecnologica del Perú, 2021. Accessed: Apr. 19, 2024. [Online]. Available: http://repositorio.utp.edu.pe/handle/20.500.12867/5101
[9] R. Raimundo and A. Rosário, “Blockchain System in the Higher Education,” *Eur J Investig Health Psychol Educ*, vol. 11, no. 1, pp. 276–293, Mar. 2021, doi: 10.3390/EJIHPE11010021.
[10] L. Koh, A. Dolgui, and J. Sarkis, “Blockchain in transport and logistics – paradigms and transitions,” *Int J Prod Res*, vol. 58, no. 7, pp. 2054–2062, Apr. 2020, doi: 10.1080/00207543.2020.1736428.
[11] P. Lafourcade and M. Lombard-Platet, “About blockchain interoperability,” *Inf Process Lett*, vol. 161, p. 105976, Sep. 2020, doi: 10.1016/J.IPL.2020.105976.
[12] M. Alshamsi, M. Al-Emran, and K. Shaalan, “A Systematic Review on Blockchain Adoption,” *Applied Sciences*, vol. 12, no. 9, p. 4245, Apr. 2022, doi: 10.3390/APP12094245.
[13] P. Paul, P. S. Aithal, R. Saavedra, and S. Ghosh, “Blockchain Technology and Its Types—A Short Review,” Dec. 2021, Accessed: May 06, 2024. [Online]. Available: https://papers.ssrn.com/abstract=4050933
[14] I. Abu-elezz, A. Hassan, A. Nazeemudeen, M. Househ, and A. Abd-alrazaq, “The benefits and threats of blockchain technology in healthcare: A scoping review,” *Int J Med Inform*, vol. 142, no. February, p. 104246, 2020, doi: 10.1016/j.ijmedinf.2020.104246.
[15] R. Ochoa, N. Nava, and D. Fusil, “Comprensión epistemológica del tesista sobre investigaciones cuantitativas, cualitativas y mixtas,” *Orbis: revista de Ciencias Humanas*, vol. 15, no. 45, pp. 13–22, 2020, Accessed: May 17, 2024. [Online]. Available: https://dialnet.unirioja.es/servlet/articulo?codigo=7407375
[16] C. D. de-la-Cruz-Galvan, “Aplicación móvil para emisión de información en tiempo real del servicio de transporte en la Universidad Nacional de Cañete, 2023. Almidón Ortiz, Carlos Alcides,” Universidad Nacional de Cañete, Cañete, 2023. Accessed: May 17, 2024. [Online]. Available: https://repositorio.undc.edu.pe/handle/123456789/108
[17] C. Ramos-Galarza, “Diseños De Investigaciónex Perimental,” *CienciAmérica*, vol. 10, no. 1, 2021.
[18] O. A. Gutierrez-Baracco and J. A. Lujan-Alfaro, “Simulación de un modelo de tecnología blockchain para garantizar la seguridad de la información del proceso de admisión de una universidad pública del Perú,” Universidad Tecnológica del Perú, 2023. Accessed: May 03, 2024. [Online]. Available: http://repositorio.utp.edu.pe/handle/20.500.12867/8240
[19] J. C. Medrano-Cabello, “Sistema de información para mejorar la gestión documentaria de la carpeta pedagógica de una institución educativa pública, Lima - 2023,” Universidad Cesar Vallejo, 2024. Accessed: May 17, 2024. [Online]. Available: https://hdl.handle.net/20.500.12692/134752
[20] L. J. Reales-Chacón, G. E. Robalino-Morales, A. C. Peñafiel-Luna, J. H. Cárdenas-Medina, and P. F. Cantuña-Vallejo, “El Muestreo Intencional No Probabilístico como herramienta de la investigación científica en carreras de Ciencias de la Salud.,” *Universidad y Sociedad*, vol. 14, no. S5, pp. 681-691., Oct. 2022, Accessed: May 17, 2024. [Online]. Available: https://rus.ucf.edu.cu/index.php/rus/article/view/3338
[21] J. G. Leon-Luque, “Business intelligence basado en Hefesto para la toma de decisiones del departamento de marketing en Favo S.A.C.,” Universidad Cesar Vallejo, 2023. Accessed: May 20, 2024. [Online]. Available: https://repositorio.ucv.edu.pe/handle/20.500.12692/120426

[22] P. A. Quiroz-Soriano and A. E. Quiroz-Soriano, “Sistema web para el proceso de reserva de espacios deportivos en la empresa Agrícola Tercer Mundo S.A., Cañete, 2023,” 2023. Accessed: Feb. 03, 2024. [Online]. Available: https://repositorio.undc.edu.pe/items/5258066a-b7b6-4ca5-9a14-1f5f1aa3946a

[23] C. P. Reyna-Vizcarra and R. C. Sanchez-Ramos, “Software con tecnologia qr geolocalizada para el control de asistencias del personal de la empresa mts group restaurantes peruanos s.a.c. cañete,2023,” 2023. Accessed: Feb. 03, 2024. [Online]. Available: https://repositorio.undc.edu.pe/items/ca27f31c-31c5-4334-ab2f-8ad97ef39d0e

[24] E. Flores-Ruiz, M. G. Miranda-Novales, M. Á. Villasís-Keever, E. Flores-Ruiz, M. G. Miranda-Novales, and M. Á. Villasís-Keever, “El protocolo de investigación VI: cómo elegir la prueba estadística adecuada. Estadística inferencial,” *Rev Alerg Mex*, vol. 64, no. 3, pp. 364–370, Jul. 2017, doi: 10.29262/RAM.V64I3.304.

[25] A. Martinez Cervantes and C. A. Molina Charaja, “Arquitectura Tecnológica para la Gestión del Historial Médico usando Blockchain en el Sector Privado de Salud,” Universidad Peruana de Ciencias Aplicadas, 2021. Accessed: May 22, 2024. [Online]. Available: https://repositorioacademico.upc.edu.pe/handle/10757/655796