UNIVERSIDAD NACIONAL DEL CALLAO
ESCUELA DE POSGRADO

UNIDAD DE POSGRADO DE LA FACULTAD DE INGENIERIA INDUSTRIAL Y DE SISTEMAS

"SISTEMA DE SEGURIDAD DE LA INFORMACIÓN PARA OPTIMIZAR LOS SERVIDORES WEB EN LA OFICINA DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIÓN DE LA FACULTAD DE INGENIERIA INDUSTRIAL Y DE SISTEMAS DE LA UNIVERSIDAD NACIONAL DEL CALLAO 2022"

TESIS PARA OPTAR EL GRADO ACADÉMICO DE MAESTRO EN INGENIERIA DE SISTEMAS

AUTORES:

MARISOL PAOLA DELGADO BALTAZAR

JORGE HERBERT VALVERDE HUAMANI

ASESORA:

Dra. ERIKA JUANA ZEVALLOS VERA

LÍNEA DE INVESTIGACIÓN: INGENIERÍA Y TECNOLOGÍA

Callao, 2023

PERÚ

Document Information

Analyzed document	TESIS-SISTEMA DE SEGURIDAD DE LA INFORMACIÓN PARA OPTIMIZAR LOS SERVIDORES WEB EN LA OFICINA DE TEC. (5).docx (D177664757)
Submitted	11/3/2023 4:01:00 AM
Submitted by	fiis posgrado
Submitter email	fiis.posgrado@unac.edu.pe
Similarity	14%
Analysis address	posgrado.fiis.unac@analysis.urkund.com

Sources included in the report

SA **Universidad Nacional del Callao / TESIS-SISTEMA INFORMÁTICO BASADO EN LA METODOLOGÍA ÁGIL(SCRUM) PARA MEJORAR LA PR ODUCTIVIDAD EN EL ALMACEN DE LA OTIC-FIIS-UNAC-CALLAO-2021”-REINOSO PALACIOS.pdf**
Document TESIS-SISTEMA INFORMÁTICO BASADO EN LA METODOLOGÍA ÁGIL(SCRUM) PARA MEJORAR LA PR ODUCTIVIDAD EN EL ALMACEN DE LA OTIC-FIIS-UNAC-CALLAO-2021”-REINOSO PALACIOS.pdf (D130266969)
Submitted by: posgrado.fiis@unac.pe
Receiver: fiis.posgrado.unac@analysis.urkund.com
23

SA **Universidad Nacional del Callao / TESIS_BRAVO LEON_26.10.22.docx**
Document TESIS_BRAVO LEON_26.10.22.docx (D148930206)
Submitted by: jcbulnest@unac.edu.pe
Receiver: fiee.investigacion.unac@analysis.urkund.com
1

SA **Universidad Nacional del Callao / Tesis - Juan Manuel Molocho 14-09-23.docx**
Document Tesis - Juan Manuel Molocho 14-09-23.docx (D174255658)
Submitted by: fiis.posgrado@unac.edu.pe
Receiver: posgrado.fiis.unac@analysis.urkund.com
2

SA **Universidad Nacional del Callao / TESIS 5S - AREVALO LLATAS JHONY.docx**
Document TESIS 5S - AREVALO LLATAS JHONY.docx (D174645868)
Submitted by: fiis.investigacion@unac.edu.pe
Receiver: fiis.investigacion.unac@analysis.urkund.com
7

SA **Universidad Nacional del Callao / TESIS_Dr_OSMART_MORALES_CHALCO.docx**
Document TESIS_Dr_OSMART_MORALES_CHALCO.docx (D171980289)
Submitted by: fiis.investigacion@unac.edu.pe
Receiver: fiis.investigacion.unac@analysis.urkund.com
27

SA **Universidad Nacional del Callao / TESIS-APLICACIÓN DE UN SISTEMA INTEGRADO DE INFORMACION DE IDENTIFICACIÓN BALISTIC A PARA MEJORAR LA PRODUCTIVIDAD EN LA POLICIA NACIONAL DEL PERÚ - 2021-CA.docx**
Document TESIS-APLICACIÓN DE UN SISTEMA INTEGRADO DE INFORMACION DE IDENTIFICACIÓN BALISTIC A PARA MEJORAR LA PRODUCTIVIDAD EN LA POLICIA NACIONAL DEL PERÚ - 2021-CA.docx (D133508111)
Submitted by: posgrado.fiis@unac.pe
Receiver: fiis.posgrado.unac@analysis.urkund.com
6

INFORMACIÓN BÁSICA

FACULTAD: FACULTAD DE INGENIERÍA INDUSTRIAL Y DE SISTEMAS

UNIDAD DE INVESTIGACIÓN: UNIDAD DE POSGRADO DE LA FACULTAD DE INGENIERÍA INDUSTRIAL Y DE SISTEMAS - UNAC.

TÍTULO: "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"

AUTORES: BACH. MARISOL PAOLA DELGADO BALTAZAR
DNI: 40088225 **/ ORCID:** 0000-0002-0278-9557

BACH. JORGE HERBERT VALVERDE HUAMANI
DNI: 43260820 **/ ORCID:** 0009-0004-9744-8158

ASESORA: DRA. ERIKA JUANA ZEVALLOS VERA
DNI: 10661202 **/ ORCID:** 0000-0002-5188-1907

LUGAR DE EJECUCIÓN: UNIVERSIDAD NACIONAL DEL CALLAO.

UNIDAD DE ANÁLISIS: OFICINA DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIÓN DE LA FACULTAD DE INGENIERÍA INDUSTRIAL Y DE SISTEMAS.

TIPO: DESCRIPTIVO Y APLICADA / **ENFOQUE:** CUANTITATIVO / **DISEÑO DE INVESTIGACIÓN: EXPERIMENTAL.**

TEMA OCDE UNAC: INGENIERÍA Y TECNOLOGÍA

HOJA DE REFERENCIA DEL JURADO Y APROBACION

PRESIDENTE: MG. ZAPATA VILLAR, LOYO PEPE

SECRETARIO: DR. MORALES CHALCO, OSMART RAÚL

MIEMBRO: DR. SAKIBARU MAURICIO, LUIS ALBERTO

MIEMBRO: MG. RAMOS CHOQUEHUANCA, ANGELINO ABAD

ASESORA: DRA. ZEVALLOS VERA, ERIKA JUANA

Libro: 1

Folio: 76

Acta: Nº 020-2023-UPG-FIIS

Fecha de sustentación: 12 de diciembre de 2023

DEDICATORIA

A Dios por darnos la vida y a nuestras familias que son el soporte material y emocional para el logro de nuestros objetivos personales y profesionales.

AGRADECIMIENTO

A todas las personas que han contribuido en la elaboración de esta Investigación; y en especial a la Dra. Erika Juana Zevallos Vera, por su valioso aporte en el desarrollo de la presente tesis

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS 3
ÍNDICE DE FIGURAS 5
RESUMEN 6
RESUMO 7
INTRODUCCIÓN 8
I. PLANTEAMIENTO DEL PROBLEMA, ... 10
1.1 Descripción de la realidad problemática, ... 10
1.2 Formulación del problema. 11
1.2.2 Problemas específicos. 11
1.3 Objetivos. 11
1.3.2 Objetivos específicos 12
1.4 Justificación. 12
1.5 Delimitantes de la investigación. 12
II. MARCO TEÓRICO 14
2.1 Antecedentes Internacionales 14
Antecedentes Nacionales 16
2.2 Bases teóricas. 17
2.3 Marco Conceptual. 17
2.4 Definición de términos básicos 29
III. HIPÓTESIS Y VARIABLES 32
3.1 Hipótesis general 32
3.1.1 Hipótesis específicas. 32
3.2 Operacionalización de las variables. 32
IV. METODOLOGÍA DEL PROYECTO. 35
4.1 Diseño de Investigación. 35
4.2 Método de investigación. 35
4.3 Población y muestra.Población. 35
4.4 Lugar de estudio y periodo desarrollado. 36

4.5 Técnicas e instrumentos para la recolección de la informacióndocumental. 36
4.6 Análisis y procesamiento de datos. 37
4.7 Aspectos Éticos en Investigación. 37
4.9 Propuesta de implementación de un sistema de seguridad de la información para optimizar los servidores web en la oficina de Tecnologías de Información y Comunicaciones de la Facultad. 40
V. RESULTADOS. 49
5.1 Resultados descriptivos. 49
5.1.1 Resultados descriptivos de la variable dependienteSERVIDOR WEB.....60
5.2. Resultados inferenciales. 72
VI. DISCUSIÓN DE RESULTADOS 85
6.1 Contrastación y demostración de la hipótesis con los resultados. 85
6.2 Contrastación de los resultados con otros estudios similares. 86
6.3 Responsabilidad ética de acuerdo con los reglamentos vigentes. 88
VII. CONCLUSIONES 89
VIII. RECOMENDACIONES 90
IX. REFERENCIAS BIBLIOGRÁFICAS 91
X. ANEXOS.....93
ANEXO N° 2 ENCUESTA PARA ADMINISTRATIVOS 95
ANEXO 3: VALIDACIÓN DEL INSTRUMENTO POR LOS JUECES EXPERTOS 99

ÍNDICE DE TABLAS

Tabla 1: Operacionalización de Variable independiente 33
Tabla 2: Operacionalización de Variable dependiente 34
Tabla 3: ¿Accede con frecuencia a la página web de la Facultad? 49
Tabla 4: ¿La información que contiene la página web de la FIIS está actualizada y organizada? 50
Tabla 5: ¿En la Facultad existe un base de datos centralizada actualizada? 51
Tabla 6: ¿La información en la página web de la FIIS cumple con los requisitos mínimos de seguridad? 52
Tabla 7: ¿Usted considera que la información del servidor web no se puede manipular ni ser alterado por terceras personas? 53
Tabla 8: ¿Usted puede acceder a los datos y recursos en el servidor web? 54
Tabla 9: ¿La información que almacena el servidor web es confiable? 55
Tabla 10: ¿Para guardar la información, utiliza espacios externos de almacenamiento de información? 56
Tabla 11: ¿Tiene conocimiento sobre los servidores web, que tiene la oficina de tecnología y comunicaiones en la Facultad? 57
Tabla 12: Resumen de procesamiento de casos 58
Tabla 13: Estadísticas de fiabilidad 58
Tabla 14: Estadísticas de elemento de resumen 59
Tabla 15: Estadísticas de escala 59
Tabla 16: Comparativo del Servidor web 60
Tabla 17: Comparativo del Índices de Funcionalidad 62
Tabla 18: Comparativo de los Índices de Fiabilidad 64
Tabla 19: Comparativo de los Índices de Usabilidad 66
Tabla 20: Comparativo de los Índices de Eficiencia 68
Tabla 21: Comparativo de los Índices de Portabilidad 70
Tabla 22: Pruebas de normalidad 72
Tabla 23: Estadísticas de muestras emparejadas productividad 73
Tabla 24: Prueba de muestras emparejadas productividad 73
Tabla 25: Prueba de normalidad de los índices de eficiencia 74

Tabla 26: Estadísticas de muestras emparejadas índices de Eficiencia 75
Tabla 27: Diferencias emparejadas índices de eficiencia 75
Tabla 28: Prueba de Normalidad de los índices de Eficacia 76
Tabla 29: Estadísticas de muestras emparejadas índices de Eficacia 77
Tabla 30: Diferencias emparejadas índices de eficiencia 77
Tabla 31: Prueba de normalidad de los Índices de Eficacia..... 78
Tabla 32: Estadísticas de muestras emparejadas índices de Eficacia 79
Tabla 33: Diferencias emparejadas índices de Eficacia..... 79
Tabla 34: Prueba de Normalidad de los índices de Eficacia 80
Tabla 35: Estadísticas de muestras emparejadas de los índices de Eficacia..... 81
Tabla 36: Diferencias emparejadas índices de Eficacia..... 81
Tabla 37: Prueba de Normalidad de los índices de Eficacia 82
Tabla 38: Estadística de muestras emparejadas índices de Eficacia..... 83
Tabla 39: Diferencias emparejadas índices de Eficacia..... 83

ÍNDICE DE FIGURAS

Figura 1: Diagrama De Dependencias Entre Objetivos De Seguridad 18
Figura 2: Modelo de cifrado con criptografía de clave pública (para proporcionar autenticación).....21
Figura 3: Mecanismos Para Prevenir, Detectar Y Recuperar La Normalidad Del Funcionamiento Del Sistema En Caso De Una Intrusión No Planificada 27
Figura 4: Equivalentes De Capas Entre Tcp/Ip Y El Modelo Osi.....28
Figura 5: Implantación De Política Y Cultura Sobre Seguridad.....29
Figura 6: Área del servidor 38
Figura 7: Gabinete.....39
Figura 8: Laboratorio de Computo de la FIIS.....40
Figura 9: En La Implementación Se Diseña La Siguiente Arquitectura 42
Figura 10: ¿Accede con frecuencia a la página web de la facultad?.....49
Figura 11: ¿La información que contiene la página web de la FIIS está actualizada y organizada? 50
Figura 12: ¿En la facultad existe una base de datos centralizada actualizada?.....51
Figura 13: ¿La información en la página web de la FIIS cumple con los requisitos mínimos de la seguridad? 52
Figura 14: ¿Usted considera que la información del servidor web no se puede manipular ni ser alterado por terceras personas?.....53
Figura 15: ¿Usted puede acceder a los datos y recursos en el servidor web?.....54
Figura 16: ¿La información que almacena el servidor web es confiable? 55
Figura 17: ¿Para guardar la información, utiliza espacios externos de almacenamiento de información?.....56
Figura 18: ¿Tiene conocimiento sobre los servidores web, que tiene la oficina de tecnología y comunicaciones en la Facultad?.....57
Figura 19: Servidor web 61
Figura 20: Índice de funcionalidad.....63
Figura 21: Índice de Fiabilidad.....65
Figura 22: Índice de Usabilidad 67
Figura 23: Índice de Eficiencia.....69
Figura 24: Índice de Portabilidad 71

RESUMEN

La presente investigación se realizó sobre la seguridad de los servidores web en la Oficina de Tecnología de Información y Comunicación (OTIC) de la Facultad de Ingeniería Industrial y de Sistemas (FIIS); se debe establecer mediante normas de funcionamiento y uso, para garantizar la protección y disponibilidad de la información de la infraestructura computacional y de los recursos informáticos.

Brindar y garantizar un nivel de seguridad, disminuir los riesgos de la seguridad de la información de forma eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y en los servidores de aplicaciones funciona con un servidor web para manejar solicitudes de contenido dinámico, tales como servlets, de aplicaciones web. Un servidor web utiliza un plug-in de servidor web para establecer y mantener conexiones HTTP y HTTPS persistentes con un servidor de aplicaciones.

El web servidor está conectado a Internet y permite intercambiar datos con otros dispositivos conectados, mientras que el software del servidor web controla cómo un usuario que accede a los archivos alojados.

El proceso de los servidores web es un ejemplo del modelo cliente / servidor. Todos los ordenadores que tienen sitios web deben tener un software de servidor web.

En la Oficina de Tecnología de Información y Comunicación de la Facultad de Ingeniería Industrial y de Sistemas; los servidores web se utilizan en el alojamiento web o el alojamiento de datos para sitios web y aplicaciones basadas en web, o aplicaciones web.

Palabras claves: seguridad, pruebas de seguridad, servidor web, vulnerabilidades.

RESUMO

Esta investigação foi realizada sobre a segurança dos servidores web do Gabinete de Tecnologias de Informação e Comunicação (OTIC) da Faculdade de Engenharia Industrial e de Sistemas (FIIS); Deve ser estabelecido através de regras de funcionamento e utilização, para garantir a proteção e disponibilidade da informação da infraestrutura informática e dos recursos informáticos.

Fornecer e garantir um nível de segurança, reduzir os riscos de segurança da informação de forma eficiente e adaptada às mudanças que ocorrem nos riscos, no ambiente e nos servidores de aplicações. Trabalha com um servidor web para tratar solicitações de conteúdo dinâmico, como servlets, de aplicações web. Um servidor da web usa um plug-in de servidor da web para estabelecer e manter conexões HTTP e HTTPS persistentes com um servidor de aplicativos.

O servidor web está conectado à Internet e permite a troca de dados com outros dispositivos conectados, enquanto o software do servidor web controla como um usuário acessa os arquivos hospedados.

O processo do servidor web é um exemplo do modelo cliente/servidor. Todos os computadores que possuem sites devem ter software de servidor web.

No Gabinete de Tecnologias de Informação e Comunicação da Faculdade de Engenharia Industrial e de Sistemas; Os servidores da Web são usados em hospedagem na Web ou hospedagem de dados para sites e aplicativos baseados na Web ou aplicativos da Web.

Palavras-chave: segurança, testes de segurança, servidor web, vulnerabilidades.

INTRODUCCIÓN

Hoy en día el servicio de internet se ha convertido en una herramienta muy importante y poderosa, clave para las comunicaciones, utilizando el protocolo de TCP/PI, como también se ha incrementado la vulnerabilidad de la información en todos los niveles y lo que requiere la seguridad de la información.

En las organizaciones, la inseguridad de los sistemas informáticos, las redes; se da en base a los déficits tecnológicos, déficit en la política respecto a la seguridad y déficit en la configuración.

En la UNAC se tiene 11 Facultades, en la actualidad se cuenta con la OTIC, que brinda soporte Tecnológico a las Facultades y las dependencias. La OTIC; es responsable de los procesos de diseño, desarrollo, adquisición, implementación, integración, mantenimiento, documentación y evaluación de los sistemas de información y la infraestructura tecnológica de la Universidad Nacional del Callao.

En ese sentido cada Facultad tiene la Oficina de Tecnología de Información y Comunicación la cual brinda soporte a las diversas áreas y oficinas de la Facultad; que alberga en sus aulas a estudiantes de pregrado y posgrado los cuales se desarrollaron en el Semestre Académico 2020 bajo las normas de emergencia sanitaria por la COVID-19, con respecto a las labores académicas y administrativas; según el decreto supremo Nº 026-2020 (EL PERUANO, 2020), “El presente decreto supremo tiene por finalidad facilitar la implementación del trabajo remoto en el sector público y privado, a efectos de evitar el contagio del COVID-19 en el centro laboral o durante el traslado de los/las trabajadores/as.”

La Oficina de Tecnología de Información y Comunicación de la Facultad de Ingeniería Industrial y de Sistemas; tiene la necesidad de volver a las clases semi presenciales y no cuenta con la tecnología actualizada para poder atender las diferentes oficinas dado que no cuenta con un área de desarrollo, soporte equipado, personal capacitado que dé solución a los diversos problemas del quehacer cotidiano en la Facultad, esto trae como consecuencia un servicio que no es satisfecho y oportuno para los estudiantes.

La información de las diversas áreas de la Facultad está aislada, no cuentan con una base de datos centralizada, no hay copias de seguridad, no cuentan con directivas, protocolos de seguridad de la información, protocolos de bioseguridad.

En este contexto la Oficina de Tecnología de Información y Comunicación de la Facultad de Ingeniería Industrial y de Sistemas; no cuenta con un servidor web que garantice la comunicación segura y sin fallos entre el servidor y el cliente para la gestión administrativa y académica de los estudiantes.

En ese contexto es de vital importancia atender esta necesidad ya que se está entrando a una la etapa de la semipresencialidad en las diversas actividades académicas y administrativas; en ese sentido se requiere contar con un Servidor Virtual Privado en Google Cloud Platform, Sistema de Sitio Educativo Web en plataforma WordPress, Sistema de Red Social tipo Facebook y tener backups semanales de todos los sistemas, todo ello para garantizar la seguridad de la Información con un conjunto de medidas preventivas y procedimientos que controlen el tratamiento de los datos que se utilizan en la Oficina de Tecnologías de Información y Comunicación de la Facultad de Ingeniería Industrial y de Sistemas.

I. PLANTEAMIENTO DEL PROBLEMA,

1.1 Descripción de la realidad problemática,

A nivel internacional la Seguridad de la Información es un factor muy importante y los recursos tecnológicos constantemente que van cambiando, evolucionando y a la vez nos trae nuevas amenazas de tecnologías emergentes. Sobre todo, los dispositivos Internet de las Cosas (IoT), smartphones y las nuevas tecnologías relacionadas con el teletrabajo, traen nuevos retos y riesgos para las instituciones.

A nivel nacional la SI tiene la necesidad de que requiere un Gobierno de Seguridad de Información con funciones, responsabilidades establecidas para lograr los objetivos de SI.

En la UNAC, la FIIS cuenta con la OTIC. Tiene una oficina que es el área del servidor, cuatro (04) laboratorios; que brindan servicio a las diversas oficinas y a los estudiantes de pregrado y posgrado.

En base a la emergencia sanitaria del COVID 19; se ha observado las deficiencias que hay en las herramientas tecnológicas en los cuatro (04) laboratorios y en las oficinas administrativas de la FIIS. Los problemas más frecuentes son: No cuentan con un servicio web que brinde la interacción con los estudiantes que pueden enviar un email a través de un formulario validado mediante el SGA, así como todo documento oficial en la plataforma del SGA. No cuentan con una arquitectura tecnológica, hay dificultad en el servicio de acceso limitado a la OTIC de la Facultad.

Es importante la SI, es un tema que abarca una amplia gama de conceptos y formas. En esta investigación se toma en cuenta y se pone énfasis en la optimización de los servidores web en la OTIC, que, constantemente tiene amenazas de fraude asistido por computadora, falta de actualización y configuración de servidores y subredes, carencia de planes de mantenimientos preventivos de la red. No cuenta con equipos de computadoras de última generación, en base a la pandemia que aún estamos atravesando los equipos se encuentran obsoletos en algunos casos inoperativos debido a que no existe un mantenimiento preventivo y correctivo. Lo que se requiere es mejorar el

sistema de cableado estructurado y no estructurado para brindar atención a los estudiantes con eficiencia y eficacia. Esto permitirá contar con estándares, aplicar buenas prácticas y elevar el nivel de modo que puedan superar potenciales ataques y violaciones; de este modo asegurar la funcionalidad del servicio, minimizar el daño de este, maximizar el retorno sobre las oportunidades y seguridad informática.

1.2 Formulación del problema.

1.2.1 Problema general.

¿En qué medida un sistema de seguridad de información optimiza los servidores web en la OTIC de la FIIS de la UNAC 2022?

1.2.2 Problemas específicos.

a) ¿En qué medida un sistema de seguridad de la información optimiza la funcionalidad de los servidores web en la OTIC de la FIIS de la UNAC 2022?
b) ¿En qué medida un sistema de seguridad de la información optimiza la fiabilidad de los servidores web en la OTIC de la FIIS de la UNAC 2022?
c) ¿En qué medida un sistema de seguridad de la información optimiza la usabilidad de los servidores web en la OTIC de la FIIS de la UNAC 2022?
d) ¿En qué medida un sistema de seguridad de la información optimiza la eficiencia de los servidores web en la OTIC de la FIIS de la UNAC 2022?
e) ¿En qué medida un sistema de seguridad de la información optimiza la portabilidad de los servidores web en la OTIC de la FIIS de la UNAC 2022?

1.3 Objetivos.

1.3.1 Objetivo general.

Determinar en qué medida un sistema seguridad de información optimiza los servidores web en la OTIC de la FIIS de la UNAC 2022.

1.3.2 Objetivos específicos

a) Determinar en qué medida un sistema de seguridad de la información optimiza la funcionalidad de los servidores web en la OTIC de la FIIS de la UNAC 2022.
b) Determinar en qué medida un sistema de seguridad de la información optimiza la fiabilidad de los servidores web en la OTIC de la FIIS de la UNAC 2022.
c) Determinar en qué medida un sistema de seguridad de la información optimiza la usabilidad de los servidores web en la OTIC de la FIIS de la UNAC 2022.
d) Determinar en qué medida un sistema de seguridad de la información optimiza la eficiencia de los servidores web en la OTIC de la FIIS de la UNAC 2022.
e) Determinar en qué medida un sistema de seguridad de la información optimiza la portabilidad de los servidores web en la OTIC de la FIIS de la UNAC 2022.

1.4 Justificación.

El desarrollo de la investigación reside en lograr hacer un diagnóstico situacional actual de la OTIC de la FIIS, en lo referente a la SI en los servidores web, identificando las varias vulnerabilidades y riesgos en la infraestructura y arquitectura de las tecnologías de información, para proponer la implementación de un sistema de seguridad y para optimizar la seguridad de la tecnología de la información basadas en las normas ISO/IEC 27000.

El resultado de esta investigación redundará en la mejora de la SI para evitar la pérdida o robo de la información.

1.5 Delimitantes de la investigación.

Teniendo como objetivo realizar la investigación, se definieron criterios los cuales van a limitar el alcance del estudio de investigación, definiendo toda restricción teórica, espacial y temporal.

Teórico

Teóricamente no hubo contratiempos en localizar información, por ende, se pudo tener toda la bibliografía para fundamentar las variables, así como sus dimensiones e indicadores.

Espacial

Para validar todos los resultados, se tomó en cuenta, proponer la implementación de sistema de SI en la OTIC de la FIIS.

Temporal

La verificación de los resultados se restringe las actividades académicas del año 2022, en base al retorno de las clases en forma presencial. (Plataforma digital única del Estado Peruano, 2022).

II. MARCO TEÓRICO

2.1 Antecedentes Internacionales

Según el autor (Martínez, y otros, 2018) en su trabajo de investigación sobre las tecnologías emergentes han proporcionado una gran ventaja a los usuarios de uso y aplicación de técnicas de Machine Learning y Big Bata. En base al almacenaje en la nube esta data puede estar distribuida en instalaciones, así como en servidores remotos. Quien hace uso no puede controlar la data así que no puede hacer una inspección visual de los enlaces de data, se concluye lo siguiente:

"El software y hardware de Bitcoins no cuentan con un desarrollo eficaz, dejando vacíos respecto a la seguridad por ende problemas al ser usados. IoT, Computación en la Nube y Bitcoin no cuentan con un reglamento, estándares, sus propias leyes, su marco para manejar su data tiene regulaciones de tipo general adoptada en el ámbito de procesamiento de data personal. Hacia un futuro, no podremos saber si va persistir esta tecnología o afianzarse, sin embargo deberemos de cumplir con todos los objetivos respecto a la SI las cuales son: la confidencialidad, la integridad y la disponibilidad".

Según el autor (Rodríguez Chang, y otros) en la presente investigación respecto a servidores web afirman que son una parte importante para que las aplicaciones web funcionen fluyendo todo tipo de información, tanto personales como empresariales. "respecto a la evaluación de la aplicación se usó una serie de pruebas con un número de 21 servidores, encontrándose los servidores web Apache y Nginx. Permitiendo analizar de manera automática un número de 19 servidores localizando más de 200 vulnerabilidades. Siendo el caso el módulo TestFile ayudo a corroborar la totalidad de los archivos específicamente configuración haciendo una interpretación y ejecutando de manera efectiva la totalidad de los controles. Donde estaba offline 21 de los servidores, se les aplico las pruebas respecto a seguridad a sus archivos de configuración. Tomando en cuenta el desarrollo de la aplicación, así como su eficacia en el transcurso de las pruebas que se le realizo se consideró como un éxito, ya que hay un cumplimiento de todos los objetivos que se planteó. Es así que, gracias

a que se eligieron tecnologías se pudo tener una aplicación la cual es modificable a su vez actualizable muy fácilmente, no siendo necesario de un especialista de seguridad para la aplicación de las pruebas, siendo actualizadas no necesitando las modificaciones en su código permitiendo que se añadan nuevos servidores web a posteriores evaluaciones. Además permite que las organizaciones que las usen puedan tener una homogeneidad respecto a seguridad del servidor web.”.

Los autores (García Bordonado, y otros, 2021), en su investigación desarrollada, concluyen que: “la parte más relevante de un ataque cibernético es que el atacante no lo hace sin antes hacer una investigación previa. Siempre hace un plan previo. El realiza una recolección de data, así como de la infraestructura de su posible víctima, así como de sus capacidades. Para que el ataque, se haga efectivo él debe introducir una carga útil o como se le conoce como programa maligno, lo que es más frecuente en los equipos de trabajo, por lo general con sistema operativo Windows. Siendo utilizados en ocasiones diferentes técnicas de ingeniería social son usados para dar la carga útil al afectado. Siendo probabilidad de éxito en c-varias ocasiones dependiendo en un 50% del afectado, ya que una vez que el archivo está enviado, ya depende del afectado si lo ejecuta al archivo o no”.

Soto Vásquez, Duber Enrique (2017), en su trabajo de investigación, desarrolla dos aspectos muy importantes de las empresas de construcción, buscando principalmente la eficiencia, el cumplir plazos, reducir costos, estándares de calidad, utilizando Sistemas de Información Enterprise (ERP, SAP; ORACLE) además de soluciones muy específicas enfocadas a restricciones del proyecto, estas son planeamiento que se utiliza en primavera, el Project, en otro punto; tambien se usa el diseño utilizando la conceptualización BIM (Building Information Modelling), viendo así la relación causal que existe entre los indicadores versus a las variables que se han descrito, incrementándose la eficiencia en 20% de la misma manera se ha desarrollado un análisis multivariada ingresando en un nivel a profundidad en base a la desempeño de

las empresas, así como su magnitud (grande, mediana y pequeña)

Antecedentes Nacionales

(LIZARES FIGUEROA, y otros, 2017) concluyen en la investigación "[…]; concluimos que a través de la implementación del programa de seguridad apache el servidor web reacciona positivamente a todas solicitudes que han sido enviadas por todos los usuarios, incluso en el transcurso al momento de ataques DDoS en tiempo real mediante del script Slowloris.".

(ALCANTARA RAMIREZ , 2019), la presente investigación aplicativa, el autor concluye "realizar un correcto procedimiento de buenas prácticas que se han establecido en los estándares para la llamada infraestructura de la computación en nube así tambien para tener seguridad en la nube permitiendo definir un conjunto de controles para cuidar la integridad, la confidencia y su disponibilidad de toda la información que se encuentra en la nube.".

En su investigación Flores (2017), desarrolló un estudio con la finalidad de incorporar en la Oficina de Gestión de Proyectos de TI en base a la norma ISO 27001, de las instituciones públicas del Perú con la finalidad de saber si esta norma es utilizada y si ha logrado mejorar respecto a la SI, haciendo uso del método de tipo cuantitativo, siendo necesario para el estudio el tener que realizar un análisis y poder obtener datos estadísticos y medir causa-efecto, utilizando herramientas llámese encuestas o cuestionarios para el personal responsable de los sistemas de las diferentes instituciones del país, haciendo un trabajo para mejorar toda estrategia para la seguridad básicamente en infraestructura crítica, minimizando el ciberdelito, pero, al desarrollar el estudio todas las organizaciones el manejo así como la planificación de la norma técnica no ha sido de las más las adecuadas, siendo considerado por el enfoque de implementación resaltando mayormente el poder requerir que se constituyan órganos para el control y así supervisar toda implementación en los organismos del país.

Cueva, Mercado (2017), implementó todo un sistema de gestión de H.C. del nosocomio de Cajamarca, utilizando la verificación para el cumplimiento en base a la norma ISO 27001, actualmente, el país mediante los organismos públicos, existen exigencias de tener una implementación de políticas las cuales gestionen la seguridad de la información, siendo urgente y necesario la implementación de normas que verifiquen toda evaluación y control respecto a estas tareas, poniendo en práctica la metodología de tipo cualitativa para poder desarrollar su estudio, utilizando herramientas que son la entrevista, así como el análisis de documentos que se requiere para que se desarrolle de forma correcta la implementación, realizando una observación directa de su entorno así como el desarrollo de todo procedimientos, dichas entrevistas se dieron al personal especialista y responsable de todos los procesos, concluyendo que el implementar controles para la mejora logra el objetivo de la implementación completa en todos los criterios que se necesita en el proceso de poner a buen recaudo toda la información.

2.2 Bases teóricas.

Tiene como fin el establecer todo escenario o marcos laborales en donde se ha realizado el estudio. Teniendo como objetivo el de presentar las fundamentaciones respecto donde se basa el estudio de investigación, teniendo en cuenta como primer punto el marco teórico realizando todo escrito de teorías que apoyan el fundamento de la investigación, para después presentar el marco conceptual, el cual describe y menciona toda las teorías y expone lo real, así como lo original del estudio.

2.3 Marco Conceptual.

2.3.1 Un Sistema de Información (SI)

Son todas las medidas catalogadas preventivas y reactivas de la persona, de la organización y de los sistemas tecnológicos que resguardan y protegen toda la información manteniendo la confidencialidad, la autenticidad e Integridad de esta.

2.3.2 Seguridad informática.

Es el paso a paso de prevenir y detectar el acceso sin autorización a un sistema informático. Esto incluye el proceso de protección contra intrusos que utilizan nuestros recursos informáticos con fines maliciosos o con fines de lucro, o incluso acceden a ellos accidentalmente. Esto incluye el proceso de protección contra intrusos que utilizan nuestros recursos informáticos con fines maliciosos o con fines de lucro, o incluso acceden a ellos accidentalmente. Lo puntos que cubre la seguridad informática son:

Confidencialidad: solo las personas autorizadas logran acceder a los recursos, data e información.

Integridad: solo las personas con autorización pueden modificar la data cuando éste sea realmente necesario.

Disponibilidad: disponibilidad de la data cuando ésta sea necesaria.

Autenticación: comunicar verdaderamente lo que es real y verídico.

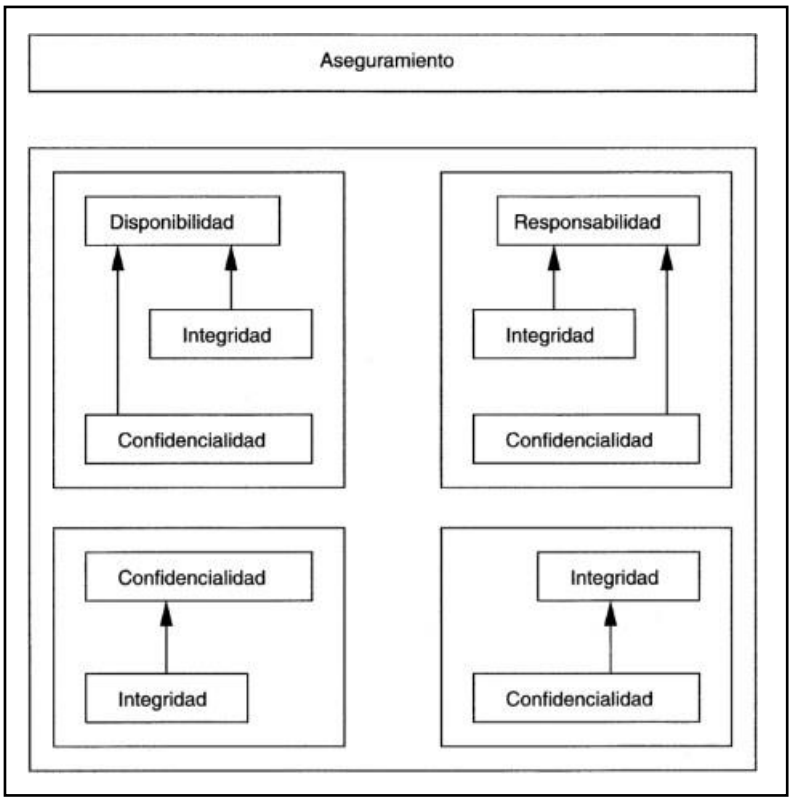

Figura 1: Diagrama de dependencias entre objetivos de seguridad

Fuente: Diagrama de dependencias entre objetivos de seguridad (Areitio, 2008 pág. 18)

2.3.3 Ataque Informático.

Propósito de ingresar a sus equipos de información, a través de la incorporación de virus y/o archivos programa malvados, de tal manera que se altere sus funciones, hacer daño o robar información importante para tu organización, el cual vienen de terceras personas, ajenas a tu empresa, esto es mediante el envío de “virus o archivos programa maligno”, hechos especialmente para esquivar toda medida de seguridad de tus servidores, consiguiendo, dañar toda información que es relevante para tu organización.

1. **Malware:** Es un software malicioso el cual tiene como objetivo el poder infiltrarse a un sistema con el fin de dañarlo.
2. **Virus:** Llámese a todo código el cual infecta a todo archivo del sistema a través de un código maligno, se requiere que el usuario lo ejecute para que funcione.
3. **Gusano:** Es un software que infecta el equipo su acción es que utilizan copias de sí mismo para luego difundirlas mediante la red.
4. **Troyanos:** Tiene el objetivo de abrir un acceso favoreciendo una entrada para otros programas maliciosos.
5. **Spyware:** El objetivo principal es extraer toda información, además de poder incluso instalar más programas sin poder darnos un aviso previo.
6. **AdWare:** Es mostrar publicidad de forma invasiva, llegando a recopilar así como de transmitir todo datos estudiando el accionar de usuarios y brindar orientación mucho mejor todo tipo de publicidad.
7. **Ransomware: S**ofisticados y modernos malwares, su objetivo es secuestrar datos (encriptándolos) pidiendo rescate por ello.

8. **Phishing:** Desarrolla múltiples técnicas de “Ingeniería social” por ejemplo suplantar identidades, con la meta de tener data privadas de los afectados.
9. **Denegación de servicio distribuido (DDoS): Tiene** el objetivo de solicitar peticiones del servidor, pretendiendo que colapse o se pueda bloquee.
10. **Inyección SQL o SQL Injection:** “Se trata de un método de ataque que está en pleno auge, debido a todo el desarrollo que ha habido en tecnologías de servicio web. Este tipo de exploit se conecta a la base de datos de la víctima a través de aplicaciones Web vulnerables, inyectando instrucciones maliciosas a la base de datos, las cuales permiten realizar desde modificaciones en los registros hasta ejecutar otros comandos en el sistema operativo base” (Garcia Moran, y otros, 2011 pág. 116).
11. **Whaling o “caza de ballenas”:** Son ataques dirigidos a perfiles C-Level,(Chief Executive Officer (CEO), Chief Operating Officer (COO), Chief Marketing Officer(CMO), Chief Financial Officer(CFO) , Chief Digital Officer(CDO), etc. Tienen la meta de sustraer credenciales de un alto nivel, toda información muy crítica o de clonar todas sus identidades para Phising.

2.3.4 Protocolos de seguridad de la información.

Los protocolos de seguridad web; viene hacer el conglomerado de reglas que tienen injerencia dentro respecto a la transmisión de data que existe la comunicación de dispositivos para realizar una confidencialidad hace hincapié a la protección de toda información frente a su divulgación a entidades o individuos no autorizados, integridad de datos es considerada como la protección todo datos frente a la modificación, supresión, duplicación o reordenación hecha por entidades que no están autorizadas. Implementar un mecanismo de seguridad es un proceso que se realiza con los siguientes pasos:

Cifrado

Firma digital

Control de acceso

Intercambio de autenticación

Tráfico de Relleno

Los protocolos de Seguridad Web tienen el propósito de ser capaces de cuidar la información brindando la confidencialidad que merecen.

a) Criptografía (Cifrado de datos). - Permite modificar la data de tal modo que, si un individuo no autorizado a acceder a la data cifrada, cifrará el mensaje enviado por el remitente, pero transpondrá el mensaje oculto hasta que el mensaje llegue a su destino y pueda descifrarse.

b) Lógica (Estructura y secuencia). Guarde la secuencia de grupos de datos de mensajes, el significado del mensaje y sepa cuándo se envió el mensaje.

c) Autenticación. - Es una forma de autenticación de identidad, una técnica utilizada para verificar que el interlocutor es quien se supone que es y no un impostor.

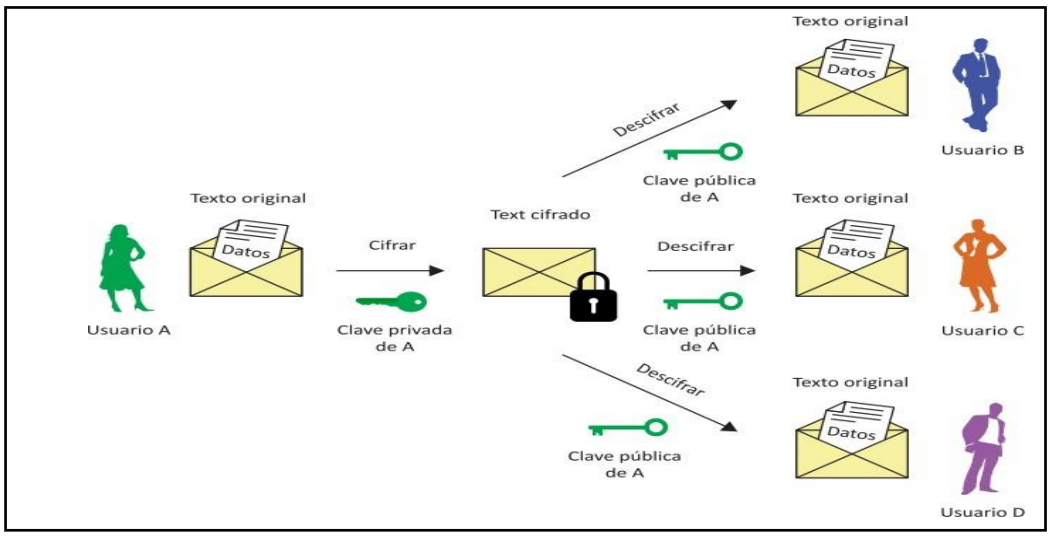

Figura 2: Modelo de cifrado con criptografía de clave pública (para proporcionar autenticación).

Fuente: Modelo de cifrado con criptografía de clave pública (para proporcionar autenticación), (Soriano pág. 51)

2.3.5 Estructura Conceptual del Sistema de Comunicación.

La conexión al sistema integrado de comunicaciones se basará en un centro de mando que conecta toda la información necesaria con las políticas y estrategias de todas las sedes regionales. La arquitectura de tecnología y comunicaciones define las relaciones entre sistemas, subsistemas, tecnologías (instrumentos o herramientas), aplicaciones y comunicaciones en un entorno de sistema de comunicaciones integrado. La solución técnica utilizada es una infraestructura de servicios web, que es informática distribuida rápida y eficiente utilizando estándares abiertos como XML, http y PHP. Implemente llamadas a métodos remotos entre aplicaciones empresariales.

2.3.6 Sistema de Seguridad (Intelligent ICI ConstrolsInc).

En los servidores web, por su estructura, abren una ventana entre tu red y el mundo. La protección que tengas con el mantenimiento, la actualización y la codificación de tu página web definirá el tamaño de dicha ventana. Hay que hacer hincapié que toda seguridad web puede ser relativa y siempre deberá de estar acompañada de dos elementos: uno interno y uno público.

La ciberseguridad es relevante porque los sitios web que no están protegidos estarán vulnerables de sufrir acontecimientos como:

- Hurto de información que se almacena en el servidor web.
- Toda data personal llámese direcciones de email hasta información de transferencias por pago a terceros para luego ser utilizarlos de manera inadecuada (robo de la identidad, tipos de extorsiones, exceso o abuso de confianza, otras estafas, etc.).
- Redirigir páginas web inadecuadas y maliciosas.
- Dar a conocer anuncios que no se desean.
- Enviar datos falsos a los bots y/o rastreadores de los motores de búsqueda para hacer SEO de “sombrero negro” (Black Hat SEO), siendo objetivo de atraer el tráfico a lugares web que no se ajustan a las prácticas de de la web.

- Hacer uso de las computadoras de los foráneos para hacer minería de criptomonedas.
- Ser receptores de ataques DDoS que pudieran atentar tu página haciendo que deje de funcionar inesperadamente, volviéndola inaccesible para los foráneos.
- Hacer descargas de software mal intencionados.

2.3.7 Tipos de Espías.

1. **Espionaje industrial.**

   Se extrae de forma ilícita toda información sobre la investigación, desarrollos y proyectos; para tener toda la ventaja de su competidor en el mercado, en tanto que el informático obtiene la data personal e intelectual.

2. **Espionaje informático.**

   Se utiliza programas del tipo spyware, que son instalados en todos nuestros dispositivos sin autorización que hacen un seguimiento de todos los movimientos de todo usuario conectado a la red para asi obtener todo un perfil de tipo comercial completo de ellos, estos programas se apropiarse de la información de las personas, así como de su información a su vez es transferida a la sede de una organización de espías con el fin de ser puesta en venta.

   Los crackers. - Son todos aquellos individuos que buscan fastidiar a otros, piratear software que están protegidos por leyes, eliminar sistemas complejos a través de virus, etc. Jóvenes con ganas de explorar de manera rápida este oficio.

2.3.8 Ataques a Nuestra Información.

Son realizados comúnmente por trabajadores internos que utilizan de mala manera sus permisos para el acceso, o personas externas que ingresan remotamente o interceptan el tráfico de la red. Además cuentan

con sistemas para pasar desapercibido y así no detecta movimientos que sospechen de eso ataques.

.

2.3.9 Métodos y Herramientas de Ataque.

Los ataques involucraban muy poca sofisticación técnica. Los insiders (empleados que no estaban conformes o personas externas a la empresa con acceso al sistemas dentro de la organización) utilizaban de mala manera sus permisos para así alterar los archivos o los registros.

Eavesdropping y PacketSniffing.

Siendo vulnerables al eavesdropping, o la pasiva intercepción (sin modificación) del tráfico de red (Se ha convertido en parte de la jerga habitual en criptografía y se refiere a ataques de escuchas, tanto sobre medios con información cifrada, como no cifrada.).

En Internet esto es realizado por packetsniffers, conocidos como programas que monitorizan los paquetes de red que están direccionados al pc donde se encuentran instalados. El sniffer es ubicado en una estación de laboral interconectada a red, como en un equipo de router o tambien en un gateway de Internet, siendo ejecutado por un usuario con acceso legítimo, o por un individuo que ha podido entrar por otros medios.

Topología de red y packetsniffers

La cantidad de tramas que puede obtener un sniffer va a depender de la topología de red, del nodo donde esté instalado y del medio de transmisión

Búsqueda de sniffers.

Existen varios métodos para localizar un rastreador y difieren dependiendo de si tiene acceso local a la máquina o necesita encontrarlos en una máquina remota. El propósito de la mayoría de las pruebas es que una máquina con una NIC en el modo incorrecto muestre

que está accediendo a datos que no desea y, por lo tanto, tiene un rastreador. Se trata de un objetivo ambicioso y difícil, que lamentablemente puede resultar imposible. A veces es completamente imposible detectar el olfateo. Por ejemplo, si un rastreador solo está diseñado para esta tarea (generalmente hardware), nunca devuelve un paquete, nunca establece una conexión, sino que siempre permanece en silencio y es simplemente imposible de detectar de forma remota. Este tipo de sniffer sólo se puede detectar inspeccionando directamente los dispositivos conectados a la red.

Técnicas de detección local.

Esta no es una tarea fácil, pero encontrar a los mirones es lo más fácil en esta situación. Normalmente es suficiente comprobar la lista de programas en ejecución para detectar anomalías (CTRL+ALT+SUPR). Otro punto de partida es el archivo de PC en sistemas Unix, como /etc/rc.d/rcX.d/* o .bashrc, y el autoexec.bat o inicio automático cuando habilitas ciertas claves de registro. Tengo una lista de programas que lo hacen. Computadoras con Windows) o tareas programadas (cron, at).

Los nuevos desarrollos y anomalías deben investigarse en detalle, ya que pueden revelar no sólo rastreadores activos sino también otros programas (virus, troyanos, gusanos, etc.) que representan una amenaza importante.

Las máquinas con sistemas operativos de la familia Unix tienen utilidades que son especialmente útiles para combatir los rastreadores. Este es ifconfig, un comando que informa el estado de todas las interfaces de red en un sistema y si alguna de ellas está en modo promiscuo. Obviamente, este método de detección de rastreadores locales depende de que el comando ifconfig funcione correctamente.

Detección remota desde el mismo segmento de red.

Este es el entorno que los administradores de seguridad deben investigar con mayor frecuencia. Existen muchas técnicas heurísticas útiles, que se enumeran a continuación. Sin embargo, es importante comprender que estas técnicas tienen algunas limitaciones y que no es

del todo posible que un rastreador esté presente en la red y pase desapercibido (falso). negativo), o una máquina o usuario completamente benigno es reconocido como fisgón (falso positivo). Según su alcance, estas tecnologías se pueden dividir en dos grupos: dependientes del sistema operativo e independientes del sistema operativo.

a) Test de Detección de Sniffer (DNS)

Algunos sniffers realizan búsquedas inversas DNS en los paquetes que capturan. En el momento que se realiza una búsqueda inversa DNS, una utilidad de detención de sniffers "huele" el pedido de las operaciones de búsqueda para poder ver si el objetivo es el que solicita el petición del host inexistente.

d) Política de seguridad.

Son procedimientos que se realizan como soporte a la seguridad, para la implementación de las políticas de seguridad se aplican diferentes mecanismos para prevenir y detectar la intrusión.

Los mecanismos de prevención se aplican antes de que ocurra un incidente, deliberadas vinculaciones a la catástrofe originada por incendios, inundaciones o destrucción de soportes informáticos.

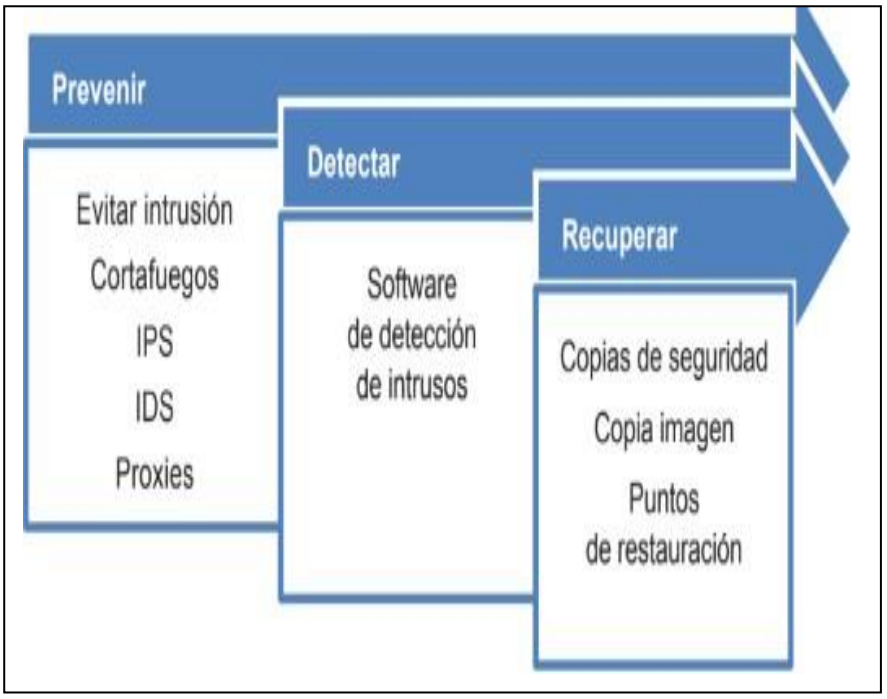

Figura 3: Mecanismos para prevenir, detectar y recuperar la normalidad del funcionamiento del sistema en caso de una intrusión no planificada.

Fuente: (Postigo Palacios, 1° edicion 2020 pág. 6)

Protocolo de Transmission Control Protocol/Internet Protocol (Protocolo de control de transmisión/Protocolo de Internet)- TCP/IP.

Es un grupo de protocolos de red que se rigen a la especificación del modelo OSI el cual se usa para establecer cierta comunicación de data entre dispositivos que están conectados mediante varias redes. “TCP/IP se divide en 4 fases, y aunque son varios los protocolos que involucran a alguna de estas fases, son protocolo TCP y el protocolo IP los más conocidos y, es por eso, que manejan el nombre al conjunto.” (Villada Romero, 2014).

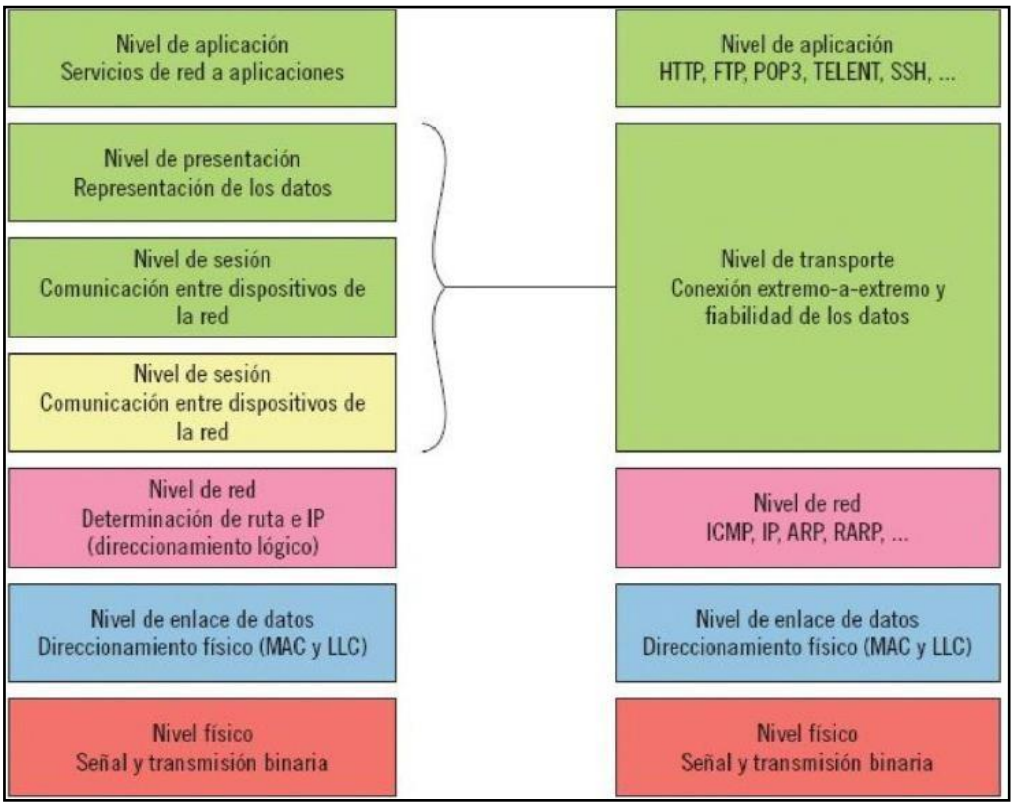

Figura 4: Equivalentes De Capas Entre Tcp/Ip Y El Modelo Osi

Fuente: (Villada Romero, 2014)

Es muy importante los controles internos informáticos, la implementar en diferentes niveles, esto permite analizar diversos elementos para una buena configuración en el sistema con la finalidad de identificar los elementos, productos, herramientas y asi identificar posibles riesgos en el entorno red, aplicaciones seguridad del ordenador.

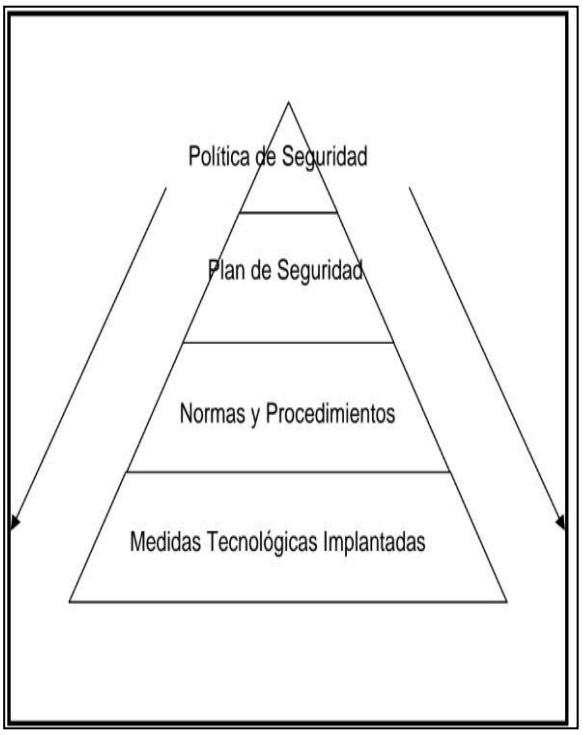

Figura 5: Implantación De Política Y Cultura Sobre Seguridad

Fuente: (Piattini Velthuis, y otros pág. 12).

2.4 Definición de términos básicos

2.4.1 **Snooping y Downloading:** Esta categoría de ataques tiene el mismo objetivo de espiar la información sin cambiarla. Sin embargo, los métodos son diferentes.

2.4.2 **Tampering o Data Diddling**: Esta categoría se refiere a cambios no autorizados en datos o software instalados en el sistema, como la eliminación de archivos.

2.4.3 **Spoofing:** Esta tecnología se utiliza para actuar en nombre de otros usuarios, normalmente realizando tareas de manipulación o espionaje. Unaforma común de suplantación de identidad implica obtener un nombre de usuario y una contraseña legítimos después de iniciar sesión en un sistemapara realizar una acción, como enviar un correo electrónico falso.

2.4.4 **Switch:** Un conmutador o conmutador de red es un dispositivo de conectividad que se utiliza para conectar todas las computadoras en una

red.Incluye computadoras, consolas, impresoras y servidores.

2.4.5 **Centro de cómputo:** Este se lleva a cabo mediante la utilización de los ordenadores los mismos que están equipados con el hardware y el softwareque son necesarios para poder cumplir con dichas actividades.

2.4.6 **Host:** Especifica el host y el número de puerto del recurso que está siendo solicitado. Esto permite al servidor origen o pasarela diferenciar entre URL que son internamente ambiguas.

2.4.7 **Seguridad**: Definido como la habilidad de poder identificar y eliminar todas las vulnerabilidades

2.4.8 **Contraseña:** Es una forma de autenticar que utiliza toda información que essecreta para poder controlar el acceso a algún recurso.

2.4.9 **Servidor:** Es un equipo informático que hace de intermediario entre las conexiones de un cliente y un servidor de destino, filtrando todos los datos**.**

2.4.10 **Un servidor proxy:** Es una tecnología que se utiliza como puente entre el origen (un ordenador) y el destino de una solicitud (Internet).

2.4.11 **Nube:** Hace mención a los servidores que son accesibles mediante el Internet, y al software y bases de datos que son ejecutados en los servidores.

2.4.12 **Hosting:** Es un servicio online el cual hace que se pueda ingresar a tu sitio web en Internet.

2.4.13 **Amenaza:** Situación o también llamado acontecimiento capaz de causar undaño a todo bien informático.

III. HIPÓTESIS Y VARIABLES

3.1 Hipótesis general

Un sistema de seguridad de la información optimiza los servidores web en la OTIC de la FIIS de la UNAC 2022.

3.1.1 Hipótesis específicas.

a) Un sistema de seguridad de la información optimiza la funcionalidad de los servidores web en la OTIC de la FIIS de la UNAC 2022?

b) Un sistema de seguridad de la información optimiza la fiabilidad de los servidores web en la OTIC de la FIIS de la UNAC 2022?

c) Un sistema de seguridad de la información optimiza la usabilidad de los servidores web en la OTIC de la FIIS de la UNAC 2022?

d) Un sistema de seguridad de la información optimiza la eficiencia de los servidores web en la OTIC de la FIIS de la UNAC 2022?

e) Un sistema de seguridad de la información optimiza la portabilidad de los servidores web en la OTIC de la FIIS de la UNAC 2022.

3.2 Operacionalización de las variables.

Variables Independiente:

Seguridad de la Información

Variable Dependiente

Servidores Web

Tabla 01: Operacionalización de la Variable independiente

.

Variable	Definición Conceptual	Definición Operacional	Dimensiones	Indicadores	Método/Técnica
Variable Independiente SEGURIDAD DE LA INFORMACIÓN	La seguridad de la información es el conjunto de medidas y técnicas utilizadas para controlar y salvaguardar todos los datos que se manejan dentro de la organización y asegurar que los datos no salgan del sistema que ha establecido la organización.	La Seguridad de la Información ha crecido mucho en estos últimos tiempos, además ha evolucionado considerablemente. Se ha convertido en una carrera acreditada mundialmente. Dentro del éste área se ofrecen muchas especializaciones que se pueden incluir al realizar la auditoría del Sistema de Gestión de Seguridad de la Información ISO-27001, como pueden ser: Planificación de la continuidad de negocio Ciencia forense digital Administración de Sistemas de Gestión de Seguridad.	Confidencialidad	NS= % CONTROL DE ACCESO+ % AUTENTICACIÓN + % AUTORIZATIÓN	Método: Deductivo Técnica: Entrevista Instrumento: Cuestionario
			Integridad	NS= % SEGURIDAD DE COMUNICACIÓN + % SEGURIDAD DE PROCEDIMIENTO + % PROTECCIÓN	
			Disponibilidad	NS= %CONTINUIDAD DE LA REGLA DEL NEGOCIO+ % ACCESS EN EL TIEMPO REQUERIDO + % ACCESS A LA INFORMACIÓN	

Fuente: Elaboración Propia

Tabla 02: Operacionalización de la Variable dependiente

Variable	Definición Conceptual	Definición Operacional	Dimensiones	Indicadores	Método/Técnica
Variable Dependiente SERVIDORES WEB	Un servidor web (server) es un ordenador de gran potencia que se encarga de "prestar el servicio" de transmitir la información pedida por sus clientes (otros ordenadores, dispositivos móviles, impresoras, personas, etc.	Un servidor web es un software y un hardware que utiliza el protocolo HTTP (Hypertext Transfer Protocol) y otros protocolos para responder a las peticiones de las clientes realizadas a través de la World Wide Web. La principal función de un servidor web es mostrar el contenido de un sitio web almacenando, procesando y entregando las páginas web a los usuarios.	Funcionalidad	EXACTITUD INTEROPERABILIDAD	Método: Deductivo Técnica: Entrevista Instrumento: Cuestionario
			Fiabilidad	RECUPERABILIDAD TOLERANCIA A FALLOS	
			Usabilidad	OPERABILIDAD ATRACTIVIDAD	
			Eficiencia	COMPORTAMIENTO EN EL TIEMPO COMPORTAMIENTO DE RECURSOS	
			Portabilidad	ADAPTABILIDAD CAPACIDAD DE REEMPLAZAMIENTO	

Fuente: Elaboración Propia

IV. METODOLOGÍA DEL PROYECTO.

4.1 Diseño de Investigación.

Se describe el proceso que se diseñó para lograr los objetivos planteados en la investigación.

La presente investigación es de tipo aplicada y descriptiva, de qué manera se manifiestan las variables y sus propiedades, así como se recolecta información sobre cada una de ellas.

Por ello será de tipo descriptiva en la cual se muestran y se identifican hechos, situaciones, rasgos, características de un objeto de estudio.

4.2 Método de investigación.

El método de investigación es deductivo, es de cuantitativo, debido a que se les asignará un valor numérico a los hallazgos, de la misma forma se presentarán cuadros estadísticos descriptivos de la variable de estudio.

Los diseños de investigación se crean a través de encuestas. Se utiliza una herramienta de evaluación para mostrar y analizar la investigación realizada en formato tabular. Se analizan variables y se utilizan herramientas de evaluación.

En esta investigación, el diseño es experimental, porque es el proceso de someter un objeto o grupo de personas a ciertas condiciones, estímulos o tratamientos de variables independientes y luego aplicar medidas para determinar su efecto sobre la variable dependiente observada. (Fidias G. Arias, 2012).

4.3 Población y muestra.

Población.

Este estudio limita su ámbito de trabajo en la UNAC, en la FIIS; la OTIC que da servicio de información y soporte tecnológico a las diversas oficinas y/o dependencias; siendo un total de 30 trabajadores administrativos, a los cuales se les hará una encuesta.

Muestra.

Consideramos en esta investigación, una muestra de 12 trabajadores administrativos.

4.4 Lugar de estudio y periodo desarrollado.

El presente estudio se desarrollará en la UNAC, en la OTIC de la FIIS, con una duración de 6 meses.

4.5 Técnicas e instrumentos para la recolección de la información documental.

La técnica utilizada en esta investigación, considerando tiempo y recursos limitados, fue creada a partir de una encuesta realizada al personal administrativo de la FIIS.

Se aplicó un cuestionario prediseñado en base a los objetivos de la investigación para permitir la captura directa de información para su procesamiento y resultados.

“El cuestionario deberá de tener en consideración el diseño de la investigación, quiere decir el planteamiento y formulación del problema los objetivos la hipótesis y variables” (Naupas, y otros, 2014 pág. 211).

“Una encuesta consta de un grupo de preguntas que están destinadas a originar que los datos necesarios para alcanzar todos objetivos de una investigación. Es un plan formal para recopilar información de la unidad de análisis y centro de la pregunta de investigación en estudio. Las encuestas generalmente consisten en un conjunto de preguntas respecto a una o más variables que se están midiendo. Las encuestas le permiten estandarizar y unificar su proceso de recolección de data. Un diseño que no es adecuado lleva a información que no es completa, recopilación de datos inexacta y, por supuesto, a la generación de información nada confiable” (CÉSAR AUGUSTO , 2006 pág. 217)

4.6 Análisis y procesamiento de datos.

Para la investigación se hizo el tratamiento estadístico y se realizó la recopilación de la data, agrupándola y se desarrollaron los estadísticos utilizando el programa Excel y el Programa Estadístico SPSS 17. Siendo necesario la elaboración de las tablas de frecuencia apreciándose la data que se tienen en forma de cantidades, así como porcentualmente, y a-posteriori se presenten las gráficas que le corresponde a la información que se obtuvo para después realizar una descripción de la interpretación de la información.

4.7 Aspectos Éticos en Investigación.

El desarrollo de este estudio respondió a la originalidad, la transparencia así como a la objetividad, con obligaciones éticas y morales y respetando las políticas y lineamientos marcados por la UNAC. Durante el desarrollo se informó al Departamento de Ingeniería de Sistemas e Ingeniería Industrial de la UNAC sobre las investigaciones y procedimientos realizados. Como investigadores, nos esforzamos por mantener la precisión de nuestros resultados y la credibilidad de la Universidad.

4.8 Situación actual de la Oficina de Tecnologías de Información y Comunicaciones de la Facultad de Ingeniería Industrial y de Sistemas.

En la actualidad la OTIC de la FIIS, cuenta con una oficina donde se encuentra una computadora que hace la función de servidor y brinda el servicio a los 4 laboratorios de cómputo, áreas y/o dependencias, brindando el soporte técnico para el desarrollo de clases de pregrado y el soporte tecnológico a las oficinas del segundo y tercer piso.

La OTIC de la FIIS; en la actualidad tiene problemas de almacenar y distribuir la información hacia los usuarios y/o dependencias; no cuenta con un servidor con tecnología de punta para un buen funcionamiento para brindar un buen servicio y la seguridad de la información en los servidores web. Se requiere un servidor basado en hardware, una máquina física que deberá de

ser integrada en una red de tipo informática que brinda un servicio especial que otros programas nombrados modelo cliente-servidor.

Figura 6: Área del servidor

Fuente: Elaboración propia.

Figura 7: Gabinete

Fuente: Elaboración propia.

Figura 8: Laboratorio de Computo de la FIIS

Fuente: Elaboración propia.

4.9 Propuesta de implementación de un sistema de seguridad de la información para optimizar los servidores web en la oficina de Tecnologías de Información y Comunicaciones de la Facultad.

Actualmente el mundo enfrenta un desarrollo estrepitoso secundado por las tecnologías nuevas, con gran influencia de las TI y las comunicaciones, permitiendo a todos los usuarios a acceder a los recursos remotos para asi tomar todo control de estos sin tener la necesidad de una presencia física.

En este estudio nos muestra la manera de optimizar los llamados tiempos para el procesamiento y su despliegue de información en el navegador Web de un Sistema, utilizando sencillas configuraciones en el servidor Apache. Estas configuraciones hachas son específicamente en base a la compresión de data y manejo de caché. El ahorro de tiempo incide directamente en una mejor percepción de parte de todo usuario referente a la usabilidad del sistema.

Se considera los requisitos de hardware:

4.9.1 Servidor en la nube.

Se debe considerar el Servidor centralizado en la red de internet y de acceso público limitado y acceso diferencial institucional. Se debe indexar todos los dominios institucionales respaldados previamente por el software Orca Security para el acceso del personal estudiantil, docente, administrativo y público; cada uno con sus espacios dirigidos.

Capacidad de cifrar el contenido de alta prioridad con el software Axcrypt, la llave de encriptado que genere, pasará a posesión del departamento asignado para la propiedad intelectual y acto seguido eliminarse de la base de datos.

4.9.2 Ordenador Especializado:

La computadora aislada de los servidores principales, con el único propósito de almacenar las llaves que descifran la información encriptada por Axcrypt.

Tener una ubicación privilegiada con seguridad y buenas condiciones de calefacción e iluminación, además de acceso solo a personal autorizado. Contar con el almacenamiento del orden de terabytes para poder abastecer de almacenamiento a los proyectos que requieran software especializado.

Se considera los rrequisitos de software:

4.9.3 Agente de seguridad en la nube orca security.

Este programa permite la protección de más de 100 activos tecnológicos en la nube sin la necesidad de omitir algunos de ellos, lo que agiliza la carga de trabajo, de la misma manera, toda data recabada en la nube se exportar y se comparte con mucha facilidad con otras demás personas y los usuarios pueden destacar esta función frente a otras.

Reconocer programas maliciosos (malware).

- Dar reconocimiento de vulnerabilidades.
- Hacer una evaluación de las contraseñas que son débiles.
- Organizar todos los riesgos dependiendo de sus características.
- Tener acceso a sus datos mediante una interfaz de usuario reconocido y amigable.

4.9.4 Programa de encriptado axcrypt

Software para el sistema operativo Windows orientado a codificar y encriptar archivos mediante un algoritmo (AES-128 y SHA-1) a su vez que genera un archivo llave para poder revertir la encriptación del archivo.

Estar implementado tanto en las funciones del servidor como en el ordenador especializado

Debe estar configurado para solo ser aplicado cuando sea solicitado para archivos de alta importancia.

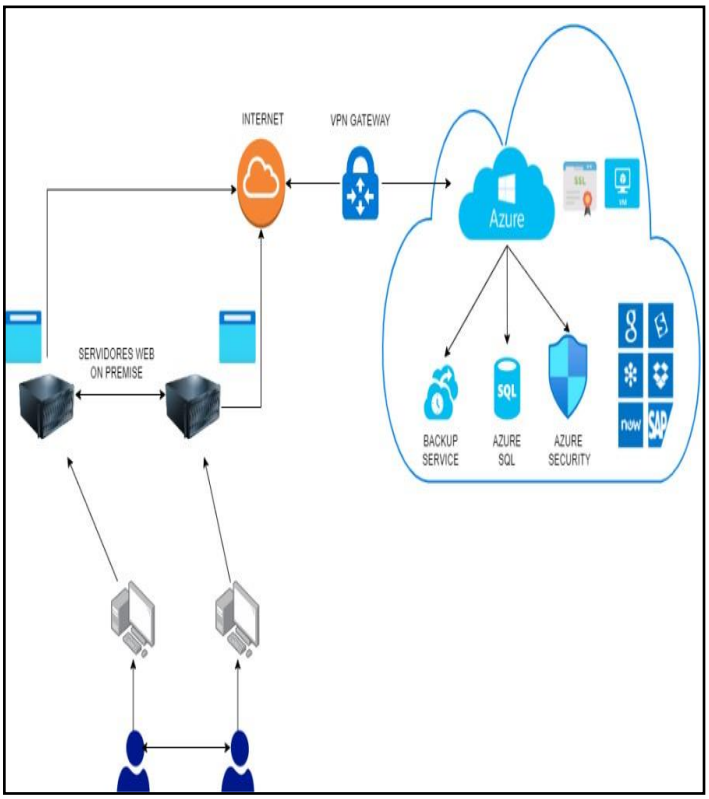

Figura 9: En La Implementación Se Diseña La Siguiente Arquitectura

Fuente: Elaboración propia.

Para lograr la migración de los servicios web de la facultad hacia la nube de Azure, se debe crear una cuenta en la nube de Azure para crear los recursos y migrarlos. Una vez tenido la cuenta, se debe crear una red virtual, y en ella una subred la cual será la misma que se usará en nuestros servidores OnPremise. Para la conexión segura, se debe crear en la nube una VPN que servirá como Gateway para la réplica de los datos. Después de ello, se generará los certificados que serán para la autenticación del personal administrativa para conectarse a la red virtual de la facultad mediante una conexión VPN de punto a sitio. Es aquí, en la configuración de la VPN donde se selecciona el protocolo IKEv2 y SSTP (SSL), que es un protocolo de túnel basado en IPSEC.

Seguido, se implementa una máquina virtual de imagen Windows Server 2019 que estará segmentada bajo la red creada. Este servidor será llamado “Servidor de Configuración”

A continuación, se prepara el servidor de configuración en la máquina virtual creada. Aquí se instalará el recurso de SQL Database donde se almacenará toda la información que recabe de lo servicios web y sus procesos respectivos. Asimismo, para que estos datos sean resguardados continuamente y el personal administrativo pueda realizar sus copias de seguridad o backup, se creara una cuenta de almacenamiento o “Azure Storage” que servirá además de lo mencionado, acceder desde cualquier parte a los datos a través de HTTP o HTTPS con una conexión segura y establecida.

Además, para que haya una replicación de los cambios desde lo servidores OnPremise a la nube o viceversa, se habilita la replicación mediante el recurso de almacén de Recovery Services, donde se elegirá el punto de origen y destino para la réplica; en este caso será la máquina virtual como origen y destino nuestro servidor OnPremise.

4.9.5 Procesos de un sistema de seguridad de la información en la Oficina de Tecnología de Información y Comunicación de la Facultad.

En la actualidad la información tiene un rol muy importante dentro de las organizaciones. La información y los procesos sustentan el sistema. Esto requiere protección contra amenazas a la integridad de la información, la confiabilidad y la estabilidad del proceso. Actualmente, los sistemas informáticos están expuestos a posibles amenazas a la seguridad informática, riesgos físicos, acceso no autorizado a la información, desastres naturales, sabotajes, incendios, accidentes y códigos maliciosos.

1. **Compromiso con la OTIC de la FIIS.**

   La OTIC; brindara las responsabilidades de seguridad de la información en los servidores webs:

   a) Formulación y aprobación de políticas de seguridad de la información.
   b) Implementación de las políticas de seguridad de la información.
   c) Proporcionar los recursos de hardware y software necesario para la seguridad de la información en los servidores webs.
   d) Aprobar la asignación de papeles específicos y responsabilidades en la SI.
   e) Hay que asegurar que los controles de seguridad informática sean coordinados con todas las áreas de la Facultad.

2. **Identificación de las amenazas sobre el sistema informático en OTIC-FIIS.**

   Es importante localizar toda amenazas sobre éstos y calcular el daño el cual puede causar el que se materialice. Es fundamental la seguridad son la confidencialidad, la integridad y la disponibilidad de la información en los servidores webs, porque se debe establecer cada una de la amenaza sobre la base de cómo se pueda ver afectada la información. Siendo las más comunes:

a) Perder información.
b) La corrupción, así como la modificación de información.
c) Robo, alterar o extravío de pc y/o sus componentes.
d) Difusión de información.
e) Interrumpir los servicios.

3. **Evaluación del riesgo sobre los bienes informáticos de la Oficina de Tecnología de Información y Comunicación de la Facultad.**

   El riesgo de cada activo informático se considera como la probabilidad de que ocurra una amenaza que afecte a ese activo. Aunque una amenaza puede afectar a múltiples activos de TI con la misma probabilidad, el resultado no es necesariamente el mismo dependiendo de la criticidad de cada activo. La evaluación de riesgos le permite conocer sus recursos técnicos e identificar qué áreas tienen mayor riesgo.

   Esto permite seleccionar e implementar adecuadamente los controles de seguridad, asegurando la correcta proporcionalidad a través de adecuadas relaciones costo/beneficio.

4. **Evaluación de la situación actual sobre la Seguridad Informática.**

   En la evolución de la tecnología de la información, no existe ningún diseño de sistema de SI que tenga en consideración de manera integral todos los factores que deben de tener en cuenta.

   Se debe considerar la implementación de estándares, medidas y procedimientos de seguridad específicos para mitigar las vulnerabilidades.

   La eficacia de los controles existentes debe evaluarse críticamente. Los resultados de este estudio ayudarán a guiar y determinar las acciones y prioridades de gestión adecuadas para abordar los riesgos de seguridad informática y los controles seleccionados para protegerlos.

La evaluación de las necesidades de protección considerada en esta sección debe conducir a la definición de los siguientes aspectos clave:

1. Qué recursos de TI es más importante proteger

2. Qué amenazas tienen más probabilidades de afectar sus recursos de TI y su impacto potencial en su negocio

3. Qué áreas están sujetas a mayores ponderaciones de riesgo y qué amenazas motivan esas áreas.

5. **Que controles de seguridad deben ser perfeccionados.**

Es importante la organización, planificación de identificar todo requisito de seguridad de la organización.

a) Establecer los tipos de protección de la información y la identificación de las amenazas a que están sometidos.

b) Evaluación que tan vulnerable y que probable ocurran las amenazas.

c) Determinar los requisitos de seguridad; instituidos por contratos, normas de tipo legal, así como técnicas que debe cumplir la empresa.

- La necesidad de protección de la información.
- Exigencias de la alta dirección.
- La necesidad de procesamiento de información.

Todo requisito de seguridad se logra identificar a través de la evaluar sus riesgos.

6. **Selección de los controles de seguridad informática**.

En la OTIC de la Facultad; Determinar los criterios para determinar si un candidato puede ser contratado o no. Por ejemplo, puede aceptar el riesgo si se establece que es bajo o si el costo del tratamiento no sería beneficioso para su empresa. Para cada riesgo identificado, se toma una decisión sobre cómo abordarlo.

a) aplicación de controles que son apropiados para minimizar todo riesgos.

b) la aceptación de riesgos de manera seria y de forma objetiva sobre las políticas.

c) eludir riesgos, que no permitan acciones que puedan propiciar los riesgos.

7. Políticas de Seguridad Informática.

la Oficina de TIC de la Facultad; Demostrar apoyo, así como compromiso con la SI estableciendo políticas de seguridad que estén en línea con los objetivos de la facultad y publicando y manteniendo estas políticas en toda la institución.

Las políticas de seguridad pueden afectar a todos los profesores y al personal.

El crear una política de seguridad es aprobada por el Decano, quien tiene la autoridad para hacer cumplir la política.

La política de seguridad desarrollada debe ser consistente con las políticas, normas, reglamentos y leyes a las que está sujeta la empresa.

Las políticas deben abordar los problemas planteados por los problemas de seguridad planteados por el sitio remoto, así como los problemas planteados en el sitio remoto por los usuarios o computadoras locales.

Las políticas de seguridad afectan a todo trabajador de las diferentes instalaciones. Por lo tanto, le recomendamos que se asegure de tener los permisos necesarios para su instalación. El crear de una política de seguridad es aprobada por el nivel más alto de liderazgo de la organización que tiene la autoridad para hacer cumplir la política. Las políticas que no se pueden implementar y hacer cumplir son inútiles.

Considera uso apropiado de los SI.

- Tener en consideración todo objeto social de la institución asi como sus características.

- Las políticas de seguridad que se implementen deben estar en línea con las políticas, regulaciones, reglas y leyes por la que la organización está sujeta.
- • Los sistemas informáticos protegidos son completamente separados e independientes. Las implicaciones para la seguridad deben considerarse en un contexto más amplio.

V. RESULTADOS.

5.1 Resultados descriptivos.

Tabla N° 3.

1. ¿ACCEDE CON FRECUENCIA A LA PAGINA WEB DE LA FACULTAD?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Muy frecuentemente	3	13,0	13,0	13,0
	Frecuentemente	5	21,7	21,7	34,8
	Ocasionalmente	12	52,2	52,2	87,0
	Raramente	2	8,7	8,7	95,7
	Nunca	1	4,3	4,3	100,0
	Total	23	100,0	100,0	

Fuente: Elaboración propia.

En la tabla N° 3, la frecuencia mayor es 12 y el porcentaje mayor es 52,2 en la frecuencia de acceso a la página web de la Universidad.

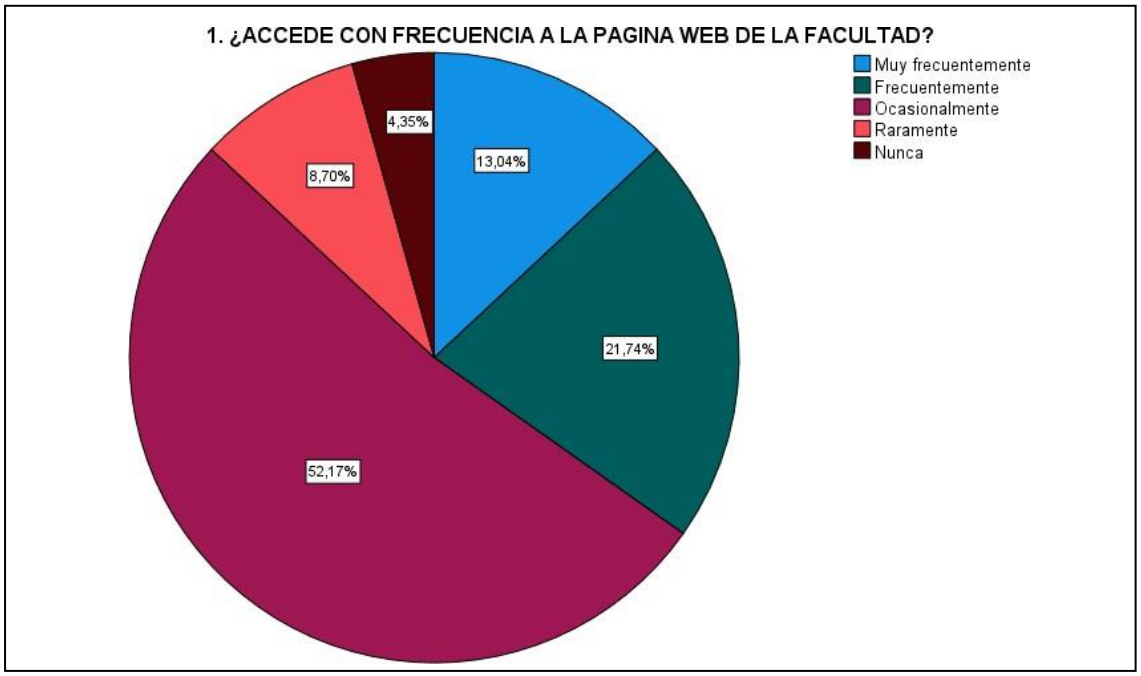

Figura 10: ¿Accede con frecuencia a la página web de la facultad?

Fuente: Elaboración propia.

Tabla N° 4.

2. ¿LA INFORMACIÓN QUE CONTIENE LA PÁGINA WEB DE LA FIIS ESTA ACTUALIZADA Y ORGANIZADA?					
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Muy frecuentemente	2	8,7	8,7	8,7
	Frecuentemente	5	21,7	21,7	30,4
	Ocasionalmente	10	43,5	43,5	73,9
	Raramente	5	21,7	21,7	95,7
	Nunca	1	4,3	4,3	100,0
	Total	23	100,0	100,0	

Fuente: Elaboración propia.

En la tabla N° 4, la frecuencia mayor es 12 y el porcentaje mayor es 52,2 en la frecuencia de acceso a la página web de la Universidad.

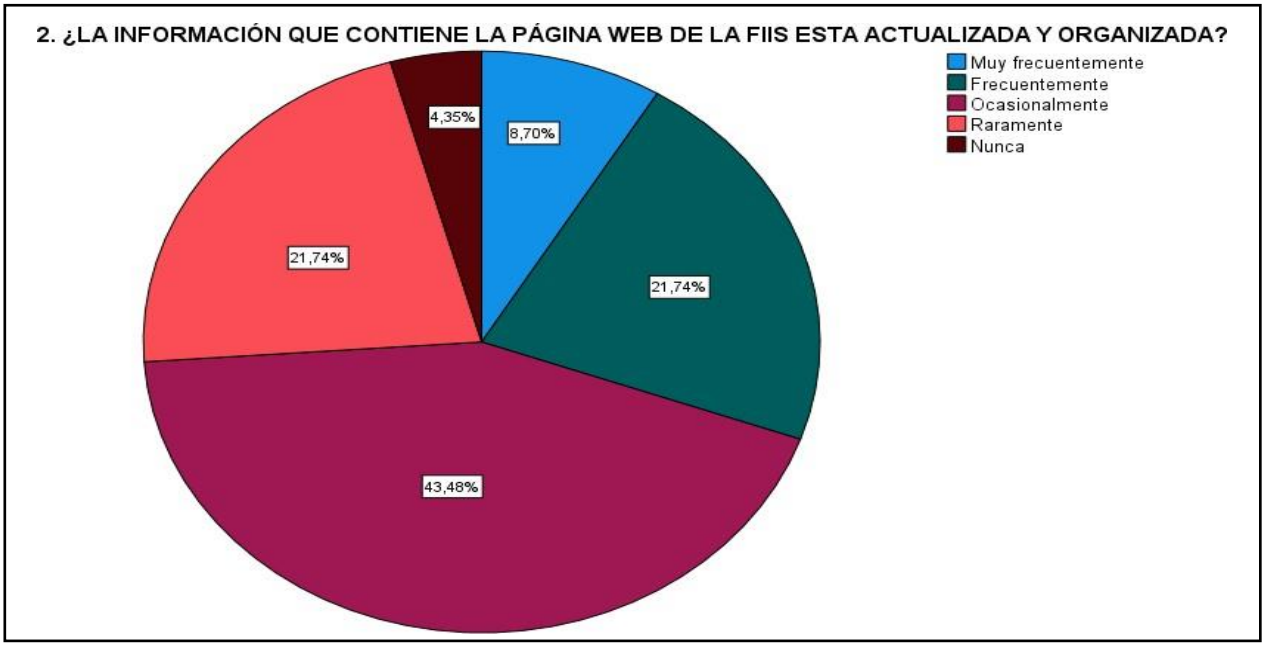

Figura 11: ¿La información que contiene la página web de la FIIS está actualizada y organizada?

Fuente: Elaboración propia.

Tabla N° 5

3. ¿EN LA FACULTAD EXISTE UN BASE DE DATOS CENTRALIZADA ACTUALIZADA?					
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Muy frecuentemente	2	8,7	8,7	8,7
	Frecuentemente	9	39,1	39,1	47,8
	Ocasionalmente	5	21,7	21,7	69,6
	Raramente	2	8,7	8,7	78,3
	Nunca	5	21,7	21,7	100,0
	Total	23	100,0	100,0	

Fuente: Elaboración propia.

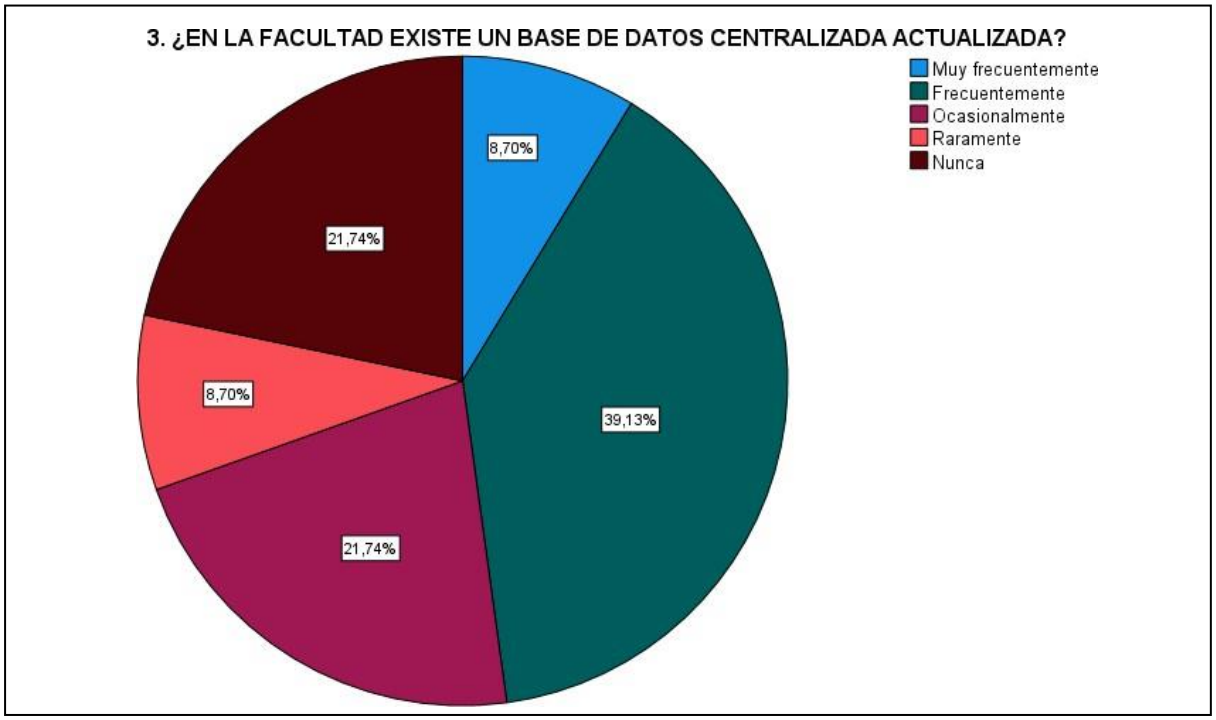

Figura 12: ¿En la facultad existe una base de datos centralizada actualizada?

Fuente: Elaboración propia.

Tabla N° 6.

4. ¿LA INFORMACIÓN EN LA PÁGINA WEB DE LA FIIS CUMPLE CON LOS REQUISITOS MÍNIMOS DE SEGURIDAD?					
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Muy frecuentemente	2	8,7	8,7	8,7
	Frecuentemente	8	34,8	34,8	43,5
	Ocasionalmente	8	34,8	34,8	78,3
	Raramente	3	13,0	13,0	91,3
	Nunca	2	8,7	8,7	100,0
	Total	23	100,0	100,0	

Fuente: Elaboración propia.

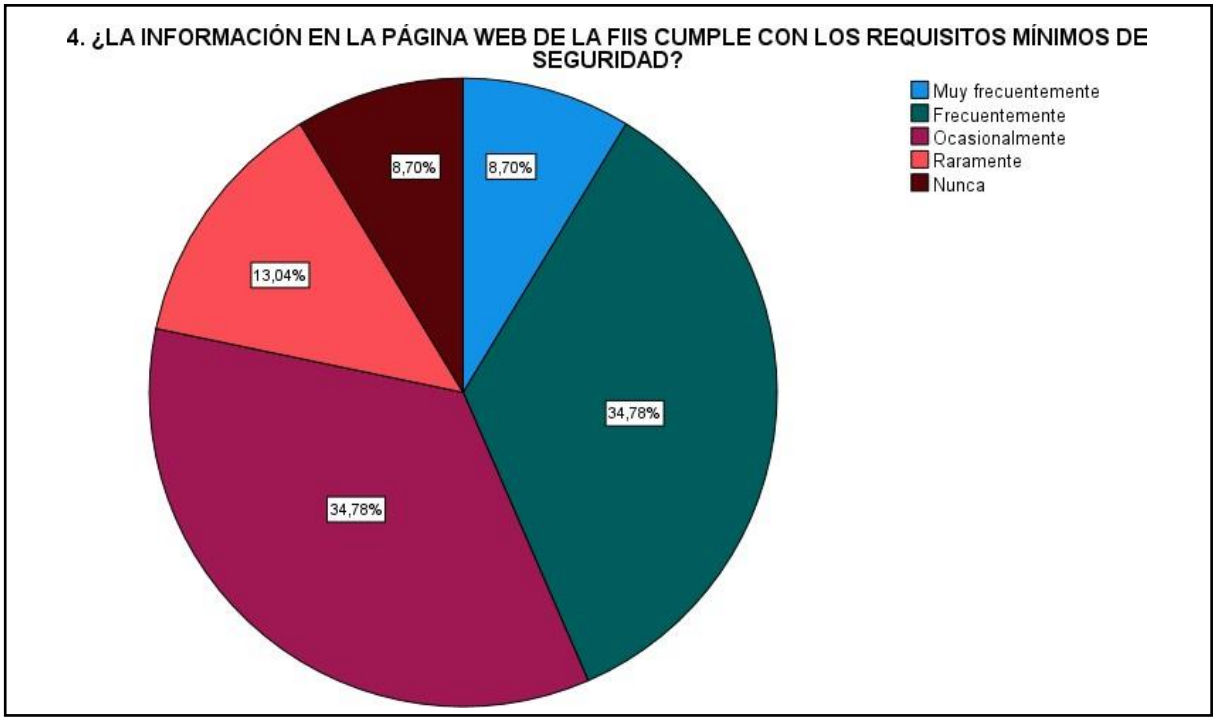

Figura 13: ¿La información en la página web de la FIIS cumple con los requisitos mínimos de la seguridad?

Fuente: Elaboración propia.

16. ¿USTED CONSIDERA QUE LA INFORMACIÓN DEL SERVIDOR WEB NO SE PUEDE MANIPULAR NI SER ALTERADO POR TERCERAS PERSONAS?					
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	S	12	52,2	52,2	52,2
	N	11	47,8	47,8	100,0
	T	23	100,0	100,0	

Tabla N° 7.

Fuente: Elaboración propia.

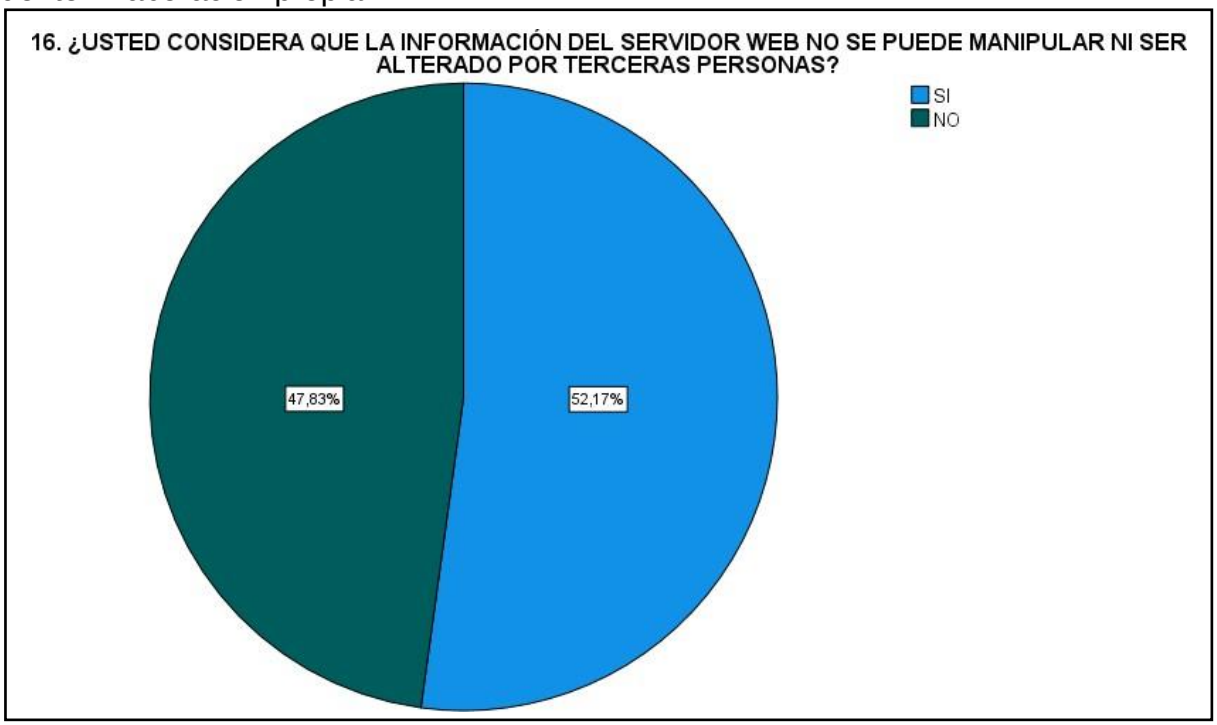

Figura 14: ¿Usted considera que la información del servidor web no se puede manipular ni ser alterado por terceras personas?

Fuente: Elaboración propia.

Tabla N° 8.

17. ¿USTED PUEDE ACCEDER A LOS DATOS Y RECURSOS EN EL SERVIDOR WEB?					
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	SI	9	39,1	39,1	39,1
	NO	14	60,9	60,9	100,0
	Total	23	100,0	100,0	

Fuente: Elaboración propia.

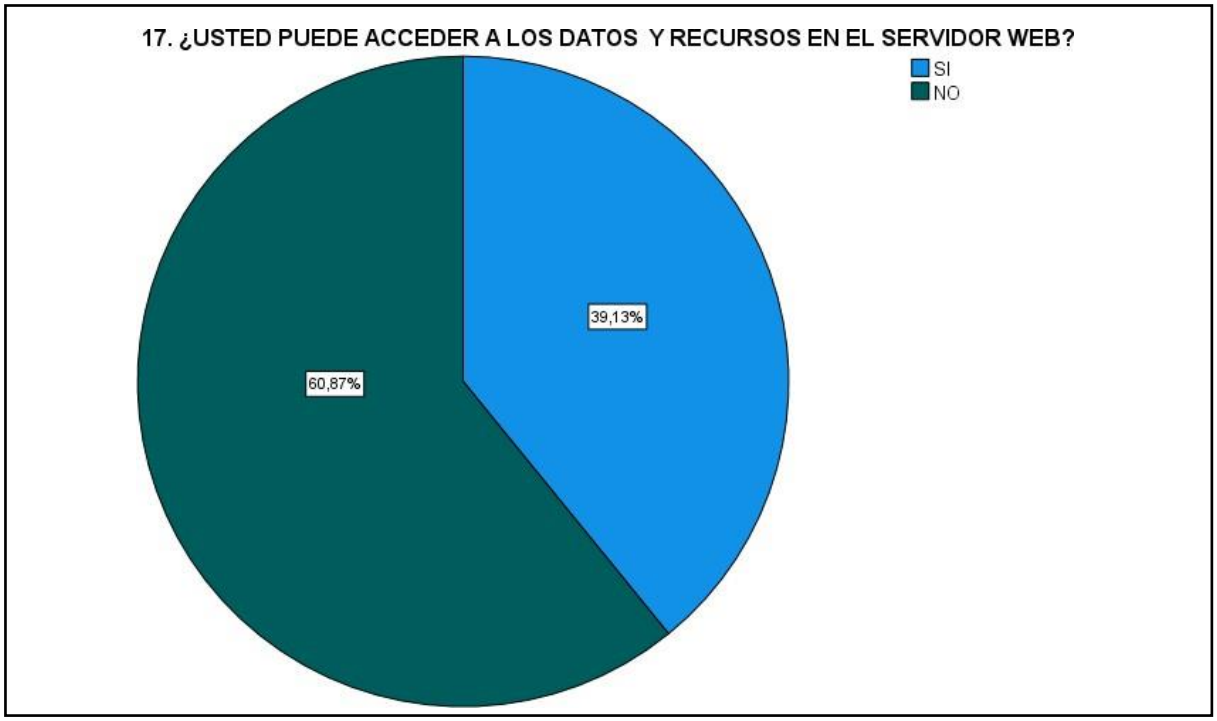

Figura 15: ¿Usted puede acceder a los datos y recursos en el servidor web?

Fuente: Elaboración propia.

Tabla N° 9.

18. ¿ LA INFORMACIÓN QUE ALMACENA EL SERVIDOR WEB ES CONFIABLE?					
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	SI	10	43,5	43,5	43,5
	NO	13	56,5	56,5	100,0
	Total	23	100,0	100,0	

Fuente: Elaboración propia.

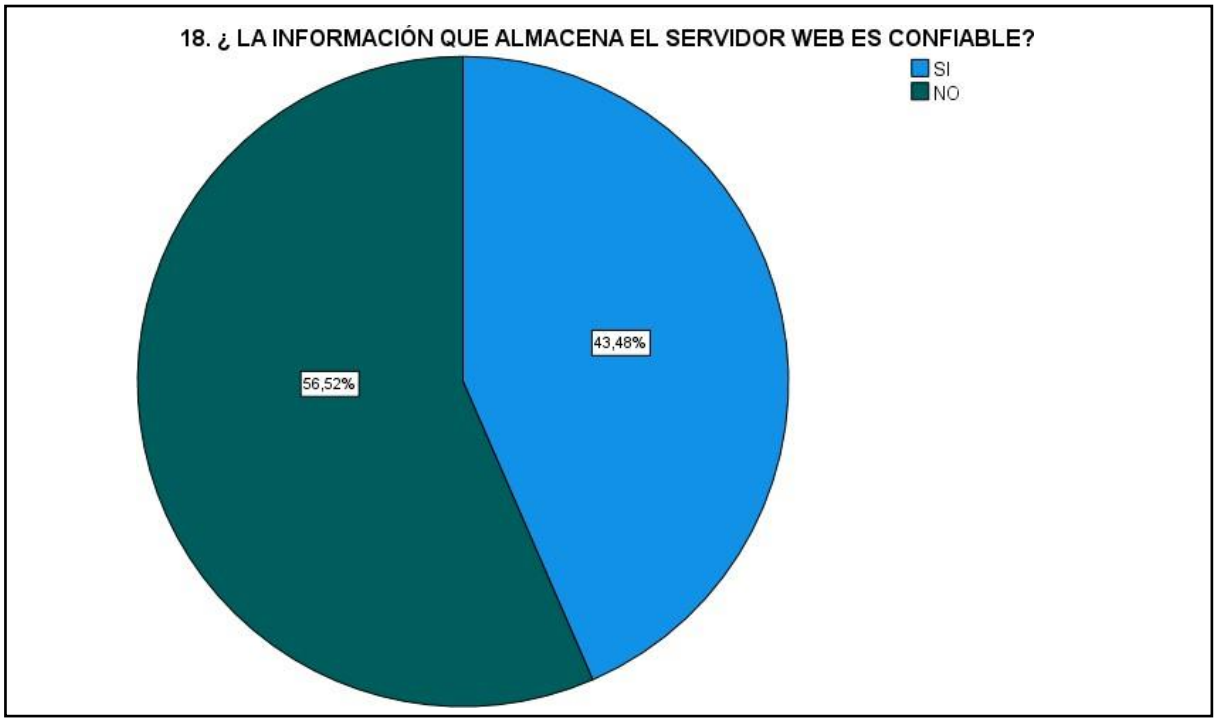

Figura 16: ¿La información que almacena el servidor web es confiable?

Fuente: Elaboración propia.

Tabla N° 10.

19. ¿PARA GUARDAR LA INFORMACIÓN, UTILIZA ESPACIOS EXTERNOS DE ALMACENAMIENTO DE INFORMACIÓN?					
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	SI	10	43,5	43,5	43,5
	NO	13	56,5	56,5	100,0
	Total	23	100,0	100,0	

Fuente: Elaboración propia.

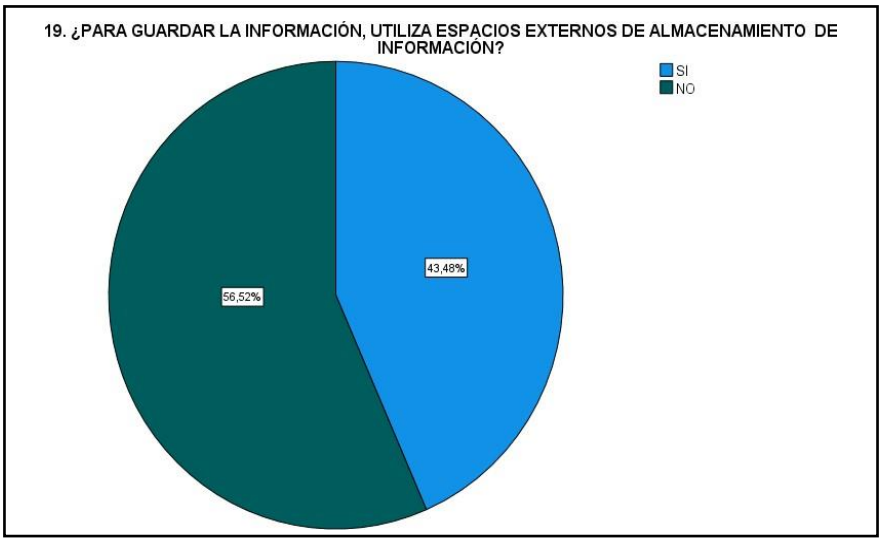

Figura 17: ¿Para guardar la información, utiliza espacios externos de almacenamiento de información?

Fuente: Elaboración propia.

Tabla N° 11.

20. ¿TIENE CONOCIMIENTO SOBRE LOS SERVIDORES WEB, QUE TIENE LA OFICINA DE TECNOLOGÍA Y COMUNICACIONES EN LA FACULTAD?					
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	SI	9	39,1	39,1	39,1
	NO	14	60,9	60,9	100,0
	Total	23	100,0	100,0	

Fuente: Elaboración propia.

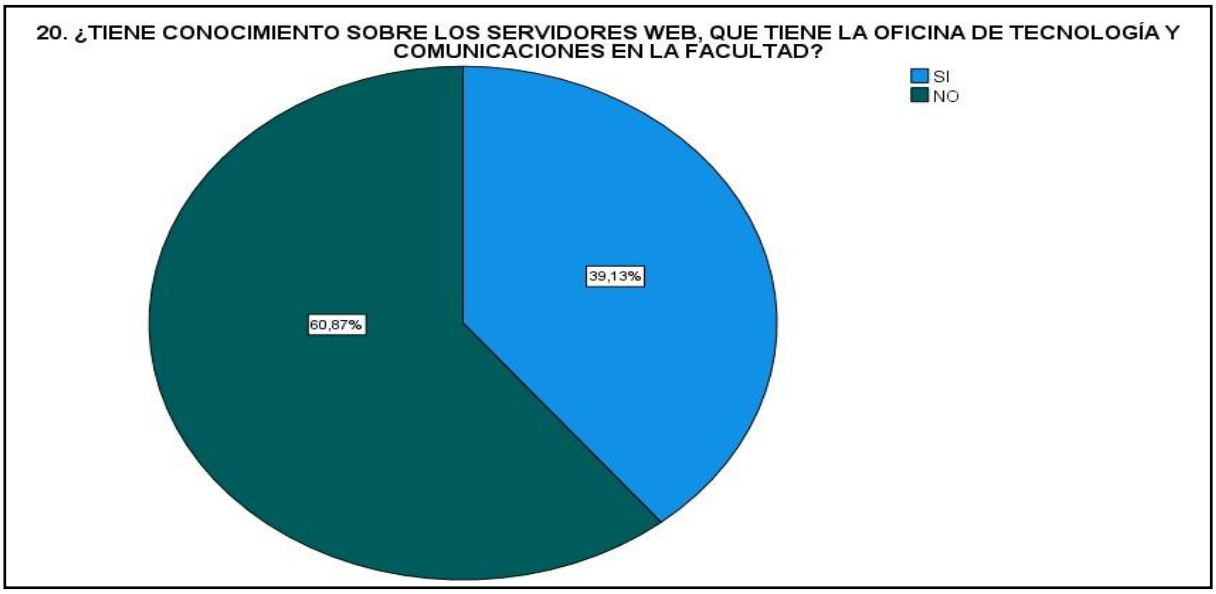

Figura 18: ¿Tiene conocimiento sobre los servidores web, que tiene la oficina de tecnología y comunicaciones en la Facultad?

Fuente: Elaboración propia.

Tabla N°12.

Resumen de procesamiento de casos

		N	%
Casos	Válido	23	100,0
	Excluido[a]	0	,0
	Total	23	100,0

Fuente: Elaboración propia.

a. La eliminación por lista se basa en todas las variables del procedimiento.

Para el procesamiento de datos se ha considerado el total de la muestra de 23 al 100%.

Tabla N°13.

Estadísticas de fiabilidad

Alfa de Cronbach	Alfa de Cronbach basada en elementos estandarizados	N de elementos
,878	,861	20

Fuente: Elaboración propia

Para el estudio se ha considerado 20 elementos del total de la muestra, el Alfa de Cronbach basada en elementos estandarizados con la estadística de fiabilidad es ,861.

Tabla N°14.

Estadísticas de elemento de resumen						
	Media	Mínimo	Máximo	Rango	Máximo / Mínimo	Varianza
Medias de elemento	2,498	1,478	3,174	1,696	2,147	,369
Varianzas de elemento	1,241	,249	2,150	1,901	8,635	,402

Estadísticas de elemento de resumen	
	N de elementos
Medias de elemento	20
Varianzas de elemento	20

Fuente: Elaboración propia.

Teniendo el resultado de los datos procesados de la varianza es ,369 para 20 elementos.

Tabla N°15.

Estadísticas de escala			
Media	Varianza	Desviación estándar	N de elementos
49,96	149,407	12,223	20

Fuente: Elaboración propia.

Como resultado el Alfa de Cronbach, la desviación estándar es 12,223 del total de 20 elementos

5.1.1 Resultados descriptivos de la variable dependiente

SERVIDOR WEB

En la tabla N° 16 visualizándose la comparación del servidor web que se tiene desde antes del mes de julio del 2022, teniendo como promedio de 62,59% y después de la aplicación del servidor web mejoró en 95.21%, realizado desde agosto del 2022 hasta el mes de octubre del 2022, Lo que indica que ha sido favorable en 32.62 %.

Tabla N° 16

COMPARATIVO DEL SERVIDOR WEB					
TIEMPO		Servidor Web Antes (%)	TIEMPO		Servidor Web Después (%)
Mayo 2022	Sem 1	61.45	Agosto 2022	Sem 25	91.56
	Sem 2	52.64		Sem 26	91.85
	Sem 3	58.66		Sem 27	92.36
	Sem 4	61.88		Sem 28	93.99
Junio 2022	Sem 5	62.74	Setiembre 2022	Sem 29	99.96
	Sem 6	63.33		Sem 30	99.23
	Sem 7	63.99		Sem 31	99.23
	Sem 8	64.89		Sem 32	99.74
Julio 2022	Sem 9	65.21	Octubre 2022	Sem 33	91.21
	Sem 10	64.99		Sem 34	95.66
	Sem 11	65.45		Sem 35	91.15
	Sem 12	65.85		Sem 36	96.52
	promedio	62.59		promedio	95.21

Fuente: Elaboración propia.

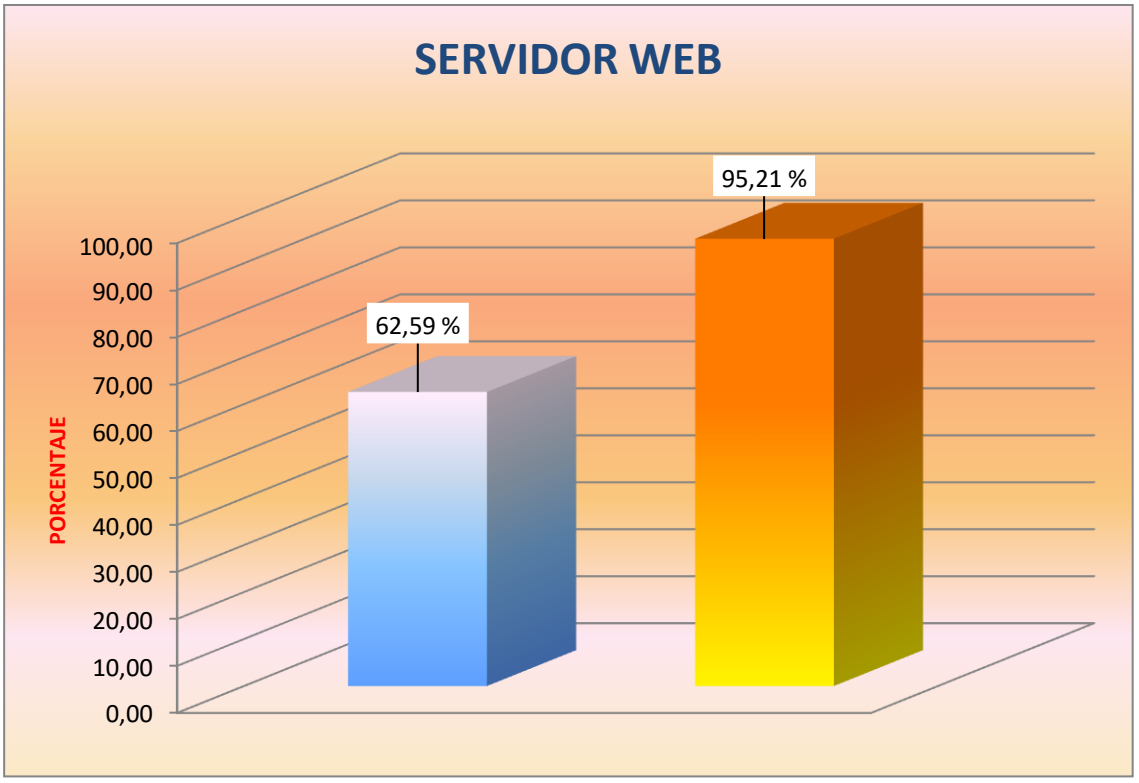

Figura 19: Servidor web

Fuente: Elaboración propia

ÍNDICES DE FUNCIONALIDAD

En la tabla N° 17 se visualiza la comparación de funcionalidad obtenido antes del mes de julio del 2022, teniendo un promedio de 64,02% y luego de la aplicación de la funcionalidad mejoró en 92.32%, realizado desde agosto del 2022 hasta el mes de octubre del 2022, Lo que indica que ha sido favorable en 28,3 %.

Tabla N°17

COMPARATIVO DEL ÍNDICES DE FUNCIONALIDAD					
TIEMPO		Indice de Funcionalidad Antes (%)	TIEMPO		Indice Funcionalidad Después (%)
Mayo 2022	Sem 1	61.45	Agosto 2022	Sem 25	89.87
	Sem 2	67.45		Sem 26	92.58
	Sem 3	58.66		Sem 27	93.55
	Sem 4	65.41		Sem 28	95.66
Junio 2022	Sem 5	62.74	Setiembre 2022	Sem 29	95.69
	Sem 6	63.33		Sem 30	89.55
	Sem 7	69.12		Sem 31	91.88
	Sem 8	64.89		Sem 32	89.55
Julio 2022	Sem 9	65.21	Octubre 2022	Sem 33	90.21
	Sem 10	64.99		Sem 34	92.99
	Sem 11	59.12		Sem 35	94.88
	Sem 12	65.85		Sem 36	91.45
	promedio	64.02		promedio	92.32

Fuente: Elaboración propia.

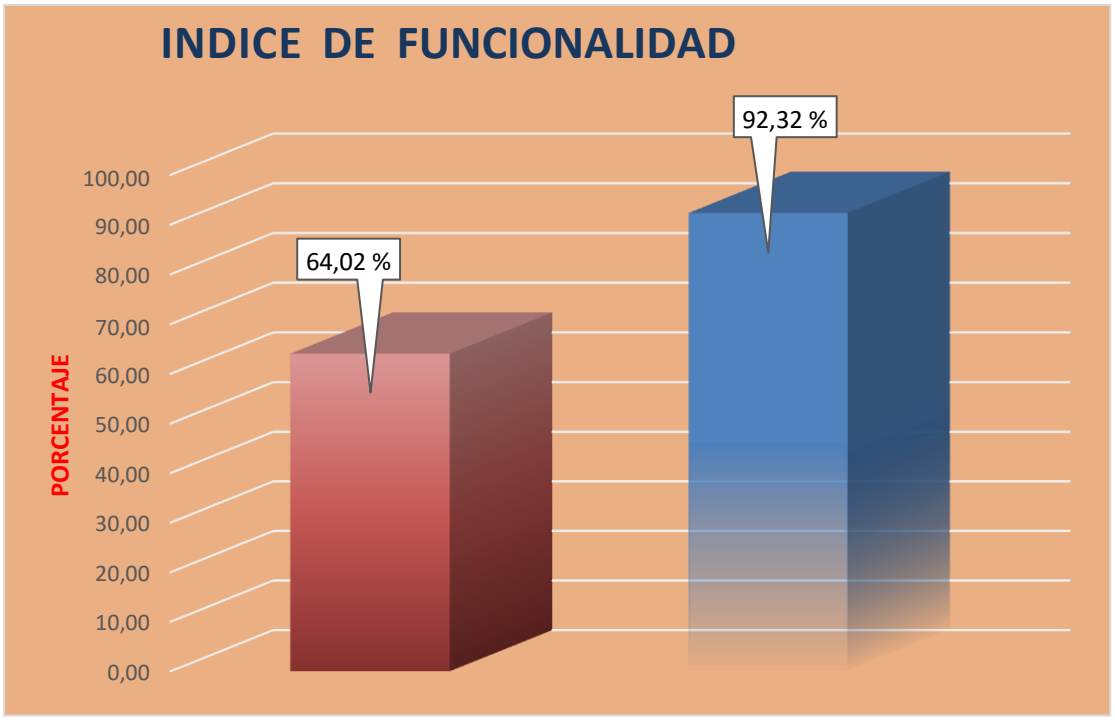

Figura 20: Índice de funcionalidad

Fuente: Elaboración propia.

ÍNDICES DE FIABILIDAD

En la tabla N° 18 en el cual se visualiza la comparación de fiabilidad obtenido antes desde el mes de julio del 2022, teniendo un promedio de 62,51% y luego de la aplicación de la fiabilidad mejoró en 95.29%, realizado desde agosto del 2022 hasta el mes de octubre del 2022, Lo que indica que ha sido favorable en 32.78 %.

Tabla N°18

COMPARATIVO DE LOS ÍNDICES DE FIABILIDAD					
TIEMPO		Indice de Fiabilidad Antes (%)	TIEMPO		Indice de Fiabilidad Después (%)
Mayo 2022	Sem 1	61.56	Agosto 2022	Sem 25	99.45
	Sem 2	59.12		Sem 26	95.68
	Sem 3	60.78		Sem 27	93.55
	Sem 4	58.98		Sem 28	94.12
Junio 2022	Sem 5	61.98	Setiembre 2022	Sem 29	95.69
	Sem 6	60.22		Sem 30	95.96
	Sem 7	65.12		Sem 31	94.26
	Sem 8	62.12		Sem 32	98.56
Julio 2022	Sem 9	69.45	Octubre 2022	Sem 33	90.21
	Sem 10	64.24		Sem 34	92.99
	Sem 11	60.59		Sem 35	94.88
	Sem 12	65.99		Sem 36	98.15
	promedio	62.51		promedio	95.29

Fuente: Elaboración Elaboración propia.

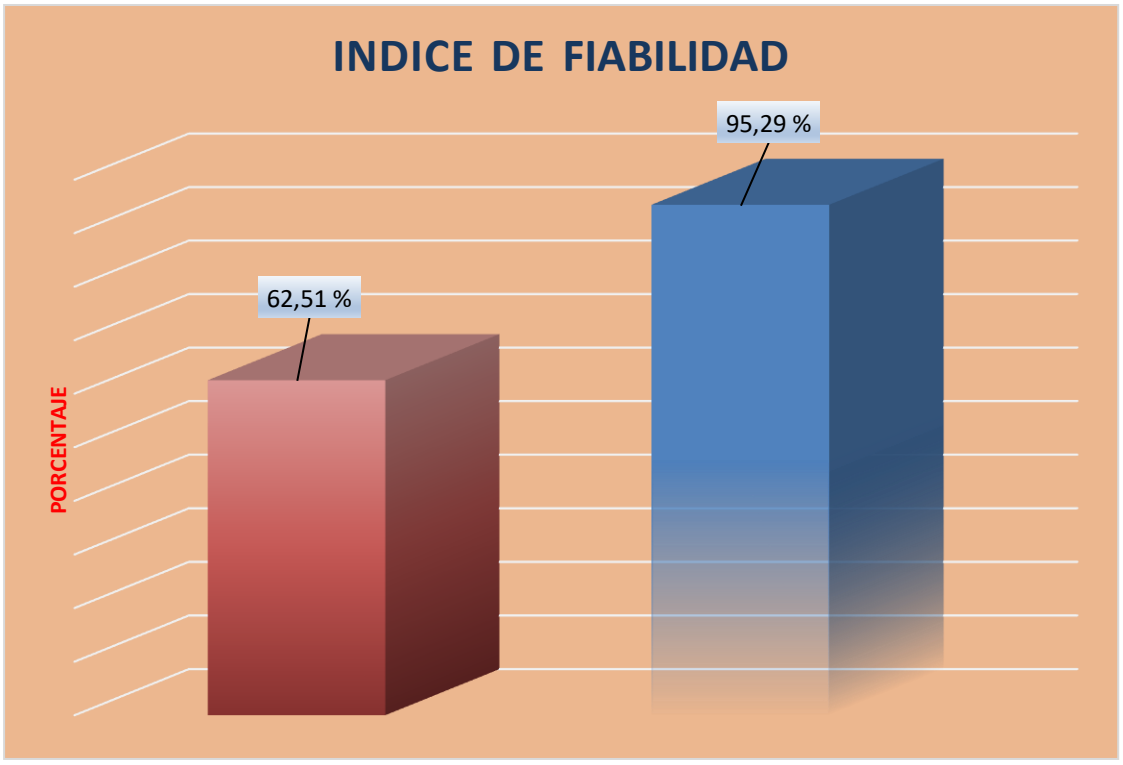

Figura 21: Índice de Fiabilidad

Fuente: Elaboración propia.

ÍNDICES DE USABILIDAD

En la tabla N° 19 en el cual se visualiza la comparación de usabilidad que se obtuvo antes desde el mes de julio del 2022, el teniendo un promedio de 63,35% y luego de la aplicación de la usabilidad mejoró en 95.77%, realizado desde agosto del 2022 hasta el mes de octubre del 2022, Lo que indica que ha sido favorable en 32.42 %.

Tabla N°19

COMPARATIVO DE LOS ÍNDICES DE USABILIDAD					
TIEMPO		Indice de Usabilidad Antes (%)	TIEMPO		Indice de Usabilidad Después (%)
Mayo 2022	Sem 1	60.55	Agosto 2022	Sem 25	98.22
	Sem 2	58.44		Sem 26	97.45
	Sem 3	60.12		Sem 27	95.23
	Sem 4	59.12		Sem 28	96.24
Junio 2022	Sem 5	62.55	Setiembre 2022	Sem 29	95.69
	Sem 6	60.25		Sem 30	95.96
	Sem 7	65.23		Sem 31	96.54
	Sem 8	66.45		Sem 32	98.54
Julio 2022	Sem 9	68.21	Octubre 2022	Sem 33	92.31
	Sem 10	67.12		Sem 34	92.99
	Sem 11	64.55		Sem 35	94.88
	Sem 12	67.56		Sem 36	95.22
	promedio	63.35		promedio	95.77

Fuente: Elaboración propia.

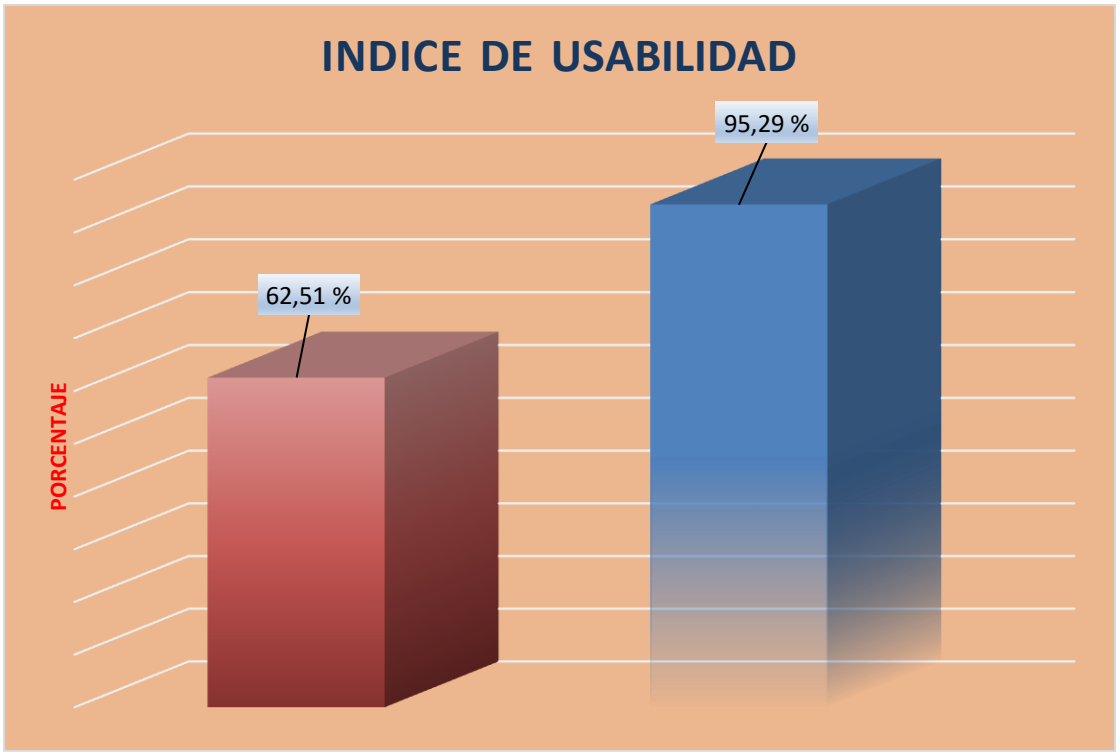

Figura 22: Índice de Usabilidad

Fuente: Elaboración propia.

ÍNDICES DE EFICIENCIA

En la tabla N° 20 se visualiza la comparación de eficiencia que se obtuvo antes desde el mes de julio del 2022, el cual muestra un promedio de 62,79% y luego de la aplicación de la eficiencia mejoró en 95.15%, realizado desde agosto del 2022 hasta el mes de octubre del 2022, Lo que indica que ha sido favorable en 32.36 %.

Tabla N°20

COMPARATIVO DE LOS ÍNDICES DE EFICIENCIA					
TIEMPO		Índice de Eficiencia Antes (%)	TIEMPO		Índice de Eficiencia Después (%)
Mayo 2022	Sem 1	61.56	Agosto 2022	Sem 25	95.23
	Sem 2	59.12		Sem 26	96.54
	Sem 3	60.78		Sem 27	93.55
	Sem 4	58.98		Sem 28	94.12
Junio 2022	Sem 5	61.98	Setiembre 2022	Sem 29	95.69
	Sem 6	64.55		Sem 30	96.25
	Sem 7	65.12		Sem 31	94.26
	Sem 8	62.12		Sem 32	98.56
Julio 2022	Sem 9	68.45	Octubre 2022	Sem 33	90.21
	Sem 10	64.24		Sem 34	92.99
	Sem 11	60.59		Sem 35	96.23
	Sem 12	65.99		Sem 36	98.15
	promedio	62.79		promedio	95.15

Fuente: Elaboración propia.

.

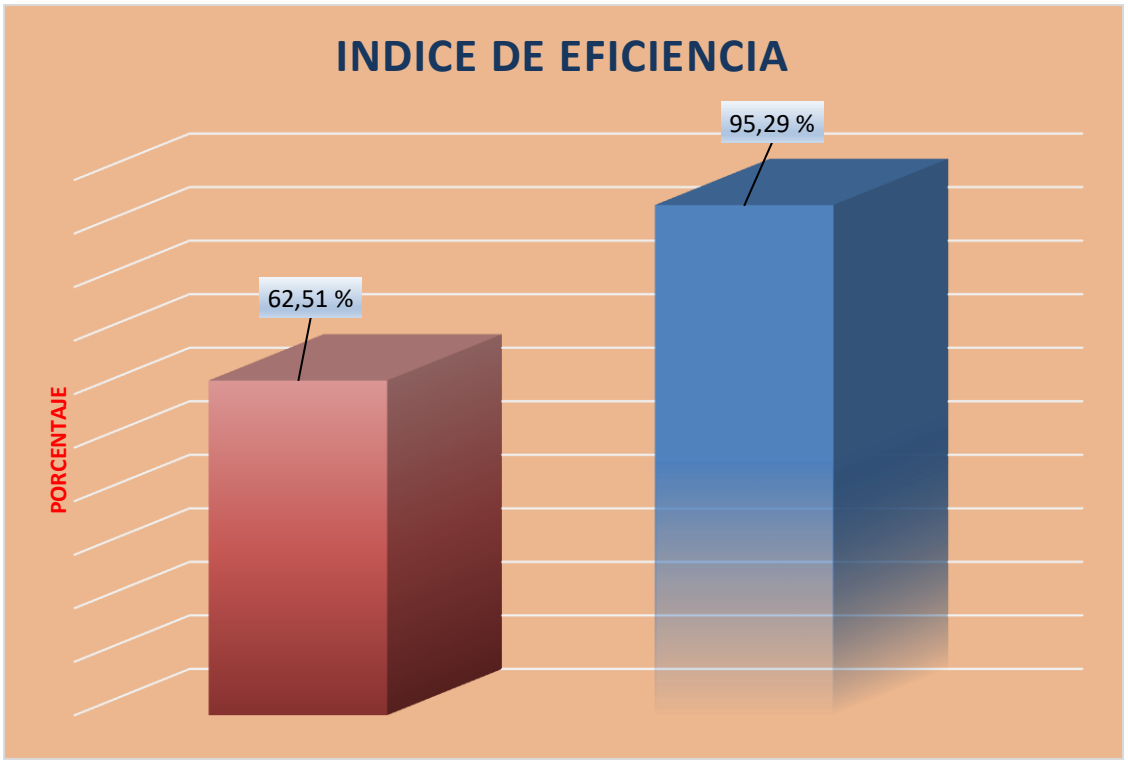

Figura 23: Índice de Eficiencia

Fuente: Elaboración propia.

.

ÍNDICES DE PORTABILIDAD

En la tabla N° 21 en el cual se visualiza la comparación de la portabilidad que se obtuvo antes desde el mes de julio del 2022, las muestras un promedio de 63,56% y luego la aplicación de la portabilidad mejoró en 95.49%, realizado desde agosto del 2022 hasta el mes de octubre del 2022, Lo que indica que ha sido favorable en 31,93 %.

Tabla N°21

COMPARATIVO DE LOS ÍNDICES DE PORTABILIDAD					
TIEMPO		Índice de Eficacia Antes (%)	TIEMPO		Índice de Eficacia Después (%)
Mayo 2022	Sem 1	61.56	Agosto 2022	Sem 25	95.23
	Sem 2	59.12		Sem 26	95.68
	Sem 3	64.23		Sem 27	96.54
	Sem 4	58.98		Sem 28	94.12
Junio 2022	Sem 5	61.98	Setiembre 2022	Sem 29	95.69
	Sem 6	63.22		Sem 30	95.96
	Sem 7	65.12		Sem 31	94.26
	Sem 8	62.12		Sem 32	97.25
Julio 2022	Sem 9	64.12	Octubre 2022	Sem 33	95.12
	Sem 10	67.45		Sem 34	92.99
	Sem 11	68.78		Sem 35	94.88
	Sem 12	65.99		Sem 36	98.15
	promedio	63.56		promedio	95.49

Fuente: Elaboración propia.

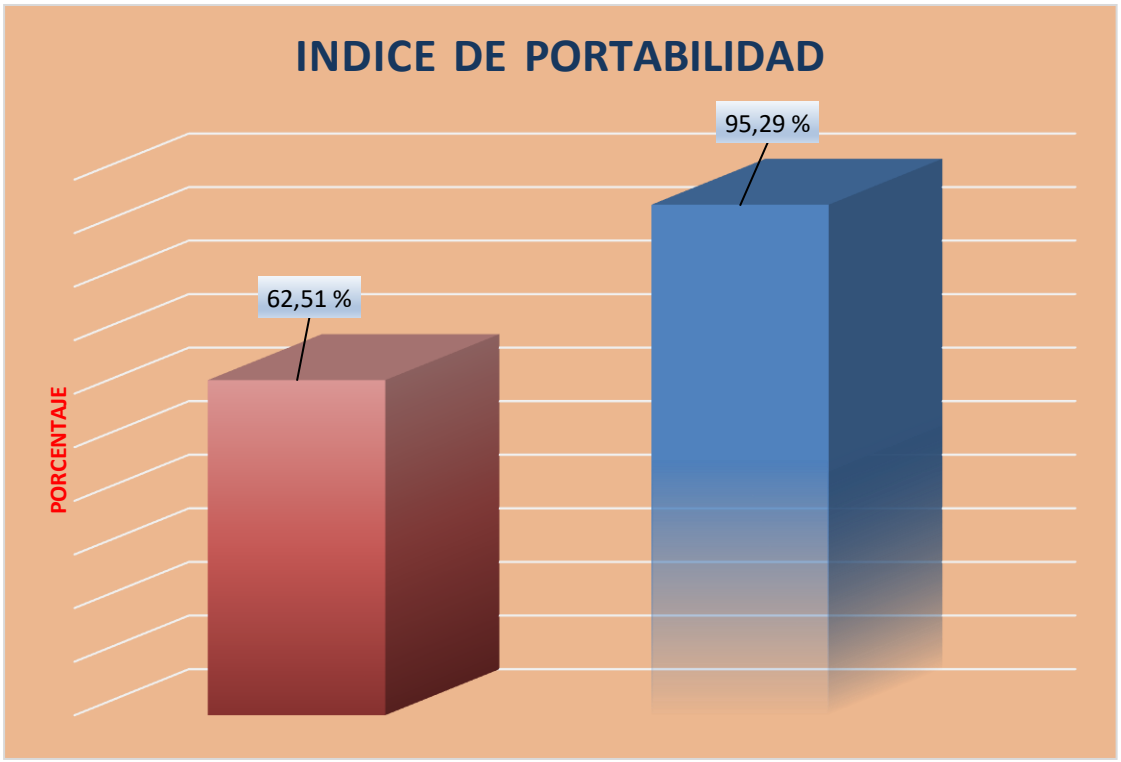

Figura 24: Índice de Portabilidad

Fuente: Elaboración propia.

5.2. Resultados inferenciales.

5.2.1 Resultados inferencial de La V.D: SERVIDOR WEB

Prueba de Normalidad

Se utilizo la prueba de normalidad para comprobar la distribución de los datos, en esta investigación se procesó 12 datos que proviene de la diferencia del antes y después, por lo cual se eligió la prueba de Shapiro-Wilk, con la siguiente regla de decisión:

Si la significancia es > 0.05, el comportamiento de la muestra es una distribución normal, y se elige el estadístico de prueba de T-Student.

Si la significancia es < 0.05, el comportamiento de la muestra es una distribución no normal. y se elige el estadístico de prueba no paramétrica de Wilcoxon.

Tabla 22. *Prueba de Normalidad*

Pruebas de normalidad

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
DIFERENCIA_SERVIDOR_WEB	,119	12	,200*	,959	12	,766

*. Esto es un límite inferior de la significación verdadera.

a. Corrección de significación de Lilliefors

Fuente: Elaboración propia.

En la tabla 22, la significancia tiene un valor de 0.766 siendo este > 0.05, por lo tanto, los datos provienen de una distribución normal, entonces para la prueba de hipótesis se eligió la prueba de T-Student.

Prueba de Hipótesis de la Variable dependiente

Ho: Un sistema de seguridad de la información no optimiza los servidores web en la OTIC de la FIIS de la UNAC 2022

Ha: Un sistema de seguridad de la información optimiza los servidores web en la OTIC de la FIIS de la UNAC 2022.

Regla de decisiónH_0:

µpa = µpd

H_a: µpa < µpd

Tabla 23: *Estadísticas de muestras emparejadas productividad*

Estadísticas de muestras emparejadas					
		Media	N	Desv. Desviación	Desv. Error promedio
Par 1	SERVIDOR_WEB DESPUES	95,2050	12	3,61850	1,04457
	SERVIDOR_WEB ANTES	62,5900	12	3,75987	1,08538

Fuente: Elaboración propia

Tabla 24: *Diferencias emparejadas productividad*

Prueba de muestras emparejadas									
		Diferencias emparejadas							
					95% de intervalo de confianza de la diferencia				
		Media	Desv. Desviación	Desv. Error promedio	Inferior	Superior	t	gl	Sig. (bilateral)
Par 1	SERVIDOR_WEB DESPUES - SERVIDOR_WEB ANTES	32,61500	4,20201	1,21302	29,94517	35,28483	26,888	11	,000

Fuente: Elaboración propia.

En la tabla Nº 24: observamos que el resultado resultante del sig. (Bilateral) resulta 0,000 siendo < que 0,05, por lo tanto, se rechaza la hipótesis nula (Ho) y se acepta la hipótesis alterna (Ha), siendo la mejora de la media del servidor web en 32.615%, habiendo una diferencia significativa, concluyendo

que: Un sistema de SI optimiza los servidores web en la OTIC de la FIIS de la UNAC 2022, incrementará en una medida significativa del 32,615%.

Prueba de hipótesis especifica 1

Prueba de Normalidad

Se utilizó la prueba de normalidad Shapiro-Wilk, por lo que, la muestra que se utilizo es < a 30 trabajadores en las que se ha hecho el estudio para esta prueba. Describiéndolo en la siguiente hipótesis para la productividad en la cual se trabajó con la diferencia:

Si el P-valor es > a 0.05, la data de la muestra viene de una distribución normal, aceptando la Ho.

Si el P- valor es < a 0.05, los datos de la muestra no provienen de una distribución normal, aceptamos la Ha.

Tabla 25: *Prueba de normalidad de los Índices de eficiencia*

Pruebas de normalidad

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
DIFERENCIA_FUNCIONALIDAD	,187	12	,200*	,908	12	,200

*. Esto es un límite inferior de la significación verdadera.

a. Corrección de significación de Lilliefors

Fuente: Elaboración propia.

En la tabla 25, la significancia tiene un valor de 0.200 siendo este > 0.05, por lo tanto, los datos provienen de una distribución normal, entonces para la prueba de hipótesis se eligió la prueba de T-Student.

Validación de Hipótesis Especifica de la variable Dependiente

Ho: Un sistema de seguridad de la información no optimiza la funcionalidad de los servidores web en la OTIC de la FIIS de la UNAC 2022.

Ha: Un sistema de seguridad de la información optimiza información optimiza la funcionalidad de los servidores web en la OTIC de la FIIS de la UNAC 2022.

Regla de decisión

H_0: µpa ≥ µpd

H_a: µpa < µpd

Tabla 26. *Estadísticas de muestras emparejadas índices de eficiencia*

Estadísticas de muestras emparejadas					
		Media	N	Desv. Desviación	Desv. Error promedio
Par 1	FUNCIONALIDAD DESPUES	92,3217	12	2,29320	,66199
	FUNCIONALIDAD ANTES	64,0183	12	3,12801	,90298

Fuente: Elaboración propia.

Tabla 27. *Diferencias emparejadas índices de eficiencia*

Prueba de muestras emparejadas									
		Diferencias emparejadas							
					95% de intervalo de confianza de la diferencia				
		Media	Desv. Desviación	Desv. Error promedio	Inferior	Superior	t	gl	Sig. (bilateral)
Par 1	FUNCIONALIDAD DESPUES - FUNCIONALIDAD ANTES	28,30333	4,27578	1,23431	25,58663	31,02004	22,930	11	,000

Fuente: Elaboración propia.

En la tabla 27, observamos que el resultado que se obtuvo del sig. (Bilateral) resulta 0,000 siendo < que 0,05, rechazando la hipótesis nula (Ho) y aceptando la hipótesis alterna (Ha), con una mejora de la media en el índice de 28,30 %, por lo que existe una diferencia significativa en los índices,

concluyendo que: Un sistema de SI optimiza la funcionalidad de los servidores web en la OTIC de la FIIS de la UNAC 2022.

Prueba de hipótesis especifica 2

Prueba de Normalidad

Se utilizo la prueba de normalidad para comprobar la distribución de los datos, en esta investigación se procesó 12 datos que proviene de la diferencia del antes y después, por lo cual se eligió la prueba de Shapiro-Wilk, con la siguiente regla de decisión:

Si la significancia es > 0.05, el comportamiento de la muestra es una distribución normal, y se elige el estadístico de prueba de T-Student.

Si la significancia es < 0.05, el comportamiento de la muestra es una distribución no normal. y se elige el estadístico de prueba no paramétrica de Wilcoxon.

Tabla 28 Prueba *de normalidad de los Índices de Eficacia*

Pruebas de normalidad						
	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
DIFERENCIA_FIABILIDAD	,198	12	,200*	,855	12	,042
*. Esto es un límite inferior de la significación verdadera.						
a. Corrección de significación de Lilliefors						

Fuente: Elaboración propia

En la tabla 28, la significancia tiene un valor de 0.042 siendo este > 0.05, por lo tanto, los datos provienen de una distribución normal, entonces para la prueba de hipótesis se eligió la prueba de T-Student.

Validación de Hipótesis Especifica de la variable Dependiente

Ho: Un sistema de seguridad de la información no optimiza la fiabilidad de los servidores web en la OTIC de la FIIS de la UNAC 2022.

Ha: Un sistema de seguridad de la información optimiza la fiabilidad de los servidores web en la OTIC de la FIIS de la UNAC 2022.

$$H_0: \mu pa = \mu pd$$

$$H_a: \mu pa < \mu pd$$

Tabla 29. *Estadísticas de muestras emparejadas índices de eficacia*

Estadísticas de muestras emparejadas					
		Media	N	Desv. Desviación	Desv. Error promedio
Par 1	FIABILIDAD DESPUES	95,2917	12	2,58775	,74702
	FIABILIDAD ANTES	62,5125	12	3,12309	,90156

Fuente: Elaboración propia

Tabla 30: Diferencias *emparejadas índices de eficacia*

Prueba de muestras emparejadas									
		Diferencias emparejadas							
					95% de intervalo de confianza de la diferencia				
		Media	Desv. Desviación	Desv. Error promedio	Inferior	Superior	t	gl	Sig. (bilateral)
Par 1	FIABILIDAD DESPUES - FIABILIDAD ANTES	32,77917	4,72544	1,36412	29,77676	35,78157	24,030	11	,000

Fuente: Elaboración propia

En la tabla Nº 30 observamos que el resultado que se obtuvo del sig. (Bilateral) resulta 0,000 siendo < que 0,05, rechazando la hipótesis nula (Ho) y aceptando la hipótesis alterna (Ha), con una mejora de la media en el índice de 32,78 %, por lo que existe una diferencia significativa en los índices, concluyendo que: Un sistema de SI optimiza la fiabilidad de los servidores web en la OTIC de la FIIS de la UNAC 2022.

Prueba de hipótesis especifica 3

Prueba de Normalidad

Se utilizo la prueba de normalidad para comprobar la distribución de los datos, en esta investigación se procesó 12 datos que proviene de la diferencia del antes y después, por lo cual se eligió la prueba de Shapiro-Wilk, con la siguiente regla de decisión:

Si la significancia es > 0.05, el comportamiento de la muestra es una distribución normal, y se elige el estadístico de prueba de T-Student.

Si la significancia es < 0.05, el comportamiento de la muestra es una distribución no normal. y se elige el estadístico de prueba no paramétrica de Wilcoxon.

Tabla 31. Prueba *de normalidad de los Índices de Eficacia*

Pruebas de normalidad

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
DIFERENCIA USABILIDAD	,129	12	,200*	,958	12	,757

*. Esto es un límite inferior de la significación verdadera.

a. Corrección de significación de Lilliefors

Fuente: Elaboración propia.

En la tabla 31, la significancia tiene un valor de 0.757 siendo este > 0.05, por lo tanto, los datos provienen de una distribución normal, entonces para la prueba de hipótesis se eligió la prueba de T-Student.

Validación de Hipótesis Especifica de la variable Dependiente

Ho: Un sistema de seguridad de la información no optimiza la usabilidad de los servidores web en la OTIC de la FIIS de la UNAC 2022.

Ha: Un sistema de seguridad de la información optimiza la usabilidad de los servidores web en la OTIC de la FIIS de la UNAC 2022.

H_0: µpa = µpd H_a:

µpa < µpd

Tabla 32. *Estadísticas de muestras emparejadas índices de eficacia*

Estadísticas de muestras emparejadas					
		Media	N	Desv. Desviación	Desv. Error promedio
Par 1	USABILIDAD DESPUES	95,7725	12	1,86938	,53964
	USABILIDAD ANTES	63,3458	12	3,57599	1,03230

Fuente: Elaboración propia

Tabla 33: Diferencias *emparejadas índices de eficacia*

Prueba de muestras emparejadas									
		Diferencias emparejadas					t	gl	Sig. (bilateral)
		Media	Desv. Desviación	Desv. Error promedio	95% de intervalo de confianza de la diferencia Inferior	Superior			
Par 1	USABILIDAD DESPUES – USABILIDAD ANTES	32,42667	4,78777	1,38211	29,38466	35,46867	23,462	11	,000

Fuente: Elaboración propia.

En la tabla Nº 33 observamos que el resultado que se obtuvo del sig. (Bilateral) resulta 0,000 siendo < que 0,05, rechazando la hipótesis nula (Ho) y aceptando la hipótesis alterna (Ha), con una mejora de la media en el índice en 32,43 %, existiendo una diferencia significativa en los índices, concluyendo que: Un sistema de SI optimiza la usabilidad de los servidores web en la OTIC de la FIIS de la UNAC 2022.

Prueba de hipótesis especifica 4

Prueba de Normalidad

Se utilizo la prueba de normalidad para comprobar la distribución de los datos, en esta investigación se procesó 12 datos que proviene de la diferencia del antes y después, por lo cual se eligió la prueba de Shapiro-Wilk, con la siguiente regla de decisión:

Si la significancia es > 0.05, el comportamiento de la muestra es una distribución normal, y se elige el estadístico de prueba de T-Student.

Si la significancia es < 0.05, el comportamiento de la muestra es una distribución no normal. y se elige el estadístico de prueba no paramétrica de Wilcoxon.

Tabla 34. Prueba *de normalidad de los Índices de Eficacia*

Pruebas de normalidad

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
DIFERENCIA_EFICIENCIA	,189	12	,200*	,891	12	,121

*. Esto es un límite inferior de la significación verdadera.

a. Corrección de significación de Lilliefors

Fuente: Elaboración propia.

En la tabla 34, la significancia tiene un valor de 0.121 siendo este > 0.05, por lo tanto, los datos provienen de una distribución normal, entonces para la prueba de hipótesis se eligió la prueba de T-Student.

Validación de Hipótesis Especifica de la variable Dependiente

Ho: Un sistema de seguridad de la información no optimiza la eficiencia de los servidores web en la OTIC de la FIIS de la UNAC 2022.

Ha: Un sistema de seguridad de la información optimiza la eficiencia de los servidores web en la OTIC de la FIIS de la UNAC 2022.

$$H_0: \mu pa = \mu pd$$
$$H_a: \mu pa < \mu pd$$

Tabla 35. *Estadísticas de muestras emparejadas índices de eficacia*

Estadísticas de muestras emparejadas					
		Media	N	Desv. Desviación	Desv. Error promedio
Par 1	EFICIENCIA DESPUES	95,1483	12	2,31039	,66695
	EFICIENCIA ANTES	62,7900	12	2,89808	,83660

Fuente: Elaboración propia.

Tabla 36: Diferencias *emparejadas índices de eficacia*

Prueba de muestras emparejadas									
		Diferencias emparejadas							
					95% de intervalo de confianza de la diferencia				
		Media	Desv. Desviación	Desv. Error promedio	Inferior	Superior	t	gl	Sig. (bilateral)
Par 1	EFICIENCIA DESPUES – EFICIENCIA ANTES	32,35833	4,27125	1,23300	29,64451	35,07216	26,243	11	,000

Fuente: Elaboración propia.

En la tabla Nº 36 observamos que el resultado obtenido del sig. (Bilateral) resulta 0,000 siendo < que 0,05, rechazando la hipótesis nula (Ho) y aceptando la hipótesis alterna (Ha), con una mejora de la media en el índice de 32,35 %, existiendo una diferencia significativa en los índices, concluyendo que: Un sistema de SI optimiza la eficiencia de los servidores web en la OTIC de la FIIS de la UNAC 2022.

Prueba de hipótesis especifica 5

Prueba de Normalidad

Se utilizo la prueba de normalidad para comprobar la distribución de los datos, en esta investigación se procesó 12 datos que proviene de la diferencia del antes y después, por lo cual se eligió la prueba de Shapiro-Wilk, con la siguiente regla de decisión:

Si la significancia es > 0.05, el comportamiento de la muestra es una distribución normal, y se elige el estadístico de prueba de T-Student.

Si la significancia es < 0.05, el comportamiento de la muestra es una distribución no normal. y se elige el estadístico de prueba no paramétrica de Wilcoxon.

Tabla 37. Prueba *de normalidad de los Índices de Eficacia*

Pruebas de normalidad

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
DIFERENCIA PORTABILIDAD	,193	12	,200*	,918	12	,268

*. Esto es un límite inferior de la significación verdadera.

a. Corrección de significación de Lilliefors

Fuente: Elaboración propia.

En la tabla 37, la significancia tiene un valor de 0.268 siendo este > 0.05, por lo tanto, los datos provienen de una distribución normal, entonces para la prueba de hipótesis se eligió la prueba de T-Student.

Validación de Hipótesis Especifica de la variable Dependiente

Ho: Un sistema de seguridad de la información no optimiza la portabilidad de los servidores web en la OTIC de la FIIS de la UNAC 2022.

Ha: Un sistema de seguridad de la información optimiza la portabilidad de los servidores web en la OTIC de la FIIS de la UNAC 2022.

$$H_0: \mu pa = \mu pd$$

$$H_a: \mu pa < \mu pd$$

Tabla 38. *Estadísticas de muestras emparejadas índices de eficacia*

Estadísticas de muestras emparejadas					
		Media	N	Desv. Desviación	Desv. Error promedio
Par 1	PORTABILIDAD DESPUES	95,4892	12	1,40742	,40629
	PORTABILIDAD ANTES	63,5558	12	3,02800	,87411

Fuente: Elaboración propia.

Tabla 39: Diferencias *emparejadas índices de eficacia*

Prueba de muestras emparejadas								
	Diferencias emparejadas					t	gl	Sig. (bilateral)
	Media	Desv. Desviación	Desv. Error promedio	95% de intervalo de confianza de la diferencia Inferior	Superior			
PORTABILIDAD DESPUES - PORTABILIDAD ANTES	31,93	3,47	1,00189	29,72	34,13	31,87	11	,000

Fuente: Elaboración propia.

En la tabla Nº 39 observamos que el resultado que se obtuvo del sig. (Bilateral) resulta 0,000 siendo < que 0,05, rechazando la hipótesis nula (Ho) y se aceptando la hipótesis alterna (Ha), con una mejora de la media en el índice de eficacia de 31,93 %, existiendo una diferencia significativa en los índices de eficacia, concluyendo que: Un sistema de SI optimiza la portabilidad de los servidores web en la OTIC de la FIIS de la UNAC 2022.

,

VI. DISCUSIÓN DE RESULTADOS

6.1 Contrastación y demostración de la hipótesis con los resultados.

En la tabla 23 que representa la constatación de la hipótesis general: se obtuvo el resultado de la significancia bilateral de 0,000 siendo menor que 0,05, por lo cual, se rechaza la hipótesis nula (Ho) y se acepta la hipótesis alterna (Ha), asimismo la media la diferencia del servidor web es 32.615%, teniendo un incremento significativo, por lo cual se infiere: Un sistema de seguridad de la información optimiza los servidores web en la OTIC de la FIIS de la UNAC 2022.

En la tabla 26, que representa la constatación de la hipótesis especifica: se obtuvo el resultado de la significancia bilateral de 0,000 siendo menor que 0,05, por lo cual, se rechaza la hipótesis nula (Ho) y se acepta la hipótesis alterna (Ha), asimismo la media diferencia del índice de 28,30 %, teniendo un incremento significativo, por lo cual infiere: Un sistema de seguridad de la información optimiza la funcionalidad de los servidores web en la OTIC de la FIIS de la UNAC 2022.

En la tabla 29 que representa la constatación de la hipótesis especifica: se obtuvo el resultado de la significancia bilateral de 0,000 siendo menor que 0,05, por lo cual, se rechaza la hipótesis nula (Ho) y se acepta la hipótesis alterna (Ha), asimismo la media diferencia del índice de 32,78 %, teniendo un incremento significativo, por lo cual infiere: Un sistema de seguridad de la información optimiza la fiabilidad de los servidores web en la OTIC de la FIIS de la UNAC 2022.

En la tabla Nº 32 que representa la constatación de la hipótesis especifica: se obtuvo el resultado de la significancia bilateral de 0,000 siendo menor que 0,05, por lo cual, se rechaza la hipótesis nula (Ho) y se acepta la hipótesis alterna (Ha), asimismo la media diferencia del índice de 32,43 %, teniendo

un incremento significativo, por lo cual infiere: Un sistema de seguridad de información optimiza la usabilidad de los servidores web en la OTIC de la FIIS de la UNAC 2022.

En la tabla Nº 35 que representa la constatación de la hipótesis especifica: se obtuvo el resultado de la significancia bilateral de 0,000 siendo menor que 0,05, por lo cual, se rechaza la hipótesis nula (Ho) y se acepta la hipótesis alterna (Ha), asimismo la media diferencia del índice de 32,35 %, teniendo un incremento significativo, por lo cual infiere: Un sistema de seguridad de la información optimiza la eficiencia de los servidores web en la OTIC de la FIIS de la UNAC 2022.

En la tabla Nº 38 que representa la constatación de la hipótesis especifica: se obtuvo el resultado de la significancia bilateral de 0,000 siendo menor que 0,05, por lo cual, se rechaza la hipótesis nula (Ho) y se acepta la hipótesis alterna (Ha), asimismo la media diferencia del índice de 31,93 %, teniendo un incremento significativo, por lo cual infiere: Un sistema de seguridad de la información optimiza la portabilidad de los servidores web en la OTIC de la FIIS de la UNAC 2022.

6.2 Contrastación de los resultados con otros estudios similares.

En la tabla N° 16 de comparación del servidor web obtenido antes desde el mes de julio del 2022, el cual tuvo un promedio de 62,59% y luego de la aplicación del servidor web mejoró en 95.21%, realizado desde agosto del 2022 hasta el mes de octubre del 2022, Lo que indica que ha sido favorable en 32.62 %, igualmente Según el autor (Rodríguez Chang, y otros) en la presente investigación sobre Los servidores web constituyen una parte fundamental para el funcionamiento de las aplicaciones web y por estos fluye toda la información de las entidades y personas, “Para evaluar la aplicación se utilizó un ambiente de pruebas con 21 servidores, dentro de los cuales se encontraban los servidores web Apache y Nginx. La aplicación permitió evaluar de

forma automática los 19 servidores encontrando más de 200 vulnerabilidades, mejorando en 42% la importancia de la seguridad en los servidores web.

En la tabla N° 17 de comparación de funcionalidad obtenido antes desde el mes de julio del 2022, el cual tuvo un promedio de 64,02% y luego de la aplicación de la funcionalidad mejoró en 92.32%, realizado desde agosto del 2022 hasta el mes de octubre del 2022, Lo que indica que ha sido favorable en 28,3 %. Igualmente, Según el autor (Martínez, y otros, 2018) en la presente investigación sobre las tecnologías emergentes han proporcionado una gran ventaja a los usuarios de uso y aplicación de técnicas de Machine Learning y Big Bata. En base al almacenamiento en la nube los datos pueden estar dispersos en ubicaciones y servidores remotos. Logrando mejorar en un 26% en su funcionalidad.

En la tabla N° 18 de comparación de fiabilidad obtenido antes desde el mes de julio del 2022, el cual tuvo un promedio de 62,51% y luego de la aplicación de la fiabilidad mejoró en 95.29%, realizado desde agosto del 2022 hasta el mes de octubre del 2022, Lo que indica que ha sido favorable en 32.78 %. Igualmente, Según el autor (Martínez, y otros, 2018) en la presente investigación sobre las tecnologías emergentes han proporcionado una gran ventaja a los usuarios de uso y aplicación de técnicas de Machine Learning y Big Bata. En base al almacenamiento en la nube los datos pueden estar dispersos en ubicaciones y servidores remotos. Logrando mejorar en un 30% en su fiabilidad.

En la tabla N° 19 de comparación de usabilidad obtenido antes desde el mes de julio del 2022, el cual tuvo un promedio de 63,35% y luego de la aplicación de la usabilidad mejoró en 95.77%, realizado desde agosto del 2022 hasta el mes de octubre del 2022, Lo que indica que ha sido favorable en 32.42 %. Igualmente, Los autores en la investigación (García Bordonado, y otros, 2021) concluyen que: “Una de las partes importantes de cualquier ciberataque es que el atacante no ataca a ninguna red de

alto nivel sin llevar a cabo una investigación adecuada. Y le da la importancia a la usabilidad del software en 36%

En la tabla N° 20 de comparación de eficiencia obtenido antes desde el mes de julio del 2022, el cual tuvo un promedio de 62,79% y luego de la aplicación de la eficiencia mejoró en 95.15%, realizado desde agosto del 2022 hasta el mes de octubre del 2022, Lo que indica que ha sido favorable en 32.36 %. Igualmente Soto Vásquez, Duber Enrique (2017), Donde se aumenta la eficiencia en 20% del mismo modo se ha desarrollado un análisis multivariado ingresando a un nivel mucho más profundo en cuanto a la segmentación de las organizaciones pequeña, mediana y grande.

En la tabla N° 21 de comparación de la portabilidad obtenido antes desde el mes de julio del 2022, el cual tuvo un promedio de 63,56% y luego de la aplicación de la portabilidad mejoró en 95.49%, realizado desde agosto del 2022 hasta el mes de octubre del 2022, Lo que indica que ha sido favorable en 31,93 %, igualmente En su estudio Flores (2017), que desarrollo un estudio implantado en la Oficina de Gestión de Proyectos de TI con base en la norma internacional 27001, de los ministerios del Perú logrando información se usara la norma internacional 27001 permitiendo mejorar la SI mediante la portabilidad aumento en 32% haciendo un método cuantitativo, siendo necesario para este estudio realizar un análisis lograr una estadísticas y así medir causa-efecto,.

6.3 Responsabilidad ética de acuerdo con los reglamentos vigentes.

De acuerdo con las normas y lineamientos de ética en investigación de la UNAC aprobados mediante resolución N° 210-2017-CU del consejo universitario del 07.06.2017, sigo el principio ético de la guía de investigación. conducta, los principios éticos del investigador de la UNAC, que son profesionalismo, apertura, objetividad, igualdad, compromiso, honestidad y confidencialidad.

VII. CONCLUSIONES

1.- La aplicación de un sistema de seguridad de la información optimiza los servidores web en la OTIC de la FIIS de la UNAC 2022, donde se demuestra el incremento en una medida significativa del 32,615%

2.- La aplicación de un sistema de seguridad de la información optimiza la funcionalidad de los servidores web en la OTIC de la FIIS de la UNAC 2022, donde se demuestra el incremento en una medida significativa del 28,30 %,

3.- La aplicación de un sistema de seguridad de la información optimiza la fiabilidad de los servidores web en la OTIC de la FIIS de la UNAC 2022, donde se demuestra el incremento en una medida significativa del 32,78 %,

4.- La aplicación de un sistema de seguridad de la información optimiza la usabilidad de los servidores web en la OTIC de la FIIS de la UNAC 2022, donde se demuestra el incremento en una medida significativa del 32,43 %,

5.- La aplicación de un sistema de seguridad de la información optimiza la eficiencia de los servidores web en la OTIC de la FIIS de la UNAC 2022, donde se demuestra el incremento en una medida significativa del 32,35 %.

6.- La aplicación de un sistema de seguridad de la información optimiza la portabilidad de los servidores web en la OTIC de la FIIS de la UNAC 2022, donde se demuestra el incremento en una medida significativa del 31,93 %,

VIII. RECOMENDACIONES

a) Mejorar el presupuesto para la implementación de un sistema de seguridad de la información que debe tratar aspectos de seguridad; considerando los recursos humanos capacitados que garanticen la instauración de controles efectivos para lograr un nivel de seguridad.
b) Se requiere capacitación sobre seguridad de la información para que los usuarios del área dejen de ser el eslabón débil y así garantizar un nivel de seguridad adecuado en las transferencias de datos requiere la integración de diferentes servicios.
c) Se de desarrollar los mecanismos de seguridad en servidores webs con los cifrado, firma digital, control de acceso, integridad de datos, intercambio de autenticación, tráfico de relleno, control de encaminamiento y notarización.
d) Crear protocolos para medir el nivel de incidencias en seguridad de la información en los servidores webs que afecta significativamente a la eficiencia de los procesos.
e) El desarrollo de estrategias de políticas de seguridad de la información está estrechamente vinculado a la eficiencia de servicios informáticos.

IX. REFERENCIAS BIBLIOGRÁFICAS

Areitio, Javier. 2008. *Seguridad de la Informacion Redes, Informatica y Sistemas de informacion.* Madrid : Ediciones Paraninfo s.a., 2008. pág. 561.

Arias, Fidas G. 2012. *EL PROYECTO DE INVESTIGACION Introduccion a la metodologia cientifica.* 6° Edicion. Caracas : Editorial Episteme, 2012.

Arias, Fidias G. 2012. *EL PROYECTO DE INVESTIGACION Introduccion a la metodologia cientifica.* Caracas : Editorial Episteme, 2012. pág. 146.

Baca Urbina, Gabriel. 2016. *Introduccion a la Seguridad informática.* s.l. : GRUPO EDITORIAL PATRIA, 2016. pág. 335.

CÉSAR AUGUSTO , BERNAL TORRES. 2006. *Metodologia de la Investigacion.* [ed.] Prentice Hall. Segunda edicion. 2006.

García Bordonado, : Sergio y Ortigosa Juarez, Álvaro Manuel. 2021. *DETECCIÓN Y ANÁLISIS DE ARTEFACTOS EN LOS PRINCIPALES TIPOS DE CIBERATAQUES.* UNIVERSIDAD AUTÓNOMA DE MADRID, Madrid, España : 2021.

Garcia Moran, Jean Paul, y otros. 2011. *Hacking y Seguridad en Internet.* Madrid : Ra-Ma, 2011. pág. 571.

LIZARES FIGUEROA, PAUL GIANCARLO y LÓPEZ BENAVIDES , MARCO ANTONIO. 2017. *PREVENCIÓN Y DETECCIÓN DE ATAQUES DE DENEGACIÓN DE SERVICIO DISTRIBUIDO (DDoS) MPLEMENTANDO EL MÓDULO QOS EN EL SERVIDOR WEB APACHE".* UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO, LAMBAYEQUE, PERU : 2017.

Martínez, Santand Carlos J. y Cruz, Gavilán Yolanda de la N. 2018. *Tendencias tecnológicas y desafíos de la seguridad informática.* Universidad Católica de Cuenca, Azuay, Ecuador : 2018.

Naupas, Paitan Humberto, y otros. 2014. *Metodologia de la Investigacion Cuantitativa-Cualititativa y Redaccion de Tesis.* Bogota : s.n., 2014. pág. 358.

Piattini Velthuis, Mario, Del Peso Navarro, Emilio y Del Peso Ruiz, Mar. *AUDITORIA DE TECNOLOGIAS Y SISTEMAS DE INFORMACION.* Madrid : Ra-Ma. pág. 691.

Postigo Palacios, Antonio. 1° edicion 2020. *Seguridad informatica.* [ed.] Ediciones Paraninfo. Madrid : s.n., 1° edicion 2020. pág. 141.

Rodríguez Chang, Leobel, Gonzáles Brito, Henry Raúl y Pérez Fernández, Dayana. *AUTOMATIZACIÓN DE PRUEBAS DE SEGURIDAD A SERVIDORES WEB.* Universidad de las Ciencias Informáticas, La Habana, Cuba : s.n.

Soriano , Miguel . *Seguridad en redes y seguridad de la información.* Primera edición . pág. 80.

Soriano , Miguel . *Seguridad en redes y seguridad de la información .*

Soriano. *Seguridad en redes y seguridad de la información.* Primera edición. pág. 80.

Villada Romero, Jose Luis. 2014. *Istalacion y configuracion del software de servidor Web.* Malaga : ic editorial, 2014.

X. ANEXOS

ANEXO Nº 1: MATRIZ DE CONSISTENCIA

TITULO: SISTEMA DE SEGURIDAD DE LA INFORMACIÓN PARA OPTIMIZAR LOS SERVIDORES WEB EN LA OFICINA DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIÓN DE LA FACULTAD DE INGENIERIA INDUSTRIAL Y DE SISTEMAS DE LA UNIVERSIDAD NACIONAL DEL CALLAO 2022"

PROBLEMA	OBJETIVOS	HIPÓTESIS	VARIABLES	DIMENSIONES	METODOLOGÍA
PROBLEMA GENERAL	**OBJETIVO GENERAL**	**HIPÓTESIS GENERAL**			
¿En qué medida un sistema de seguridad de la información optimiza los servidores web en la oficina de tecnologías de información y comunicación de la facultad de ingeniería industrial y de sistemas de la universidad nacional del callao 2022? **PROBLEMA ESPECÍFICO** 1.-¿En qué medida un sistema de seguridad de la información optimiza la funcionalidad de los servidores web en la oficina de tecnologías de información y comunicación de la facultad de ingeniería industrial y de sistemas de la universidad nacional del callao 2022?	Determinar en qué medida un sistema de seguridad de la información optimiza los servidores web en la oficina de tecnologías de información y comunicación de la facultad de ingeniería industrial y de sistemas de la universidad nacional del callao 2022. **OBJETIVO ESPECÍFICO** 1.-Determinar en qué medida un sistema de seguridad de la información optimiza la funcionalidad de los servidores web en la oficina de tecnologías de información y comunicación de la facultad de ingeniería industrial y de sistemas de la universidad nacional del callao 2022?	Un sistema de seguridad de la información optimiza los servidores web en la oficina de tecnologías de información y comunicación de la facultad de ingeniería industrial y de sistemas de la universidad nacional del callao 2022. **OBJETIVO ESPECÍFICO** 1.-Un sistema de seguridad de la información optimiza la funcionalidad de los servidores web en la oficina de tecnologías de información y comunicación de la facultad de ingeniería industrial y de sistemas de la universidad nacional del callao 2022.	**VARIABLE INDEPENDIENTE** Seguridad de la Información	• Integridad • Disponibilidad • Confiabilidad	**Tipo de Investigación:** Aplicada **Nivel o Alcance de Investigación:** Explicativo **Enfoque de Investigación:** Cuantitativo **Enfoque de Investigación:** Longitudinal

2.-¿En qué medida un sistema de seguridad de la información optimiza la fiabilidad de los servidores web en la oficina de tecnologías de información y comunicación de la facultad de ingeniería industrial y de sistemas de la universidad nacional del callao 2022? 3.-¿En qué medida un sistema de seguridad de la información optimiza la usabilidad de los servidores web en la oficina de tecnologías de información y comunicación de la facultad de ingeniería industrial y de sistemas de la universidad nacional del callao 2022? 4.-¿En qué medida un sistema de seguridad de la información optimiza la eficiencia de los servidores web en la oficina de tecnologías de información y comunicación de la facultad de ingeniería industrial y de sistemas de la universidad nacional del callao 2022? 5.-¿En qué medida un sistema de seguridad de la información optimiza la portabilidad de los servidores web en la oficina de tecnologías de información y comunicación de la facultad de ingeniería industrial y de sistemas de la universidad nacional del callao 2022?	2.- Determinar en qué medida un sistema de seguridad de la información optimiza la fiabilidad de los servidores web en la oficina de tecnologías de información y comunicación de la facultad de ingeniería industrial y de sistemas de la universidad nacional del callao 2022. 3.- Determinar en qué medida un sistema de seguridad de la información optimiza la usabilidad de los servidores web en la oficina de tecnologías de información y comunicación de la facultad de ingeniería industrial y de sistemas de la universidad nacional del callao 2022. 4.- Determinar en qué medida un sistema de seguridad de la información optimiza la eficiencia de los servidores web en la oficina de tecnologías de información y comunicación de la facultad de ingeniería industrial y de sistemas de la universidad nacional del callao 2022. 5.-Determinar en qué medida un sistema de seguridad de la información optimiza la portabilidad de los servidores web en la oficina de tecnologías de información y comunicación de la facultad de ingeniería industrial y de sistemas de la universidad nacional del callao 2022.	2.- Un sistema de seguridad de la información optimiza la fiabilidad de los servidores web en la oficina de tecnologías de información y comunicación de la facultad de ingeniería industrial y de sistemas de la universidad nacional del callao 2022. 3.- Un sistema de seguridad de la información optimiza la usabilidad de los servidores web en la oficina de tecnologías de información y comunicación de la facultad de ingeniería industrial y de sistemas de la universidad nacional del callao 2022. 4.- Un sistema de seguridad de la información optimiza la eficiencia de los servidores web en la oficina de tecnologías de información y comunicación de la facultad de ingeniería industrial y de sistemas de la universidad nacional del callao 2022. 5.- Un sistema de seguridad de la información optimiza la portabilidad de los servidores web en la oficina de tecnologías de información y comunicación de la facultad de ingeniería industrial y de sistemas de la universidad nacional del callao 2022.	**VARIABLE DEPENDIENTE** Servidores Web	• Funcionalidad • Fiabilidad • Usabilidad • Eficiencia • Portabilidad	**Método:** Deductivo **Diseño:** Experimental **Población:** 30 **Muestra:** 12 **Técnica:** Entrevista **Instrumento:** Cuestionario

ANEXO N° 2 ENCUESTA PARA ADMINISTRATIVOS

1. ¿ACCEDE CON FRECUENCIA A LA PÁGINA WEB DE LA FACULTAD?
   a. Muy frecuente
   b. Frecuentemente
   c. Ocasionalmente
   d. Raramente
   e. nunca
2. ¿LA INFORMACIÓN QUE CONTIENE LA PÁGINA WEB DE LA FIIS ESTA ACTUALIZADA Y ORGANIZADA?

   a. Muy frecuente
   b. Frecuentemente
   c. Ocasionalmente
   d. Raramente
   e. nunca

3. ¿EN LA FACULTAD EXISTE UN BASE DE DATOS CENTRALIZADA?

   a. Si
   b. No

4. ¿LA INFORMACIÓN EN LA PÁGINA WEB DE LA FIIS CUMPLE CON LOS REQUISITOS MÍNIMOS DE SEGURIDAD?

   a. Muy frecuente
   b. Frecuentemente
   c. Ocasionalmente
   d. Raramente
   e. nunca

5. ¿CON QUE FRECUENCIA REALIZA SUS COPIAS DE SEGURIDAD DE LA INFORMACIÓN EN EL SERVIDOR WEB DE LA FACULTAD DE INGENIERÍA INDUSTRIAL Y DE SISTEMAS?

   a. Muy frecuente
   b. Frecuentemente
   c. Ocasionalmente
   d. Raramente
   e. nunca

6. ¿QUÉ IMPORTANCIA LE OTORGA A LA SEGURIDAD DE LA INFORMACIÓN EN LOS SERVIDORES WEB?
   a. Muy importante
   b. Importante
   c. Moderadamente importante
   d. De poca importancia
   e. Sin importancia
7. ¿Cuál de los siguientes incidentes de seguridad de información se han presentado en la Oficina de Tecnología de Información y Comunicación?
   a. Propagación de virus informático.
   b. Pérdida de información por accidente o negligencia
   c. Acceso no autorizado a sus sistemas
   d. Sustracción de información por terceros
   e. Ninguno

8. ¿Cuál es la prioridad que otorga los tópicos seguridad de la información en la en la Oficina de Tecnología de Información y Comunicación?
   a) Altamente prioritarios
   b) De prioridad media
   c) De prioridad baja
   d) Con ninguna prioridad

9. ¿Usan indicadores para medir la efectividad de seguridad de la información?
   a) Si b) No

10. ¿CUENTAN CON POLÍTICAS Y PROCEDIMIENTOS DE SEGURIDAD DE INFORMACIÓN EN EL SERVIDOR WEB?
    a. Muy frecuente
    b. Frecuentemente
    c. Ocasionalmente
    d. Raramente
    e. nunca

11. ¿CONSIDERA IMPORTANTE LAS MEDIDAS DE SEGURIDAD EN LOS SERVIDORES WEB EN LA OFICINA DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIÓN DE LA FIIS?
    a. Muy frecuente
    b. Frecuentemente
    c. Ocasionalmente
    d. Raramente
    e. nunca

12. ¿QUÉ INCIDENTES DE SEGURIDAD DE INFORMACIÓN SE PRESENTARON EN LA OFICINA DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIÓN DE LA FIIS?
    a) Infección por virus
    b) Virus por e-mail
    c) Abuso de privilegios
    d) Uso de una vulnerabilidad conocida de la aplicación
    e) Deducción de contraseñas
    f) Ninguno

13. ¿Cómo cree que se originaron los incidentes en la seguridad de información?
    a) Hackers
    b) Usuarios
    c) Tecnología desfasada
    d) Desconocimiento de las políticas de seguridad.
14. ¿CUÁL ES LA FRECUENCIA DE ACTUALIZACIÓN DE LAS MEDIDAS DE SEGURIDAD DE LA INFORMACIÓN EN LOS SERVIDORES WEB?

    a. Muy frecuente
    b. Frecuentemente
    c. Ocasionalmente
    d. Raramente
    e. nunca

15. ¿CÓMO CONSIDERA EL DESARROLLO DE ESTRATEGIAS DE SEGURIDAD DE INFORMACIÓN?
    a) Muy importante
    b) Importante
    c) Medio importante
    d) Poco importante

ANEXO 3: VALIDACIÓN DEL INSTRUMENTO POR LOS JUECES EXPERTOS

FICHA DE VALIDEZ POR JUECES EXPERTOS

ESCALA DE CALIFICACIÓN

Estimado (a): DR. JUAN FRANCISCO RAMÍREZ VELIZ

Teniendo como base los criterios que a continuación se presentan, se le solicita dar su opinión sobre el instrumento de recolección de datos que se adjunta:

Marque con una **(X)** en **SI** o **NO**, en cada criterio según su opinión.

CRITERIOS	SI	NO	OBSERVACIÓN
1. El instrumento recoge información que permite dar respuesta al problema de investigación.	X		
2. El instrumento propuesto responde a los objetivos del estudio.	X		
3. La estructura del instrumento es adecuada.	X		
4. Los ítems del instrumento responden a la operacionalización de las variables.	X		
5. La secuencia presentada facilita el desarrollo del instrumento.	X		
6. Los ítems son claros y entendibles.	X		
7. El número de ítems es adecuado para su aplicación.	X		

Opinión de aplicabilidad: Aplicable [X] **Aplicable después de corregir [ ]**

No aplicable [ ]

SUGERENCIAS:

.....

.....

Apellidos y nombres del juez validador. Dr/ Mg: Dr. JUAN FRANCISCO RAMÍREZ VELIZ

DNI: 08200815, **Especialidad del validador: metodólogo [ ] tematico [X]**

estadístico [ ]

16 de Nov. del 2023

Firma del Experto Informante

FICHA DE VALIDEZ POR JUECES EXPERTOS

ESCALA DE CALIFICACIÓN

Estimado (a): Mg. Herbert Junior Grados Espinoza

Teniendo como base los criterios que a continuación se presentan, se le solicita dar su opinión sobre el instrumento de recolección de datos que se adjunta:

Marque con una **(X)** en **SI** o **NO**, en cada criterio según su opinión.

CRITERIOS	SI	NO	OBSERVACIÓN
1. El instrumento recoge información que permite dar respuesta al problema de investigación.	X		
2. El instrumento propuesto responde a los objetivos del estudio.	X		
3. La estructura del instrumento es adecuada.	X		
4. Los ítems del instrumento responden a la operacionalización de las variables.	X		
5. La secuencia presentada facilita el desarrollo del instrumento.	X		
6. Los ítems son claros y entendibles.	X		
7. El número de ítems es adecuado para su aplicación.	X		

Opinión de aplicabilidad: Aplicable [X] **Aplicable después de corregir** [ ]

No aplicable [ ]

SUGERENCIAS:

.....

.....

Apellidos y nombres del juez validador. Dr/ Mg: Mg. Herbert Junior Grados Espinoza

DNI: 46168554 **, Especialidad del validador: metodólogo** [ ] **tematico** [X]

estadístico [ ]

08 de Nov. del 2023

Firma del Experto Informante

FICHA DE VALIDEZ POR JUECES EXPERTOS

ESCALA DE CALIFICACIÓN

Estimado (a): MG. VICTOR EDGARDO ROCHA FERNÁNDEZ

Teniendo como base los criterios que a continuación se presentan, se le solicita dar su opinión sobre el instrumento de recolección de datos que se adjunta:

Marque con una **(X)** en **SI** o **NO**, en cada criterio según su opinión.

CRITERIOS	SI	NO	OBSERVACIÓN
1. El instrumento recoge información que permite dar respuesta al problema de investigación.	X		
2. El instrumento propuesto responde a los objetivos del estudio.	X		
3. La estructura del instrumento es adecuada.	X		
4. Los ítems del instrumento responden a la operacionalización de las variables.	X		
5. La secuencia presentada facilita el desarrollo del instrumento.	X		
6. Los ítems son claros y entendibles.	X		
7. El número de ítems es adecuado para su aplicación.	X		

Opinión de aplicabilidad: Aplicable [X] **Aplicable después de corregir** [ ]

No aplicable [ ]

SUGERENCIAS:

.....

.....

Apellidos y nombres del juez validador. Dr/ Mg: MG. VICTOR EDGARDO ROCHA FERNÁNDEZ

DNI: 18843120 **Especialidad del validador: metodólogo** [ ] **tematico** [ ]

estadístico [X]

10 **de** Nov. **del 20** 23

V. E. R. F.

Firma del Experto Informante

FICHA DE VALIDEZ POR JUECES EXPERTOS

ESCALA DE CALIFICACIÓN

Estimado (a): Mg. José Antonio Farfán Aguilar

Teniendo como base los criterios que a continuación se presentan, se le solicita dar su opinión sobre el instrumento de recolección de datos que se adjunta:

Marque con una **(X)** en **SI** o **NO**, en cada criterio según su opinión.

CRITERIOS	SI	NO	OBSERVACIÓN
1. El instrumento recoge información que permite dar respuesta al problema de investigación.	X		
2. El instrumento propuesto responde a los objetivos del estudio.	X		
3. La estructura del instrumento es adecuada.	X		
4. Los ítems del instrumento responden a la operacionalización de las variables.	X		
5. La secuencia presentada facilita el desarrollo del instrumento.	X		
6. Los ítems son claros y entendibles.	X		
7. El número de ítems es adecuado para su aplicación.	X		

Opinión de aplicabilidad: Aplicable [X] **Aplicable después de corregir [ ]**

No aplicable [ ]

SUGERENCIAS:

.....

.....

Apellidos y nombres del juez validador. Dr/ Mg: Mg. José Antonio Farfán Aguilar

DNI: 08144446, **Especialidad del validador: metodólogo [ ] tematico [X]**

estadístico [ ]

03 de Nov. del 20 23

Firma del Experto Informante