UNIVERSIDAD NACIONAL DEL ALTIPLANO

FACULTAD DE INGENIERÍA MECÁNICA ELÉCTRICA, ELECTRÓNICA Y SISTEMAS

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

ANÁLISIS DE RIESGOS DEL SISTEMA DE INFORMACIÓN WEB DEL COLEGIO DE INGENIEROS DEL PERÚ – CONSEJO DEPARTAMENTAL PUNO PARA IDENTIFICAR VULNERABILIDADES Y AMENAZAS MEDIANTE LA METODOLOGÍA OWASP – 2024

TESIS

PRESENTADA POR:

MIREYA YARUMI MACHACA PAMPAMALLCO

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO DE SISTEMAS

PUNO – PERÚ

2024

Mireya Yarumi Machaca Pampamallco

ANÁLISIS DE RIESGOS DEL SISTEMA DE INFORMACIÓN WEB DEL COLEGIO DE INGENIEROS DEL PERÚ – CONSEJO DEPAR...

My Files
My Files
Universidad Nacional del Altiplano

Detalles del documento

Identificador de la entrega
trn:oid:::8254:410002697

Fecha de entrega
27 nov 2024, 7:56 a.m. GMT-5

Fecha de descarga
27 nov 2024, 8:06 a.m. GMT-5

Nombre de archivo
Tesis Mireya Yarumi Machaca Pampamallco (3).pdf

Tamaño de archivo
4.8 MB

211 Páginas

40,230 Palabras

230,599 Caracteres

turnitin Página 1 of 226 - Portada Identificador de la entrega trn:oid:::8254:410002697

18% Similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para ca...

Filtrado desde el informe

- Bibliografía
- Coincidencias menores (menos de 10 palabras)

Fuentes principales

15% Fuentes de Internet
2% Publicaciones
11% Trabajos entregados (trabajos del estudiante)

Marcas de integridad

N.º de alerta de integridad para revisión

Caracteres reemplazados
156 caracteres sospechosos en N.º de páginas
Las letras son intercambiadas por caracteres similares de otro alfabeto.

Los algoritmos de nuestro sistema analizan un documento en profundidad para buscar inconsistencias que permitirían distinguirlo de una entrega normal. Si advertimos algo extraño, lo marcamos como una alerta para que pueda revisarlo.

Una marca de alerta no es necesariamente un indicador de problemas. Sin embargo, recomendamos que preste atención y la revise.

Dr. Fidel Ernesto Ticona Yanqui
INGENIERO DE SISTEMAS

Dra. Guina Guadalupe Solomayor Altamora
INGENIERO DE SISTEMAS

turnitin Página 2 of 226 - Descripción general de integridad Identificador de la entrega trn:oid:::8254:410002697

DEDICATORIA

Dedico el presente trabajo de investigación a Dios, fuente de sabiduría y fortaleza, y a mis queridos padres, Carmen Rosa y Oswaldo, por su esfuerzo, amor y apoyo incondicional en cada momento de mi vida. También extiendo mi gratitud a mis abuelos, tíos, amigos y, de manera especial, a mi hermanita menor, Tayna Miley, por su cariño, compañía. Gracias a cada uno de ustedes por inculcarme valores sólidos y por estar siempre a mi lado en este camino de aprendizaje y crecimiento personal.

Mireya Yarumi Machaca Pampamallco

AGRADECIMIENTOS

Agradezco profundamente a mis padres, tíos, abuelos y a mi hermanita menor, por su incondicional apoyo, perseverancia y confianza, que me alentaron a seguir siempre adelante a lo largo de esta etapa de mi vida. Su amor y fortaleza han sido mi mayor inspiración.

A mi asesor de tesis, Dr. Fidel Ernesto Ticona Yanqui, quien ha sido un faro en este proceso, siempre dispuesto a brindar su ayuda. Su paciencia, dedicación y guía fueron fundamentales para el desarrollo de mi proyecto de investigación, por lo que le expreso mi más sincera gratitud.

A los miembros del jurado evaluador, por guiar y encaminar la culminación de la presente tesis.

A la Universidad Nacional del Altiplano – Puno, por permitirme desarrollarme profesionalmente y brindarme las herramientas necesarias para alcanzar mis metas.

A los docentes de mi querida y prestigiosa Escuela Profesional de Ingeniería de Sistemas, quienes con su dedicación y enseñanza constante contribuyeron significativamente a mi formación. En esta escuela viví experiencias inolvidables y tuve la oportunidad de participar en diversos eventos organizados, los cuales enriquecieron mi aprendizaje y fortalecieron mi crecimiento personal y profesional.

A todos aquellos que, de una u otra forma, participaron en esta etapa de mi vida. Especialmente a mis amigos Ernesto y Melania, quienes estuvieron presentes en los momentos más difíciles y me brindaron su apoyo incondicional, ayudándome a seguir adelante.

Mireya Yarumi Machaca Pampamallco

ÍNDICE GENERAL

CAPÍTULO II

REVISIÓN DE LITERATURA

Área: Seguridad y Auditoria de Sistemas de Información

Tema: Análisis de riesgos del sistema de información web del Colegio de Ingenieros del Perú – Consejo Departamental Puno para identificar vulnerabilidades y amenazas mediante la metodología OWASP – 2024

ÍNDICE DE TABLAS

Pág.

ÍNDICE DE FIGURAS

Pág.

ÍNDICE DE ANEXOS

Pág.

ACRÓNIMOS

OWASP:	Open Web Application Security Project
MAGERIT:	Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información
CIP:	Colegio de Ingenieros del Perú
CIP – CDP:	Colegio de Ingenieros del Perú – Consejo Departamental Puno
IDOR:	Insecure Direct Object Reference
TIC:	Tecnologías de la Información y Comunicaciones
BD:	Base de Datos
PHP:	Hypertext Preprocessor
API:	Application Programming Interface
CSS:	Cascading Style Sheets
CMS:	Content Management System

RESUMEN

El aumento del uso de tecnologías digitales durante la pandemia ha incrementado los riesgos de ciberseguridad, exponiendo a las organizaciones a ataques y robos de datos que comprometen sus sistemas y operaciones en la nube. La falta de una adecuada gestión de estos riesgos puede generar pérdidas económicas y reputaciones, lo que hace crucial la implementación de estrategias de ciberseguridad para proteger la información y asegurar la continuidad operativa en un entorno cada vez más digitalizado. El presente trabajo de investigación tuvo como objetivo desarrollar un análisis de riesgos utilizando la metodología OWASP para identificar vulnerabilidades y amenazas en el sistema de información web del Colegio de Ingenieros del Perú, Consejo Departamental Puno. Para ello, se emplearon diversas herramientas de software con el fin de detectar posibles fallos de seguridad en la plataforma. La investigación fue de tipo mixto, porque se combinó métodos cuantitativos y cualitativos, lo que permite ampliar las dimensiones, lograr un entendimiento más profundo y eficiente. Tras someter el sistema web de la institución a pruebas de vulnerabilidad, se obtuvieron los siguientes resultados cuantitativos: directorios expuestos, una vulnerabilidad crítica ante ataques de diccionario, un proceso inseguro de restauración de contraseñas y fallos en la plataforma WordPress. En cuanto a los aspectos cualitativos, la evaluación reveló debilidades en el manejo de equipos informáticos, la falta de capacitaciones y la necesidad de implementar políticas de seguridad. El impacto estimado de estos riesgos en la disponibilidad del sistema web se situó entre el 80% y el 90%, lo que resalta la urgencia de adoptar medidas preventivas.

Palabras Clave: Análisis de Riesgos, Ciberseguridad, Sistema web, Vulnerabilidades,

ABSTRACT

The increased use of digital technologies during the pandemic has increased cybersecurity risks, exposing organizations to attacks and data theft that compromise their cloud systems and operations. Failure to properly manage these risks can lead to financial and reputational losses, making it crucial to implement cybersecurity strategies to protect information and ensure operational continuity in an increasingly digitalized environment. The objective of this research work was to develop a risk analysis using the OWASP methodology to identify vulnerabilities and threats in the web information system of the College of Engineers of Peru, Departmental Council of Puno. To do this, various software tools were used to detect possible security flaws in the platform. The research was of a mixed type, because quantitative and qualitative methods were combined, which allows for expanding the dimensions and achieving a deeper and more efficient understanding. After subjecting the institution's web system to vulnerability tests, the following quantitative results were obtained: exposed directories, a critical vulnerability to dictionary attacks, an insecure password reset process, and failures in the WordPress platform. In terms of qualitative aspects, the assessment revealed weaknesses in the management of computer equipment, a lack of training, and the need to implement security policies. The estimated impact of these risks on the availability of the web system was between 80% and 90%, which highlights the urgency of adopting preventive measures.

Keywords: Risk Analysis, Cybersecurity, Web System, Vulnerabilities.

CAPITULO I

INTRODUCCIÓN

El éxito de cualquier entidad u organización depende mucho de cómo manejen o implementen los controles que mitiguen cualquier evento de vulnerabilidad, estos pueden consecuentemente afectar las actividades normales de muchas organizaciones.

El sistema web del Colegio de Ingenieros del Perú, Consejo Departamental Puno, la entidad no presenta un mapa de riesgos y tampoco la capacidad de respuesta inmediata frente a un posible ataque, amenaza o vulnerabilidad que tiene respectos a la seguridad de la información.

Por esta razón se aplicó la metodología OWASP (Open Web Application Security Project) para identificar ataques y vulnerabilidades en el sistema web del CID-Consejo Departamental Puno, fundamental para la gestión de procesos y datos críticos de la sede.

Además el análisis realizado incluyó una evaluación integral del estado actual del sistema y la implementación de medidas basadas en OWASP para garantizar los principios de disponibilidad, confidencialidad e integridad de la información. Este enfoque permitió mitigar vulnerabilidades, fortalecer la seguridad del sistema y asegurar su eficiencia en el soporte de los procesos institucionales. OWASP cumple una doble misión: promover la seguridad de las aplicaciones mediante educación, sensibilización, adopción de buenas prácticas para reducir riesgos y vulnerabilidades, y ofrecer herramientas y recursos de evaluación que permiten fortalecer la protección frente a amenazas.

El objetivo general de esta investigación fue desarrollar un análisis de riesgos de los sistemas de información web del Colegio de Ingenieros del Perú, Consejo

Departamental Puno, utilizando la metodología OWASP. Los objetivos específicos incluyeron la identificación de los activos de la institución y la valoración de las amenazas a las que está expuesto el sistema de información web mediante la metodología MAGERIT. Además, se realizó el análisis siguiendo los procedimientos establecidos por OWASP para llevar a cabo pruebas de vulnerabilidad. Finalmente, se evaluaron los riesgos de seguridad relacionados con las vulnerabilidades identificadas y se midió el impacto en el sistema web del Colegio de Ingenieros del Perú, Consejo Departamental Puno.

La investigación fue estructurada de la siguiente forma, como primer capítulo se tiene introducción, el planteamiento del problema, la justificación, los objetivos e hipótesis. Como segundo capítulo se tiene, revisión de literatura, antecedentes, bases teóricas y marco conceptual. En el tercer capítulo se tiene materiales y métodos, tipo de investigación, el nivel de investigación, el diseño de la investigación, la población y muestra, técnicas de recolección de datos, técnicas de procesamiento de datos. Finalmente, en el cuarto capítulo se tiene resultados en base a la estructura de metodología OWASP. Esta información resultó esencial para el desarrollo de estrategias efectivas que fortalezcan la ciberseguridad de la institución, asegurando la protección de la información sensible en el entorno digital y alineándose con las mejores prácticas y recomendaciones establecidas por OWASP.

1.1. PLANTEAMIENTO DEL PROBLEMA

A nivel internacional, algunas de las preocupaciones de seguridad más obvias implican el acceso no autorizado a los sistemas de información por parte de usuarios externos, robo de credenciales, información personal y financiera de los usuarios. Todos estos errores son causados por una posible mala gestión de los niveles de usuarios y sus

respectivos permisos según la jerarquía del sitio. El acceso no autorizado y una mala administración del sistema pueden provocar fugas de información, tiempos de respuesta lentos para las funciones de la página y errores de autenticación en la aplicación (Marulanda & Díaz, 2018).

A nivel nacional, la tecnología está en constante innovación y con ella surgen nuevas vulnerabilidades. Las empresas públicas y privadas que quieren mantenerse a la vanguardia a menudo utilizan estas técnicas, pero rara vez realizan análisis detallados para identificar problemas, o incluso cuando implementan estas técnicas, no tienen las herramientas para identificarlas porque muchas de estas vulnerabilidades son difíciles de detectar (LLanos & Cerda, 2019).

A nivel local, específicamente en el Colegio de Ingenieros del Perú, Consejo Departamental Puno, como una institución deontológica sin fines de lucro, es el representante a los ingenieros profesionales a nivel de la región de Puno, dentro de sus actividades como órgano competente, responsable de ejercer facultades sancionatorias contra los ingenieros que no cumplan con las normativas establecidas por violaciones éticas, una de las aplicaciones más utilizadas son el sistemas web como servicio con soluciones, puesto que estas facilitan la gestión de información, la planificación de recursos, trámites, la automatización de los flujos de trabajo y por su puesto velar por la parte de seguridad de las mismas.

Actualmente, el Colegio de Ingenieros del Perú, Consejo Departamental Puno, enfrenta un problema significativo al no contar con un mapa de riesgos ni con una capacidad de respuesta inmediata frente a ataques o vulnerabilidades que comprometan la seguridad de la información que gestiona. Esta carencia pone en riesgo la integridad, confidencialidad y disponibilidad de los datos, exponiendo a la institución a brechas de

seguridad y pérdidas de información crítica. Garantizar la confiabilidad del sistema web es esencial, ya que la información gestionada es uno de los principales activos de la institución y debe ser protegida para prevenir cualquier amenaza que comprometa su seguridad.

Muchos ataques se llevan a cabo utilizando herramientas que explotan rutas alternativas para detectar debilidades en los sistemas web, con el objetivo de robar información y causar daños a la entidad. Estas vulnerabilidades a menudo se originan en las etapas de desarrollo de los sistemas web, debido a malas prácticas en la programación, configuraciones inadecuadas o el uso de usuarios y contraseñas fáciles de descifrar. Todas estas deficiencias son causantes de vulnerabilidades que los cibercriminales pueden aprovechar para llevar a cabo sus ataques.

Por esta razón, se aplicó la metodología OWASP, con el fin de llevar a cabo una auditoría de seguridad en el sistema web del Colegio de Ingenieros del Perú, Consejo Departamental Puno, lo cual fue vital para la organización puesto que con esta información, la institución puede tomar decisiones informadas para reforzar sus defensas y reducir la exposición a riesgos.

1.2. FORMULACIÓN DEL PROBLEMA

1.2.1. Problema general

¿El análisis de riesgos del sistema de información web del Colegio de Ingenieros del Perú, Consejo Departamental Puno permitirá identificar vulnerabilidades y amenazas mediante la metodología OWASP?

1.2.2. Problemas específicos

- ¿La identificación de los activos de la institución mediante la metodología MAGERIT permitirá valorar de las amenazas a las que está expuesta el sistema web del Colegio de Ingenieros del Perú, Consejo Departamental Puno?
- ¿El desarrollo del proceso de análisis de acuerdo a los procedimientos establecidos por OWASP permitirá realizar pruebas de vulnerabilidad al sistema web del Colegio de Ingenieros del Perú, Consejo Departamental Puno?
- ¿La evaluación de riesgos de seguridad ligados a los riesgos y amenazas permitirá medir el impacto en el sistema web del Colegio de Ingenieros del Perú, Consejo Departamental Puno?

1.3. JUSTIFICACIÓN DE LA INVESTIGACIÓN

Muchas de las organizaciones actualmente se encuentran en un proceso de transformación digital, todo fue acelerado por la coyuntura de la pandemia del Covid – 19, es por ello que están más propensas a los ataques y riesgos de ciberseguridad. Hoy por hoy, están empezando a tomar conciencia de proteger la información que se encuentra en la nube, dando importancia a lo que es la ciberseguridad y la gestión de riesgos.

Por lo tanto, realizar esta investigación resultó tanto justificable como necesario, ya que permitió analizar los riesgos de vulnerabilidad a los que el sistema web del Colegio de Ingenieros del Perú, Consejo Departamental Puno, estaba expuesto. Este análisis fue esencial para identificar, evaluar amenazas potenciales y riesgos asociados, sentando las bases para implementar medidas correctivas y fortalecer la seguridad del sistema ante posibles ataques.

Una vez que el Colegio de Ingenieros del Perú, Consejo Departamental Puno, identifique claramente los riesgos y vulnerabilidades detectados durante el análisis, será fundamental implementar medidas preventivas y correctivas efectivas. Estas acciones garantizarán niveles de seguridad adecuados, mitigando posibles riesgos y protegiendo la integridad de la información. Este trabajo de investigación no solo beneficia a la institución, sino también a cualquier organización con sistemas web, que siempre están expuestos a ataques cibernéticos capaces de comprometer páginas y sistemas de información. La aplicación de medidas de seguridad basadas en las directrices de OWASP mejora la eficiencia del software web y fortalece la protección de datos confidenciales, asegurando un entorno digital más seguro.

1.4. OBJETIVOS DE LA INVESTIGACIÓN

1.4.1. Objetivo General

Desarrollar el análisis de riesgos mediante la Metodología OWASP para identificar vulnerabilidades y amenazas en el sistema de información web del Colegio de Ingenieros del Perú, Consejo Departamental Puno.

1.4.2. Objetivos Específicos

- Identificar los activos de la institución y valorar de las amenazas a las que está expuesta el sistema de información web del Colegio de Ingenieros del Perú, Consejo Departamental Puno mediante la metodología MAGERIT.
- Desarrollar el proceso de análisis de acuerdo a los procedimientos establecidos por OWASP para realizar pruebas de vulnerabilidad al sistema web del Colegio de Ingenieros del Perú, Consejo Departamental Puno.

- Evaluar los riesgos de seguridad existentes ligados a los riesgos y amenazas para medir el impacto en el sistema web del Colegio de Ingenieros del Perú, Consejo Departamental Puno.

1.5. HIPÓTESIS DE LA INVESTIGACIÓN

1.5.1. Hipótesis General

La aplicación de la Metodología OWASP identifica vulnerabilidades y amenazas en el sistema de información web del Colegio de Ingenieros del Perú, Consejo Departamental Puno.

CAPÍTULO II

REVISIÓN DE LITERATURA

2.1. ANTECEDENTES DE LA INVESTIGACIÓN

2.1.1. Antecedentes Internacionales

Marulanda & Díaz (2018) llevaron a cabo un trabajo de investigación cuyo objetivo fue analizar los riesgos de seguridad de la información en el sistema de comercio electrónico SiembraViva.com, utilizando la guía de pruebas de la metodología OWASP versión 3.0. Esta metodología es reconocida por ser gratuita y de acceso abierto, bajo el proyecto OWASP (Open Web Application Security Project), se empleó para realizar auditorías a través de pruebas de pentesting. El enfoque de la investigación fue exploratorio, descriptivo y explicativo. Tras la aplicación de las pruebas de la metodología OWASP, se evaluó el estado actual de la seguridad del sistema, lo que permitió identificar diversas vulnerabilidades. Los resultados indicaron que la versión de PHP utilizada presentaba aproximadamente 38 vulnerabilidades reportadas en el CVE, de las cuales 7 fueron consideradas particularmente críticas en el sistema analizado. En respuesta a estos hallazgos, se implementaron acciones correctivas para reducir los riesgos a un nivel mínimo y se establecieron niveles de seguridad que ayudaron a prevenir posibles fallos y pérdidas de información en el sistema.

Gallegos (2019) en su proyecto de investigación tuvo como objetivo implementar controles de seguridad en una aplicación web utilizando la metodología OWASP Top 10 2017, con el fin de mitigar los riesgos que afectan la seguridad del sitio. Se realizaron tres tipos de ataques: inyección SQL, pérdida

de autenticación y exposición de datos sensibles. En la inyección SQL, se identificaron malas prácticas en la programación, específicamente en las consultas directas a la base de datos. En cuanto a la exposición de datos sensibles, se detectaron vulnerabilidades a través del puerto 80 (HTTP), lo que permitía que herramientas espía, como Wireshark, capturaran el tráfico y los paquetes transferidos. Para mitigar este riesgo, se implementó el cifrado de datos mediante el protocolo SSL, asegurando el tráfico a través del puerto 443 (HTTPS). Otro ataque evaluado fue el de fuerza bruta, donde se identificó una vulnerabilidad en la captura de credenciales (usuario y contraseña). Utilizando Burp *Suite* y configurando el proxy, se interceptaron peticiones de tipo POST en el sitio web, lo que permitió identificar los campos atacados, como username y password. El control aplicado para este ataque también consistió en el uso del certificado SSL, logrando proteger el tráfico de información y evitar la intercepción de datos críticos.

Delgado (2020) en su trabajo de investigación se enfocó en analizar determinadas tareas que permitió cumplir con el proceso de evaluación a las aplicaciones web y las redes inalámbricas de uso frecuente en la universidad, con el fin de poder encontrar posibles vulnerabilidades que pueden existir empleando la metodología OWASP. Luego de llevar a cabo cada una de las pruebas utilizando la herramienta Nessus que se aplicaron a las redes inalámbricas fueron nulas, es decir no se encontraron vulnerabilidades encontrando en 0 algún tipo de riesgo que pueda ser vulnerable frente a un ataque de un intruso y pueda cometer actos delictivos, al ejecutar otra de las herramientas de OWASP que fue la de perteneciente a la metodología mencionada se concluyó que los ataques llevados a cabo fueron bloqueados satisfactoriamente. Una vez culminada la auditoría de

análisis se estimó que en promedio, dichas aplicaciones y redes inalámbricas cumplen con un 90% de seguridad.

Morocho & Tasan (2020) en su trabajo de investigación, tuvieron como objetivo principal desarrollar un sitio web para el voto electrónico en las elecciones de la Asociación de Estudiantes de la Carrera de Ingeniería en Tecnologías de la Información, utilizando la metodología OWASP. El estudio fue de tipo cuasi experimental y de enfoque cuantitativo. Al realizar pruebas de penetración con Kali Linux, se identificaron vulnerabilidades en los sitios web desarrollados, el que fue enfocado bajo OWASP demostró ser menos susceptible a ataques informáticos, alcanzando un 91.75% de seguridad, en comparación con el sitio desarrollado rápidamente, que solo logró un 19.15% de seguridad. A través de la metodología OWASP, se logró un mayor nivel de seguridad para el sitio de votación electrónica al aplicar criterios basados en su Top Ten de detección de vulnerabilidades, enfatizando aspectos fundamentales como disponibilidad, confidencialidad, integridad, autenticidad y confiabilidad. En contraste, el sitio desarrollado vertiginosamente se centró únicamente en la funcionalidad, lo que resultó en un mayor número de vulnerabilidades.

Gamboa (2021) en su trabajo de investigación, tuvo como objetivo analizar las posibles vulnerabilidades en las aplicaciones web de la Universidad Técnica de Ambato, utilizando la metodología OWASP. El estudio fue de carácter descriptivo y explicativo, basado en información documentada y empleando métodos inductivos y deductivos. Como resultados, de las 57 pruebas realizadas, se registraron 10 con riesgo alto, 11 con riesgo medio y 12 con riesgo bajo. También se identificaron las versiones del servidor web, el lenguaje de programación, frameworks y tipos de software. Asimismo, se determinó que

algunas de las vulnerabilidades encontradas eran falsos positivos y que no todas las pruebas se pudieron realizar debido a restricciones de programación, accesos limitados y funcionalidad de la aplicación web.

Arboleda & Lopez (2022) en su investigación, los autores se basaron en la metodología OWASP – 2021, ejecutaron un Pentesting en un software de aplicación web con el fin de detectar posibles vulnerabilidades en el código fuente y promover la aplicación de una programación segura. Tras finalizar el proceso de Pentesting, elaboraron un informe detalladado que incluía una evaluación completa de las vulnerabilidades detectadas y presentaron recomendaciones para mejorar la seguridad de las aplicaciones web. Finalmente, los resultados indicaron que el número de vulnerabilidades de alto riesgo en las aplicaciones web no excedió más de una vulnerabilidad crítica por plataforma. Sin embargo, se identificaron varias vulnerabilidades, siendo las más problemáticas las fallas en la integridad del software y los datos, componentes vulnerables y desactualizados, una incorrecta configuración de seguridad y la pérdida de control de acceso. Estas conclusiones subrayan la importancia de contar con medidas de seguridad efectivas, especialmente en plataformas que manejan información sensible, como las utilizadas en instituciones académicas y otras organizaciones en Perú, que pueden ser blanco de ataques similares.

Chancusing & Guasumba (2022) en su trabajo de investigación, realizaron un análisis de vulnerabilidades utilizando la metodología OWASP ASVS, enfocado en el desarrollo de un sistema de Smart Home. El objetivo principal fue estudiar las limitaciones y beneficios en el área de domótica. Para ello, implementaron un prototipo de Smart Home, específicamente un sistema de iluminación inteligente, con el propósito de analizar las vulnerabilidades en un

entorno real y obtener resultados confiables. Luego de realizar el análisis de vulnerabilidades sobre el prototipo, lograron identificar diferencias en 14 aspectos de seguridad, entre ellos: autenticación, gestión de sesiones, control de acceso, validación de entradas, criptografía en reposo, registro de errores, protección de datos y servicios web. La metodología OWASP ASVS les proporcionó una base sólida para comprender los riesgos y mejorar la seguridad de las soluciones domóticas, ofreciendo así una perspectiva clara sobre las vulnerabilidades encontradas.

2.1.2. Antecedentes nacionales

Taype (2020) en su trabajo de investigación propuso un manual de procedimientos que fue realizado en base la metodología OWASP Mobile Security Project, bajo el proceso de evaluación de seguridad de una aplicación móvil Android, la cual permitió hacer una selección sobre los requisitos o criterios de seguridad de aplicaciones móviles para los clientes de la empresa Entelgy, una vez obtenido los resultado, este contribuyó a la empresa con los resultados, estos fueron detallados por cada etapa de evaluación, lo cual ayudó a la empresa para que pueda realizar una correcta verificación de seguridad acorde a los riesgos a los que la organización se encontraba expuesta, para luego asociarlos a alguno de los requisitos de OWASP Mobile Security Verification Standard.

Palacios (2021) tuvo como finalidad aplicar un pentesting para detectar posibles vulnerabilidades en el sistema web de la gestión administrativa de la empresa Devhuayra S.A.C. ubicada en el departamento de Huancayo, el método de investigación fue analítico, inductivo y deductivo, el tipo de investigación fue aplicada. En los resultados obtenidos, la auditoría de seguridad se ejecutó en fases,

las cuales incluyeron reconocimiento, escaneo y explotación de vulnerabilidades, siguiendo las metodologías NIST SP-800-115, OSSTMM y OWASP Top 10. Esto permitió clasificar las vulnerabilidades encontradas en el sistema web de la organización. En total, se identificaron 10 vulnerabilidades, las cuales fueron clasificadas según su gravedad en una escala específica. De estas, el 40% fueron consideradas críticas, el 10% como importante, el 30% como moderadas, y el 20% se clasificaron como de bajo impacto. Gracias a la aplicación de pentesting realizada para el Sistema web de la Gestión Administrativa redujo las vulnerabilidades en el impacto general con un 39.72%, hasta un máximo del 55.56% en cuanto al aprovechamiento de las vulnerabilidades encontradas.

Calvo (2022) en su proyecto de investigación, planteó como objetivo determinar la existencia de relación entre la aplicación del pentesting y la seguridad informática en los equipos tecnológicos de la Universidad Nacional Santiago Antúnez de Mayolo. Su estudio tuvo un diseño no experimental, ya que no se modificaron variables y trabajó con una única muestra. Los resultados a los que llegó al hacer la aplicación del pentesting se relacionó de manera significativa con la seguridad informática, con una correlación alta y un coeficiente de Spearman de 0.779. Mediante el uso de las pruebas de OWASP, se lograron identificar varias vulnerabilidades, entre ellas, fue la implementación del servidor Apache, que mostró un impacto global bajo de 2.750 y un nivel alto de probabilidad de 6.125. Otra vulnerabilidad detectada fue en PHP, con un impacto global bajo de 1.500 y un nivel medio de probabilidad de 5.

2.2. MARCO TEÓRICO

2.2.1. MAGERIT

MAGERIT es una metodología desarrollada y promovida por el Consejo Superior de Administración Electrónica (CSAE), centrada en el análisis y gestión de riesgos. Su objetivo no solo es identificar y estudiar los riesgos en los sistemas de información, sino también realizar un análisis profundo de los posibles impactos que puedan derivarse de una violación de seguridad. A través de esta metodología, se identifican las amenazas que pueden comprometer a los sistemas de información, se determinan las vulnerabilidades, y finalmente, se obtienen resultados que permiten proponer medidas para mitigar estos riesgos y proteger los activos de las organizaciones. En cuanto a la gestión de Riesgos, los análisis permiten tomar medidas adecuadas para comprender, prevenir, impedir, reducir o controlar los riesgos que hayan sido identificados y de esta manera reducir al mínimo su potencialidad o sus posibles perjuicios.

Para una mejor toma de decisiones de los órganos de gobiernos, la presente metodología implementa un proceso de gestión de riesgos dentro de un marco de trabajo teniendo en cuenta los riesgos derivados del uso de tecnologías de la información. Existen una infinidad de aproximaciones referentes al problema de análisis de riesgos, entre ellas se tiene herramientas de soporte, las guías informales entre otras. Cada una de ellas permite centrarse en el análisis de riesgos para saber qué tan seguros o inseguros pueden llegar a ser los sistemas (Administración Electrónica, 2012).

Por ende el reto principal de toda organización es identificar la complejidad del problema al que se enfrenta esto va en el sentido de que se tiene

que evaluar un sin fin de elementos que se deben de considerar y deben de ser evaluados. Para ello MAGERIT persigue los siguientes objetivos:

Directos:

- Los responsables directos de las organizaciones de información deben ser informados de los riesgos potenciales y de cómo gestionarlos de manera efectiva.
- Ofrecer un enfoque sistemático para evaluar los peligros asociados con el uso de las TIC.
- Mantener bajo control los riesgos y ayudar a planificar y encontrar el tratamiento apropiado.

Indirectos:

- Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

2.2.2. OWASP

OWASP por sus siglas en inglés (Open Web Application Security Project) con traducción al español, proyecto de seguridad de aplicaciones web abiertas, es una organización sin fines de lucro globalmente reconocida, cuya misión es mejorar la seguridad del software. Fundada en 2001, OWASP promueve la creación de aplicaciones web seguras a través de herramientas, recursos y metodologías de seguridad abierta y es accesible para todos. La organización es conocida por su enfoque colaborativo, ofreciendo guías, estándares, y metodologías que ayudan a los desarrolladores, auditores y profesionales de

seguridad a identificar y mitigar vulnerabilidades en aplicaciones web. (OWASP, 2021)

OWASP propone varias metodologías para evaluar la seguridad en aplicaciones web. Una de las más destacadas es la Guía OWASP Testing Guide, que proporciona un conjunto de pasos clave para realizar pruebas de vulnerabilidad. Las cuales son:

- Recopilación de Información: Se recolecta la mayor cantidad de información sobre la aplicación, como los servidores, sistemas operativos, servicios y estructuras de red.
- Análisis de la Configuración: Revisión de configuraciones incorrectas en los servidores y aplicaciones.
- Análisis de Vulnerabilidades: Se realiza una búsqueda exhaustiva de fallos conocidos y configuraciones incorrectas.
- Pruebas de Autenticación: Evaluar la seguridad de los mecanismos de autenticación, como contraseñas débiles o configuraciones incorrectas.
- Pruebas de Autorización: Revisión de los controles de acceso a recursos y sistemas.
- Pruebas de Manejo de Sesiones: Analizar cómo se manejan las sesiones de usuario para detectar posibles ataques de secuestro de sesión.
- Validación de Entradas: Comprobar la seguridad en la validación de entradas del usuario, para evitar ataques como inyecciones SQL.
- Pruebas de Seguridad de los Datos: Evaluación del cifrado y la integridad de los datos almacenados y en tránsito.

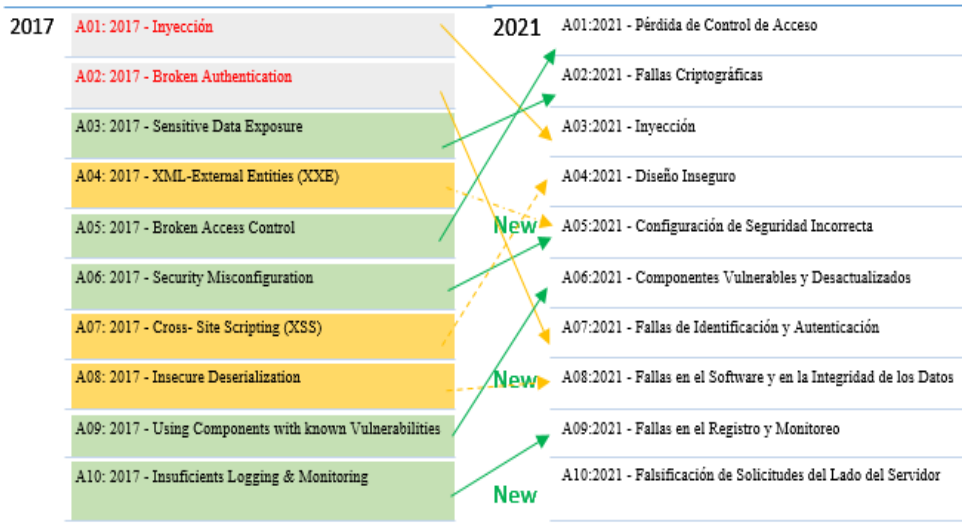
Esta guía es un recurso ampliamente utilizado por desarrolladores y profesionales de seguridad para identificar y mitigar riesgos en sistemas web, enfocándose en una evaluación exhaustiva y detallada. Por otro lado, una de las variantes más conocidas es el OWASP Top 10, un recurso que destaca las principales vulnerabilidades en aplicaciones web. En la actualización de OWASP Top 10 del año 2021, se realizaron cambios significativos, se incorporaron tres nuevas categorías de vulnerabilidades para abordar las amenazas más recientes y críticas. Cuatro categorías con cambios de nombre y alcance, estas modificaciones se realizaron para centrar la atención en las causas fundamentales de las vulnerabilidades, en lugar de enfocarse solo en los síntomas. Este enfoque permite a los desarrolladores y auditores abordar las vulnerabilidades desde la raíz, la lista publicada por la organización OWASP (Open Web Application Security Project) identifica las diez principales vulnerabilidades de seguridad en aplicaciones web como se muestra en la Figura 1.

Es esencial porque prioriza amenazas críticas para que las organizaciones enfoquen sus esfuerzos en mitigar los riesgos más importantes, existen una actualización constante para reflejar las amenazas emergentes y presenta un guía de mejores prácticas para desarrolladores y auditores de seguridad.

Para la investigación permitió enfocar los esfuerzos como la del Colegio de Ingenieros del Perú, Consejo Departamental Puno**,** que buscó identificar riesgos de seguridad en el sistema web, OWASP Top 10 sirve como una guía para priorizar los análisis y pruebas de vulnerabilidad. Permitió centrar la atención en los aspectos más críticos y con mayor riesgo. De esta manera, la institución pudo adoptar un enfoque proactivo hacia la ciberseguridad, elevando sus estándares de protección y mejorando la resiliencia del sistema ante futuros ciberataques.

Figura 1

Cambios en el Top 10 de 2021



Nota: (OWASP, 2021)

A continuación se muestra la metodología OWASP 2021 que consiste en los siguientes procesos:

2.2.3. Pérdida de Control de Acceso

Ahora fue considerada como la más crítica en seguridad de aplicaciones web, subió a la primera posición debido al alto riesgo que representa. Los datos indicaron que, en promedio, el 3,81% de las aplicaciones probadas tenían una o más Common Weakness Enumerations (CWEs), con más de 318.000 ocurrencias dentro de la categoría. Además, las 34 CW son relacionadas con la pérdida de control de acceso fueron las más frecuentes, superando a cualquier otra categoría en términos de apariciones en aplicaciones, lo que la convirtió en el riesgo más común y peligroso para las aplicaciones web. Esta tendencia reflejó la necesidad de mejorar los controles de acceso para mitigar las vulnerabilidades que permiten a los atacantes acceder indebidamente a datos o funcionalidades restringidas (OWASP, 2021).

2.2.4. Fallas Criptográficas

Subió a la segunda posición, antes conocida como A3:2017-exposición de datos sensibles, que era más una característica que una causa raíz. El nuevo nombre se centró en las fallas relacionadas con la criptografía, como se ha hecho implícitamente antes. Esta categoría frecuentemente conllevó a la exposición de datos confidenciales o al compromiso del sistema (OWASP, 2021).

Para Miranda (2022) los fallos criptográficos se han convertido en un problema muy grande en el mundo, porque se convirtieron muy dependientes de las grandes transacciones digitales y las comunicaciones en línea que hacen uso de la criptografía, en el mismo contexto hoy en día se debe dar una atención especial a los algoritmos criptográficos a nivel global entorno a la ciberseguridad.

2.2.5. Inyección SQL

Trata de un clásico que siempre se encontró en el top 10 de OWASP, va relacionado directamente con la validación de datos y permitir aquella información ya sea directa o indirectamente alterados por algún usuario (Aguilar, 2013).

La Inyección ha descendido hasta la tercera posición en el OWASP Top 10 (2021). Aunque sigue siendo una amenaza significativa, el 94% de las aplicaciones probadas mostró algún tipo de vulnerabilidad de inyección, con una tasa máxima de incidencia del 19% y un promedio de 3.37%. Esta categoría incluyó 33 CWEs, registrando 274.000 ocurrencias, la segunda mayor cantidad en las aplicaciones analizadas. En esta edición, Cross-Site Scripting (XSS) ha sido incorporado a esta categoría de riesgo, ampliando su alcance para incluir otros tipos de inyecciones más allá de las clásicas inyecciones SQL (OWASP, 2021).

2.2.6. Diseño Inseguro

Esta categoría se encuentra en el top 10 de OWASP porque es una nueva creación que aborda los diversos riesgos relacionados con los errores de diseño y arquitectura web (Tarlogic, 2022).

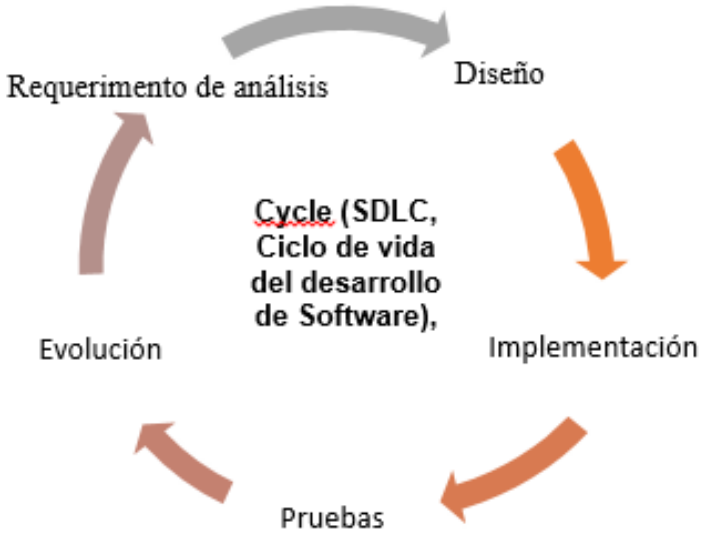
Esta es una nueva inclusión en el OWASP Top 10 de 2021, que pone el foco en los riesgos derivados de fallas en el diseño de las aplicaciones. Categoría que además subraya la importancia de adoptar prácticas de seguridad desde las primeras etapas del desarrollo, moviendo las actividades de seguridad a la izquierda del ciclo de desarrollo.

El diseño inseguro no puede ser corregido solo con una implementación perfecta, ya que los controles de seguridad necesarios nunca fueron concebidos para proteger contra ataques específicos. Para superar este desafío, es esencial integrar modelos de amenazas, patrones de diseño seguro y arquitecturas de referencia desde el principio del proceso de desarrollo de los sistemas, pero no se trata solo se los errores que se presenten en la implementación del código, si no vas más allá, teniendo como problema esencial de cómo se estructura y conceptualiza el sistema, la consideración de las políticas de seguridad también son muy importantes.

Corredera (2023) reafirma que es una de las categorías amplias, la cual es la que representa las debilidades, Sin embargo, esta no es la fuente de todas las categorías de riesgo del top de OWASP, pues existe una diferencia en lo que es diseño inseguro y la implementación de esta, la razón es que poseen diferentes causas y diversas soluciones (OWASP, 2021).

Figura 2

Ciclo de vida del Desarrollo de Software



Nota: (Hacking Knowledge, 2023)

Así mismo presenta algunos ejemplos de riesgo:

- No se realiza un correcto seguimiento a cada etapa del SDLC, o no se toman en cuenta etapas tempranas.
- No se toman en consideración un diseño previo de la infraestructura tecnológica que estará soportando la aplicación ni de los componentes de la misma.
- No se comunican los requerimientos con claridad.
- No se cuenta con algoritmos y reglas de negocio de las tareas que estará desarrollando la aplicación.

2.2.7. Configuración de Seguridad equivocada

Subió desde la sexta posición en la edición anterior del OWASP Top 10. Esta categoría es una de las más comunes, ya que el 90% de las aplicaciones probadas presentaron alguna configuración incorrecta, con una tasa de incidencia

promedio del 4.5% y más de 208.000 ocurrencias de debilidades conocidas (CWEs). El aumento de software altamente configurable ha hecho que estas vulnerabilidades sean más frecuentes. Además, en esta edición, la categoría Entidades Externas XML (XXE) se integra en este tipo de riesgo (OWASP, 2021).

2.2.8. Componentes Desactualizados y Vulnerables

Es la nueva denominación de la categoría antes llamada "Uso de Componentes con Vulnerabilidades Conocidas". Subió desde la novena posición en la edición de 2017 al sexto lugar en 2021. Aunque es un problema difícil de evaluar y probar, es fundamental porque el uso de software desactualizado y con componentes vulnerables sigue siendo un gran riesgo. Esta es la única categoría que no tiene ninguna Common Vulnerabilities and Exposures (CVE) asociada con las debilidades (CWEs) incluidas, lo que complica su evaluación (OWASP, 2021).

2.2.9. Fallas de Identificación y Autenticación

Anteriormente conocida como "Pérdida de Autenticación", descendió desde la segunda posición en la lista de 2017. Esta categoría ahora abarca Common Weakness Enumerations (CWEs) relacionadas con fallas en la identificación de usuarios, además de la autenticación. Aunque sigue siendo crucial, la adopción creciente de frameworks estandarizados para gestionar la autenticación ha contribuido a mitigar parte de este riesgo (OWASP, 2021).

2.2.10. Fallas en el Software e Integridad de los Datos

Es una nueva categoría que fue incluida en la edición de 2021 del OWASP Top 10, se centra en las suposiciones incorrectas relacionadas con las actualizaciones de software (OWASP, 2021).

2.2.11. Fallas en el Registro y Monitoreo

Es una categoría que ha sido revisada y ampliada en la edición 2021 del OWASP Top 10. Anteriormente era conocida como A10:2017 - Registro y Monitoreo Insuficiente. En tanto descendió del décimo al noveno lugar en el ranking por lo cual se ha expandido para incluir una gama más amplia de tipos de fallas. A pesar de que es difícil de probar y no está bien representada en los datos de CVE/CVSS, las vulnerabilidades en esta categoría pueden tener un impacto significativo, afectando directamente la visibilidad del sistema, la efectividad de las alertas de incidentes y la capacidad para llevar a cabo análisis forenses tras un incidente de seguridad (OWASP, 2021).

Para los atacantes ingresar a los sistemas y obtener acceso para poder extraer, alterar, o posiblemente destruir la información de cualquier entidad se debe realizar un adecuado registro y monitoreo de los sistemas internos y está a la vez pueda tener una respuesta inmediata frente a estos posibles ataques (Morales, 2022).

2.2.12. Falsificación de Solicitudes del Lado del Servidor

Esta categoría refleja la percepción de la comunidad sobre la importancia de la seguridad, actualmente no se encuentra completamente representada en los datos disponibles, esto indica una preocupación creciente por los riesgos asociados con la falsificación de solicitudes, lo que puede comprometer la integridad y la seguridad de las aplicaciones web. El proceso de la metodología OWASP y la mejora continua permite que los que desarrollan sistemas web, logren comprender todos los parámetros que da valor agregado a la hora de ejecutar códigos, de esta manera podrán comprender mejor y realizar buenas

practicas a la hora de la programación, logrando así concretar un buen trabajo que beneficiará a la organización (Walteros et al. 2019).

A través de este enfoque integral, OWASP permite evaluar y mitigar riesgos relacionados con la seguridad, asegurando que todas las vulnerabilidades sean detectadas y abordadas para proteger la integridad de los sistemas (Delgado, 2020).

2.2.13. Gestión y análisis de riesgos

Para Rodríguez & Peralta (2013) es elemental que para cualquier tipo de organización, este debe de conocer a qué tipo de riesgos están expuestos y sometidos, pero es imprescindible poderlos gestionar de manera inmediata, esta implica dos grandes tareas como se ve en la Figura 3.

Figura 3

Gestión y Análisis de Riesgos

Nota: (Rodríguez & Peralta, 2013)

De acuerdo con Castro et al. (2020), el análisis de riesgos es una herramienta clave de gestión que facilita la toma de decisiones tanto antes de lanzar un servicio como durante su operación. Es un proceso dinámico y continuo que debe aplicarse a lo largo de todo el ciclo de vida del proyecto. Cada vez que se obtenga nueva información que pueda introducir o modificar un riesgo, será necesario realizar un nuevo análisis y, si es preciso, ajustar las prioridades para

mitigar los riesgos de manera efectiva. Esto garantiza que el proyecto se mantenga alineado con los objetivos de seguridad y protección establecidos. Al identificar y priorizar los riesgos más críticos, se pueden tomar medidas preventivas de manera proactiva, reduciendo la probabilidad de incidentes y sus posibles impactos. Este enfoque iterativo también ayuda a mejorar la resiliencia del sistema a lo largo del tiempo, ajustándose a nuevas amenazas y tecnologías emergentes, asegurando así una gestión de riesgos más robusta y adaptativa. Para ello se tiene:

- **Activos:** Son componentes del sistema de información (o relacionados con él) que apoyan el propósito de la organización. La información, los datos, los servicios, las aplicaciones (software), los equipos (hardware), las comunicaciones, los recursos administrativos, los recursos físicos y los recursos humanos son todos componentes de esta categoría (Rodríguez & Peralta, 2013).

2.2.14. Vulnerabilidad

La vulnerabilidad es un concepto clave en la seguridad de la información y ciberseguridad, ya que representa cualquier punto débil en un sistema, red, aplicación o activo que podría ser aprovechado por una amenaza o atacante. Es una propiedad que puede resultar del diseño del sistema, su implementación, configuración, o de fallas en procesos o controles. Las vulnerabilidades también pueden surgir de errores humanos, fallas tecnológicas, o incluso cambios en el entorno operativo. Al evaluar el grado de vulnerabilidad, es fundamental considerar no solo la debilidad en sí misma, sino también la importancia de la información que está en riesgo. Si la información es crítica o confidencial, el impacto de esa vulnerabilidad será mayor, incluso si la debilidad es pequeña. Por

lo tanto, el valor del activo influye directamente en la gravedad de la vulnerabilidad (ISO 27001, 2020).

2.2.15. Amenaza

Una amenaza se refiere a cualquier evento o circunstancia que pueda explotar una vulnerabilidad en un sistema o activo de información para causar daño o comprometer su seguridad. Estas amenazas pueden ser deliberadas, como los ataques cibernéticos, o accidentales, como errores humanos o fallos técnicos, las amenazas son agentes externos o internos que pueden causar incidentes de seguridad si no se mitigan adecuadamente. Pueden clasificarse según su naturaleza y origen. Se distinguen cuatro tipos principales: no humanas, que incluyen eventos naturales o fallos tecnológicos; humanas involuntarias, como errores o accidentes sin intención de causar daño; humanas intencionadas con presencia física, donde personas con acceso directo al sistema realizan acciones maliciosas, como sabotajes o robos; y humanas intencionadas de origen remoto, como ciberataques ejecutados por hackers mediante medios digitales sin acceso físico al sistema. Estas clasificaciones ayudan a identificar y gestionar los riesgos más eficientemente, según lo establece la norma (ISO 27001, 2020).

2.2.16. Nessus

Es una herramienta única diseñada para detectar fallas de seguridad en dispositivos mediante el uso de una amplia base de datos que contiene vulnerabilidades conocidas. Realiza escaneos de vulnerabilidades en diversos sistemas operativos, lo que permite identificar puntos débiles en la infraestructura de TI. Ofrece tanto versiones de pago como de código abierto, lo que lo hace accesible para diferentes tipos de usuarios. Las vulnerabilidades detectadas por

Nessus son errores informáticos o fallas que representan amenazas para la seguridad de un sistema, y su identificación es esencial para proteger los activos y la información de una organización (Cilleruelo, 2024).

2.2.17. Nmaps

Nmap (Network Mapper) es una herramienta de código abierto utilizada para escanear redes, descubrir dispositivos, servicios y puertos abiertos. Se emplea principalmente para evaluar la seguridad de redes, identificar servicios en ejecución y detectar vulnerabilidades. Disponible para sistemas Linux, permite identificar aplicaciones instaladas, así como escanear puertos y direcciones IP dentro de una red, lo que facilita el análisis de posibles puntos débiles y amenazas en la infraestructura de red. Nmap es esencial para los administradores de sistemas y expertos en seguridad en la identificación de riesgos y en la mejora de la protección de redes (Shivanandhan, 2023).

2.3. MARCO CONCEPTUAL

2.3.1. Sistema web

Para Alarcon (2024) es un tipo de software la cual se ejecuta en un servidor remoto y se accede a través de un navegador web, estos permiten que los usuarios interactuen con ellos a través de internet, sin necesidad de instalar software adicional, a diferencia de las aplicaciones convencionales que requieren ser descargadas e instaladas en un dispositivo. Los sistemas web son extremadamente flexibles y accesibles debido a su diseño para ser independientes de plataformas o sistemas operativos particulares en donde los usuarios pueden acceder a los servidores remotos desde cualquier dispositivo conectado a internet, lo que facilita la colaboración y el trabajo en remoto. Se compone de un frontend (interfaz de

usuario) que interactúa con el usuario y un backend (servidor y base de datos) que procesa, almacena y gestiona la información solicitada. Existen aspectos adicionales que subrayan la complejidad y la importancia de construir, mantener y asegurar un sistema web de alto rendimiento para que sea seguro, eficiente y adaptable.

2.3.2. Vulnerabilidades Informáticas

2.3.2.1. Vulnerabilidad

Con base a Feito (2007) la vulnerabilidad se refiere a la posibilidad de sufrir daño o ser afectado negativamente por una amenaza. También puede describirse como la capacidad de ser persuadido o tentado, la falta de control sobre ciertas circunstancias, o la debilidad de una posición de poder. En el contexto de la seguridad, la vulnerabilidad es una debilidad inherente a un sistema o activo que puede ser explotada, lo que podría resultar en una pérdida de confidencialidad, integridad o disponibilidad. Entonces la importancia se base en las características y circunstancias de una persona o grupo de personas que afectan su capacidad de anticipar, lidiar, resistir y recuperarse de una amenaza en un momento determinado (Rivera, 2011).

2.3.3. Vulnerabilidad Informática

Con respecto a las vulnerabilidades informáticas según Santander (2023), es una falla en un sistema que puede ser utilizada por alguien con malas intenciones para comprometer su seguridad. Las vulnerabilidades pueden presentarse de varios tipos, pueden ser de hardware, software, y pueden ser explotadas o utilizadas por atacantes. Así mismo González & Montesino (2018)

afirman que la vulnerabilidades son errores, debilidades, fallas, o algún dispositivo del sistema que lleva a un error de confidencialidad.

Una vulnerabilidad puede ser:

- Buffer overflow: Esta es una de las vulnerabilidades causadas por la gran cantidad de datos copiados en el buffer, que puede causar una sobre escritura de espacios de memoria adyacentes al sobrepasar el tamaño del buffer (León & Gervacio, 2015).
- Vulnerabilidades de la condición de carrera: Esta presente vulnerabilidad generalmente se da cuando se cumple varios procesos y estas acceden al mismo tiempo a un recurso compartido (Villacis, 2022).
- Error de formato en cadenas: Esta se presenta cuando las aplicaciones aceptan sin validar la entrada de datos las cuales son proporcionadas por el usuario, de tal manera se puede afirmar que esta vulnerabilidad es proveniente de descuidado al momento de realizar la programación, los leguajes como C/C++, son los más afectados por la presente vulnerabilidad, consecuentemente es casi seguro que se produzca un robo de información y datos de los usuarios (Villacis, 2022).
- Vulnerabilidades complejas de Windows: Esta es una de las vulnerabilidades más comunes entre los usuarios, también es conocida como Windows Spoofing, la cual consiste en que un atacante puede tener el control de un ordenador y por medio de ella pueda realizar notificaciones o enviar mensajes a la víctima, en ocasiones este suele tener mensajes de que hemos sido beneficiarios de un premio de alguna empresa reconocida, o talvez sea realizado mediante juegos o situaciones similares (Villacis, 2022).

- Cross Site Scripting: Esta vulnerabilidad se presenta cuando los atacantes logran incrustar scripts maliciosos en las páginas web. Según SeoEstudios, (2020) son fragmentos las cuales contienen códigos, y su principal objetivo es la de añadir funciones dentro de una página web, lo que facilita a los atacantes poder obtener usuarios y contraseñas pero no necesariamente en la web que es del usuario si no en la del atacante (Fabra, 2022).
- Inyección de SQL: Al igual que las anteriores vulnerabilidades esta afecta específicamente a los servidores de base de datos de las organizaciones, pues estas son la red de equipos zombies utilizan los recursos de la empresa para actividades ilícitas (Castro, 2020).

2.3.3.1. Clasificación de Vulnerabilidades

Navarro (2018) señala que las vulnerabilidades se pueden clasificar según el tipo de sistema que afectan. Estas clasificaciones incluyen:

- Vulnerabilidad de bajo nivel y software malicioso. Afecta al sistema operativo y aplicaciones a bajo nivel propiciadas generalmente por los errores que se cometen en la hora de ejecutar y programar los códigos como los Buffer overflow mencionados anteriormente (Serra et al. 2021).
- Vulnerabilidad de red. Son aquellas que afectan a los softwares y componentes de una red, incluidas las interconexiones entre estos. El análisis de vulnerabilidad en redes complejas se enfoca en medir y evaluar el impacto que tendría la eliminación o fallo de un componente de la red, lo que podría comprometer la seguridad, estabilidad y funcionalidad de todo el sistema (Lotero & Hurtado, 2015).

- Vulnerabilidades en las aplicaciones web. Estas vulnerabilidades se agravan cuando los usuarios gestionan información en la nube, siendo clasificadas como de alto nivel. En aplicaciones web, este tipo de vulnerabilidades representa aproximadamente un 45% del total de otras vulnerabilidades, lo que resalta la importancia de implementar medidas de seguridad robustas en entornos de cloud computing y aplicaciones web (Lotero & Hurtado, 2015).

2.3.4. Amenazas informáticas

Las amenazas y las vulnerabilidades están estrechamente relacionadas si se toma en cuenta a cualquier organismo que emplea los datos, simplemente verán que existen amenazas tanto de origen interno y externo, por ejemplo, las agresiones técnicas, naturales o humanas, documentadas por ISO 27001 (Guevara et al. 2023).

2.3.5. Intrusos en las redes

- Hacker: Se refiere a una persona con experiencia en computadoras y habilidades sobresalientes en programación, estos individuos utilizan su conocimiento para explorar y comprender sistemas informáticos, a menudo buscando aprender más y expandir sus capacidades técnicas. En origen ellos no ingresan a los sistemas ajenos con propósito malicioso o para beneficio personal, existe una confusión mediática en cuanto sus objetivos, los hackers siempre estarán en una continua búsqueda de información, logran aprender día a día obteniendo información sin barreras. Para Bustamante (2020) la palabra hacker se ha ido desvirtuando,

y es por lo que ha ido surgiendo la diferenciación entre white hats, grey hats y black hats (Ángeles & Cilleres, 2022),

- Cracker: También le dan el término de hacker, cuyas intenciones van más allá de realizar una investigación, su fin contiene maliciosa, irrumpe en un sistema, usualmente lo hace por medio de una red, desvía o vulnerara las claves o licencias de software, o en otros casos, pueden crear brechas en la seguridad del sistema de manera deliberada (Duque & Tamayo, 2019).
- Phreakers: Son conocidas como aquellas personas que hacen uso de técnicas por vía telefónica, poseen un gran conocimiento referente a la telefonía, y logran vulnerar gracias a los errores de seguridad de las grandes compañías telefónicas para realizar llamadas gratuitas (Duque & Tamayo, 2019).
- Spammers: Son responsables del envío masivo de mensajes de correo electrónico no solicitados utilizando redes como internet, consecuentemente causa colapsos de servidores y sobrecarga en los buzones de correo de los usuarios. Se han presentado casos donde estos correos una vez abiertos contienen virus informáticos (Gómez, 2019).

No es necesario ser un hacker para realizar acciones maliciosas a los sistemas de información; muchas veces, una persona con conocimientos avanzados en hacking puede realizar acciones maliciosas por diversión, por desconocimiento, entre otros motivos. Es importante recordar que el personal de una empresa es su talón de Aquiles, por lo que han surgido nuevos sistemas de ataque como los siguientes:

- Ingeniería social: En este contexto, el atacante se vale de interacción humana y habilidades sociales para obtener información confidencial

sobre una organización. Este enfoque, conocido como ingeniería social**,** permite a los hackers acceder a datos sensibles a través de conversaciones o manipulaciones sutiles. Al engañar a las personas, especialmente a aquellos en posiciones clave dentro de la organización, los atacantes pueden eludir medidas de seguridad y obtener la información que desean (Martínez, 2006).

- Ingeniería social inversa: En este caso el atacante crea un rol de autoridad y demuestra que tiene la capacidad de brindar ayuda a los usuarios y estos lo llaman ante algún imprevisto, de esta manera aprovecha la oportunidad para pedir la información necesaria y así solucionar el problema tanto del usuario como el propio. Un claro ejemplo es cuando el hacker sabotea un sistema, y es el mismo que se ofrece para dar solución al problema, aprovechando la situación para auto promoverse y hacerse parecer que da asistencia a un problema (Susatama, 2022).
- Trashing (cartoneo): Generalmente, son personas que se encargan de rastrear en las papeleras de búsqueda, dónde la información que fue eliminada de un ordenador puede ser vulnerada por ellos (Bustamante, 2020).
- Terroristas y robos: Esta no se refiere a las personas que ponen bombas o queman autobuses, sino a cualquier persona que ataca al sistema simplemente para causar daño. La información de los computadores, al igual que los discos magnéticos y el software, puede copiarse fácilmente una vez que está haya sido vulnerada. Los terroristas no solo han demostrado que tienen habilidades en el marketing en línea, sino también se han vuelto personas expertas en recopilar datos sensibles de los más de

mil millones de sedes que forman la telaraña mundial, se les facilita realizar localizaciones gracias al Internet, pueden encontrar a sus objetivos sin importar desde dónde lo hagan, centrales nucleares, edificios públicos, aeropuertos y puertos, así como las medidas antiterroristas (Weimann, 2017).

- Intrusos remunerados: Es el grupo de atacantes más peligroso de un sistema, aunque es el menos común en las redes convencionales debido a que suele afectar más a las grandes empresas. Se trata de personas con gran un gran conocimiento del sistema, que son contratados por una tercera persona para que esta pueda sustraer información importante para luego obtener beneficios (Gómez, 2019).
- Personal interno: Son aquellas que provienen del personal que trabaja dentro de la propia organización. A menudo, este riesgo pasa desapercibido porque se asume un ambiente de confianza entre los empleados. Estas vulnerabilidades pueden surgir de manera intencional, cuando un empleado actúa con malicia, o de forma involuntaria, como resultado de errores o negligencia. La combinación de acceso a información crítica y la falta de vigilancia puede facilitar que estas amenazas se materialicen (IBM, 2022).
- Ex–Empleados y curiosos: Se trata del personal que dejó de laborar en la organización por alguna situación de descontento, fallas de un sistema que conocen para dañarlo como venganza por algún hecho que creen injusto. Se dan casos en que por venganza, pueden acceder en algunos casos a través de cuentas de usuario que todavía no han sido canceladas en los equipos y servidores de la organización (Gómez, 2019).

2.3.6. Seguridad de Información en sistemas web

Según Balseca et al. (2021) el tema de la seguridad de la información ha sido discutido por diversos autores, quienes han llegado a una comprensión común centrada en la protección de la confidencialidad**,** integridad **y** accesibilidad de la información. Este enfoque incluye no solo la tecnología**,** sino también los procesos y las personas, con el fin de reducir las amenazas que afectan a la información. Como resultado, en la actualidad se han implementado diferentes medidas y técnicas para fortalecer la seguridad en este ámbito.

A ello Chiluiza & Enciso (2023) afirman que el primer paso crucial en la seguridad de los sistemas es la detección de cualquier amenaza a la que estén expuestos. Esto permite tomar medidas preventivas contra posibles ataques. Sin embargo, destacan que, dado que las redes están en constante evolución, abordar este tema se ha vuelto cada vez más complejo debido a las crecientes exigencias operativas y la alta demanda de seguridad.

Para Tarazona (2007) la seguridad de información de cualquier organización va más allá de un simple problema de vulnerabilidad de información, básicamente esta debería estar orientada a la protección de la información de manera intelectual, debe ser parte primordial y por último se debe realizar una evaluación y actualización constantemente. La seguridad informática como conjunto de tecnologías, procesos y prácticas fueron diseñadas para la protección de redes, dispositivos, programas y datos en caso de algún ciberataque, hackeo, daño o acceso no autorizado tanto a nivel interno como externo dentro de las organizaciones.

CAPÍTULO III

MATERIALES Y MÉTODOS

3.1. UBICACIÓN GEOGRÁFICA DEL ESTUDIO

La presente investigación se desarrolló en la ciudad de Puno, en el Colegio de Ingenieros del Perú, Consejo Departamental de Puno, ubicado en Jr. Mariano H. Cornejo Nro. 130, Barrio Independencia como se muestra en la Figura 4. La filial de Puno se estableció en la ciudad de Puno, con la elección de su primera junta directiva para el período de 1967-1968 (Colegio de Ingenieros - Consejo Departamental de Puno, 2023).

País : Perú

Departamento : Puno

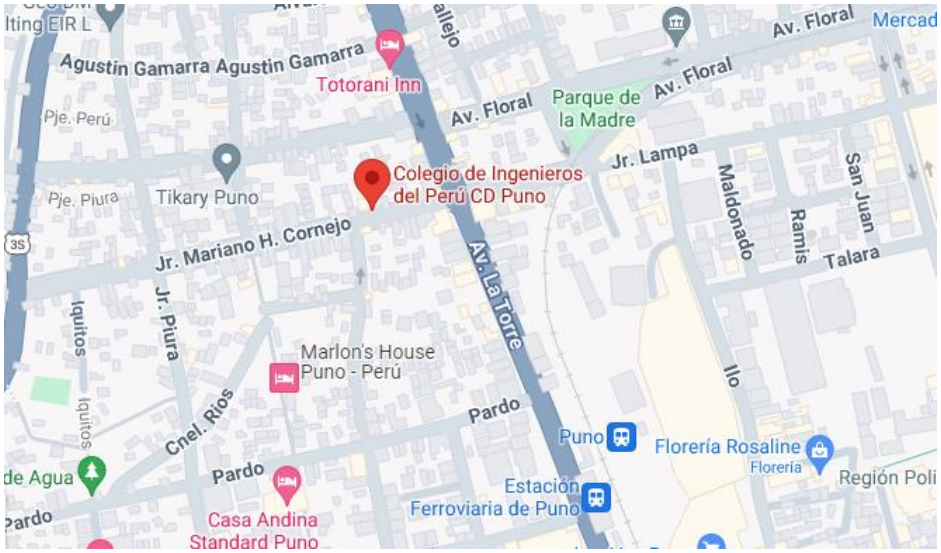
Provincia : Puno

Distrito : Puno

Lugar : Colegio de Ingenieros del Perú, Consejo Departamental Puno

Figura 4

Ubicación geográfica de estudio



Nota: Extraído de Google Maps.

3.2. OPERACIONALIZACIÓN DE VARIABLES

VARIABLE INDEPENDIENTE

X= Metodología OWASP

VARIABLE DEPENDIENTE

Y= Sistema de información web del Colegio de Ingenieros del Perú, Consejo Departamental Puno.

MATRIZ DE CONSISTENCIA

Tabla 1

Matriz de consistencia

	PREGUNTAS	OBJETIVOS	HIPÓTESIS	VARIABLES E INDICADORES	METODOLOGÍA
GENERAL	**Problema principal** ¿Cómo desarrolla el análisis de riesgos mediante la metodología OWASP para identificar vulnerabilidades y amenazas en el sistema de información web del Colegio de Ingenieros del Perú, Consejo departamental Puno?	**Objetivo principal** Desarrollar el análisis de riesgos mediante la metodología OWASP para identificar vulnerabilidades y amenazas en el sistema de información web del Colegio de Ingenieros del Perú, Consejo Departamental Puno.	**Hipótesis principal** La metodología OWASP permite desarrollar el análisis de riesgos en el sistema de información web del Colegio de Ingenieros del Perú, Consejo Departamental Puno para identificar vulnerabilidades y amenazas.	**Variable Independiente** Metodología OWASP **Unidad** Las Guías de OWASP **Dimensión** • Recopilación de información • Pruebas de gestión de configuración e implementación • Comprobación del Sistema de Autenticación • Pruebas de Validación de Datos • Pruebas de automatización • Pruebas de gestión de sesión • Pruebas de validación de ingreso • Prueba de Ajax	**Tipo** Investigación mixta (cuantitativo y cualitativo) **Diseño** Cuasi-experimental **Población** Los usuarios del sistema web del CIP-Puno **Muestra** 500 usuarios del sistema web del CIP-Puno **Técnicas y instrumentos** • Revisión • Bibliografía • Observación • Encuesta • Entrevista • Cuestionarios • Análisis de contenido de documentos.
ESPECIFICAS	¿La identificación de los activos de la institución mediante la metodología MAGERIT permitirá valorar de las amenazas a las que está expuesta el sistema web del Colegio de Ingenieros del Perú, Consejo Departamental Puno?	Identificar los activos de la institución y valorar de las amenazas a las que está expuesta el sistema de información web del Colegio de Ingenieros del Perú, Consejo Departamental Puno mediante la metodología MAGERIT.	Al identificar los activos de la institución mediante la metodología MAGERIT se espera valorar de las amenazas a las que está expuesta el sistema de información web del Colegio de Ingenieros del Perú, Consejo Departamental Puno		

	¿El desarrollo del proceso de análisis de acuerdo a los procedimientos establecidos por OWASP permitirá realizar pruebas de vulnerabilidad al sistema web del Colegio de Ingenieros del Perú. Consejo Departamental Puno?	Desarrollar el proceso de análisis de acuerdo a los procedimientos establecidos por OWASP para realizar pruebas de vulnerabilidad al Sistema web del Colegio de Ingenieros del Perú, Consejo Departamental Puno.	Al desarrollar el proceso de análisis de acuerdo a los procedimientos establecidos por OWASP se realiza las pruebas de vulnerabilidad al sistema web del Colegio de Ingenieros del Perú, Consejo Departamental de Puno.	**Indicadores** • Pérdida de Control de Acceso • Fallas Criptográficas • Inyección • Diseño Inseguro • Configuración de Seguridad Incorrecta • Componentes Vulnerables y Desactualizados • Fallas de Identificación y Autenticación • Fallas en el Software y en la Integridad de los Datos • Fallas en el Registro y Monitoreo • Falsificación de Solicitudes del Lado del Servidor **Variable Dependiente** Sistemas de información web del Colegio de Ingenieros del Perú, Consejo Departamental Puno. **Unidad** Sistema de información **Dimensión** Diseño del sistema web **Indicadores** Usabilidad	• Recopilación de datos existentes. **Instrumentos** • Fichas de bibliografías • Ficha de observación • Guía de entrevistas
	¿La evaluación de riesgos de seguridad ligados a los riesgos y amenazas permitirá medir el impacto en el sistema web del Colegio de Ingeniero, Consejo Departamental Puno?	Evaluar los riesgos de seguridad existentes ligados a los riesgos y amenazas para medir el impacto en el sistema web del Colegio de Ingenieros, Consejo Departamental Puno.	Al evaluar los riesgos de seguridad existentes ligados a los riesgos y amenazas se espera medir el impacto en el sistema web Colegio de Ingenieros del Perú, Consejo departamental Puno.		

Nota: Elaboración propia

3.3. DISEÑO Y MÉTODO DE LA INVESTIGACIÓN

3.3.1. Tipo de Investigación

La investigación tuvo un enfoque mixto, combinando métodos cuantitativos y cualitativos para abordar el análisis de riesgos y vulnerabilidades

en el sistema web del Colegio de Ingenieros del Perú, Consejo Departamental Puno.

Desde el enfoque cuantitativo, se midió y cuantificó la efectividad de OWASP en la detección de riesgos, proporcionando datos objetivos que respaldan los hallazgos. Por otro lado, el enfoque cualitativo permitió recopilar información no numérica, ofreciendo una visión realista, transparente y práctica de los aspectos estudiados. Esto facilitó una comprensión más profunda de conceptos complejos, contribuyendo a una investigación integral que combina precisión numérica con interpretaciones detalladas del contexto, logrando ampliar las dimensiones del proyecto y proporcionando un análisis más completo y robusto

La investigación de tipo mixto, tienen ventajas y desventajas, por lo que la combinación de ambas ayuda a obtener un resultados más completos porque integra los beneficios de cada una de las dos metodologías; ofrece un enfoque integral que combina y analiza los datos estadísticos con conocimientos contextualizados más profundos, y permite verificar los resultados de varias fuentes (Santandar Universidades, 2021).

3.3.2. Nivel de Investigación

Esta investigación es de nivel aplicada, ya que se centró en identificar y analizar las debilidades de seguridad presentes en aplicaciones web, específicamente en el sistema del Colegio de Ingenieros del Perú, Consejo Departamental Puno. Utilizando las directrices y herramientas proporcionadas por OWASP, se buscó no solo evaluar riesgos y vulnerabilidades

A través de este enfoque, no solo se busca identificar posibles amenazas, sino también priorizar y proponer soluciones efectivas para mitigar riesgos,

asegurando la protección del sistema web del Colegio de Ingenieros del Perú, Consejo Departamental Puno, antes de que dichas vulnerabilidades puedan ser explotadas (Tecana American University, 2023).

3.3.3. Diseño de Investigación

El diseño de esta investigación fue cuasi-experimental, dado que se buscó probar una hipótesis causal mediante la manipulación de al menos una variable independiente. Este enfoque se aplicó considerando que no fue posible asignar aleatoriamente las unidades de investigación a los grupos, debido a restricciones éticas o logísticas inherentes al contexto del estudio. Este tipo de diseño permitió evaluar el impacto de las directrices de OWASP sobre la seguridad del sistema web del CIP - Consejo Departamental Puno, dentro de un entorno controlado, pero representativo de la realidad operativa (Fernández et al.,.2014).

3.4. POBLACIÓN Y MUESTRA

3.4.1. Población

En esta investigación, la población incluyó a todos los usuarios del sistema web del Colegio de Ingenieros del Perú, Consejo Departamental Puno. Dentro de esta población, se consideraron tanto a los 14,000 ingenieros colegiados que utilizan el sistema, como a los cinco encargados responsables de la administración y soporte técnico del mismo. Este enfoque permitió abarcar una visión integral, considerando tanto la experiencia de los usuarios como la perspectiva técnica de los administradores del sistema.

3.4.2. Muestra

En esta investigación, se utilizó el muestreo estratificado desproporcional, un método probabilístico diseñado para destacar subgrupos específicos dentro de la población. Este enfoque consistió en dividir la población total en estratos, seleccionando de forma aleatoria a los miembros finales de cada grupo para incluirlos en la muestra. Este método permitió obtener conclusiones más precisas y comparables entre los distintos subgrupos, siendo especialmente adecuado para analizar comportamientos o características particulares en cada estrato, optimizando así la representatividad y relevancia de los datos recolectados. Se debe tener en cuenta que un muestreo desproporcional cada estrato contendrá una fracción diferente y se muestra en la siguiente Tabla 2.

Tabla 2

Total de usuarios del sistema web del CIP

ÁREA	TOTAL
Oficina general de tecnologías de información, sistemas y estadística	5
Encargados de centro de computo	4
Total de usuarios colegiados (consejo departamental puno)	14000
TOTAL	**14009**

Nota: Adaptado de acuerdo a la información obtenida en el CIP- Puno

La muestra estratificada desproporcional, porque se dividirá la población en 3 estratos debido a que los miembros de cada grupo tienen una posición e interés diferente.

- Área 1 (Oficina General de Tecnologías de Información, Sistemas y Estadística)**:**

$$\text{Proporción} = \frac{5}{14009} = 0.00036 = 0.036\%$$

- Área 2 (Encargados de Centro de Cómputo)**:**

$$\text{Proporción} = \frac{4}{14009} = 0.00029 = 0.029\%$$

- Área 3 (Usuarios Colegiados)**:**

$$\text{Proporción} = \frac{14000}{14009} = 0.99936 = 99.936\%$$

Calcular el Tamaño de la Muestra para Cada Estrato: Con una muestra total de 500 personas:

- Área 1: $n1 = 0.00036\ x\ 500 = 0.018 = 0$
- Área 2: $n2 = 0.00029\ x\ 500 = 0.018 = 0$
- Área 3: $n3 = 0.99936\ x\ 500 = 499.68 = 500$

De acuerdo a los resultados, los dos primeros estratos (Áreas 1 y 2) tienen un tamaño muy pequeño en comparación con el tamaño total de la muestra y la población general, lo que hace que la muestra proporcional de estos estratos sea prácticamente cero. Esto significa que la mayoría de la muestra provendrá del Estrato 3 (Usuarios Colegiados). Por lo que se realizará un ajuste para asegurar que estos estratos estén representados en la muestra, aunque sea en un número mínimo y quedaría de la siguiente manera:

- Área 1: 1 persona
- Área 2: 1 persona
- Área 3: El resto de la muestra, 498 personas

Tabla 3

Muestreo estratificado desproporcional

Estrato	Población	Desproporcional	Muestra
1	5	0.036%	1
2	4	0.029%	1
3	14000	99.93%	480
TOTAL	**14009**	**100%**	**500**

Nota: Elaboración propia

3.5. MÉTODO PARA LA RECOLECCIÓN DE LOS DATOS

En esta investigación se emplearon técnicas de campo, utilizando la encuesta como herramienta principal para evaluar la seguridad en aplicaciones web bajo el enfoque de OWASP. Diseñada para identificar vulnerabilidades, la encuesta midió la percepción de los usuarios sobre la seguridad, su comprensión de los riesgos y la importancia de las buenas prácticas. También permitió evaluar la implementación de medidas de seguridad y recopilar datos sobre el cumplimiento de normas. Alineadas con los riesgos de OWASP, las preguntas complementaron el análisis técnico, proporcionando una visión integral y datos originales de la población estudiada. Según Creswell (2015) se presentan diversos métodos de recolección de datos, como encuestas, análisis documental, entrevistas y observación, junto con recomendaciones para seleccionar el más adecuado según el proyecto de investigación.

3.5.1. Técnicas

- Encuestas: La presente técnica es un método de investigación popular porque permite obtener, elaborar datos de manera rápida y efectiva, lo que hace que los resultados sean más precisos, por ello es de gran utilidad y muy ventajosa principalmente en las fases de exploración y en los estudios

descriptivos Repullo, Donado, & Casas (2003). De tal manera que se espera obtener información relevante y precisa para el presente proyecto.

- Observación: La observación es un método sistemático y objetivo para registrar y verificar visualmente los hechos y comportamientos del entorno real. Permite captar lo que ocurre con precisión para posteriormente interpretarlo, ya sea con fines descriptivos, analíticos o explicativos, desde una perspectiva científica. (Campos & Lule, 2012).

3.5.2. Instrumentos

- Guía de Preguntas: Como herramienta de recolección de datos, es una actividad que requiere seriedad y responsabilidad. En este caso, el instrumento fue diseñado con preguntas reflexivas, cuidadosamente estructuradas, para garantizar la obtención de información relevante y precisa. Este enfoque permite profundizar en los aspectos clave de la investigación y asegura que los datos recopilados sean útiles para cumplir con los objetivos planteados (Araque, 2019).

3.6. MÉTODOS PARA EL ANÁLISIS DE LOS DATOS

Es fundamental aplicar técnicas de análisis de datos después de recopilar la información necesaria, ya que esto permite comprender con mayor claridad la situación actual. En un estudio no correlacional, el enfoque se centra en describir detallada y precisamente las variables y el entorno estudiado, sin buscar establecer relaciones causales entre estas. Este enfoque proporciona una visión más profunda y contextualizada, facilitando una mejor interpretación de los datos y permitiendo tomar decisiones fundamentadas en los hallazgos obtenidos.

CAPÍTULO IV

RESULTADOS Y DISCUSIÓN

4.1. DESCRIPCIÓN DEL CASO DE ESTUDIO

El presente estudio se enfocó en analizar, desarrollar e identificar las vulnerabilidades y factores de amenaza en el sistema web del Colegio de Ingenieros del Perú, Consejo Departamental Puno, basado en la metodología OWASP es de código abierto, la cual se enfoca en la seguridad de los sistemas web, cuyo fin es determinar y combatir las posibles causas que originen que el sistema web sea insegura. El CIP - Puno, es una organización no lucrativa que agrupa a todos los ingenieros profesionales de todas las especialidades de la región de Puno.

En cuanto a la situación actual de la institución posee el sistema web; CIP, Consejo Departamental Puno, este contiene información actualizada, sobre el proceso de colegiación ordinaria o el de certificado de habilitado, mostrando de manera detallada lo requisitos y trámites que se debe de realizar de manera presencial y virtual, también se encuentra el servicios de búsqueda, el cual muestra comunicados importantes referentes a la organización, se logra ver la información de los representantes de cada especialidad que conforman el Consejo Departamental Puno desde el período 2022 – 2024.

Al ser un sistema que engloba a todos los ingenieros de las diferentes especialidades también ofrece cursos vigentes en las cuales uno puede inscribirse la plataforma, muy aparte de ello se encuentra el servicio de validación de certificados que sean otorgados por la institución. Así mismo se encuentra la ventana de eventos que mediante un calendario se pude visualizar la información de los evento próximos del Colegio de Ingenieros del Perú, Consejo Departamental Puno.

4.1.1. Institución donde se realizó la investigación

- RUC : 20206923327
- Razón Social : Colegio de Ingenieros del Perú Consejo Departamental Puno
- Tipo de empresa : Colegios profesionales
- Estado : Activo
- Condición : Habido
- Fecha de Inicio de Actividades : 22/01/1987
- Dirección Legal : Jr. Mariano H Cornejo Nro. 130 Barrio Independencia
- País : Perú
- Departamento : Puno
- Provincia : Puno
- Distrito : Puno
- Página Web : https://web.cippuno.org.pe/asamblea-departamental/

4.1.1.1. Misión

Somos una institución deontológico, sin fines de lucro, que representa y agrupa a los ingenieros profesionales del Perú, de todas las especialidades, que cautela y preserva el comportamiento ético de sus miembros, y debe asegurar al Perú que cuenta con una profesión nacional que ejerce la ingeniería en un contexto de orden, respeto, competitividad, calidad y ética, y que está enraizada en sus valores sociales, culturales y políticos, como base fundamental en el proceso de desarrollo de la nación.

4.1.1.2. Visión

Ser reconocida como una institución sólida, que patrocina el manejo eficiente del conocimiento, con la finalidad de orientar a la sociedad peruana en las grandes decisiones, fomentando la práctica de valores y comportamiento ético de los ingenieros profesionales, así como elevando la calidad de la ingeniería, apoyando el crecimiento del país en el contexto de la globalización.

4.1.1.3. Representantes de la Institución

Consejo departamental CIP – Puno período 2022- 2024

- **Decano:** Ing. Jhomar Marcelino Tonconi Quispe
- **Vicedecano:** Ing. Mirko Daniel Nuñez Carpio
- **Director Secretario:** Ing. Gilmer Salas Madera
- **Director Prosecretario:** Ing. Edwin Miraval Condori
- **Director Tesorero:** Ing. Angel Rodrigo Coaquira Velásquez
- **Director Protesorero:** Ing. Bailon Sacachipana Chuquicallata
- **Director**
  - Ing. Gustavo Sanchez Capaquira
  - Ing. Elvis Augusto Aliaga Payehuanca
  - Ing. Julio Fredy Chura Acero
  - Ing. Marco Miguel Sucapuca Rojas
  - Ing. Ronald Raul Arce Coaquira

Miembros asamblea Departamental CIP – Puno

- **Cod. CIP 54418:** Ing. Percy Arturo Ginez Choque

- **Cod. CIP 101592:** Ing. Ángel Ubaldo Acero Taiña
- **Cod. CIP 48099:** Ing. Alejandro Apaza Tarqui
- **Cod. CIP 104292:** Ing. Germán Fermín Godoy Ruelas
- **Cod. CIP 42435:**Ing. Leonel Palomino Ascencio
- **Cod. CIP 64014:** Ing. Verardo Marcelo H. Mestas Vilca
- **Cod. CIP 84457:** Ing. Alfredo Abraham Bartolo León
- **Cod. CIP 72121:** Ing. Porfirio Ulíses Hurtado Chávez
- **Cod. CIP 99102:** Ing. Marco Eddy Quiroz Coaquira
- **Cod. CIP 58258:** Ing. Éudes Rigoberto Apaza Estaño
- **Cod. CIP 124010:** Ing. José Luis Bruna Sucasaca
- **Cod. CIP 62014:** Ing. Dawes Ramos Alata
- **Cod. CIP 61943:** Ing. Rodolfo Fredy Arpasi Chura
- **Cod. CIP 67583:** Ing. Edwin Vilca Coila
- **Cod. CIP 101541:** Ing. Donny Silvestre Mendoza Monroy

4.1.2. Funcionalidades del sistema web del CIP

El sistema web del Colegio de Ingenieros del Perú, Consejo Departamental Puno, está diseñado para garantizar una operación eficiente y segura mediante servicios clave como la autenticación de usuarios, la gestión centralizada de información institucional, y una plataforma de servicios en línea para trámites y consultas.

4.1.2.1. Servicios de certificados

El sistema web permite a los usuarios colegiados visualizar los cursos disponibles, las fechas en las que se llevarán a cabo y realizar su

inscripción. Estos cursos están dirigidos a diversas profesiones de ingeniería. Al finalizar el curso, el usuario puede validar su certificado utilizando el código proporcionado en el mismo, asegurando la autenticidad y validez del documento.

4.1.2.2. Servicio de Alquiler del ambiente CIP Puno

El sistema web proporciona información sobre el costo de alquiler de instalaciones para diversos eventos, como eventos especiales y académicos. Estos costos están estructurados en tarifas diferenciadas según el tipo de usuario: ingenieros colegiados, ingenieros habilitados y público general. De esta manera, se asegura que los miembros del Colegio de Ingenieros del Perú, Consejo Departamental Puno disfruten de tarifas preferenciales, mientras que el público general tiene acceso a las instalaciones bajo condiciones específicas y costos determinados.

4.1.2.3. Servicio de CIP virtual

El sistema web del Colegio de Ingenieros del Perú, Consejo Departamental de Puno, permite a los ingenieros colegiados crear una cuenta para acceder a una plataforma que facilita la gestión de trámites y servicios en línea. Al ingresar con su código de usuario y contraseña, los colegiados pueden actualizar su información personal, gestionar certificados, inscribirse en capacitaciones, mantenerse informados sobre actividades, noticias y eventos institucionales. Además, la plataforma fomenta la interacción entre colegiados mediante foros y redes de comunicación, ofreciendo un entorno seguro y eficiente que de confianza, significativamente su experiencia y vinculación con el colegio.

4.1.2.4. Búsqueda de Colegiados del CIP

El sistema web ofrece una forma rápida y eficiente para buscar colegiados, brindando dos opciones principales de búsqueda. La primera opción es por el Documento Nacional de Identidad (DNI) o por los nombres del colegiado. La segunda opción es a través de los apellidos y nombres completos. Además, el sistema requiere completar otros campos para afinar la búsqueda, facilitando así la localización precisa de la información del colegiado.

4.1.3. Caracterización de los activos del sistema web del CIP

Dentro de la institución pueden surgir diversas vulnerabilidades, no solo en el sistema web, sino también en el entorno asociado en el que este opera, ya que dicho entorno influye directamente en el desarrollo y seguridad del sistema. Estas vulnerabilidades pueden abarcar tanto aspectos tecnológicos como organizativos, lo que resalta la importancia de adoptar un enfoque integral para identificar y mitigar los riesgos. Es esencial considerar estos factores para garantizar la confidencialidad, integridad y disponibilidad de la información manejada por la institución. Esto permite proteger el flujo de datos y minimizar los riesgos de acceso no autorizado, pérdida de información o alteraciones que puedan comprometer la seguridad y operatividad de los sistemas, asegurando así la estabilidad y confianza en la gestión de los recursos tecnológicos.

A continuación, se abarca los objetivos planteados, partiendo desde realizar el análisis respectivo, en cuanto a los activos de la institución, para ello se utiliza a MAGERIT versión 3.0 como herramienta la cual permite tomar decisiones acorde a riesgos derivados del uso de las TICs, una vez identificadas a

través de la metodología OWASP se realiza pruebas de vulnerabilidad para luego detallar el proceso de comprobación de cada vulnerabilidad encontrada en el sistema web del Colegio de Ingenieros del Perú, Consejo Departamental Puno.

- En primer lugar, se lleva a cabo la identificación y análisis del funcionamiento del sistema web del Colegio de Ingenieros del Perú, Consejo Departamental Puno. Mediante una exploración adecuada siguiendo la metodología MAGERIT, se logran identificar las diferentes funcionalidades y activos relevantes de la institución, así como las posibles amenazas que pueden surgir y las estrategias para proteger dichos activos.
- En segundo lugar, se accede al sistema web para evaluar su funcionamiento, identificando cada una de sus funcionalidades. En esta fase, el sistema web se somete a pruebas utilizando la metodología OWASP, lo que permite identificar todas las vulnerabilidades a las que podría estar expuesto el sistema web del Colegio de Ingenieros del Perú, Consejo Departamental Puno.

Es fundamental señalar que esta investigación se centra exclusivamente en el impacto de las vulnerabilidades identificadas mediante la metodología OWASP en el sistema web del Colegio de Ingenieros del Perú, Consejo Departamental Puno. No obstante, el Colegio debe considerar otras contingencias o vulnerabilidades que pueden surgir, las cuales no se limitan únicamente a ataques directos al sistema. Estas pueden incluir:

- El ambiente físico dónde se encuentran los equipos informáticos.
- El fluido eléctrico, dónde se encuentra la planta eléctrica principal o alterna.

- Señalizaciones en cuanto a la ubicación de áreas dentro de la institución.
- Los sistemas de acceso en cuanto a la acción preventiva frente a un posible acto de vulnerabilidad.

4.2. RESULTADOS

Se realizó una visita institucional al Colegio de Ingenieros del Perú, Consejo Departamental Puno, durante la cual se llevó a cabo una entrevista con el jefe encargado de la oficina tecnología y sistemas, se aplicó una encuesta a los usuarios colegiados. Los resultados de la encuesta, detallados en los Anexos correspondientes, se enfocan en identificar vulnerabilidades y tipos de ataques cibernéticos dentro del marco de la metodología OWASP.

El propósito principal de esta encuesta fue evaluar el nivel de conocimiento y la percepción que tienen los ingenieros colegiados sobre los riesgos de seguridad informática, tanto a nivel profesional como institucional. Los resultados obtenidos proporcionan una visión detallada de las principales áreas de preocupación y vulnerabilidad en relación con las categorías de OWASP, permitiendo identificar puntos críticos de exposición.

Esta información resultó esencial para el desarrollo de estrategias efectivas que fortalezcan la ciberseguridad de la institución, asegurando la protección de la información sensible en el entorno digital y alineándose con las mejores prácticas y recomendaciones establecidas por OWASP.

4.3. OBJETIVO ESPECÍFICO 1

Durante la primera fase se aplicó a MAGERIT versión 3.0, cabe recordar que su objetivo parte por identificar los activos con los que cuenta la institución para luego

realizar una estimación y las posibles amenazas al recurso, toda la información se recolectó a través de entrevistas directas a los trabajadores en el área de Oficina de Tecnología y Sistemas del Colegio de Ingenieros, Consejo Departamental Puno, puesto que son los elementos principales con los que cuenta la organización, es vital para el respectivo tratamiento de información, a la hora de realizar el análisis respectivo en base a MAGERIT lo cual permitirá identificar de manera fiable las vulnerabilidades encontradas en el sistemas mediante OWASP.

4.3.1. Identificación de activos

Se identificó los activos que van relacionados con la gestión de la información y posterior a ello se evaluó cada uno de ellos en función de su importancia para la entidad.

La tipificación de activos incluyó tanto información documental relevante como un método para identificar las amenazas y las protecciones adecuadas según la naturaleza del activo. La clasificación de los activos se llevó a cabo de manera jerárquica, asignándoles un código que indicaba su posición en la jerarquía, un nombre y una breve descripción de sus características.

Este enfoque multidimensional facilitó una comprensión más precisa y completa de la naturaleza de los activos y su importancia en la estructura organizativa y operativa. Al permitir esta versatilidad en la clasificación, se evitó la rigidez de modelos tradicionales y se promovió una visión más dinámica y contextualizada. Asimismo, se permitió que un activo perteneciera a múltiples tipos de manera simultánea, ya que su pertenencia a un tipo no lo hacía incompatible con su asignación a otros. A continuación, se presentaron las tablas correspondientes.

Tabla 4

Activos esenciales - Oficina de Tecnología y Sistemas

Activos esenciales [essential]				
N°	**Capa**	**Código**	**Activos**	**Unid**
AE01	DATOS [data]	[mult]	Multimedia (animación, fotografías, texto, videos)	-
AE02		[dc]	Datos de las certificaciones	-
AE03		[dgi)	Datos de gestión interna	-
AE04	INFORMACIÓN [info]	[doc]	Documentos	-
AE05		[ig]	Informes generados	-
AE06		[tpc]	Trámites para colegiatura	-
AE07		[inp]	Información pública	-
AE08		[ir]	Información restringida	-
AE09		[dv]	Datos vitales	-
AE010		[dca]	Datos de control de acceso	-
AE011	SERVICIO [service]	[serin]	Servicio de internet	**1**
AE012		[email]	Correo electrónico del Colegio de Ingenieros del Perú – Consejo Departamental Puno	-

Nota: Obtenido de la información y observación en campo

Tabla 5

Activos de aplicaciones informáticas - Oficina de Tecnología y Sistemas

Aplicaciones informáticas [apinf]				
N°	**Capa**	**Código**	**Activos**	**Unid**
AI01	SOFWARE [data]	[swi]	Sistema web del Colegio de Ingenieros del Perú, Consejo departamental Puno (https://www.cip.org.pe/)	1
AI02		[dc]	Navegador web Google Chrome	16

N°	Código	Activos	Unid
AI03	[sio]	Sistema operativo Windows y Linux	16
AI03	[bd]	Base de datos	1
AI04	[sbck]	Sistema de Backup (respaldos)	1
AI06	[gsc]	Gestor de contenidos	1
AI07	[ser]	Servidor	1

Nota: Obtenido de la información y observación en campo

Tabla 6

Activos de equipos informáticos - Oficina de Tecnología y Sistemas

Equipos Informáticos [einf]				
N°	**Capa**	**Código**	**Activos**	**Unid**
AI01	HARDWARE [hwre]	[ces]	Computadoras de escritorio	16
AI02		[rou]	Router	2
AI03		[cms]	Cámaras de seguridad	1
AI03		[mou]	Mouse	16
AI04		[tec]	Teclado	16
AI05		[mon]	Monitor	16
AI06		[did]	Disco duro	16
AI07		[cpu]	Unidad central de proceso (CPU)	16
AI08		[imp]	Impresoras	2
AI09		[cpp]	Computadoras personales – Laptop	2
A0I0		[mm]	Memoria RAM	16

Nota: Obtenido de la información y observación en campo

Tabla 7

Activos de redes de comunicaciones - Oficina de Tecnología y Sistemas

Comunicaciones [comu]				
N°	Capa	Código	Activos	Unid
AC01	REDES DE COMUNICACIÓN [recomu]	[lan]	Red local LAN	-
AC02		[rou]	Red privada (Meet)	1
AC03		[cms]	Red telefónica	1
AC03		[mou]	Red inalámbrica	1
AC04		[tec]	Telefonía móvil	-

Nota: Obtenido de la información y observación en campo

Tabla 8

Activos de soporte informático - Oficina de Tecnología y Sistemas

Soporte de Información [soinf]				
N°	Capa	Código	Activos	Unid
AS01	SOPORTE DE INFORMACIÓN [soinf]	[alm]	Almacenamiento en la nube (Drive de Google)	-
AS02		[repr]	Proyector multimedia	1
AS03		[rtel]	Dispositivos (USB)	4
AS03		[rein]	Hard drive	2
AS04		[temo]	Tarjetas de memoria (SD, microSD, etc.)	4

Nota: Obtenido de la información y observación en campo

Tabla 9

Activos de equipamiento auxiliar - Oficina de Tecnología y Sistemas

Equipamiento Auxiliar [eqax]				
N°	Capa	Código	Activos	Unid
AA01	EQUIPAMIENTO [equip]	[cae]	Cableado eléctrico	-
AA02		[car]	Cableado de la red	-
AA03		[esen]	Estabilizador de energía	4
AA03		[fua]	Fuentes de alimentación	-
AA04		[idbio]	Identificador biométrico	

Nota: Obtenido de la información y observación en campo

Tabla 10

Activos de instalaciones - Oficina de Tecnología y Sistemas

Instalaciones [inst]				
N°	Capa	Código	Activos	Unid
AA01	EQUIPAMIENTO [equip]	[cae]	Oficinas	2
AA02		[car]	Sala de capacitaciones y trabajo en general	1
AA03		[esen]	Sala de atención	1

Nota: Obtenido de la información y observación en campo

Tabla 11

Activos de personal - Oficina de Tecnología y Sistemas

Personal [per]				
N°	Capa	Código	Activos	Unid
PP01	PERSONAL [per]	[eninf]	Encargado de informática	4
PP02		[car]	Personal encargado	2
PP03		[esen]	Personal administrativo	1

Nota: Obtenido de la información y observación en campo

4.3.2. Valoración de activos

Se realizó un análisis mediante tablas, con la respectiva distinción y separación hasta llegar a cada principio o elementos mediante una escala para calificar el valor de los activos con las que cuenta la institución, respecto a la magnitud y riesgo de impacto que estas puedan presentar.

Tabla 12

Escala para calificación de los activos de la institución

Escala para calificar el valor de los activos	
MB	Muy Bajo
B	Bajo
M	Medio
A	Alto
MA	Muy alto

Nota: MAGERIT v3, Libro II – Catálogo

Tabla 13

Criterios de valoración de activos

Valor			Criterio
10		Muy alto	Daño muy grave a la institución
7	9	Alto	Daño grave a la institución
4	6	Medio	Daño importante a la institución
1	3	Bajo	Daño menor a la institución
0		Despreciable	Daño irrelevante

Nota: MAGERIT v3, Libro II – Catálogo

Tabla 14

Dimensiones de seguridad

Dimensiones de seguridad		
[dis]	Los recursos están disponibles cuando sea necesario	Disponibilidad
[int]	En el proceso de envío, la información no puede ser modificada	Integridad
[con]	Garantiza la confidencialidad de las comunicaciones	Confidencialidad
[au]	Enviada por quien se presenta como el remitente	Autenticidad
[nr]	No es posible negar la autoría del mensaje	No repudio

Nota: MAGERIT v3, Libro II – Catálogo

Tabla 15

Valoración de activos - Oficina de Tecnología y Sistemas

Activos esenciales [essential]							Dimensiones				
N°	**Capa**	**Cód.**	**Activos**	**Uni**	**C/U**	**C. Total**	**[dis]**	**[int]**	**[con]**	**[au]**	**[nr]**
AE01	**DATOS** [data]	[mult]	Multimedia (animación, fotografías, texto, videos)	-	-	-	7	7	10	9	8
AE02		[dc]	Datos de las certificaciones	-	-	-	9	9	8	8	7
AE03		[dgi)	Datos de gestión interna	-	-	-	9	8	9	8	8
AE04	**INFORMACIÓN** [info]	[doc]	Documentos	-	-	-	9	9	8	9	8
AE05		[ig]	Informes generados	-	-	-	8	8	8	8	7
AE06		[tpc]	Trámites	-	-	-	7	7	8	7	7
AE07		[inp]	Información pública	-	-	-	7	6	7	7	
AE08		[ipe]]	Información personal	-	-	-	9	8	8	9	7
AE09		[ir]	Información restringida	-	-	-	10	9	9	8	8
AE010		[dca]	Datos de control de acceso	-	-	-	9	9	8	9	6

N°	Capa	Cód.	Activos	Uni	C/U	C. Total	[dis]	[int]	[con]	[au]	[nr]
AE011	**SERVICIO** [service]	[serin]	Servicio de Internet	**1**	S/.1560.00	S/.1560.00	10	9	8	8	8
AE012		[email]	Correo electrónico del Colegio de Ingenieros del Perú – Consejo Departamental Puno	-	-	-	9	9	8	9	8

Aplicaciones informáticas [apinf]							**Dimensiones**				
N°	**Capa**	**Cód.**	**Activos**	**Unid**	**C/U**	**C. Total**	**[dis]**	**[int]**	**[con]**	**[au]**	**[nr]**
AI01	**SOFWARE** [data]	[swi]	Sistema web del Colegio de Ingenieros del Perú - Consejo departamental Puno (https://www.cip.org.pe/)	1	S/. 1,500	S/. 1,500	9	9	9	8	8
AI02		[dc]	Navegador web Google Chrome	16	-	-	10	9	9	9	8
AI03		[sio]	Sistema operativo Windows y Linux	16	-	-	10	9	8	9	8

Equipos Informáticos [einf]							**Dimensiones**				
N°	**Capa**	**Cód.**	**Activos**	**Unid**	**C/U**	**C. Total**	**[dis]**	**[int]**	**[con]**	**[au]**	**[nr]**
EI01	**HARDWARE** [hwre]	[ces]	Computadoras de escritorio	16	S/.3,500	S/.56000	10	9	9	9	9
EI02		[rou]	Router	2	S/350	S/700	10	9	9	9	8

N°		Cód.	Activos	Uni	C/U	C. Total	[dis]	[int]	[con]	[au]	[nr]
EI03		[cms]	Cámaras de seguridad	1	S/.2192.4	S/.2192.4	8	7	8		
EI04		[mou]	Mouse	16	S/.40.50	S/. 648	9	8	9		
EI05		[tec]	Teclado	16	S/.35	S/.560	10	9	9		
EI06		[mon]	Monitor	16	S/.155	S/.2480	10	9	9		
EI07		[did]	Disco duro	16	S/.200	S/3200	10	8	8	9	
EI08		[cpu]	Unidad central de proceso (CPU)	16	S/.940	S/.15040	9	9		8	
EI09		[imp]	Impresoras	2	S/.2700	S/.5400	8	9	8	9	9
EII0		[cpp]	Computadoras personales – laptop	2	S/.4500	S/.9000	10	9	9	9	9
EI11		[mm]	Memoria RAM	16	S/.250	S/. 4000	10	9	8		

Comunicaciones [comu]

Dimensiones

N°	Capa	Cód.	Activos	Unid	C/U	C. Total	[dis]	[int]	[con]	[au]	[nr]
AC01	**REDES DE COMUNI**	[lan]	Red local LAN	-	-	-	9	8	9	7	
AC02		[rou]	Red privada (Meet)	1	S/.930	S/.930	10	9	9	9	

N°	Capa	Cód.	Activos	Unid	C/U	C. Total	[dis]	[int]	[con]	[au]	[nr]
AC03		[cms]	Red telefónica	1	S/90	S/90	9	10	9	9	
AC04		[mou]	Red inalámbrica	1	S/.260	S/.260	10	8	9	10	9
AC05		[tec]	Telefonía móvil	-	S/.85	S/.85	8	9	8	7	

Soporte de Información [soinf]							**Dimensiones**				
N°	**Capa**	**Cód.**	**Activos**	**Unid**	**C/U**	**C. Total**	**[dis]**	**[int]**	**[con]**	**[au]**	**[nr]**
AS01	**SOPORTE DE INFORMACIÓN** [soinf]	[alm]	Almacenamiento en la nube (Drive de Google)	-	-	-	8	7	8		8
AS02		[repr]	Proyector multimedia	1	S/.4500	S/.4500	10	9			8
AS03		[rtel]	Dispositivos (USB)	4	S/.65	S/.260	7	7	6	6	
AS03		[rein]	Hard drive	2	S/.300	S/.600	9	8	8	7	7
AS04		[temo]	Tarjetas de Memoria (SD, microSD, etc)	4	S/.60	S/.64	10	9	8	9	

Equipamiento Auxiliar [eqax]							**Dimensiones**				
N°	**Capa**	**Cód.**	**Activos**	**Unid**	**C/U**	**C. Total**	**[dis]**	**[int]**	**[con]**	**[au]**	**[nr]**
AA01	**EQUIPAMIENTO** [equip]	[cae]	Cableado eléctrico	-	-	-	10	10	9		
AA02		[car]	Cableado de la red	-	-	-	10	9		9	8

N°		Cód.	Activos	Unid	C/U	C. Total	[dis]	[int]	[con]	[au]	[nr]
AA03		[esen]	Estabilizador de energía	4	-	-	10	8		8	
AA03		[fua]	Fuentes de alimentación	-	-	-	10	9	9	9	
			Instalaciones [inst]					**Dimensiones**			
N°	**Capa**	**Cód.**	**Activos**	**Unid**	**C/U**	**C. Total**	**[dis]**	**[int]**	**[con]**	**[au]**	**[nr]**
AA01	**EQUIPAMIENTO** [equip]	[cae]	Oficinas	2	-	-	8	7	6	7	
AA02		[car]	Sala de capacitaciones y trabajo en general	1	-	-	8	7	4	8	7
AA03		[esen]	Sala de atención	1	-	-	8	5	4		
			Personal [inst]					**Dimensiones**			
N°	**Capa**	**Cód.**	**Activos**	**Unid**	**C/U**	**C. Total**	**[dis]**	**[int]**	**[con]**	**[au]**	**[nr]**
PP01	**PERSONAL** [per]	[eninf]	Encargado de informática	4	-	-	10	9	10		
PP02		[car]	Personal encargado	2	-	-	9	8	9		
PP03		[esen]	Personal administrativo	1	-	-	8	8	9		

Nota: Elaboración propia

4.3.3. Caracterización de las amenazas

Para la siguiente actividad, se identificó las amenazas potenciales para el recurso, la estimación de su frecuencia y su respectiva degradación. Como primer paso se reconoció las amenazas a los activos, para lo cual se considerara el siguiente listado de amenazas proporcionado por la metodología MAGERIT versión 3.0. Posterior a ello se identificó las amenazas para el presente caso de estudio, en particular los activos de la entidad del área de la Oficina de Tecnología y Sistemas del Colegio de Ingenieros del Perú, Consejo Departamental Puno.

Para lo cual se realizó la siguiente clasificación:

- [DN]: Desastres naturales
- [OR] De origen industrial
- [EF] Fallos y errores no intencionados
- [AIN] Ataques deliberados

Tabla 16

Identificación de Amenazas - Oficina de Tecnología y Sistemas

Ítem		Amenazas	Descripción ambiental/ física/ natural
DESASTRES NATURALES **[DN]**	**DN1**	Fuego **[N.1]**	Debido a posibles incendios, pueda que acabe con los recursos con los que cuenta el sistema web de la institución e información física.
	DN2	Daños por Agua **[N.2]**	Debido a posibles inundaciones pueden afectar a los recursos del sistema web del CIP, Consejo Departamental Puno.
	DN2	Tormenta Eléctrica **[N.3]**	Debido a posibles descargas de electricidad natural puede que afecte a los recursos del sistema web.
	DN3	Cambios/ Fenómenos climáticos **[N.4]**	Debido a las alteraciones del clima o eventos extremos como tormentas, inundaciones o sequías, que pueden causar daños a equipos, infraestructura o interrumpir operaciones.

	Ítem	Amenazas	Descripción ambiental/ física/ natural
ORIGEN INDUSTRIAL **[ORI]**	**OR1**	Contaminación Mecánica **[I.1]**	Debido a posibles construcciones cerca de la institución, que generan vibraciones, polvo, contaminación entre otros pueden afectar a los recursos y equipos informáticos.
	OR2	Contaminación Electromagnética **[I.2]**	Debido a las posibles interferencias radiales, campos magnéticos y radiaciones de calor pueden afectar al desarrollo de actividades del sistema web del CIP – Consejo Departamental Puno.
	OR3	Desastres Industriales **[I.3]**	Debido a una posible sobrecarga eléctrica pueden afectan a los equipos informáticos de la institución.
	OR4	Averías de origen físico o lógico **[I.4]**	Debido a posibles fallos de los equipos informáticos, fallos de los programas con las que se gestiona información relevante dentro del sistema web del CIP – Consejo Departamental Puno.
	OR5	Corte de suministro de eléctrico **[I.5]**	Debido a corte de energías sin aviso se pueden perder información o trabajos en proceso.
	OR6	Condiciones inadecuadas de temperatura o humedad **[I.6]**	Debido a altas temperaturas, o excediendo en la cantidad de trabajo en los equipos pueden afectar en el desempeño normal de sus tareas.
	OR7	Fallo de servicios de comunicaciones **[I.7]**	Debido a pérdidas de medios de comunicación o destrucción de ellas pueden afectar a la institución.
	OR8	Degradación de los soportes de almacenamiento de datos **[I.8]**	Debido al uso de los equipos tecnológicos de la institución por un prolongado tiempo pueden tener fallas en cuanto a su funcionamiento.
	OR9	Interrupción de otros servicios y suministros esenciales **[I.9]**	Debido a posibles interrupciones de cualquier medio o recurso dependiendo de su operación, cualquier tipo de interrupción pueden afectar significativamente a los procesos llevados en la institución.
FALLOS Y ERRORES NO	**EF1**	Errores de los Usuarios **[E1]**	Debido mala usabilidad y la experiencia del usuario del servicio pueden repercutir en el desarrollo normal de actividades dentro de la organización.
	EF2	Errores de los Administradores **[E2]**	Debido a los errores cometidos por los responsables en la instalación y ejecución de programas.
	EF3	Errores de Monitorización **[E3]**	Debido a la falta de registros de actividades y recopilación de información.

Ítem	Amenazas	Descripción ambiental/ física/ natural
EF4	Errores de Configuración **[E4]**	Debido a una mala configuración de otorgamiento de privilegios a los usuarios del sistema web pueden afectar en registros erróneos.
EF5	Deficiencias en la organización **[E5]**	Debido a las acciones desorganizadas del personal y errores por falta de acción.
EF6	Difusión de software dañino **[E6]**	Debido a una propagación de virus mediante ya sea a causa de archivos adjuntos, descargas de Internet, enlaces en redes sociales y aplicaciones sospechosas.
EF7	Errores de [re-]encaminamiento **[E7]**	Debido a errores de encaminamiento de información a través de una ruta, mediante el sistema web, correos o red incorrecta de la institución.
EF8	Errores de Secuencia **[E8]**	Debido a una alteración no intencionada en el envió de mensajes masivos en tiempo real desde los equipos de la institución.
EF9	Fugas de Información **[E9]**	Debido a la eliminación accidental o intencional de información importante, causada por fallos técnicos, errores humanos, malware o desastres naturales.
EF10	Alteración accidental de la información **[E10]**	Debido a errores humanos, fallos técnicos o problemas en los sistemas pueden afectar la precisión y confiabilidad de la información almacenada o procesada.
EF11	Destrucción de información **[E11]**	Debido a la eliminación permanente de datos, pueden afectar a la institución asegurando que la información no se pueda recuperar ni utilizar nuevamente.
EF12	Vulnerabilidades de los programas (software) **[E12]**	Debido a las vulnerabilidades del software pueden existir fallos que permiten a atacantes comprometer la seguridad del sistema web de la institución.
EF13	Errores de mantenimiento y actualización del programa (software) **[E13]**	Debido a una mala gestión de mantenimiento y actualización puede llevar a fallos de seguridad, errores de funcionamiento y disminución del rendimiento del sistema web de la institución.
EF14	Errores de mantenimiento y actualización del (hardware) **[E14]**	Debido a fallos en los procesos de reparación, mejorara o reemplazo de componentes físicos de los equipos pueden afectar en el correcto funcionamiento y rendimiento del sistema web.
EF15	Caída del sistema por agotamiento de recursos **[E15]**	Debido a la caída del sistema web se podría interrumpir el funcionamiento de un sitio web, impidiendo su acceso o uso, puede ser causada por sobrecarga, fallos técnicos o ataques cibernéticos.

	Ítem	Amenazas	Descripción ambiental/ física/ natural
	EF16	Pérdidas de equipos **[E16]**	Debido a la pérdida o robo de hardware, puede causar interrupciones en el trabajo, pérdida de datos y costos para reemplazar los dispositivos.
	EF17	Deficiencias de la organización **[E17]**	Debido a posibles problemas internos pueden afectar la eficiencia, la seguridad o el desempeño, como falta de procesos claros, mala gestión o comunicación deficiente.
	EF18	Indisponibilidad de trabajadores **[E18]**	Debido a la ausencia o falta de acceso de empleados necesarios para llevar a cabo tareas, puede afectar la operación y productividad de la institución.
ATAQUES INTENCIONADOS [AIN]	**AI1**	Manipulación de la configuración **[A1]**	Debido a cambios no autorizados o incorrectos en los ajustes del sistema que pueden comprometer la seguridad, el rendimiento o la estabilidad del software o hardware.
	AI2	Suplantación de la identidad del usuario **[A2]**	Debido a que alguien se hace pasar por otra persona pueden acceder a información, recursos o servicios de manera fraudulenta.
	AI3	Abuso de privilegios de acceso **[A3]**	Debido al uso indebido de accesos o permisos elevados para realizar acciones no autorizadas, como robar datos, modificar configuraciones o causar daños al sistema web.
	AI4	Usos no previsto **[A4]**	Debido al uso de recursos, sistemas o información, que pueden causar problemas de seguridad, rendimiento o costos imprevistos.
	AI5	Difusión de software dañino **[A5]**	Debido a la propagación de virus intencionados puede causar daños, robo de información o interrupción del funcionamiento del sistema web.
	AI6	[Re-]encaminamiento de mensajes **[A6]**	Debido a la redirección datos de forma deliberada para fines fraudulentos, como el robo de información o la interceptación de comunicaciones.
	AI7	Accesos no autorizados **[A7]**	Debido a entradas sin permiso a sistemas web, los datos o recursos, pueden ocurrir robos de información, modificaciones indebidas o daños.
	AI8	Monitorización de tráfico **[A8]**	Debido a una insuficiente o incorrecta supervisión del tráfico de red, puede llevar a la pérdida de datos, falta de detección de amenazas o problemas de rendimiento.
	AI9	Repudio **[A9]**	Debido al rechazo o no reconocimiento de operaciones realizadas en un sistema web, puede dificultar la resolución de problemas y el rastreo de actividades.

Ítem	Amenazas	Descripción ambiental/ física/ natural
AI10	Interceptación de información (escucha) **[A10]**	Debido a la captura no autorizada de información mientras se transmite, que puede llevar al robo de datos o violaciones de privacidad.
AI11	Modificación deliberada de la información **[A11]**	Debido a la modificación no autorizada de datos de manera malintencionada**,** pueden comprometer la integridad y la confiabilidad de la información.
AI12	Destrucción de información **[A12]**	Debido a la eliminación deliberada de datos para causar daño, ocultar actividades o impedir el acceso a la información.
AI13	Divulgación de información **[A13]**	Debido a la difusión deliberada de datos con el propósito de influir, engañar o causar daño.
AI14	Manipulación de programas **[A14]**	Debido al empleo de software diseñado para causar daño**,** robar información o comprometer sistemas.
AI15	Manipulación de equipos **[A15]**	Debido al empleo de dispositivos diseñados para actividades fraudulentas, como el espionaje, el robo de datos o la interrupción de servicios.
AI16	Robo **[A16]**	Debido al robo deliberado de bienes o información con el propósito de obtener beneficio o causar daño.
AI17	Ataque destructivo **[A17]**	Debido a la eliminación deliberada de datos para causar daño, ocultar actividades ilícitas o impedir el acceso a la información.
AI18	Ocupación Enemiga [**A18]**	Debido a lugares ocupados y ausencia de dominio sobre los dispositivos.
AI19	Indisponibilidad de Personal **[A19]**	Debido al daño a la disponibilidad del personal.
AI20	Extorción **[A20]**	Debido a la coacción ejercida sobre una persona mediante amenazas para forzarla a actuar de una manera específica.
AI21	Ingeniería social **[A21]**	Explotación de la confianza de las personas para que lleven a cabo acciones que benefician a terceros.

Nota: MAGERIT v3, Libro II – Catálogo

4.3.4. Valoración de las amenazas

Se estimó la probabilidad en porcentajes de ocurrencia y degradación de la realización de amenazas sobre los recursos identificados, logrando identificar con éxito la importancia relativa de los distintos activos que enfrentaban amenazas.

De acuerdo a la información presentado por MAGERIT versión 3.0, se pudo realizar el cálculo en base a la siguiente Tabla 18. Se tomó en cuenta que, si los activos de la institución obtenían una calificación de impacto muy alto (MA), debían ser atendidos de manera inmediata.

Tabla 17

Probabilidad de Ocurrencia amenaza

Probabilidad de ocurrencia	
1	Muy raro
2	Improbable
3	Posible
4	Probable
5	Prácticamente segura

Nota: MAGERIT v3, Libro II – Catálogo

Tabla 18

Degradación

	Degradación %	
Depreciable	0%	10%
Bajo	20%	30%
Medio	40%	60%
Alto	70%	80%
Muy alto	90%	100%

Nota: MAGERIT v3, Libro II – Catálogo

Tabla 19

Caracterización de amenazas a los activo de la institución

Activos esenciales [esencial]								
N°	**Cód.**	**Activos**	**Probabilidad de ocurrencia de materialización de amenazas**	**Dimensiones**				
				[dis]	**[int]**	**[con]**	**[au]**	**[nr]**
AE01	**[mult]**	**Multimedia (animación, fotografías, texto, videos)**	**3**	**60%**	**70%**	**70%**	**70%**	**50%**
	OR8	Degradación de los soportes de almacenamiento de datos [I.8]	3		60%			50%
	EF8	Errores de secuencia [E8]	3	40%	20%	70%		20%
	AI4	Usos no previsto [A4]	4	60%	50%			
	EF11	Destrucción de información [E11]	2		50%			
	AI11	Modificación deliberada de la información [A11]	3	40%	70%	40%	70%	
AE02	**[dc]**	**Datos de las certificaciones**	**4**	**40%**	**40%**	**80%**	**30%**	**40%**
	AI11	Modificación deliberada de la información [A11]	4		40%	80%		
	OR8	Degradación de los soportes de almacenamiento de datos [I.8]	3	40%	40%			
	AI4	Usos no previsto [A4]	5	40%			30%	
	EF7	Errores de [re-]encaminamiento [E7]	4		40%	30%		40%
AE03	**[dgi)**	**Datos de gestión interna**	**4**	**90%**	**70%**	**80%**	**70%**	**20%**

Activos esenciales [esencial]								
N°	**Cód.**	**Activos**	**Probabilidad de ocurrencia de materialización de amenazas**	**Dimensiones**				
				[dis]	**[int]**	**[con]**	**[au]**	**[nr]**
	OR9	Interrupción de otros servicios y suministros esenciales [I.9]	3	80%	50%			
	EF11	Destrucción de información [E11]	4	40%	80%	50%		
	AI13	Divulgación de información [A13]	5			80%	20%	20%
AE04	**[doc]**	**Documentos**	**4**	**70%**	**70%**	**60%**	**80%**	**50%**
	EF11	Destrucción de información [E11]	4			60%	80%	50%
	AI13	Divulgación de información [A13]	4	50%	60%	50%		
	OR8	Degradación de los soportes de almacenamiento de datos [I.8]	4	70%	70%			
AE05	**[ig]**	**Informes generados**	**2**	**70%**	**60%**	**50%**	**80%**	**40%**
	EF9	Fugas de información [E9]	3			50%	80%	40%
	DN1	Fuego [N.1]	2	40%	50%	50%		
	DN2	Daños por agua [N.2]	2	60%	60%			
AE06	**[tpc]**	**Trámites**	**4**	**80%**	**60%**	**50%**	**60%**	**50%**
	EF11	Destrucción de información [E11]	4	80%	60%		40%	50%
	EF9	Fugas de información [E9]	5			50%	60%	
	AI4	Usos no previsto [A4]	4	80%				
AE07	**[inp]**	**Información pública**	**4**	**90%**	**50%**	**60%**	**40%**	**50%**
	EF1	Errores de los usuarios [E1]	4		30%		40%	50%

Activos esenciales [esencial]								
N°	**Cód.**	**Activos**	**Probabilidad de ocurrencia de materialización de amenazas**	**Dimensiones**				
				[dis]	**[int]**	**[con]**	**[au]**	**[nr]**
	EF5	Deficiencias en la organización [E5]	4	50%		40%		
	EF9	Fugas de información [E9]	3	50%		50%	50%	40%
	EF11	Destrucción de información [E11]	5	80%	70%	30%		
	AI3	Abuso de privilegios de acceso [A3]	4	50%	60%	60%		
AE09	**[ir]**	**Información restringida**	**4**	**80%**	**70%**	**60%**	**30%**	**40%**
	AI4	Usos no previsto [A4]	4	80%	70%		30%	
	EF9	Fugas de información [E9]	4	30%		60%	30%	40%
	EF11	Destrucción de información [E11]	4	70%	60%	30%		
AE011	**[dca]**	**Datos de control de acceso**	**3**	**30%**	**40%**	**0%**	**0%**	**10%**
	EF18	Indisponibilidad de trabajadores [E18]	2	30%	40%			10%
	EF13	Errores de mantenimiento y actualización del programa (software) [E13]	3	30%	20%			10%
AE012	**[serin]**	**Servicio de internet**	**4**	**90%**	**50%**	**80%**	**80%**	**30%**
	EF7	Errores de [re-]encaminamiento [E7]	5	30%			80%	30%
	OR4	Averías de origen físico o lógico[I.4]	3	70%	50%		30%	
	OR5	Corte de suministro de eléctrico[I.5]	4	70%	50%			
	OR7	Fallo de servicios de comunicaciones [I.7]	4	50%	50%			
	EF15	Caída del sistema por agotamiento de recursos [E15]	4	90%	50%	80%		

Activos esenciales [esencial]								
N°	**Cód.**	**Activos**	**Probabilidad de ocurrencia de materialización de amenazas**	**Dimensiones**				
				[dis]	**[int]**	**[con]**	**[au]**	**[nr]**
AE013	**[email]**	**Correo electrónico del Colegio de Ingenieros – Consejo Departamental Puno**	**3**	**80%**	**90%**	**70%**	**70%**	**60%**
	EF1	Errores de los usuarios [E1]	3	50%	30%	40%	30%	30%
	OR4	Averías de origen físico o lógico[I.4]	2	50%	30%			
	OR7	Fallo de servicios de comunicaciones [I.7]	4	70%	70%			
	OR9	Interrupción de otros servicios y suministros esenciales [I.9]	3	60%	50%			
	EF7	Errores de [re-]encaminamiento [E7]	4	60%	70%	50%	60%	60%
	EF6	Difusión de software dañino [E6]	5	60%	90%	70%	70%	60%
	EF8	Errores de secuencia [E8]	3	80%		60%		30%

Aplicaciones informáticas [apinf]								
N°	**Cód.**	**Activos**	**Probabilidad de ocurrencia de materialización de amenazas**	**Dimensiones**				
				[dis]	**[int]**	**[con]**	**[au]**	**[nr]**
AI01	**[swi]**	**Sistema web del Colegio de Ingenieros Consejo departamental Puno (https://www.cip.org.pe/)**	**4**	**90%**	**80%**	**50%**	**20%**	**20%**
	AI1	Manipulación de la configuración [A1]	5	60%	50%	50%	20%	

Aplicaciones informáticas [apinf]								
N°	**Cód.**	**Activos**	**Probabilidad de ocurrencia de materialización de amenazas**	**Dimensiones**				
				[dis]	**[int]**	**[con]**	**[au]**	**[nr]**
	EF15	Caída del sistema por agotamiento de recursos [E15]	3	70%				
	EF12	Vulnerabilidades de los programas (software) [E12]	5	70%	50%	30%		
AI02	**[dc]**	**Navegador web Google Chrome**	**4**	**100%**	**90%**	**90%**	**100%**	**50%**
	EF12	Vulnerabilidades de los programas (software) [E12]	4	100%	90%	90%	100%	50%
	EF13	Errores de mantenimiento y actualización del programa (software) [E13]	4	80%				
AI03	**[sio]**	**Sistema operativo Windows y Linux**	**4**	**70%**	**60%**	**60%**	**0%**	**0%**
	AI4	Usos no previsto [A4]	4	20%	20%			
	AI7	Accesos no autorizados [A7]	3	50%				
	EF6	Difusión de software dañino [E6]	4	70%		60%		
	OR4	Averías de origen físico o lógico[I.4]	4	30%	60%			
Equipos Informáticos [einf]								
N°	**Cód.**	**Activos**	**Probabilidad de ocurrencia de materialización de amenazas**	**Dimensiones**				
				[dis]	**[int]**	**[con]**	**[au]**	**[nr]**
EI01	**[ces]**	**Computadoras de escritorio**	**3**	**80%**	**60%**	**70%**	**30%**	**70%**

Equipos Informáticos [einf]								
N°	**Cód.**	**Activos**	**Probabilidad de ocurrencia de materialización de amenazas**	**Dimensiones**				
				[dis]	**[int]**	**[con]**	**[au]**	**[nr]**
	OR3	Desastres industriales [I.3]	2	30%		30%		
	OR4	Averías de origen físico o lógico[I.4]	5	70%	50%			
	OR5	Corte de suministro de eléctrico [I.5]	4	50%				
	AI1	Manipulación de la configuración [A1]	3	70%	60%	50%		50%
	AI15	Manipulación de equipos [A15]	4	60%		70%		70%
	EF14	Errores de mantenimiento y actualización del (hardware) [E14]	3	80%	20%			
	AI16	Robo [A16]	2	70%		70%		10%
EI02	**[rou]**	**Router**	**3**	**90%**	**80%**	**50%**	**50%**	**20%**
	OR3	Desastres industriales [I.3]	4	30%				
	OR1	Contaminación mecánica [I.1]	4	50%				
	OR6	Condiciones inadecuadas de temperatura o humedad [I.6]	4	50%	20%			
	OR4	Averías de origen físico o lógico[I.4]	4	70%				
	AI15	Manipulación de equipos [A15]	3	90%	80%			
	EF14	Errores de mantenimiento y actualización del (hardware) [E14]	3	90%			10%	
	OR5	Corte de suministro de eléctrico [I.5]	3	70%		50%		
	AI16	Robo [A16]	2	50%			50%	20%
EI03	**[cms]**	**Cámaras de seguridad**	**3**	**60%**	**0%**	**60%**	**0%**	**0%**
	OR3	Desastres industriales [I.3]	3	20%		30%		

Equipos Informáticos [einf]								
N°	**Cód.**	**Activos**	**Probabilidad de ocurrencia de materialización de amenazas**	**Dimensiones**				
				[dis]	**[int]**	**[con]**	**[au]**	**[nr]**
	OR1	Contaminación mecánica [I.1]	4	50%				
	OR6	Condiciones inadecuadas de temperatura o humedad [I.6]	4	50%		60%		
	OR4	Averías de origen físico o lógico[I.4]	4	40%				
	AI15	Manipulación de equipos [A15]	4	60%				
	EF14	Errores de mantenimiento y actualización del (hardware) [E14]	3	60%				
	OR5	Corte de suministro de eléctrico [I.5]	4	60%				
	AI16	Robo [A16]	1	30%				
EI04	**[mou]**	**Mouse**	**3**	**80%**	**40%**	**0%**	**0%**	**0%**
	OR3	Desastres industriales [I.3]	3	30%				
	OR4	Averías de origen físico o lógico[I.4]	4	50%				
	AI15	Manipulación de equipos [A15]	3	40%	40%			
	EF14	Errores de mantenimiento y actualización del (hardware) [E14]	4	60%	30%			
	OR5	Corte de suministro de eléctrico [I.5]	4	60%				
	AI16	Robo [A16]	2	80%				
EI05	**[tec]**	**Teclado**	**3**	**80%**	**40%**	**0%**	**0%**	**0%**
	OR3	Desastres industriales [I.3]	3	30%				
	OR1	Contaminación Mecánica [I.1]	3	50%				

Equipos Informáticos [einf]								
N°	**Cód.**	**Activos**	**Probabilidad de ocurrencia de materialización de amenazas**	**Dimensiones**				
				[dis]	**[int]**	**[con]**	**[au]**	**[nr]**
	OR4	Averías de origen físico o lógico[I.4]	4	50%				
	AI15	Manipulación de equipos [A15]	3	40%	40%			
	EF14	Errores de mantenimiento y actualización del (hardware) [E14]	4	60%	30%			
	OR5	Corte de suministro de eléctrico [I.5]	4	60%				
	AI16	Robo [A16]	2	80%				
EI06	**[mon]**	**Monitor**	**3**	**80%**	**60%**	**40%**	**0%**	**10%**
	OR3	Desastres industriales [I.3]	3	30%				
	OR1	Contaminación mecánica [I.1]	4	50%				
	OR4	Averías de origen físico o lógico[I.4]	3	50%	40%			
	AI15	Manipulación de equipos [A15]	4	50%				10%
	OR5	Corte de suministro de eléctrico [I.5]	4	60%		40%		
	AI4	Usos no previsto [A4]	3		60%			
	AI16	Robo [A16]	1	80%				
EI07	**[did]**	**Disco duro**	**3**	**80%**	**70%**	**70%**	**10%**	**30%**
	OR3	Desastres industriales [I.3]	3	30%				
	OR6	Condiciones inadecuadas de temperatura o humedad [I.6]	4	50%				
	OR1	Contaminación mecánica [I.1]	3	50%	40%			
	OR4	Averías de origen físico o lógico[I.4]	4	50%			10%	
	AI13	Divulgación de información [A13]	4	60%	70%			30%

Equipos Informáticos [einf]								
N°	**Cód.**	**Activos**	**Probabilidad de ocurrencia de materialización de amenazas**	**Dimensiones**				
				[dis]	**[int]**	**[con]**	**[au]**	**[nr]**
	EF13	Errores de mantenimiento y actualización del programa (software) [E13]	3	50%		60%		
	AI7	Accesos no autorizados [A7]	1	80%		70%		10%
	AI16	Robo [A16]	3	40%				
EI08	**[cpu]**	**Unidad central de proceso (CPU)**	**3**	**60%**	**70%**	**60%**	**20%**	**30%**
	OR3	Desastres industriales [I.3]	3	30%		30%		
	OR6	Condiciones inadecuadas de temperatura o humedad [I.6]	4	50%			20%	
	OR1	Contaminación mecánica [I.1]	4	50%				
	OR4	Averías de origen físico o lógico[I.4]	4	50%	40%			
	AI15	Manipulación de equipos [A15]	3	60%	70%			30%
	EF14	Errores de mantenimiento y actualización del (hardware) [E14]	3	50%		60%		30%
	OR5	Corte de suministro de eléctrico [I.5]	3			30%		
	AI16	Robo [A16]	2	60%				
EI09	**[imp]**	**Impresoras**	**4**	**80%**	**60%**	**60%**	**20%**	**0%**
	OR3	Desastres industriales [I.3]	2	30%		30%		
	OR1	Contaminación mecánica [I.1]	4	50%			20%	
	OR4	Averías de origen físico o lógico[I.4]	5	80%	50%			
	OR5	Corte de suministro de eléctrico [I.5]	3					
	AI1	Manipulación de la configuración [A1]	3	70%	60%	60%		

Equipos Informáticos [einf]								
N°	**Cód.**	**Activos**	**Probabilidad de ocurrencia de materialización de amenazas**	**Dimensiones**				
				[dis]	**[int]**	**[con]**	**[au]**	**[nr]**
	EF14	Errores de mantenimiento y actualización del (hardware) [E14]	4	30%	30%			
EI10	**[cpp]**	**Computadoras personales – Laptop**	**3**	**90%**	**60%**	**80%**	**60%**	**70%**
	OR1	Contaminación mecánica [I.1]	2	30%		30%		
	OR3	Desastres industriales [I.3]	2	50%			50%	
	OR4	Averías de origen físico o lógico[I.4]	4	80%	50%			
	OR5	Corte de suministro de eléctrico [I.5]	4	50%				
	AI1	Manipulación de la configuración [A1]	3	70%	60%	60%	60%	50%
	AI15	Manipulación de equipos [A15]	4	70%		70%		70%
	EF14	Errores de mantenimiento y actualización del (hardware) [E14]	4	90%	40%			
	AI16	Robo [A16]	2	90%		80%		10%
EI11	**[mm]**	**Memoria RAM**	**3**	**80%**	**30%**	**70%**	**10%**	**10%**
	OR1	Contaminación mecánica [I.1]	4	80%				
	OR4	Averías de origen físico o lógico[I.4]]	4	50%			10%	
	AI15	Manipulación de equipos [A15]	3	60%				
	EF14	Errores de mantenimiento y actualización del (hardware) [E14]	4	60%	30%	70%		
	OR5	Corte de suministro de eléctrico [I.5]	4					10%
	AI16	Robo [A16]	2	30%				

Comunicaciones [comu]								
N°	**Cód.**	**Activos**	**Probabilidad de ocurrencia de materialización de amenazas**	**Dimensiones**				
				[dis]	**[int]**	**[con]**	**[au]**	**[nr]**
AC01	**[lan]**	**Red local LAN**	**4**	**90%**	**80%**	**70%**	**90%**	**40%**
	OR7	Fallo de servicios de comunicaciones [I.7]	4	90%	40%	30%	90%	
	EF13	Errores de mantenimiento y actualización del programa (software) [E13]	4	30%	30%			30%
	EF15	Caída del sistema por agotamiento de recursos [E15]	4	30%				40%
	OR5	Corte de suministro de eléctrico [I.5]	4	50%	50%			
	OR4	Averías de origen físico o lógico[I.4]	4	60%	80%	70%	60%	30%
AC02	**[rou]**	**Red privada (Meet)**	**4**	**60%**	**60%**	**40%**	**30%**	**40%**
	OR7	Fallo de servicios de comunicaciones [I.7]	4	60%	60%	30%	10%	
	OR9	Interrupción de otros servicios y suministros esenciales [I.9]	3	30%	60%			
	OR2	Contaminación electromagnética [I.2]	3	30%				
	EF4	Errores de configuración [E4]	4		50%	40%	30%	40%
AC03	**[cms]**	**Red telefónica**	**3**	**60%**	**50%**	**0%**	**0%**	**10%**
	OR7	Fallo de servicios de comunicaciones [I.7]	3	60%				10%
	OR4	Averías de origen físico o lógico[I.4]	3	30%	50%			
AC04	**[mou]**	**Red inalámbrica**	**3**	**60%**	**60%**	**40%**	**30%**	**50%**
	EF4	Errores de configuración [E4]	3	60%	60%		10%	50%
	EF14	Errores de mantenimiento y actualización del (hardware) [E14]	3	50%	40%			

Comunicaciones [comu]								
N°	**Cód.**	**Activos**	**Probabilidad de ocurrencia de materialización de amenazas**	**Dimensiones**				
				[dis]	**[int]**	**[con]**	**[au]**	**[nr]**
	OR2	Contaminación electromagnética [I.2]	3	30%				
	EF15	Caída del sistema por agotamiento de recursos [E15]	3	60%	50%	40%	30%	20%
AC05	**[tec]**	**Telefonía móvil**	**3**	**60%**	**50%**	**50%**	**30%**	**10%**
	EF14	Errores de mantenimiento y actualización del (hardware) [E14]	4	60%	50%			
	OR2	Contaminación electromagnética [I.2]	3	50%	40%			
	EF7	Errores de [re-]encaminamiento [E7]	3	30%	40%	50%	30%	10%

Soporte de Información [soinf]								
N°	**Cód.**	**Activos**	**Probabilidad de ocurrencia de materialización de amenazas**	**Dimensiones**				
				[dis]	**[int]**	**[con]**	**[au]**	**[nr]**
AS01	**[alm]**	**Almacenamiento en la nube (Drive de Google)**	**4**	**70%**	**60%**	**70%**	**30%**	**30%**
	OR9	Interrupción de otros servicios y suministros esenciales [I.9]	4	40%	50%	40%	20%	30%
	AI4	Usos no previsto [A4]	4	30%	50%	40%	20%	30%
	AI2	Suplantación de la identidad del usuario [A2]	4			40%		30%
	AI13	Divulgación de información [A13]	4	50%	50%	70%	10%	10%
	EF7	Errores de [re-]encaminamiento [E7]	4	70%	60%	50%	30%	30%

Soporte de Información [soinf]								
N°	**Cód.**	**Activos**	**Probabilidad de ocurrencia de materialización de amenazas**	**Dimensiones**				
				[dis]	**[int]**	**[con]**	**[au]**	**[nr]**
AS02	**[repr]**	**Proyector multimedia**	**3**	**50%**	**60%**	**0%**	**0%**	**0%**
	OR4	Averías de origen físico o lógico[I.4]	3	50%				
	EF17	Deficiencias de la organización [E17]	3	30%				
	OR5	Corte de suministro de eléctrico [I.5]	2	40%	60%			
AS03	**[rtel]**	**Dispositivos (USB)**	**3**	**70%**	**70%**	**60%**	**50%**	**30%**
	AI4	Usos no previsto [A4]	4	20%	50%	30%	50%	30%
	EF1	Errores de los usuarios [E1]	3	30%	50%	60%	10%	20%
	EF6	Difusión de software dañino [E6]	3	70%	70%			
	OR4	Averías de origen físico o lógico[I.4]	2	50%	50%			
AS04	**[rein]**	**Hard drive**	**3**	**70%**	**60%**	**50%**	**50%**	**20%**
	EF11	Destrucción de información [E11]	3	60%	50%	50%	20%	
	EF1	Errores de los usuarios [E1]	3	30%	40%	40%	50%	20%
	OR4	Averías de origen físico o lógico[I.4]	2	70%	60%			
	EF6	Difusión de software dañino [E6]	3	50%	50%			
	AI4	Usos no previsto [A4]	4	30%	50%	40%	50%	20%
AS05	**[temo]**	**Tarjetas de Memoria (SD, microSD, etc)**	**3**	**60%**	**70%**	**50%**	**40%**	**30%**
	EF11	Destrucción de información [E11]	3	60%	50%	50%	30%	
	EF1	Errores de los usuarios [E1]	3	30%	40%			
	OR4	Averías de origen físico o lógico[I.4]	2	60%	70%	40%	40%	30%
	EF6	Difusión de software dañino [E6]	3	50%	50%			
	AI4	Usos no previsto [A4]	4	30%	50%	40%	20%	20%

Equipamiento Auxiliar
[eqax]

N°	Cód.	Activos	Probabilidad de ocurrencia de materialización de amenazas	Dimensiones				
				[dis]	**[int]**	**[con]**	**[au]**	**[nr]**
AA01	**[cae]**	**Cableado eléctrico**	**4**	**60%**	**60%**	**50%**	**10%**	**40%**
	OR5	Corte de suministro de eléctrico [I.5]	4	60%				
	OR2	Contaminación electromagnética [I.2]	3		40%			20%
	OR4	Averías de origen físico o lógico[I.4]	4	50%	60%	50%	10%	40%
AA02	**[car]**	**Cableado de la red**	**3**	**80%**	**70%**	**50%**	**30%**	**20%**
	OR2	Contaminación electromagnética [I.2]	3	50%	50%			
	OR7	Fallo de servicios de comunicaciones [I.7]	4	60%	70%	50%	30%	10%
	OR3	Desastres Industriales [I.3]	3	50%	50%			
	OR8	Degradación de los soportes de almacenamiento de datos [I.8]	3	80%	50%			10%
	DN3	Cambios/ Fenómenos climáticos [N.4]	3	30%	50%	20%		20%
AA03	**[esen]**	**Estabilizador de energía**	**4**	**60%**	**70%**	**10%**	**90%**	**10%**
	OR7	Fallo de servicios de comunicaciones [I.7]	4	60%	50%		10%	10%
	OR8	Degradación de los soportes de almacenamiento de datos [I.8]	3	50%	70%	10%	90%	
	OR4	Averías de origen físico o lógico[I.4]	4	50%	30%		10%	10%
AA04	**[fua]**	**Fuentes de alimentación**	**3**	**60%**	**50%**	**0%**	**0%**	**0%**
	OR4	Averías de origen físico o lógico[I.4]	2	60%	50%			
	OR5	Corte de suministro de eléctrico [I.5]	3	50%	30%			

Instalaciones [inst]								
N°	**Cód.**	**Activos**	**Probabilidad de ocurrencia de materialización de amenazas**	**Dimensiones**				
				[dis]	**[int]**	**[con]**	**[au]**	**[nr]**
AA01	**[cae]**	**Oficinas**	**2**	**90%**	**80%**	**50%**	**20%**	**50%**
	DN1	Fuego [N.1]	1	90%	80%	30%		
	AI4	Usos no previsto [A4]	3	20%	30%	50%	20%	50%
	OR1	Contaminación mecánica [I.1]	3	60%				
AA02	**[car]**	**Sala de capacitaciones y trabajo en general**	**3**	**60%**	**50%**	**50%**	**20%**	**50%**
	OR7	Fallo de servicios de comunicaciones [I.7]	3	50%	50%			
	AI4	Usos no previsto [A4]	3	30%	30%	50%		10%
	AI7	Accesos no autorizados [A7]	4	60%	50%	50%	20%	50%
AA03	**[esen]**	**Sala de atención**	**4**	**90%**	**50%**	**80%**	**30%**	**30%**
	AI4	Usos no previsto [A4]	4	90%	40%	80%		30%
	OR1	Contaminación mecánica [I.1]	3	10%	50%		30%	20%

Personal [per]								
N°	**Cód.**	**Activos**	**Probabilidad de ocurrencia de materialización de amenazas**	**Dimensiones**				
				[dis]	**[int]**	**[con]**	**[au]**	**[nr]**
PP01	**[eninf]**	**Encargado de informática**	**4**	**80%**	**70%**	**80%**	**80%**	**10%**
	EF9	Fugas de información [E9]	3	40%	40%			
	AI19	Indisponibilidad de personal [A19]	4	60%		80%	30%	

Personal [per]								
N°	**Cód.**	**Activos**	**Probabilidad de ocurrencia de materialización de amenazas**	**Dimensiones**				
				[dis]	**[int]**	**[con]**	**[au]**	**[nr]**
	AI7	Accesos no autorizados [A7]	4	50%		70%	80%	
	AI21	Ingeniería social [A21]	4	80%	70%	70%	80%	10%
	AI3	Abuso de privilegios de acceso [A3]	4		50%	60%	60%	60%
PP02	**[car]**	**Personal encargado**	**3**	**80%**	**70%**	**80%**	**80%**	**60%**
	EF9	Fugas de información [E9]	3	40%	40%			
	AI19	Indisponibilidad de personal [A19]	3	60%		80%	30%	
	AI3	Abuso de privilegios de acceso [A3]	3	50%		70%	80%	
	AI21	Ingeniería social [A21]	4	80%	70%	70%	80%	10%
	AI7	Accesos no autorizados [A7]	4		50%	60%	60%	60%
PP03	**[esen]**	**Personal administrativo**	**4**	**80%**	**70%**	**80%**	**80%**	**60%**
	EF9	Fugas de Información [E9]	3	40%	40%			
	AI15	Manipulación de equipos [A15]	4	60%		80%	30%	
	AI19	Indisponibilidad de personal [A19]	4	50%		70%	80%	
	AI3	Abuso de privilegios de acceso [A3]	4	80%	70%	70%	80%	10%
	AI21	Ingeniería social [A21]	4		50%	60%	60%	60%
	AI7	Accesos no autorizados [A7]	4		50%	60%	60%	60%

Nota: Elaboración propia

4.4. OBJETIVO ESPECÍFICO 2

Una vez que se identificaron los activos de la institución y se analizaron las probabilidades de ocurrencia de estos, se determinó que afectaban al sistema web de la institución. Esto permitió observar desde el interior de la institución diversas variables que podían influir negativamente y, a su vez, evidenciaban las vulnerabilidades a las que estaba expuesto.

4.4.1. Ejecución de la Metodología OWASP

En este apartado se detalló la metodología OWASP utilizada para realizar las pruebas de intrusión en el sistema web de la institución. Posteriormente, se describió el proceso de comprobación de vulnerabilidades. Para llevar a cabo la prueba de intrusión, OWASP propuso dos fases fundamentales:

- **Fase 1 Modo pasivo:** En esta fase se identificaron todas las funcionalidades disponibles en el sistema web del Colegio de Ingenieros del Perú, Consejo Departamental Puno. Asimismo, se analizó la lógica de la aplicación, centrándose en los puntos de acceso del sistema web, como encabezados, parámetros y cookies con el objetivo de comprender el comportamiento y la estructura del sistema, lo que permitió establecer una base sólida para las pruebas de intrusión y el análisis de seguridad.

- **Fase 2 Modo activo:** En esta fase se sometió al sistema web a las pruebas de vulnerabilidad las cuales fueron sugeridas por la metodología OWASP. Durante este proceso, se identificaron todas las posibles vulnerabilidades a las que el sistema web estuvo expuesto, proporcionando un análisis detallado de los riesgos y debilidades detectado.

Tabla 20

Pruebas de vulnerabilidad

Categoría	Número de Referencia	Nombre de prueba
Recopilación de información	OWASP-RI-001	Robots, Spiders y Crawlers
	OWASP-RI-002	Reconocimiento mediante motores de búsqueda
	OWASP-RI-003	Reconocer los puntos de entrada de la aplicación
	OWASP-RI-004	Test de firma digital para aplicaciones web.
	OWASP-RI-005	Descubrimiento de aplicaciones
	OWASP-RI-006	Analizar Códigos de Errores
Pruebas de gestión de configuración e implementación	OWASP-PG-001	Test de SSL/TLS
	OWASP-PG-002	Test de receptor de escucha de la BD
	OWASP-PG-003	Test de gestión de configuración de la infraestructura
	OWASP-PG-004	Test de gestión de configuraciones
	OWASP-PG-005	Gestión de extensiones de archivo
	OWASP-PG-006	Copias de seguridad y archivos antiguos
	OWASP-PG-007	Paneles de control para la gestión de la infraestructura
Comprobación del sistema de autenticación	OWASP-ID-001	Envío de credenciales mediante un canal seguro y cifrado
	OWASP-ID-002	Enumeración de usuarios
	OWASP-ID-003	Pruebas de diccionario
	OWASP-ID-004	Eludir el sistema de autenticación.
	OWASP-ID-005	Verificar sistemas de recuperación o restauración de contraseñas que presenten vulnerabilidades
	OWASP-ID-006	Evaluación de la gestión del caché del navegador y del proceso de cierre de sesión.
	OWASP-ID-007	Evaluación de la gestión del caché del navegador y cierre de sesión.
	OWASP-ID-008	Pruebas de CAPTCHA
	OWASP-ID-009	Pruebas para autenticación de factores múltiples
	OWASP-ID-010	Prueba de situaciones adversas
Pruebas de Validación de Datos	OWASP-PA-001	Prueba de XSS Reflejado
	OWASP-PA-002	Prueba de XSS Almacenado
	OWASP-PA-003	Prueba de XSS basado en DOM
	OWASP-PA-004	Prueba de XSS basado en Flash
	OWASP-PA-005	Inyección SQL

	Número de Referencia	Nombre de prueba
	OWASP-PA-006	Inyección LDAP
	OWASP-PA-007	Inyección ORM
	OWASP-PA-008	Inyección XML
	OWASP-PA-009	Inyección SSI
	OWASP-PA-010	Inyección XPath
Pruebas de automatización	OWASP-AZ-001	Ruta Transversal
	OWASP-AZ-002	Para Evitar Esquema de Autorización
	OWASP-AZ-003	Prueba de escalada de privilegios
Pruebas de gestión de sesión	OWASP-GS-001	Prueba del Esquema de Gestión de Sesión
	OWASP-GS-002	Prueba de atributos de Cookies
	OWASP-GS-003	Prueba de Fijación de Sesión
	OWASP-GS-004	Prueba de Variables de Sesión Expuestas
Pruebas de validación de ingreso	OWASP-VI-001	Ataques a través de Comodines SQL
	OWASP-VI-002	Bloqueo de Cuentas de Usuarios
Pruebas de servicios web	OWASP-SW-002	Prueba de REST/parámetros HTTP GET
	OWASP-SW-002	Adjuntos SOAP maliciosos
Prueba de Ajax	OWASP-PX-002	Vulnerabilidades Ajax

Nota: Adaptado de la guía de pruebas de OWASP

4.4.2. Recopilación de información

En la primera fase parte se realizó una evaluación de seguridad al sistema web de la institución, se enfocó en recopilar la mayor cantidad de información posible sobre el sistema web con el objetivo de comprender y ver su funcionamiento. En una prueba de intrusión, la recopilación de información es un paso esencial puesto que la prueba de reconocimiento de información pasivo se lleva a cabo sin intervenir en los servidores ni que estos produzcan registros de seguridad.

Es posible obligar al sistema web a filtrar información al exterior mediante mensajes de error devueltos, o revelar las versiones y tecnologías utilizadas por la aplicación web mediante el uso de herramientas de acceso público, como motores de búsqueda, scanners o peticiones HTTP simples.

4.4.2.1. OWASP-RI-001 (Spiders, Robots, y Crawlers)

La exploración y recopilación de los recursos relacionados con la aplicación web, como la configuración robots.txt, que los motores de búsqueda utilizan con frecuencia para clasificar los enlaces internos, es una fase de este proceso de recopilación de información.

Robots.txt: Los crawlers, robots y spiders web inspeccionan los sitios web y luego acceden para adquirir su contenido. El protocolo de exclusión de robots del fichero robots.txt que se encuentra en la raíz del sistema web regula estrictamente su comportamiento.

Figura 5

Configuración Archivo robots.txt

Nota: Adaptado de Google [Fotografía]

La Figura 5 identificó el robot.txt, este archivo protegió áreas administrativas y facilitó la indexación del sitio, fue bastante eficiente pero actualmente Google empezó a cambiar el algoritmo, dejando de lado el robot.txt, consecuentemente accedían sin problemas, todos los robots, crawlers y spider accedían sin problema al sistema web para indexarlas.

Al mostrarse la directiva User-agent: * mostró que las reglas de seguimiento se aplicaron a todos los crawlers, robots y spiders. Sobre la directiva Disaflow indicó al robot que no debe acceder a cualquier página del sistema web, específicamente en /wp-admin/. Por otro lado Allow indicó que está permitiendo que cualquiera pueda acceder al enlace.

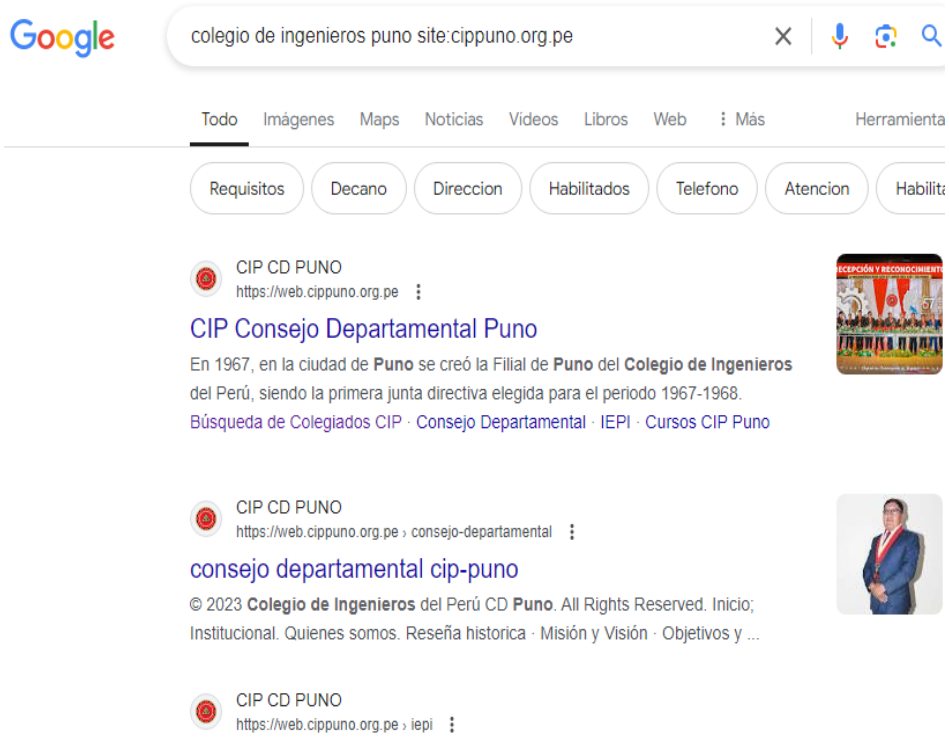
4.4.2.2. OWASP-RI-002 (Reconocimiento mediante motores de búsqueda)

Al finalizar el proceso de crawling, los robots comienzan a indexar el contenido de las páginas web en función de los elementos más relevantes para la búsqueda.

- Colegio de Ingenieros Puno site:cippuno.org.pe

Figura 6

Colegio de Ingenieros Puno site:cippuno.org.pe Google.com

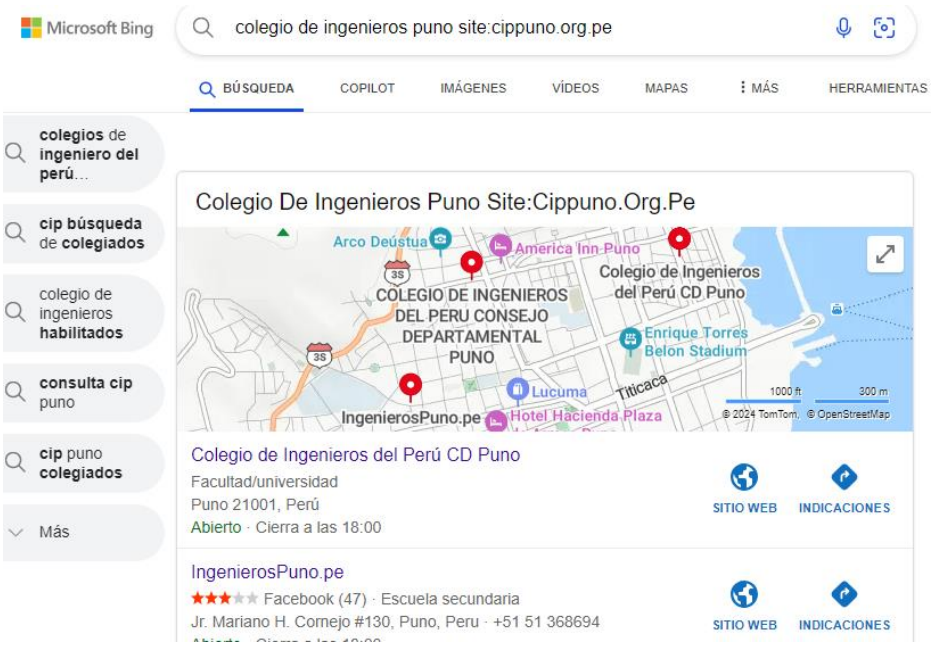


Nota: Adaptado de Google [Fotografía]

El comando site: en Google se usó para limitar los resultados de búsqueda a un dominio específico, esta herramienta fue muy práctica para buscar información acerca del sistema web del Colegio de Ingenieros del Perú, Consejo Departamental Puno. Además se verificó de manera específica si el sitio web de la institución está indexada en Google, tal como se muestra en la Figura 6, la cual evidenció que mediante site: facilitó la búsqueda de manera precisa y específica dentro del sitio web. Actualmente Google ya no muestra la cantidad de resultados en números las cuales se mostraban en la parte superior con la cantidad de páginas indexadas, debido a que google está realizando pruebas y es posible que desaparezcan completamente.

Figura 7

Colegio de Ingenieros Puno site:cippuno.org.pe Bing.com



Nota: Adaptado de Google [Fotografía]

En la Figura 7 se evidenció los resultados del sistema web del Colegio de Ingenieros del Perú, Consejo Departamental Puno, realizado

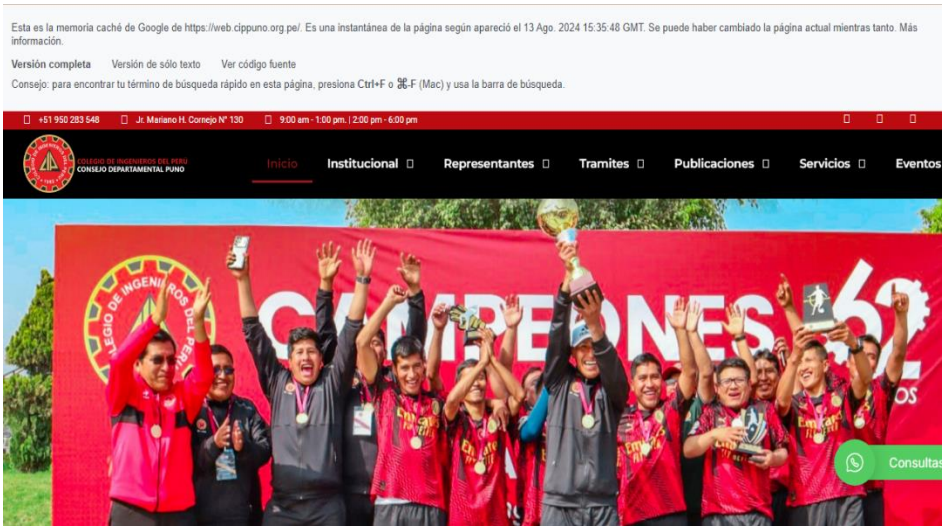
con el motor de búsqueda web de Microsoft, Bing.com, donde de igual manera ya no se muestran los resultados.

- Cache:cippuno.org.pe

En la se muestra una captura de pantalla que es la última del sitio web de Colegio de Ingenieros del Perú, Consejo Departamental Puno realizada por los motores de búsqueda.

Figura 8

Cache:cippuno.org.pe Google.com



Nota*:* Adaptado de cippuno.org.pe [Fotografía]

La Figura 8 se mostró el cache de sistema web de CIP, la cual corresponde al 13 de Agosto de 2024 15:35:48 GMT, último día en que Google hizo el rastreo del sistema web cippuno.org.pe.

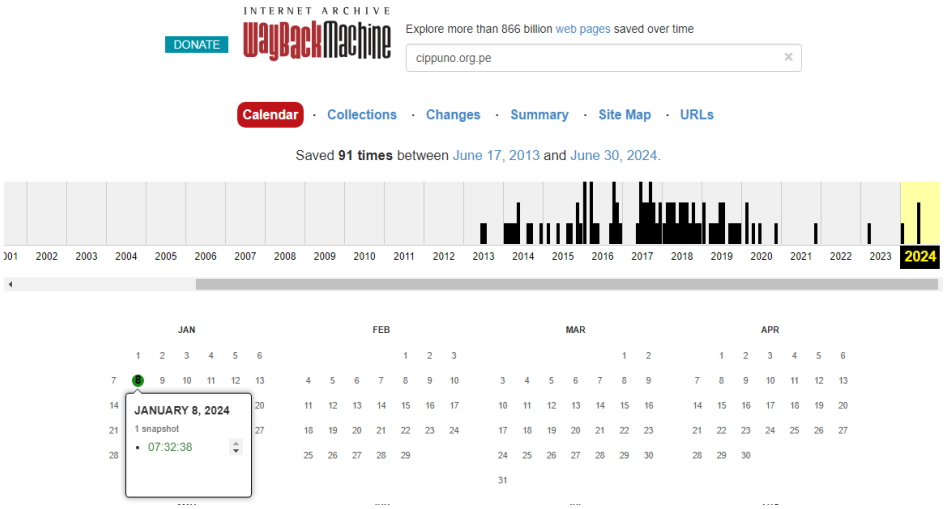
- Archive.org cippuno.org.pe

Archive.org sirve como una biblioteca digital que preserva el pasado de internet y proporciona acceso a contenido digital en diversas formas. Esto fue muy útil puesto que refleja todos los

cambios históricos en el sistema web de la institución, donde se pudo recuperar contenido perdido y ver cómo era el sitio web en el pasado.

Figura 9

Archive.org cippuno.org.pe Google.com



Nota: Adaptado de Google [Fotografía]

En la Figura 9 se examinó el sistema web cippuno.org.pe, dónde se observa que el desarrollo del sitio comenzó en junio de 2013. Según Archive.org, se registraron aproximadamente 91 modificaciones en la línea de tiempo desde el 17 de junio de 2013 hasta el 30 de junio de 2024.

Figura 10

Cippuno.org.pe 6 de marzo 2023

Nota: Adaptado de Google [Fotografía]

Figura 11

Cippuno.org.pe 15 de agosto 2022

Nota: Adaptado de Google [Fotografía]

En la Figura 10 y Figura 11 se observaron informaciones sobre el registro de un dominio, incluyendo los detalles del propietario, fechas importantes y servidores DNS. Fue usado con la finalidad de verificar la disponibilidad de dominio y obtener datos de contacto relacionados con ellos.

Tabla 21

Registro Whois cippuno.org.pe

cippuno.org.pe Registro a whols
Domain Name: cippuno.org.pe Sponsoring Registrar: NIC.PE Domain Status: ok Registrant Name: CIP - Consejo Departamental Puno Admin Name: COLEGIO DE INGENIEROS DEL PERU CONSEJO DEPARTAMENTAL PUNO Admin Email: cip.cdpuno.ots@gmail.com Name Server: ns.rcp.net.pe Name Server: ns2.rcp.net.pe >>> Last update of WHOIS database: 2024-08-14T02:05:09.252Z

Nota: Realizado según Whois data base

Interpretación

La Tabla 21 muestra el registro WHOIS la cual proporciona detalles técnicos y administrativos sobre el dominio cippuno.org.pe. Se logró observar el nombre del dominio: cippuno.org.pe. En cuanto al registrador patrocinador: NIC.PE: es la entidad que gestiona los registros de dominios con el ccTLD (country code Top-Level Domain) .pe (Perú). El estado del dominio indicó que el dominio está activo y en buen estado. No hubo restricciones o problemas reportados. Los servidores de nombres son los servidores de nombres que gestionan las solicitudes DNS para el dominio. RCP (Red Científica Peruana) es una red de servicios en Perú, lo que refiere que el dominio fue asociado con infraestructura local en Perú. La última actualización de la base de datos WHOIS fue el 2024-08-14T02:05:09.252Z.

El dominio cippuno.org.pe fue registrado por el CIP, Consejo Departamental Puno y administrado por la misma institución. Su estado fue activo y utiliza servidores de nombres proporcionados por RCP en Perú. La información administrativa incluyó un contacto a través de Gmail, lo cual puede ser relevante para la gestión del dominio y la comunicación. La última actualización de la información de WHOIS fue el 14 de agosto de 2024.

4.4.2.3. OWASP-RI-003 (Reconocer los puntos de entrada de la aplicación)

La identificación de puntos de entrada de la aplicación mediante métodos GET y POST es una tarea esencial para entender cómo una

aplicación web interactúa con los usuarios y cómo se manejan los datos a través de formularios, enlaces, y APIs.

El método GET se utiliza para solicitar datos de un servidor y recuperar información, pero no es adecuado para datos sensibles, ya que estos se adjuntan a la URL. En contraste, el método POST permite enviar datos al servidor de forma más segura, ya que no expone la información en la URL. Además, el uso de Google Colab resultó muy útil, ya que combina un entorno de notebook fácil de usar con recursos computacionales avanzados y colaboración en línea, siendo ideal para científicos de datos, investigadores y desarrolladores que trabajan con Python.

Al momento de verificar las solicitudes al sitio web del Colegio de Ingenieros del Perú, Consejo Departamental Puno, se encontró que utilizan los dos tipos de peticiones; GET y POST.

Tabla 22

HTTPS Header petición GET

HTTPS Header petición GET
Date: Tue, 20 Aug 2024 20:53:53 GMT Server: Apache/2.4.41 (Ubuntu) Link: <https://web.cippuno.org.pe/wp-json/>; rel="https://api.w.org/", <https://web.cippuno.org.pe/wp-json/wp/v2/pages/6446>; rel="alternate"; title="JSON"; type="application/json", <https://web.cippuno.org.pe/>; rel=shortlink Vary: Accept-Encoding Content-Encoding: gzip Content-Length: 34203 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html; charset=UTF-8

Nota: Realizado según Colabority (GET)

Interpretación

En la Tabla 22 reflejó los metadatos asociados a una respuesta HTTP que un servidor envía a un cliente (como un navegador web), estos encabezados ayudan a gestionar cómo se entrega y procesa la respuesta entre el servidor y el cliente, optimizando la comunicación, la seguridad y la eficiencia del intercambio de datos. El servidor Apache en Ubuntu respondió a una solicitud proporcionando una página HTML comprimida en formato gzip. Además, mantuvo la conexión abierta, permitiendo la posibilidad de procesar solicitudes adicionales de manera eficiente.

Tabla 23

HTTPS Header petición POST

HTTPS Header petición POST
Tabla de Encabezados HTTPS (POST): --- Date: Tue, 20 Aug 2024 22:40:26 GMT Server: Apache/2.4.41 (Ubuntu) Link: <https://web.cippuno.org.pe/wp-json/>; rel="https://api.w.org/", <https://web.cippuno.org.pe/wp-json/wp/v2/pages/6446>; rel="alternate"; title="JSON"; type="application/json", <https://web.cippuno.org.pe/>; rel=shortlink Vary: Accept-Encoding Content-Encoding: gzip Content-Length: 34203 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html; charset=UTF-8

Nota: Realizado según Colabority (POST)

Interpretación

La Tabla 23 de encabezados muestra que el servidor responció a la solicitud POST con una página HTML comprimida, utilizando Apache en un entorno Ubuntu. El contenido fue optimizado para transferencia

eficiente, con la conexión mantenida abierta para futuras solicitudes. Además, se incluyeron enlaces útiles para acceder a la API de WordPress y a otras representaciones del contenido.

4.4.2.4. OWASP-RI-004 (Test de firma digital para webs)

Conocer el tipo y la versión exacta del servidor web es crucial en el proceso de análisis del sistema web del Colegio de Ingenieros del Perú, Consejo Departamental Puno, ya que nos permitió identificar posibles vulnerabilidades específicas de esas versiones y seleccionar los exploits adecuados para utilizar durante las pruebas, lo que puede influir significativamente en el desarrollo de estas.

Tabla 24

Cabecera de respuesta HTTP

Cabecera de respuesta HTTP	
Cabecera	**Valor**
Date	Wed, 21 Aug 2024 00:02:25 GMT
Server	Apache/2.4.41 (Ubuntu)
Link	rel="https://api.w.org/", ; rel="alternate"; title="JSON"; type="application/json", ; rel=shortlink
Vary	Accept-Encoding
Content-Encoding	gzip
Content-Length	34203
Keep-Alive	timeout=5, max=100
Connection	timeout=5, max=100
Content-Type	text/html; charset=UTF-8

Nota: Realizado según Colabority (HTTP)

Interpretación

La Tabla 24 mostró una cabecera de respuesta HTTP, la cual incluyó información importante sobre la respuesta del servidor web, sobre cómo se fue procesado y entregado el contenido solicitado, incluyendo información sobre compresión, tipo de contenido, y políticas de conexión.

4.4.2.5. OWASP-RI-005 (Descubrimiento de aplicaciones)

Hoy en día, es común que una sola dirección IP aloje múltiples dominios. Durante el análisis de puertos, se observa que algunos servicios, aunque estén instalados en el servidor, no son accesibles ni para los usuarios de la página web ni para quienes realizan un análisis de los servicios. Por ejemplo, el puerto 80, que suele utilizarse para el servicio HTTP, puede mostrar un mensaje de error al intentar acceder externamente, indicando que el servicio no está instalado, a pesar de que debería estar disponible.

Es habitual que se proporcionen direcciones IP junto con sus nombres, pero estos nombres pueden tener asignaciones adicionales que no se especifican de inmediato. Además, las URLs de las aplicaciones web a menudo contienen errores y no reflejan correctamente el contenido publicado, lo que puede deberse a una configuración incorrecta del servidor o a enlaces de configuración.

Para verificar la correcta configuración y determinar qué servicios están activos o instalados en el servidor, se realizaron pruebas específicas en el sitio web en cuestión.

Tabla 25

Consulta los servicios configurados - Nmap

Consulta los servicios configurados con Nmap
Reading package lists... Done Building dependency tree... Done Reading state information... Done nmap is already the newest version (7.91+dfsg1+really7.80+dfsg1-2ubuntu0.1). 0 upgraded, 0 newly installed, 0 to remove and 45 not upgraded. Starting Nmap 7.80 (https://nmap.org) at 2024-08-21 19:47 UTC Nmap scan report for cippuno.org.pe (161.132.49.216) Host is up (0.19s latency). Not shown: 996 closed ports PORT STATE SERVICE VERSION 21/tcp open ftp vsftpd 3.0.5 22/tcp open ssh OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; protocol 2.0) 80/tcp open http nginx 1.18.0 (Ubuntu) 443/tcp open ssl/http nginx 1.18.0 (Ubuntu) Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel Service detection performed. Please report any incorrect results at https://nmap.org/submit/ . Nmap done: 1 IP address (1 host up) scanned in 20.79 seconds

Nota: Realizado según Colabority (Nmap)

Interpretación

La Tabla 25 muestra los resultados del escaneo realizado con Nmap, donde se identificaron los servicios y puertos abiertos en el servidor del dominio cippuno.org.pe. Los puertos detectados incluyeron el puerto 21 para FTP (transferencia de archivos), el 22 para SSH (acceso remoto seguro), el 80 para HTTP (transmisión estándar de datos web) y el 443 para HTTPS (versión segura de HTTP con cifrado). Estos servicios son esenciales para la operatividad y comunicación del servidor. El servidor utiliza un sistema operativo basado en Unix o Linux, como se refleja en la información del CPE (Common Platform Enumeration) proporcionada.

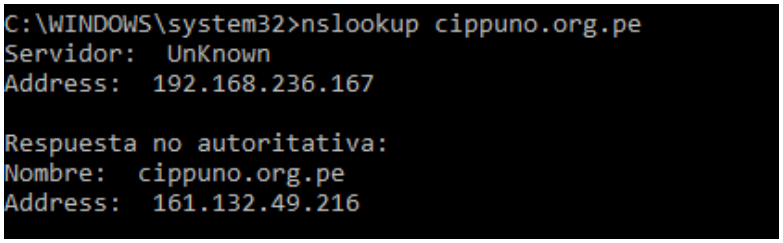
La detección de servicios realizados por Nmap, identificaron puertos y versiones como activos. La información proporcionada fue útil para evaluar la seguridad del servidor, ya que cada servicio puede tener vulnerabilidades específicas. Respecto a los puertos cerrados no se mostraron, pero se sabe que 996 puertos están cerrados. Este escaneo reveló la presencia de servicios comunes en servidores web, como FTP, SSH, HTTP y HTTPS, y puede ser la base para realizar un análisis de seguridad más profundo.

- **Transferencias de zona DNS**

Se consultan los servidores de nombres asociados a la dirección IP del Sistema web de Colegio de Ingenieros del Perú, Consejo Departamental Puno, el siguiente comando permitió realizar una consulta sobre la información solicitada:

Figura 12

Consulta de Servidores de Nombres para el sistema web del CIP



Nota: Realizado según CMD Windows (DNS)

Interpretación

En la Figura 12 se mostró los resultados de la consulta DNS para obtener la dirección IP del dominio cippuno.org.pe. La consulta se dirigió al servidor DNS con la dirección IP 192.168.236.167, cuyo nombre no se pudo determinar. Como respuesta, se identificó que el dominio cippuno.org.pe tiene asignada la dirección IP 161.132.49.216.

4.4.2.6. OWASP-RI-006 (Analizar Códigos de Errores)

Es común encontrar códigos de error y alertas creados por el servidor durante el análisis y prueba de aplicaciones web. Se puede obtener información útil sobre cippuno.org.pe mediante solicitudes particulares. Dado que brindan información sobre el servidor, las bases de datos, los errores y otros elementos técnicos relacionados con la aplicación web, estos códigos de error son esenciales para el proceso de prueba.

Para evaluar la seguridad del sitio cippuno.org.pe y para las siguientes fases del análisis de vulnerabilidades, esta información fue fundamental.

- HTTP 404 Not Found

Figura 13

404 Error page not found

Nota: Adaptado de cippuno.org.pe [Fotografía]

Interpretación

En la Figura 13 se observó al 404 Error page not found y esto se debe a que se hizo un acceso manual, el código brindó información sobre

el servidor web que hospeda la aplicación y sus componentes relacionados estos casos son muy frecuentes en las páginas web puesto que los usuarios a menudo escriben URLs incorrectas o hacen clic en enlaces rotos que llevan a páginas que ya no existen, también puede ser por que las páginas o archivos pueden ser movidos o eliminados sin actualizar los enlaces internos o externos entre otros.

Figura 14

Cabecera HTTP 404 Error page not found

```
C:\WINDOWS\system32>curl -I https://web.cippuno.org.pe/home/owasp
HTTP/1.1 404 Not Found
Date: Wed, 21 Aug 2024 23:41:31 GMT
Server: Apache/2.4.41 (Ubuntu)
Expires: Wed, 11 Jan 1984 05:00:00 GMT
Cache-Control: no-cache, must-revalidate, max-age=0
Link: <https://web.cippuno.org.pe/wp-json/>; rel="https://api.w.org/"
Content-Type: text/html; charset=UTF-8
```

Nota: Realizado según Colabority (404 Error page not found)

Interpretación

En la Figura 14 mostró que el servidor está configurado con Apache en Ubuntu, y que una solicitud a la URL /home/owasp resultó en un error 404 Not Found. Las cabeceras del servidor revelaron directivas para el manejo de caché, así como información sobre el tipo de contenido y enlaces relacionados con la API del sitio, datos clave para identificar el sistema operativo y las versiones de las aplicaciones utilizadas.

4.4.3. Pruebas de gestión de configuración e implementación

El análisis de infraestructura o topología de la arquitectura web del servidor implica examinar la estructura y organización de los componentes que soporta un sitio web o aplicación web. Este análisis es crucial para entender cómo

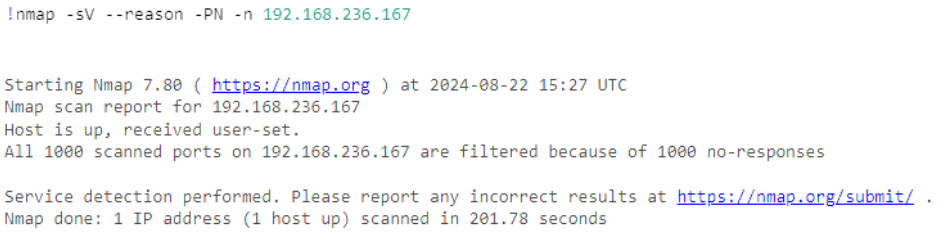
se distribuyen los recursos y cómo interactúan los diferentes elementos del sistema.

4.4.3.1. OWASP-PG-001 (Pruebas de SSL/TLS)

Las pruebas de SSL/TLS implicaron evaluar la seguridad y configuración de los protocolos SSL (Secure Sockets Layer) y TLS (Transport Layer Security) en un servidor web. Estos protocolos cifran la comunicación entre el cliente y el servidor para proteger la privacidad e integridad de los datos transmitidos. El propósito de esta prueba fue para garantizar que los mecanismos de cifrado estén correctamente implementados y libres de vulnerabilidades que puedan ser aprovechadas por atacantes.

Figura 15

Reconocimiento de servicios SSL



Nota: Realizado según Colabority (Reconocimiento de SSL con Nmap)

Interpretación

En la Figura 15 se hizo un escaneo con Nmap, en dónde se identificó los servicios asociados a los puertos SSL/TLS, en el cual se muestra el host que está en línea, pero todos los puertos escaneados están filtrados, lo que podría indicar que el host está protegido por un firewall o que no tiene servicios expuestos en los puertos escaneados.

- Script ssl-enum-ciphers

El script ssl-enum-ciphers es una herramienta de Nmap que enumera los cifrados SSL/TLS disponibles en un servidor. Su función principal es verificar la seguridad de los cifrados soportados por el servidor, identificando debilidades como el uso de algoritmos inseguros o configuraciones incorrectas.

El script también muestra información sobre los protocolos SSL/TLS soportados, los tamaños de clave, y otros detalles relevantes para evaluar la robustez de la seguridad en la comunicación cifrada del servidor. Es intrusivo y genera múltiples conexiones al servidor, lo que lo hace notorio.

Figura 16

Nmap Script ssl-enum-ciphers

```
!nmap -sV --script ssl-enum-ciphers -p 443 web.cippuno.org.pe


Starting Nmap 7.80 ( https://nmap.org ) at 2024-08-22 00:27 UTC
Nmap scan report for web.cippuno.org.pe (161.132.41.185)
Host is up (0.19s latency).

PORT    STATE SERVICE VERSION
443/tcp open  ssl/ssl Apache httpd (SSL-only mode)
|_http-server-header: Apache/2.4.41 (Ubuntu)
| ssl-enum-ciphers:
|   TLSv1.2:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (ecdh_x25519) - A
|       TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (ecdh_x25519) - A
|       TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (ecdh_x25519) - A
|       TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (dh 2048) - A
|       TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (dh 2048) - A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (ecdh_x25519) - A
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (ecdh_x25519) - A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (ecdh_x25519) - A
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (ecdh_x25519) - A
|       TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (dh 2048) - A
|       TLS_DHE_RSA_WITH_AES_128_CBC_SHA (dh 2048) - A
|       TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (dh 2048) - A
|       TLS_DHE_RSA_WITH_AES_256_CBC_SHA (dh 2048) - A
|       TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 2048) - A
```

Nota: Realizado según Colabority (Reconocimiento de SSL con nmap)

Interpretación

En la Figura 16 se mostró que el puerto 443, utilizado para HTTPS, estaba configurado para conexiones seguras SSL/TLS, soportando TLS 1.2 con algoritmos de cifrado de alta fuerza (A). El servidor priorizó cifrados seguros, asegurando la protección de los datos transmitidos. Se recomienda realizar revisiones periódicas para mantener esta configuración actualizada y libre de vulnerabilidades.

Tabla 26

Resultado completo de análisis Nmap Script ssl-enum-ciphers

Análisis Script ssl-enum-ciphers - Resultados
Starting Nmap 7.80 (https://nmap.org) at 2024-08-22 00:27 UTC Nmap scan report for web.cippuno.org.pe (161.132.41.185) Host is up (0.19s latency). PORT STATE SERVICE VERSION 443/tcp open ssl/ssl Apache httpd (SSL-only mode) |_http-server-header: Apache/2.4.41 (Ubuntu) | ssl-enum-ciphers: | TLSv1.2: | ciphers: | TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (ecdh_x25519) - A | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (ecdh_x25519) - A | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (ecdh_x25519) - A | TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (dh 2048) - A | TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (dh 2048) - A | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (ecdh_x25519) - A | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (ecdh_x25519) - A | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (ecdh_x25519) - A | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (ecdh_x25519) - A | TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (dh 2048) - A | TLS_DHE_RSA_WITH_AES_128_CBC_SHA (dh 2048) - A | TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (dh 2048) - A | TLS_DHE_RSA_WITH_AES_256_CBC_SHA (dh 2048) - A | TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - A | TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048) - A | TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 2048) - A | TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 2048) - A | TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A | TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A | compressors: | NULL

Análisis Script ssl-enum-ciphers - Resultados

| cipher preference: server
|_ least strength: A

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 38.05 seconds

Nota: Realizado según Colabority (Resultados de Análisis Script ssl-enum-ciphers)

Interpretación

En la Tabla 26 presentó los resultados completos, destacando que el servidor web está configurado de manera óptima en términos de seguridad SSL/TLS. Utilizó cifrados modernos y seguros para proteger las comunicaciones, lo que garantiza una configuración robusta. Sin embargo, se recomienda realizar revisiones periódicas para asegurar que la seguridad se mantenga actualizada y eficaz frente a posibles vulnerabilidades.

- Evaluación de vulnerabilidades SSL utilizando OpenSSL

La evaluación de vulnerabilidades SSL utilizando OpenSSL es el proceso de usar la herramienta OpenSSL para analizar y detectar posibles debilidades en la configuración de SSL/TLS en un servidor.

Esto incluye la identificación de certificados inseguros, cifrados débiles o configuraciones incorrectas que podrían comprometer la seguridad de las comunicaciones. Además, permite detectar el uso de protocolos obsoletos, como versiones anteriores de SSL/TLS, que ya no se consideran seguros, y evaluar si las configuraciones actuales cumplen con las mejores prácticas recomendadas.

Tabla 27

Evaluación de vulnerabilidades SSL utilizando OpenSSL

Evaluación de vulnerabilidades SSL utilizando OpenSSL
Reading package lists... Done Building dependency tree... Done Reading state information... Done openssl is already the newest version (3.0.2-0ubuntu1.17). openssl set to manually installed. 0 upgraded, 0 newly installed, 0 to remove and 44 not upgraded. CONNECTED(00000003) depth=2 C = US, O = Internet Security Research Group, CN = ISRG Root X1 verify return:1 depth=1 C = US, O = Let's Encrypt, CN = R10 verify return:1 depth=0 CN = web.cippuno.org.pe verify return:1 Certificate chain 0 s:CN = web.cippuno.org.pe i:C = US, O = Let's Encrypt, CN = R10 a:PKEY: rsaEncryption, 2048 (bit); sigalg: RSA-SHA256 v:NotBefore: Jun 30 00:59:02 2024 GMT; NotAfter: Sep 28 00:59:01 2024 GMT 1 s:C = US, O = Let's Encrypt, CN = R10 i:C = US, O = Internet Security Research Group, CN = ISRG Root X1 a:PKEY: rsaEncryption, 2048 (bit); sigalg: RSA-SHA256 v:NotBefore: Mar 13 00:00:00 2024 GMT; NotAfter: Mar 12 23:59:59 2027 GMT --- Server certificate -----BEGIN CERTIFICATE----- MIIE9TCCA92gAwIBAgISBOxlfLV2nr56jxj0w2QkWLAkMA0GCS qGSIb3DQEBCwUA MDMxCzAJBgNVBAYTAlVTMRYwFAYDVQQKEw1MZXQncyB FbmNyeXB0MQwwCgYDVQQD EwNSMTAwHhcNMjQwNjMwMDA1OTAyWhcNMjQwOTI4MDA 1OTAxWjAdMRswGQYDVQQD ExJ3ZWIuY2lwcHVuby5vcmcucGUwggEiMA0GCSqGSIb3DQEBA QUAA4IBDwAwggEK AoIBAQDmPIw+QWzk+exaRiTiK0VTyd7QdfdyMuIZLV2MFi8s86 97ORVYMrP3WbO9 ocNx0fBMHmompdEuvNxIwsdEUU3hk8motmffupqYizH1nsB0Rnrd 6EdvYc31krzj

VWAs9POpivdR2GzPntr+t43it0EWZOElrULhYlHr5HNqQxXd1Qecs
RPwECQOanIn
ulLUAHmUqZ0teGB2aA1fISBcUQ3nB+GqZ5k8SUfNmTVu4jM5gH
92K7QwG4Rhal9m
3Z2h0J0+JxWe+hbOyqjizrTWfhKbCXx706MhdLbPhf894/6PONjTe
RDwR0oJ+HvM
8CsRMQw25czKiSkyCXuo8WBaoobtAgMBAAGjggIXMIICEzAOB
gNVHQ8BAf8EBAMC
BaAwHQYDVR0lBBYwFAYIKwYBBQUHAwEGCCsGAQUFBwM
CMAwGA1UdEweb/wQCMAAw
MAowCAYGZ4EMAQIBMIIBBQYKKwYBBAHWeQIEAgSB9gSB
8wDxAHYAGZgQcQnw1lIu
MIDSnj9ku4NuKMz5D1KO7t/OSj8WtMoAAAGQZt38fgAABAMA
RzBFAiEAyaoe73D7
Hf7l1XJ/47hQmV7aLWX0Dp3H8zfyb4iFEvcCIHdvKmaBXUIuiH/E
CWE9HnIOYVpr
fBhUeYV91bAN7PrzAHcA7s3QZNXbGs7FXLedtM0TojKHRny87N
7DUUhZRnEftZsA
AAGQZt38dwAABAMASDBGAiEAmhFEqO1WobQ2LR3bKFt0B0
LPg+8o18IeJHY6K8Df
Ow8CIQDWfYe+Lk1jNGlRG4TvtcsZM0t3A63R2eAB1XDtuPJgeTA
NBgkqhkiG9w0B
smEZ/zx0bM9DZDNEYx30Hz8Z7P6gEmxhC6Ca/TrMygmI8AqIlZw
B1BzeHnVMpy4k
rCSH0DQGMKQQI91IdHQEja/OVd2+UUWPmg==
-----END CERTIFICATE-----
subject=CN = web.cippuno.org.pe
issuer=C = US, O = Let's Encrypt, CN = R10

No client certificate CA names sent
Peer signing digest: SHA256
Peer signature type: RSA-PSS
Server Temp Key: X25519, 253 bits

SSL handshake has read 3127 bytes and written 400 bytes
Verification: OK

New, TLSv1.3, Cipher is TLS_AES_256_GCM_SHA384
Server public key is 2048 bit
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
Early data was not sent
Verify return code: 0 (ok)

Post-Handshake New Session Ticket arrived:

```
SSL-Session:
    Protocol  : TLSv1.3
    Cipher    : TLS_AES_256_GCM_SHA384
    Session-ID:
8C8AD8412A117514F39DE3771F0B1FDAD29C6EBF94EAA08FA8
65CEBB87B8E376
    Session-ID-ctx:
    Resumption PSK:
    PSK identity hint: None
    SRP username: None
    TLS session ticket lifetime hint: 300 (seconds)
    TLS session ticket:

    Start Time: 1724429308
    Timeout   : 7200 (sec)
    Verify return code: 0 (ok)
    Extended master secret: no
    Max Early Data: 0
---
read R BLOCK
---
Post-Handshake New Session Ticket arrived:
SSL-Session:
    Protocol  : TLSv1.3
    Cipher    : TLS_AES_256_GCM_SHA384
    Session-ID:
C27CBBA6682A5A21A958D2FCCC5D649B67AA546A94181B0DC
E25B0913D816191
    Session-ID-ctx:
    Resumption                                        PSK:
841F656DABB82C1F90691247040AACCBE1D429680285DA41959
23E667A5307BBAA52AF37AD10D588058AFC1777D07CB1
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    TLS session ticket lifetime hint: 300 (seconds)
    TLS session ticket:
    Start Time: 1724429308
    Timeout   : 7200 (sec)
    Verify return code: 0 (ok)
    Extended master secret: no
    Max Early Data: 0
---
read R BLOCK
closed
```

Nota: Realizado según Colabority (Resultados de Análisis OpenSSL)

Interpretación

En la Tabla 27 se mostró una información detallada de una conexión SSL/TLS establecida con el servidor web.cippuno.org.pe utilizando OpenSSL. Aquí se destacaron varios puntos importantes, el certificado del servidor es válido y está emitido por Let's Encrypt, con una cadena de confianza que incluye el certificado raíz de ISRG Root X1, el Cifrado TLS_AES_256_GCM_SHA384 es un cifrado fuerte y moderno, el código de verificación: 0 (ok), indica que el certificado es válido y la conexión es segura. Este resultado indicó que la configuración SSL/TLS del servidor web.cippuno.org.pe es adecuada y segura, cumpliendo con las buenas prácticas actuales para comunicaciones encriptadas.

4.4.3.2. OWASP-PG-002 (Test de receptor de escucha de la BD)

Esta prueba fue fundamental para asegurar que los servicios de base de datos estén funcionando correctamente y puedan comunicarse con las aplicaciones que dependen de ellos. Para ello se utiliza la herramienta Nmap para escanear puertos específicos que suelen ser utilizados por los servicios de base de datos.

Figura 17

Script Oracle test de receptor de escucha a la BD

```
!nmap --script oracle-tns-version -p 1521 161.132.49.216


Starting Nmap 7.80 ( https://nmap.org ) at 2024-08-23 17:01 UTC
Nmap scan report for 161.132.49.216
Host is up (0.15s latency).

PORT     STATE  SERVICE
1521/tcp closed oracle

Nmap done: 1 IP address (1 host up) scanned in 0.86 seconds
```

Nota: Realizado según Colabority (receptor de escucha a la BD)

Tabla 28

Resultados Test de receptor de escucha

Resultados Test de receptor de escucha
Starting Nmap 7.80 (https://nmap.org) at 2024-08-23 17:01 UTC Nmap scan report for 161.132.49.216 Host is up (0.15s latency). PORT STATE SERVICE 1521/tcp closed oracle Nmap done: 1 IP address (1 host up) scanned in 0.86 seconds

Nota: realizado según Colabority - Resultados completos

Interpretación

En la Figura 17 y en la Tabla 28 se realizó el escaneo cuales mostraron que el puerto 1521/tcp en la IP 161.132.49.216 está cerrado. Este puerto es típicamente utilizado para el servicio Oracle, pero en este caso no está en uso en el host.

Concluyendo así que encontrado el puerto cerrado significa que no se pueden establecer conexiones a través de él, lo cual reduce la superficie de ataque de un sistema, evitando potenciales intentos de acceso no autorizado. Cuando un puerto está abierto para ciertos servicios, es crucial restringir su acceso únicamente a las direcciones IP autorizadas. Además, deben implementarse medidas de seguridad adicionales, como firewalls **y** listas de control de acceso (ACL)**,** para minimizar riesgos y garantizar que solo usuarios legítimos puedan conectarse al servicio. Estas acciones refuerzan la protección del sistema contra accesos no autorizados o potenciales ataques.

4.4.3.3. OWASP-PG-003 (Test de gestión de configuración de la infraestructura)

Se utilizó para asegurar que los componentes de un sistema estén configurados correctamente y de manera consistente. Estas pruebas verifican que las configuraciones cumplen con los estándares establecidos, que se implementan correctamente en todos los entornos (desarrollo, pruebas, producción) y que los cambios se gestionan de manera controlada. Esto ayuda a minimizar riesgos, garantizar la seguridad y mantener la eficiencia operativa del sistema.

Figura 18

Head (comando)

Nota: Realizado según Colabority – Head

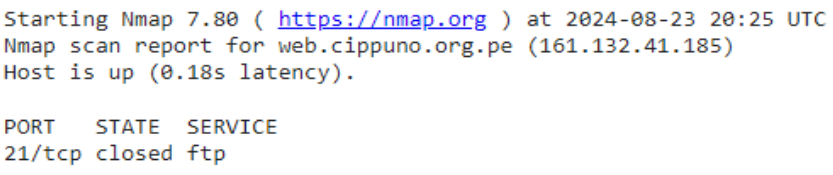
Interpretación

En la Figura 18 se mostró los resultados obtenidos utilizando el comando Head**,** el cual permitió identificar un aspecto relevante: el tipo de servidor que maneja las solicitudes es Apache/2.4.41 (Ubuntu)**.** Esta información fue clave para comprender la infraestructura del sistema y evaluar posibles ajustes o mejoras en la configuración del servidor. Con los datos obtenidos, es posible identificar vulnerabilidades que puedan comprometer el sistema web del Colegio de Ingenieros del Perú, Consejo Departamental Puno. Estos hallazgos son fundamentales para fortalecer la

seguridad, implementar medidas de mitigación y aplicar actualizaciones necesarias, garantizando así un sistema más robusto y protegido contra posibles riesgos futuro.

Figura 19

Comando FTP



Nota: Realizado según Colabority – FTP

Interpretación

La Figura 19 presentó los resultados del escaneo, los cuales indicaron que el puerto 21 (FTP) del servidor web.cippuno.org.pe estuvo cerrado. Esto sugiere que el servicio FTP no está activo en ese puerto o que el servidor está configurado para rechazar conexiones FTP. Por lo tanto, este puerto no representa un factor de vulnerabilidad en el sistema web.

4.4.3.4. OWASP-PG-004 (Test de gestión de configuración)

Estas pruebas aseguran que la aplicación funcione de manera óptima y segura al verificar la correcta implementación y gestión de sus configuraciones. Configurar adecuadamente cada componente de la arquitectura de una aplicación es crucial para prevenir errores que podrían poner en riesgo la seguridad de toda la infraestructura.

Para ello se utilizó a Nikto, esta herramienta es un escáner de vulnerabilidades web que realiza un análisis exhaustivo de los servidores

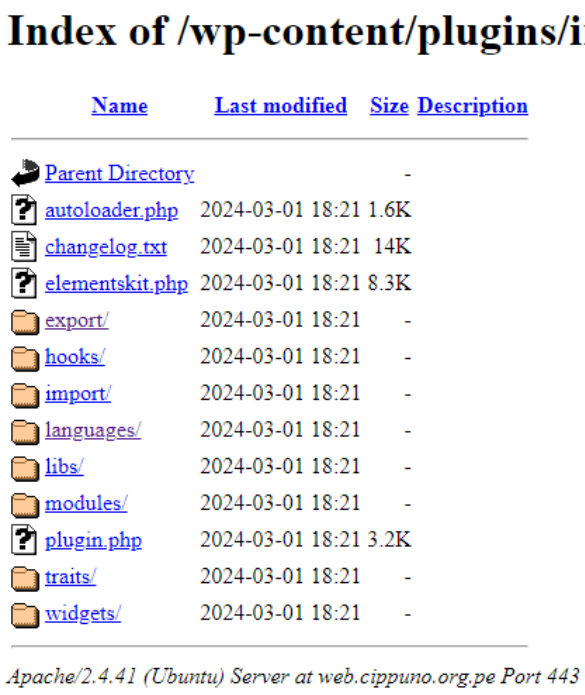
web para identificar posibles problemas de seguridad. Es capaz de detectar configuraciones incorrectas, vulnerabilidades conocidas, archivos peligrosos, scripts vulnerables y versiones desactualizadas de software, entre otros riesgos. Además, Nikto puede analizar múltiples aspectos de la seguridad, como la identificación de directorios y archivos potencialmente inseguros, la presencia de configuraciones incorrectas de cabeceras HTTP, y la verificación de certificados SSL/TLS mal configurados.

- Indexación de directorios

  La indexación de directorios es una función del servidor web que muestra una lista de archivos en un directorio cuando no hay un archivo de índice. Al explorar distintos directorios, se obtuvo respuesta de índices que contienen información sensible.

Figura 20

Indexación de directorios wp-includes del sistema web



Nota: Realizado según wp-content/plugins/import/

Interpretación

En la Figura 20 se mostró la posibilidad de acceder al contenido de un directorio específico, lo que expone información sensible de la instalación, como plugins, temas, lenguajes, archivos multimedia y otros datos críticos. Este acceso no autorizado podría ser aprovechado para recopilar detalles sobre la estructura del sistema, aumentando el riesgo de ataques dirigidos.

Tabla 29

Lista de directorios sensibles y accesibles

Lista de directorios sensibles y accesibles	Descripción	Posibles Consecuencias
/wp-content/uploads/	Almacena archivos multimedia subidos al sitio (imágenes, videos, documentos).	Exposición de archivos sensibles o privados, que pueden ser utilizados para ingeniería social o identificación de vulnerabilidades.
/wp-content/languages/	Contiene archivos de traducción del sitio.	Aunque no suelen ser altamente sensibles, un atacante podría obtener información sobre la configuración del sitio o inyectar archivos maliciosos.
/wp-admin/js/	Almacena scripts JavaScript utilizados en el panel de administración.	Su modificación de estos archivos puede introducir vulnerabilidades de cross-site scripting (XSS), comprometiendo la seguridad del panel de administración
/wp-admin/maint/	Archivos relacionados con el mantenimiento del sitio.	Exposición podría permitir a un atacante interrumpir el mantenimiento o manipular el estado del sitio.

Lista de directorios sensibles y accesibles	Descripción	Posibles Consecuencias
/wp-admin/	Directorio principal del panel de administración de WordPress.	Acceso no autorizado podría comprometer completamente la administración del sitio, permitiendo a los atacantes modificar configuraciones, agregar usuarios, o inyectar código malicioso.
/wp-json/	Punto de entrada para la API REST de WordPress.	Exposición puede revelar datos sensibles a través de la API, como publicaciones, usuarios y configuraciones. Mal configurado, puede permitir a atacantes realizar acciones no autorizadas.
/wp-admin/includes/	Contiene archivos PHP usados para funciones administrativas.	Exponer estos archivos puede permitir a un atacante estudiar y explotar funcionalidades administrativas críticas, comprometiendo la seguridad del sitio.
/wp-content/languages/plugins/	Almacena traducciones para plugins instalados.	Exposición de estos archivos podría revelar información sobre los plugins utilizados, ayudando a un atacante a identificar vulnerabilidades específicas.
/wp-content/languages/themes/	Contiene archivos de traducción para temas instalados.	Podría ayudar a un atacante a obtener información sobre el tema y sus posibles vulnerabilidades.
/wp-includes/	Contiene archivos del núcleo de WordPress que definen la funcionalidad principal del CMS.	Exponer estos archivos puede permitir a los atacantes estudiar el código fuente y descubrir posibles vulnerabilidades.
/wp-includes/certificates/	Almacena certificados de seguridad usados por WordPress.	Si se exponen, podrían comprometer la seguridad SSL del sitio, permitiendo ataques man-in-the-middle.
/wp-includes/fonts/	Contiene fuentes usadas por el tema o plugins.	Poca sensibilidad directa, pero un atacante podría modificar archivos para inyectar código malicioso.

Lista de directorios sensibles y accesibles	Descripción	Posibles Consecuencias
/wp-includes/css/	Almacena hojas de estilo CSS que controlan la apariencia del sitio.	Modificación de estos archivos puede cambiar la apariencia del sitio o ser utilizada para inyectar código malicioso.
/wp-includes/images/	Contiene imágenes usadas por el núcleo de WordPress.	Poca sensibilidad, pero podrían ser reemplazadas con archivos maliciosos.
/wp-admin/css/	Almacena hojas de estilo para el panel de administración.	Su modificación podría afectar la apariencia y usabilidad del panel de administración o inyectar código que robe credenciales de administrador.
/wp-admin/images/	Contiene imágenes usadas en el panel de administración.	Similar al directorio CSS, exposición puede llevar a modificaciones que afecten el panel de administración.
wp-content/plugins/import/libs/	Contiene librerías de plugins de importación en WordPress.	Puede permitir a atacantes obtener archivos sensibles, potencialmente explotando vulnerabilidades o comprometiendo el sitio web.

Nota: Elaboración propia

Interpretación

En la Tabla 29 presentó un resumen de cada uno de los directorios listados y las posibles consecuencias de su exposición. La protección de estos directorios es esencial para prevenir el acceso no autorizado a información o funciones sensibles, lo que podría comprometer la seguridad y el funcionamiento del sitio web. Implementar medidas de control de acceso y restringir la visibilidad de estos directorios reduce significativamente el riesgo de explotación.

4.4.3.5. OWASP-PG-005 (Gestión de extensiones de archivo)

Mediante la herramienta Nikto, se realizó un escaneo de seguridad del sitio web, identificando posibles vulnerabilidades como archivos de configuración que no están protegidos, scripts expuestos y configuraciones de seguridad débiles**.**

Este tipo de análisis es crucial para identificar archivos que puedan contener información sensible, como claves de acceso, configuraciones internas o datos expuestos accidentalmente, los cuales podrían ser aprovechados por atacantes para comprometer la integridad y seguridad del sistema. Además, Nikto es capaz de detectar configuraciones débiles, versiones desactualizadas de software o servicios, y vulnerabilidades conocidas en servidores web. La herramienta también genera reportes detallados que pueden ser utilizados por administradores para priorizar y corregir los problemas detectados. Al ser de código abierto y altamente personalizable, Nikto permite a los equipos de seguridad ajustarse a las necesidades específicas del entorno que están evaluando.

Figura 21

Prueba de extensiones

```
!nikto -h https://web.cippuno.org.pe


- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          161.132.41.185
+ Target Hostname:    web.cippuno.org.pe
+ Target Port:        443
+ Start Time:         2024-08-25 17:09:18 (GMT0)
---------------------------------------------------------------------------
+ Server: Apache/2.4.41 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
```

Nota: Realizado según Nikto

Tabla 30

Búsqueda de extensiones

Extensión	Situación
.txt	No se encontró
.log	No se encontró
.php	No se encontró
.aspx	No se encontró
.html	No se encontró
.config	No se encontró
.zip	No se encontró
.txt	No se encontró
.java	No se encontró
.doc	No se encontró
.pdf	No se encontró
.xls	No se encontró
.ppt	No se encontró
.old	No se encontró

Nota: Realizado según Nikto

Interpretación

En la Tabla 30 se presentó los resultados obtenidos tras realizar un escaneo del sitio web mediante la herramienta Nikto, enfocado en identificar archivos con extensiones específicas que pudieran estar expuestos. Los resultados no revelaron la presencia de archivos con dichas extensiones, lo cual es un indicador positivo en términos de seguridad. Estos hallazgos refuerzan la idea de que el sitio cuenta con un manejo responsable de los archivos almacenados.

4.4.3.6. OWASP-PG-006 (Copias de seguridad y archivos antiguos)

Es común que el servidor gestione los archivos alojados, pero algunos carecen de la documentación adecuada, lo que podría revelar información sensible sobre la infraestructura. Además, que el sistema web presenta versiones desactualizadas de complementos en el código fuente y esto puede exponer vulnerabilidades, facilitando la tarea de identificar fallas o aprovechar puertas traseras de los atacantes. Las copias realizadas pueden crear extensiones no deseadas, que no están relacionadas con los archivos originales.

Algunas recomendaciones es que no se deben de editar archivos directamente en el servidor, ya que los editores pueden generar copias de seguridad visibles para los usuarios. Comprimir archivos en extensiones como .zip o .rar durante los backups es riesgoso y no deben alojarse en el servidor. Una buena gestión de archivos evita referencias o ficheros obsoletos en la aplicación. Se debe configurar la aplicación para evitar la creación de archivos que queden almacenados en el servidor y puedan ser explotados.

4.4.3.7. OWASP-PG-007 (Paneles de control para la gestión de la infraestructura)

Las interfaces de administración del sitio web están diseñadas para asignar privilegios según el tipo de usuario, permitiendo el acceso al panel de administración con funcionalidades específicas basadas en roles y permisos establecidos. Las siguientes pruebas se realizaron para determinar si las funcionalidades con privilegios especiales pueden ser

accesibles para usuarios estándar o no autorizados. Al acceder al directorio /wp-admin/, se nos redirigió al panel de inicio de sesión para usuarios,

Figura 22

Inicio de sesión

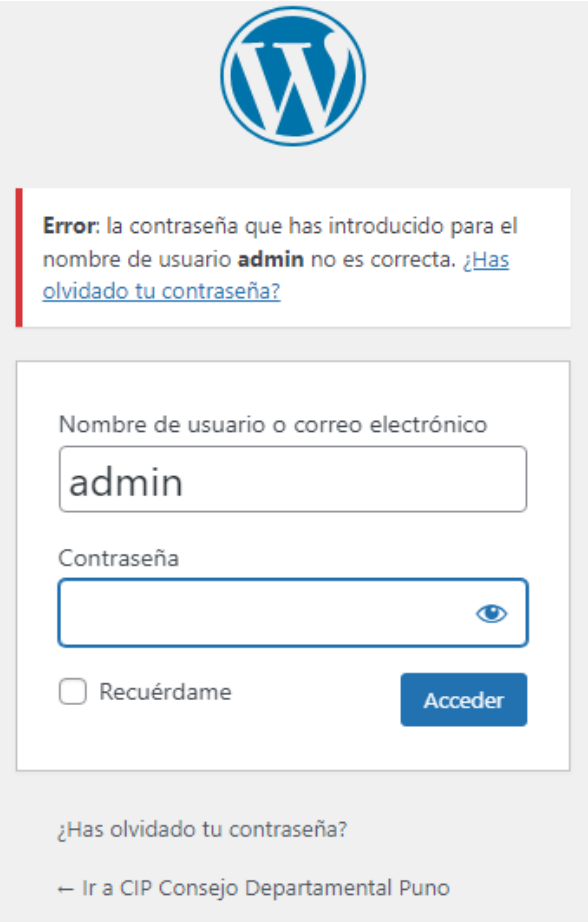
Nota: Adaptado de cippuno.org.pe [Fotografía]

Interpretación

En la Figura 22 se observó que el archivo wp-login.php no estaba desactivado en el sistema web, lo cual pudo representar un riesgo significativo para la seguridad del sitio. La presencia activa de este archivo permite a los atacantes realizar intentos de acceso continuo al panel de administración mediante ataques de fuerza bruta. wp-login.php es el archivo responsable de manejar el inicio de sesión en WordPress, y si no se implementan medidas adecuadas para protegerlo, puede ser explotado por individuos malintencionados que intenten adivinar las credenciales de acceso.

Figura 23

Notificación de error de usuario y contraseña



Nota: Adaptado de cippuno.org.pe [Fotografía]

Interpretación

En la Figura 23 se identificó una vulnerabilidad crítica, en dónde el sistema de inicio de sesión no limita los intentos de acceso e informa si el nombre de usuario o la contraseña son incorrectos con ello nos damos cuenta que también existen 2 usuarios, admin, imagen. Esto permite a los atacantes utilizar herramientas automatizadas para probar múltiples combinaciones de credenciales, aumentando el riesgo de intrusión. La exposición del archivo wp-login.php también facilita ataques de enumeración de usuarios. Para mitigar estos riesgos, es crucial

implementar medidas como limitar los intentos de inicio de sesión, usar autenticación de dos factores y proteger el acceso con firewalls.

- Métodos HTTP soportados en el sistema web

El método HTTP OPTIONS se utiliza para consultar al servidor sobre los métodos HTTP permitidos para un recurso, ayudando a identificar las operaciones posibles antes de realizar una solicitud específica. Aunque es útil para verificar las capacidades del servidor, también puede revelar información que los atacantes podrían aprovechar durante una fase de reconocimiento.

Por ello, conocer y configurar adecuadamente los métodos soportados en el sistema web del Colegio de Ingenieros del Perú, Consejo Departamental Puno, es esencial para prevenir manipulaciones no deseadas y garantizar la seguridad del sistema.

Figura 24

Métodos HTTP soportados en el servido

```
!nmap --script http-methods web.cippuno.org.pe


Starting Nmap 7.80 ( https://nmap.org ) at 2024-08-25 19:20 UTC
Nmap scan report for web.cippuno.org.pe (161.132.41.185)
Host is up (0.28s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
443/tcp open  https
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS

Nmap done: 1 IP address (1 host up) scanned in 30.38 seconds
```

Nota: Adaptado de cippuno.org.pe por colab

Interpretación

En la Figura 24 el escaneo realizado con Nmap al sitio web.cippuno.org.pe (IP 161.132.41.185) muestra que los puertos esenciales están configurados y operativos: el puerto 22/tcp (SSH) está abierto, permitiendo acceso remoto para la administración del servidor; el puerto 80/tcp (HTTP) está habilitado para la navegación web mediante métodos como GET, HEAD, POST y OPTIONS; y el puerto 443/tcp (HTTPS) está operativo, garantizando conexiones seguras con los mismos métodos. La mayoría de los demás puertos están cerrados, lo que refuerza la seguridad al limitar puntos de entrada no necesarios.

4.4.4. Comprobación del Sistema de Autenticación

Se refiere al proceso de evaluar y verificar la efectividad y seguridad del sistema de autenticación de un sitio web o aplicación. Este sistema es responsable de validar las credenciales (como nombre de usuario y contraseña) de los usuarios que intentan acceder a la plataforma. Cuyo objetivo es asegurar de que solo los usuarios autorizados puedan acceder a las áreas protegidas de la aplicación, prevenir accesos no autorizados y proteger la integridad de la información sensible.

El proceso de evaluación de seguridad en los sistemas web abarca una amplia variedad de pruebas diseñadas para garantizar la protección de los datos y la infraestructura del sistema. Entre estas pruebas se incluyen evaluaciones de resistencia a ataques de fuerza bruta, que buscan determinar si un atacante puede acceder al sistema probando combinaciones de contraseñas de manera masiva.

4.4.4.1. OWASP-ID-001 (Envío de credenciales mediante un canal seguro y cifrado)

Figura 25

Transmisión por el canal cifrado con HTTP

Nota: Adaptado de cippuno.org.pe

Interpretación

En la Figura 25 se verificó que las credenciales de usuario se transmiten a través de un canal cifrado para evitar interceptaciones por parte de usuarios no autorizados. El análisis confirmó que el sitio web cippuno.org.pe implementa mecanismos de seguridad adecuados.

4.4.4.2. OWASP-ID-002 (Enumeración de usuarios)

Ocurre cuando un atacante puede identificar si un nombre de usuario es válido en un sistema, debido a las diferencias en las respuestas de autenticación. Esto puede facilitar ataques como fuerza bruta. OWASP recomienda usar respuestas genéricas y limitar intentos de inicio de sesión para mitigar esta vulnerabilidad. Al realizar múltiples pruebas en el sistema, es posible identificar una lista de usuarios, lo que podría facilitar un ataque de fuerza bruta.

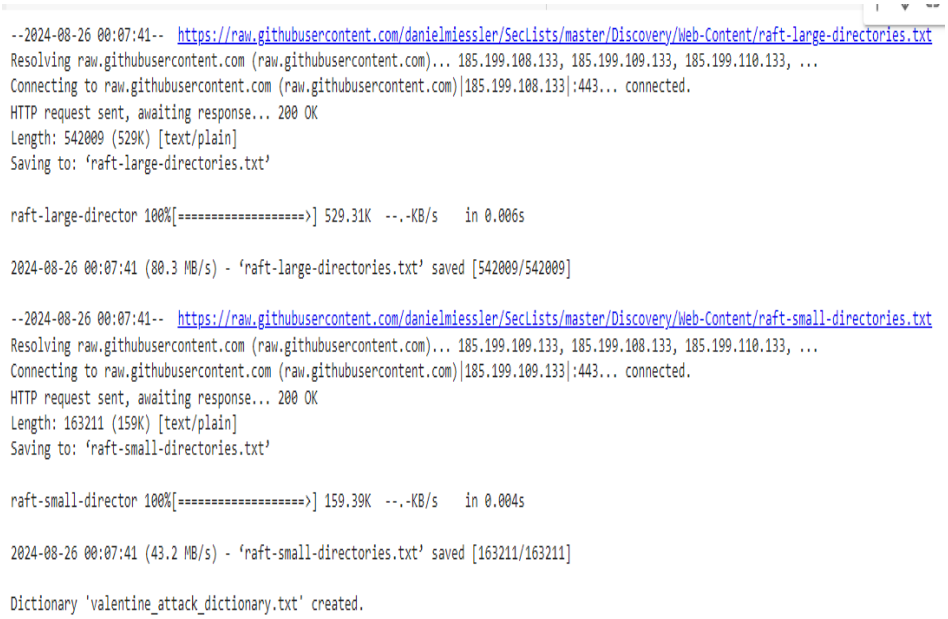
Esta información es exclusiva del administrador de la página y no puede ser proporcionada para evitar filtraciones; por lo tanto, no se puede realizar esta prueba.

4.4.4.3. OWASP-ID-003 (Pruebas de diccionario)

Se utilizan las pruebas de diccionario para intentar adivinar contraseñas al probar una lista extensa de combinaciones de palabras comunes, contraseñas conocidas o patrones predefinidos. Esto ayuda a identificar si las contraseñas de un sistema son lo suficientemente fuertes o si son vulnerables a ataques de fuerza bruta, donde se explotan contraseñas débiles o previsibles. Teniendo en cuenta la vulnerabilidad de la Figura 23, se usará para realizar a valentine_atack_diccionario.sh este es un diccionario de ataque creado o descargado con el objetivo de realizar un escaneo de directorios o un ataque de fuerza bruta en un sitio web.

Figura 26

Valentine_attack_dictionary.txt



```
--2024-08-26 00:07:41--  https://raw.githubusercontent.com/danielmiessler/SecLists/master/Discovery/Web-Content/raft-large-directories.txt
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.108.133, 185.199.109.133, 185.199.110.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.108.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 542009 (529K) [text/plain]
Saving to: 'raft-large-directories.txt'

raft-large-director 100%[===================>] 529.31K  --.-KB/s    in 0.006s

2024-08-26 00:07:41 (80.3 MB/s) - 'raft-large-directories.txt' saved [542009/542009]

--2024-08-26 00:07:41--  https://raw.githubusercontent.com/danielmiessler/SecLists/master/Discovery/Web-Content/raft-small-directories.txt
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.109.133, 185.199.108.133, 185.199.110.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.109.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 163211 (159K) [text/plain]
Saving to: 'raft-small-directories.txt'

raft-small-director 100%[===================>] 159.39K  --.-KB/s    in 0.004s

2024-08-26 00:07:41 (43.2 MB/s) - 'raft-small-directories.txt' saved [163211/163211]

Dictionary 'valentine_attack_dictionary.txt' created.
```

Nota: Adaptado de valentine_attack_dictionary.txt

Interpretación

En la Figura 26 se muestra que se descargaron con éxito dos archivos de diccionario del repositorio SecLists en GitHub: raft-large-directories.txt *y* raft-small-directories.txt, los cuales contenían listas de posibles directorios comunes para tareas de escaneo. Además, se creó un diccionario personalizado llamado valentine_attack_dictionary.txt para realizar pruebas de fuerza al sitio web del Colegio de Ingenieros del Perú, Consejo Departamental Puno. Por otro lado, en la Figura 27 se evidenció que durante una auditoría de seguridad se identificó cgi-bin como una posible contraseña válida, y el proceso de descifrado concluyó con este hallazgo. Esto reveló un posible riesgo en el sistema que requería atención inmediata para reforzar la seguridad.

Figura 27

Prueba de diccionario

```
    response = requests.post(target_url, data=data)

    if "Invalid username or password" not in response.text:
      print(f"Possible password found: {password}")
      break  # Detenerse si se encuentra una contraseña válida

print("Password cracking finished.")


Possible password found: cgi-bin
Password cracking finished.
```

Nota: Adaptado de valentine_attack_dictionary.txt

4.4.4.4. OWASP-ID-004 (Pruebas de Fuerza Bruta)

El ataque de fuerza bruta es una técnica conocida que busca acceder a un sistema con el fin de explotarlo o extraer información valiosa. Este

ataque se basa en intentar todas las combinaciones posibles hasta lograr el acceso deseado.

En el contexto de una aplicación web, es crucial identificar una cuenta válida en el sistema y luego probar diferentes contraseñas hasta lograr la entrada. El ataque de fuerza bruta es un método en el que un atacante prueba todas las combinaciones posibles de contraseñas hasta encontrar la correcta. Existen varios tipos, como el ataque de diccionario, el ataque híbrido y el relleno de credenciales, entre otros.

Las consecuencias pueden incluir acceso no autorizado, interrupciones del servicio y compromiso de múltiples cuentas. Para protegerse, es crucial usar contraseñas fuertes, implementar autenticación multifactorial, limitar intentos de inicio de sesión, usar CAPTCHAs y monitorear la actividad de inicio de sesión. Para esta prueba no se tuvo la autorización, ya que podría impactar el rendimiento de la página y afectar el servicio a los usuarios.

4.4.4.5. OWASP-ID-005 (Eludir el sistema de autenticación)

Eludir el sistema de autenticación significa evitar o superar los mecanismos de seguridad diseñados para verificar la identidad de los usuarios. Esto se puede lograr mediante técnicas como el uso de credenciales robadas, explotación de vulnerabilidades en el sistema, o aprovechamiento de debilidades en el proceso de autenticación. El objetivo es obtener acceso no autorizado al sistema web, aplicaciones o datos protegidos. Para esta prueba no se tuvo la autorización, ya que podría impactar el rendimiento del sistema web.

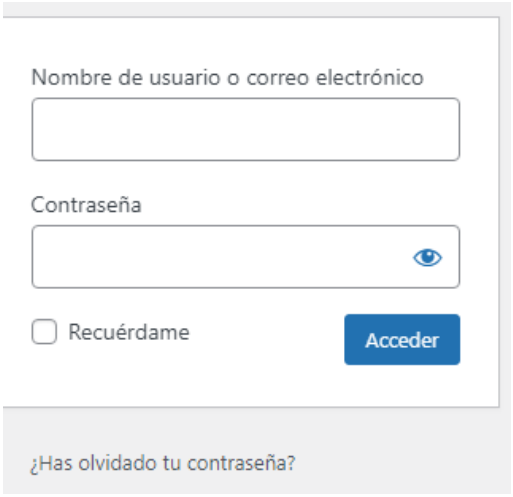
4.4.4.6. OWASP-ID-006 (Verificar sistemas de recuperación o restauración de contraseñas que presenten vulnerabilidades)

Comprobar sistemas de recordatorio o restauración de contraseñas vulnerables implica evaluar si los mecanismos utilizados para recuperar o restablecer contraseñas en una aplicación o sistema tienen fallos de seguridad que puedan ser explotados. Estos sistemas son esenciales para garantizar que los usuarios puedan recuperar el acceso a sus cuentas en caso de olvidar sus contraseñas, pero su diseño y configuración deben ser robustos para evitar riesgos.

Las vulnerabilidades comunes incluyen la falta de validación adecuada de identidad, el envío de enlaces de restablecimiento sin cifrado, la reutilización de tokens de restablecimiento, o preguntas de seguridad débiles o predecibles. Si un atacante logra explotar estas debilidades, podría obtener acceso no autorizado a cuentas sensibles, comprometiendo la seguridad de los datos almacenados en el sistema web.

Figura 28

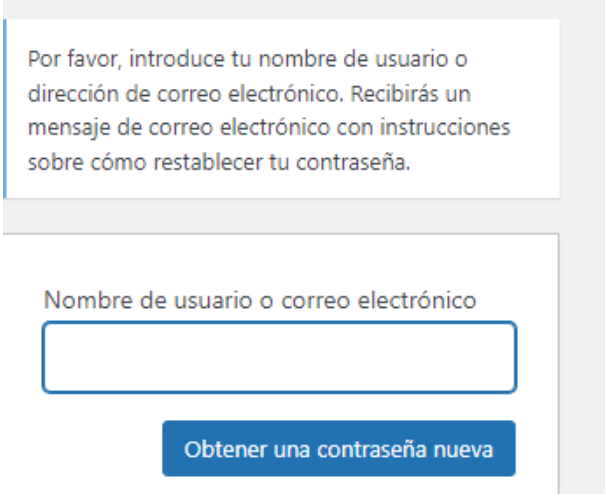
Restauración de contraseñas vulnerables



Nota: Adaptado de cippuno.org.pe

Figura 29

Recuperación de usuario o dirección de correo electrónico



Nota: Adaptado de cippuno.org.pe

Interpretación

En la Figura 28 y Figura 29 se observaron el proceso de restablecimiento de contraseñas, el cual funciona de la siguiente manera: el usuario solicita el restablecimiento, el sistema pide la dirección de correo electrónico registrada, y luego envía un correo al usuario. Este correo contiene un enlace que dirige a un formulario para ingresar una nueva contraseña. Al momento que la aplicación web recibe la petición del restablecimiento se muestra un formulario que solicita el correo electrónico registrado, también es posible retroceder el proceso si se recordó la contraseña tal como se puede observar. El sistema permitió contraseñas con requisitos de seguridad mínimos. Dado el nivel de seguridad necesario para la página, las contraseñas deberían cumplir con requisitos más estrictos. Además, el usuario debería responder preguntas de seguridad o verificar su identidad mediante un método adicional para completar la solicitud.

4.4.4.7. OWASP-ID-007 (Evaluación de la gestión del caché del navegador y cierre de sesión)

La gestión del caché del navegador y el cierre de sesión son elementos críticos para la seguridad de las aplicaciones web, especialmente cuando manejan información sensible. Una mala configuración del caché puede exponer datos confidenciales almacenados temporalmente, como páginas privadas o tokens de autenticación, lo que podría ser aprovechado por atacantes.

- Caché del Navegador: Las aplicaciones web deben manejar correctamente la configuración del caché para evitar la exposición no autorizada de datos sensibles. Esto incluye verificar que las páginas que contienen información confidencial no se almacenan en el caché del navegador, lo que podría permitir a un usuario posterior acceder a información que no le pertenece.

- Salida de Sesión: Este es el proceso de cierre de sesión debe eliminar completamente todas las credenciales de la sesión activa y cualquier información de sesión almacenada en el navegador. Esto asegura que, después de cerrar sesión, el usuario no pueda acceder a áreas protegidas sin volver a autenticar su identidad. Las pruebas deben verificar que la sesión se invalida de manera efectiva y que el navegador no almacene datos de sesión que puedan ser reutilizados por otros usuarios. Para llevar a cabo pruebas al sitio web analizado, se utilizó un plugin llamado EditThisCookie el cual permite visualizar todas las cookies

asociadas a una sesión específica y el valor de cada una de ellas. También se hizo uso de la herramienta ofrecida en el navegador Google Chrome Colab.

Para evaluar la gestión del caché y el cierre de sesión, se deben realizar pruebas que verifiquen que las respuestas HTTP deshabilitan adecuadamente el almacenamiento en caché y que el contenido privado no es accesible después del cierre de sesión. Estas medidas fortalecen la seguridad del sistema y protegen la privacidad del usuario.

Figura 30

Cookies almacenadas del sitio web

```
import requests

url = 'https://web.cippuno.org.pe/'
response = requests.get(url)
cookies = response.cookies

print(cookies)
```

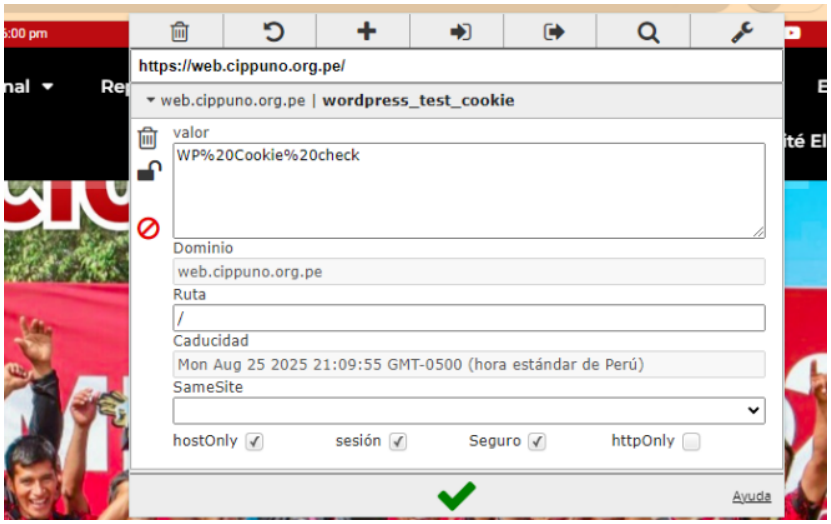
Nota: Adaptado de cippuno.org.pe por Colab

Interpretación

En la Figura 30 se observó el código que permitió enviar una solicitud GET al sitio web especificado y luego imprimió las cookies que se almacenan en la respuesta. Como resultado se observa <RequestsCookieJar[]>, lo que significa que actualmente no hay cookies almacenadas en el contenedor ([] indica que está vacío). Este objeto es útil para gestionar cookies, permitiendo su almacenamiento, recuperación y manipulación entre las diferentes solicitudes que realiza un script o aplicación web.

Figura 31

Cookies custon data username



Nota: Adaptado de EditThisCookie

Interpretación

En la Figura 31 se observó varios aspectos como la fecha de caducidad de la cookie es para el año 2025 mediante la evaluación de EditThisCookie tiene una fecha de caducidad establecida en el futuro distante, lo cual permanecerá en el navegador del usuario por un período más largo, manteniendo la sesión o configuraciones a través de múltiples visitas al sitio web. Esto puede ser útil para recordar las preferencias del usuario, pero también puede presentar riesgos de seguridad si las cookies almacenan información sensible y no se manejan adecuadamente.

4.4.4.8. OWASP-ID-008 (Pruebas de CAPTCHA)

Un CAPTCHA como mecanismo de seguridad distingue humanos y bots automatizados en sitios web. Funciona presentando desafíos, como identificar letras distorsionadas o seleccionar imágenes, que son fáciles para los humanos pero difíciles para los bots. Su objetivo es evitar que los

bots realicen acciones maliciosas, como crear cuentas falsas o lanzar ataques automatizados, protegiendo así la seguridad del sitio web. Las pruebas de CAPTCHA son cruciales para asegurar que una aplicación web está protegida contra una variedad de ataques automatizados, mientras se mantiene una buena experiencia de usuario y accesibilidad para todos los usuarios. Estas pruebas forman parte de un enfoque de seguridad integral para proteger aplicaciones web contra el abuso automatizado y son recomendadas por OWASP en su guía de seguridad.

Para la presente prueba en el sistema web cippuno.org.pe carece de un sistema de CAPTCHA para el registro de nuevos usuarios, realización de consultas de colegiados, recuperación de contraseñas, entre otros, lo que permite el registro y uso indiscriminado de cuentas en el sitio.

Sin un sistema CAPTCHA, el sitio web es vulnerable a la creación masiva de cuentas falsas por bots, lo que puede llevar a abusos como spam o sobrecarga de recursos. También es susceptible a ataques de fuerza bruta, facilitando intentos masivos de acceso no autorizado. Además, el sitio corre el riesgo de sufrir ataques de denegación de servicio (DoS), que pueden sobrecargar el servidor y hacerlo inaccesible, y a la sustracción de datos automatizada, permitiendo la extracción de información sensible.

4.4.4.9. OWASP-ID-009 (Test para verificar la autenticación de factores múltiples)

Evaluar la solidez de un sistema de autenticación es esencial, ya que se trata de una etapa delicada que está directamente relacionada con la protección de información sensible de los usuarios. El objetivo de estas

pruebas es verificar factores adicionales que aseguren que el usuario tenga dispositivo de acceso físico además de la contraseña pero por la delicadeza del manejo de información no se realizó pero se presenta algunas de las amenazas más comunes, las cuales son:

- Phishing: Engaño para revelar credenciales a través de correos o sitios falsos.
- Robo de Contraseñas: Obtención de contraseñas mediante fuerza bruta o captura en tránsito.
- Ingeniería Social: Manipulación para obtener información de acceso.
- Ataques de Fuerza Bruta: Probar todas las combinaciones posibles de contraseñas.
- Uso de Contraseñas Débiles: Contraseñas simples o predecibles.
- Secuestro de Sesiones: Uso no autorizado de cookies o tokens de sesión.
- Exposición de Credenciales en Texto Plano: Credenciales transmitidas sin cifrar.
- Explotación de Vulnerabilidades: Aprovechamiento de fallos en el software de autenticación.

4.4.4.10. OWASP-ID-010 (Prueba de situaciones adversas)

Se refiere a evaluar cómo el sistema maneja condiciones inesperadas o erróneas, como entradas inválidas, falta de recursos, o interrupciones en la red. El objetivo es identificar vulnerabilidades que podrían ser explotadas durante estas situaciones, asegurando que el

sistema se comporte de manera segura y controlada, incluso bajo circunstancias adversas.

Al realizar múltiples acciones sobre un mismo elemento en una aplicación web, es crucial que los cambios se reflejen de inmediato. Si las modificaciones no se actualizan al instante, el funcionamiento de la aplicación podría verse afectado, lo que podría generar resultados inesperados y problemas en el rendimiento del sistema web.

Para esta prueba no se realizó porque no hubo una autorización para realizarla ya que podría afectar el servicio del sistema para los usuarios.

4.4.5. Pruebas de Validación de Datos

Las aplicaciones web están constantemente expuestas a nuevas amenazas creadas por individuos malintencionados que buscan explotar la información confidencial proporcionada por los clientes a las empresas. Sin embargo, una amenaza aún más peligrosa proviene de la información que los usuarios introducen y la que el sistema genera a través de procesos implementados por los desarrolladores.

Esta información, que puede ser utilizada por otros procesos o mostrada a los usuarios durante interacciones con el sistema, es especialmente vulnerable si no se gestiona adecuadamente.

Si no se implementan medidas de seguridad adecuadas, esta información podría ser manipulada, expuesta a accesos no autorizados o utilizada para realizar ataques comprometiendo la integridad, confidencialidad y disponibilidad del sistema web.

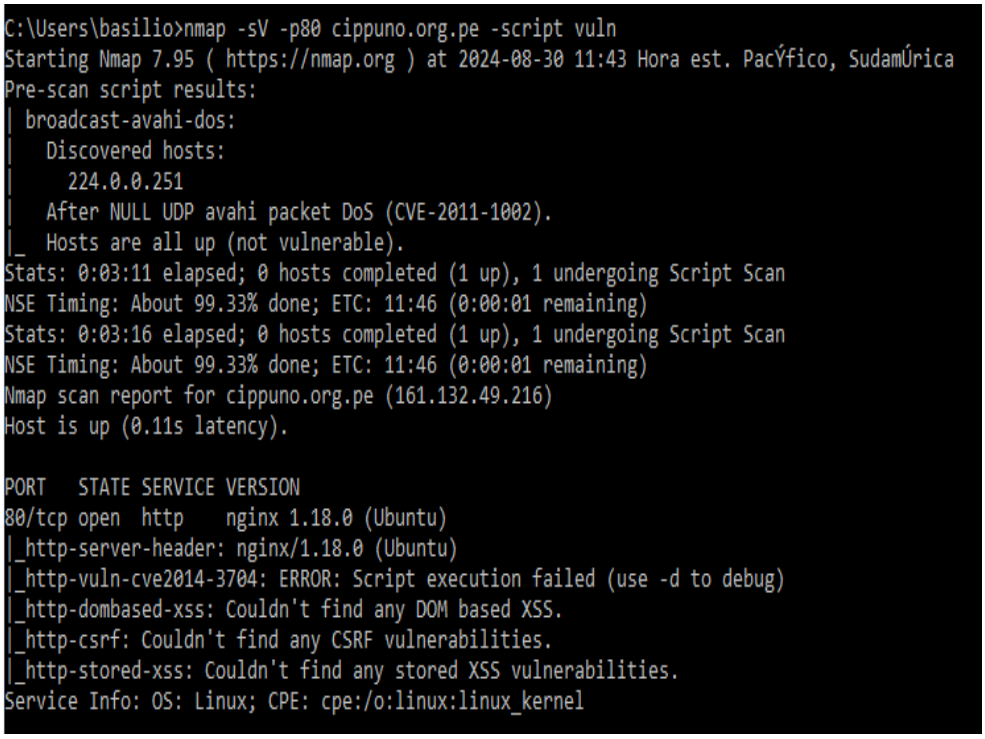
Además, la falta de validación de datos puede facilitar ataques como la inyección de código malicioso, lo que podría derivar en la explotación de vulnerabilidades críticas en la aplicación.

- **Análisis XSS. Cross Site Scripting**

En los resultados no se encontraron explícitamente vulnerabilidades de Cross-Site Scripting (XSS). Sin embargo, tras realizar un escaneo de vulnerabilidades mediante WPScan, se logró identificar varias características y configuraciones del sistema web. Estos hallazgos incluyeron la presencia de plugins, archivos sensibles y configuraciones específicas, esta información obtenida es crucial para evaluar el estado de seguridad del sistema y tomar medidas preventivas frente a posibles riesgos.

Figura 32

Prueba de vulnerabilidades (XSS, CSRF)



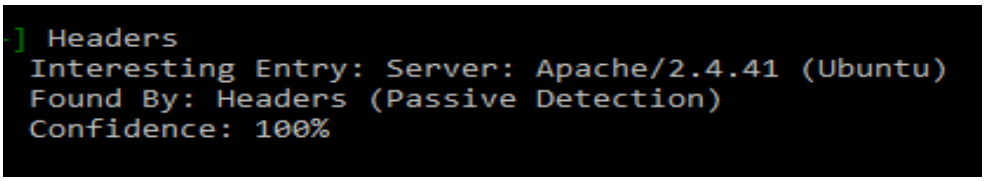
Nota: Adaptado de WPScan

Interpretación

En la Figura 32 se observó el escaneo que indicó que el servidor web cippuno.org.pe tiene configuraciones de seguridad razonables, con varias pruebas comunes de vulnerabilidades que no detectaron problemas significativos (XSS, CSRF). Sin embargo, hay un error en la prueba para la vulnerabilidad CVE-2014-3704, lo que sugiere la necesidad de realizar una evaluación más detallada para confirmar la ausencia de esta vulnerabilidad. En general, el servidor parece estar bien protegido, pero siempre es recomendable continuar con evaluaciones periódicas y mantener actualizado el software del servidor para asegurar la protección contra nuevas vulnerabilidades.

Figura 33

Headers



Nota: Adaptado de WPScan

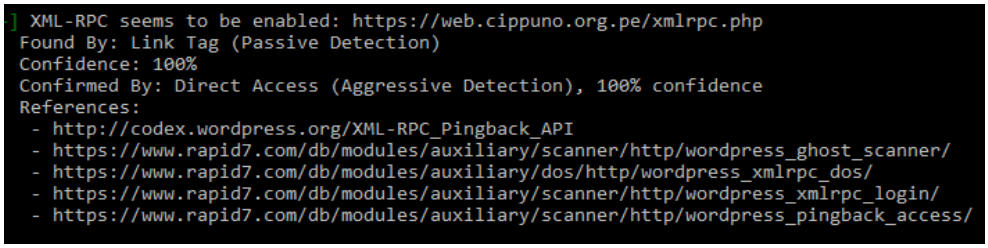
Interpretación

En la Figura 33 se observó un encabezado el cual indica que el sitio web usa el servidor Apache/2.4.41 en Ubuntu. Esta versión de Apache es de 2019, por lo que podría tener vulnerabilidades si no se han aplicado parches recientes.

Es recomendable actualizar Apache, revisar las configuraciones de seguridad y realizar auditorías periódicas para proteger el servidor.

Figura 34

XML-RPC seems to be enabled



Nota: Adaptado de WPScan

Interpretación

En la Figura 34 se observa que el XML-RPC está habilitado en el sitio web, lo que puede ser un riesgo de seguridad. Es una funcionalidad que permite la interacción remota, pero también es un objetivo común para ataques como fuerza bruta o DoS. Si no es necesaria, se recomienda desactivarla.

Figura 35

Robots, txt found

Nota: Adaptado de WPScan

Interpretación

En la Figura 35 se encontró el archivo robots.txt del sitio web este contiene entradas que indican restricciones para el acceso a las áreas /wp-admin/ y /wp-admin/admin-ajax.php. Esta entrada en robots.txt indicó que esos directorios no debían ser rastreados o indexados por los motores de búsqueda. Sin embargo, sigue siendo accesible públicamente, lo que significa

que cualquier persona que conozca esta ruta puede intentar acceder a ella directamente, aunque no esté indexada por los motores de búsqueda.

Figura 36

WordPress readme found

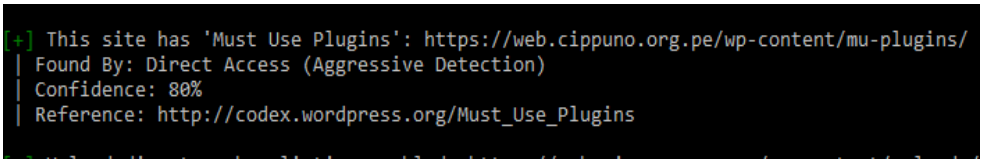
Nota: Adaptado de WPScan

Interpretación

En la Figura 36 se encontró el archivo readme.html de WordPress en el sitio, este archivo generalmente contiene información sobre la versión de WordPress instalada y puede ser utilizado por atacantes para identificar vulnerabilidades específicas relacionadas con esa versión.

Figura 37

Must use plugin



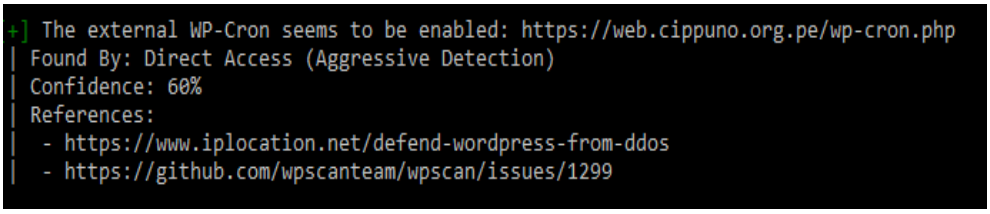
Nota: Adaptado de WPScan

Interpretación

En la Figura 37 se observó que el sitio tiene activados Must Use Plugins (plugins obligatorios), estos son plugins instalados automáticamente por el administrador de WordPress y no pueden ser desactivados por usuarios normales. Esto podría implicar que hay plugins que son esenciales para el funcionamiento del sitio y no pueden ser manipulados fácilmente.

Figura 38

The external WP-Cron to be enabled



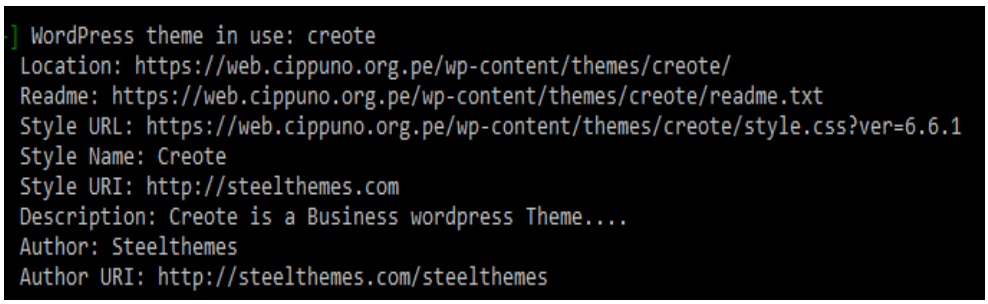
Nota: Adaptado de WPScan

Interpretación

En la Figura 38 se observó que el sitio tuvo habilitado el WP-Cron externo, lo cual es un sistema de tareas programadas en WordPress. Sin embargo, dado que la detección tiene una confianza del 60%, no es completamente seguro. Tener WP-Cron habilitado puede ser un riesgo si no se gestiona correctamente, ya que puede ser explotado en ataques DDoS está bien protegido.

Figura 39

WordPress theme in use



Nota: Adaptado de WPScan

Interpretación

En la Figura 39 se observa el tema de WordPress y se está utilizando en el sitio es Creote, un tema de negocios desarrollado por Steelthemes, incluyendo su nombre, descripción y el enlace al autor donde se puede encontrar en los archivos CSS y readme.txt del tema.

Figura 40

Upload directory has listing enable

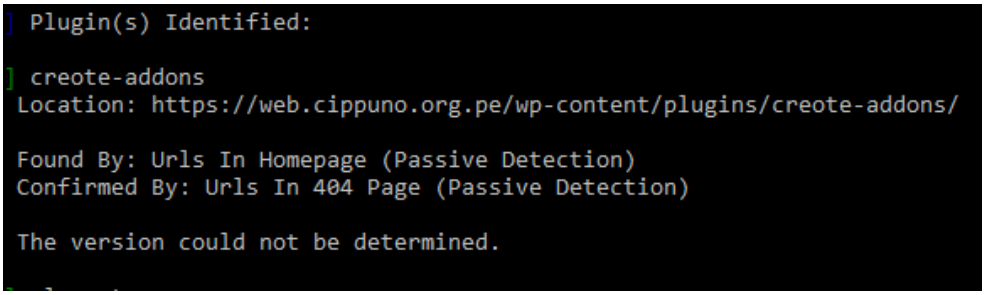
Nota: Adaptado de WPScan

Interpretación

En la Figura 40 se observó el directorio de subida de archivos en el sitio web, esta contiene la lista de directorios habilitada**.** Esto significa que cualquier persona puede ver y acceder a los archivos que han sido subidos a este directorio, lo cual puede ser un riesgo de seguridad para la institución, si los archivos no están protegidos adecuadamente podría ser explotada por personas malintencionadas.

Figura 41

Plugin(s)



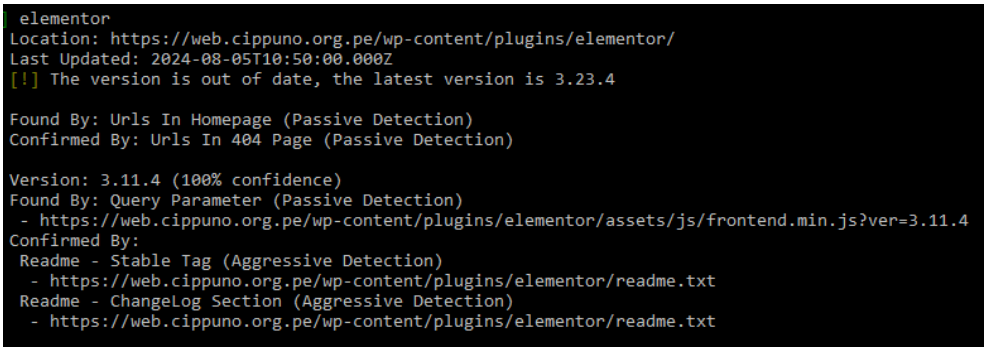
Nota: Adaptado de WPScan

Interpretación

En la Figura 41 se encontró la presencia del plugin creote-addons en el sitio, pero sin determinar la versión específica de este. Esto podría ser útil si se realiza una auditoría de seguridad o un análisis de los componentes del sitio.

Figura 42

Elementor



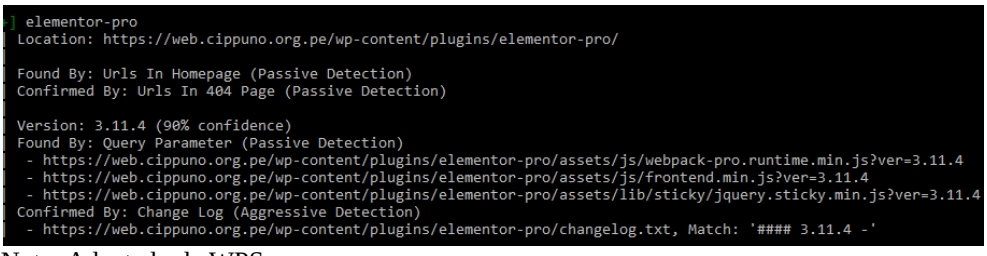
Nota: Adaptado de WPScan

Interpretación

En la Figura 42 se identificó el plugin Elementor Pro del sitio web https://web.cippuno.org.pe, por el método de detección pasiva, esta especifica que se encontraron varias URLs relacionadas con el plugin en la página de inicio y en la página 404 del sitio web mientras que por el la detección agresiva se realizó la confirmación mediante el análisis de un archivo de registro de cambios (changelog.txt) que se encontró en el mismo sitio web. La versión del plugin ha sido identificada como 3.11.4 con un 90% de confianza. En cuanto a la detección pasiva se hizo coincidir las URLs de los archivos JavaScript con parámetros de versión que apuntan a la versión 3.11.4, dicha versión también fue confirmada por el análisis del changelog.

Figura 43

Elementor Pro



Nota: Adaptado de WPScan

Interpretación

En la Figura 43 se observó el plugin Elementor Pro versión 3.11.4, se identificó en https://web.cippuno.org.pe. La detección pasiva incluyó URLs en la página de inicio y en la página 404, mientras que la detección agresiva se basó en el changelog del plugin.

- Inyección SQL

Una inyección SQL es un tipo de vulnerabilidad de seguridad en aplicaciones web donde un atacante puede incrustar comandos SQL maliciosos en una base de datos a través de una entrada no validada o controlada por el usuario.

Esta vulnerabilidad ocurre cuando una aplicación web incluye datos proporcionados por el usuario en una consulta SQL sin una validación o filtrado adecuado pero de acuerdo al escaneo que se realizó no se encontró ninguna vulnerabilidad con referente a ellas es por ello que no se ejecutó ninguna prueba.

Es importante conocer que si se realizan los ataques pueden permitir al atacante realizar acciones no autorizadas, como leer, modificar o eliminar datos, y en algunos casos, tomar control total del servidor de base de datos. Existen 3 tipos.

- Inyección SQL Clásica: Inserción de código SQL directamente en la consulta.
- Inyección SQL Basada en Tiempo: El atacante usa técnicas para inducir retrasos en la respuesta del servidor como indicador de la vulnerabilidad.

- Inyección SQL Ciega: El atacante no recibe los resultados de la consulta, pero puede inferir información mediante la respuesta de la aplicación a las consultas.

Desde la Figura 32 hasta Figura 43 se observó la información detallada del escaneo mediante WPScan, no se proporcionó un token de API de WPScan, lo que significa que la información sobre vulnerabilidades específicas no se incluyó en el escaneo.

Para obtener datos sobre vulnerabilidades, se necesitaría realizar otro escaneo proporcionando un token de API, la cual permitiría a WPScan comparar las versiones de plugins, temas, y WordPress con su base de datos de vulnerabilidades conocidas pero no hubo autorización para realizarlas. En conclusión no se han detectado vulnerabilidades explícitas, pero se han identificado varios puntos de interés que podrían requerir una evaluación adicional, especialmente si se proporcionan más detalles mediante el uso de un token de API, los cuales se detallan a continuación:

- Plugins Desactualizados: Elementor y Elementor Pro están desactualizados, dado que las versiones antiguas de estos plugins son conocidas por tener vulnerabilidades, algunas de las cuales podrían incluir XSS. Otros plugins desactualizados como Essential Addons for Elementor Lite, Popup Builder, y Revolution Slider también pueden ser susceptibles a vulnerabilidades XSS si no se actualizan.
- Directorio de Subidas Accesible: El directorio de subidas (/wp-content/uploads/) tiene la listado habilitado. Esto podría ser aprovechado

para inyectar scripts maliciosos en archivos subidos, lo que podría ser una fuente de ataques XSS.

- XML-RPC Habilitado: Aunque no es directamente relacionado con XSS, tener el XML-RPC habilitado pudo aumentar la superficie de ataque, permitiendo a los atacantes explotar otras vulnerabilidades que pudieron incluir XSS. XML-RPC es un protocolo que permite a los sistemas externos interactuar con un servidor web a través de solicitudes remotas, como la publicación de contenido o la ejecución de comandos. Si bien este servicio puede ser útil para aplicaciones como WordPress, donde facilita interacciones como la publicación remota y la gestión de contenidos, también introduce riesgos si no está debidamente protegido.

4.4.6. Evaluación de riesgos

Luego de realizarse las pruebas basadas en OWASP se obtuvieron datos valiosos que permitieron una evaluación detallada de las vulnerabilidades presentes en el sistema web del CIP-Puno. Esta evaluación de riesgos constituyó una parte fundamental de la gestión de la seguridad, ya que identificó puntos críticos que podrían ser explotados por atacantes. La aplicación de estas medidas fue clave para garantizar la integridad, confidencialidad y disponibilidad de la información gestionada por la organización. Asimismo, los resultados obtenidos sirvieron como punto de partida para diseñar protocolos de seguridad más robustos, orientados a la prevención de ataques futuros y la mitigación de riesgos. Este enfoque proactivo fortaleció significativamente la capacidad de respuesta frente a incidentes, consolidando una infraestructura más segura y resiliente frente a las amenazas emergentes.

Tabla 31

Evaluación de riesgos en base a OWASP

Número de Referencia	Nombre de prueba	Vulnerabilidades encontradas	Efectuada / No efectuada
OWASP-RI-001	Robots, Spiders y Crawlers.	N.A	SI
OWASP-RI-002	Reconocimiento mediante motores de búsqueda.	N.A	SI
OWASP-RI-003	Reconocer los puntos de entrada de la aplicación.	N.A	SI
OWASP-RI-004	Test de firma digital para aplicaciones web.	N.A	SI
OWASP-RI-005	Descubrimiento de aplicaciones.	N.A	SI
OWASP-RI-006	Analizar Códigos de Errores.	N.A	SI
OWASP-PG-001	Test de SSL/TLS.	N.A	SI
OWASP-PG-002	Test de receptor de escucha de la BD.	N.A	SI
OWASP-PG-003	Test de gestión de configuración de la infraestructura.	N.A	SI
OWASP-PG-004	Test de gestión de configuraciones.	N.A	SI
OWASP-PG-005	Gestión de extensiones de archivo.	Directorios expuestos	SI
OWASP-PG-006	Copias de seguridad y archivos antiguos.	N.A	SI
OWASP-PG-007	Paneles de control para la gestión de la infraestructura.	wp-login.php no está desactivado (vulnerabilidad crítica), En cuanto al inicio de sesión no limita los intentos de acceso e informa si el nombre de usuario o la contraseña son incorrectos.	SI
OWASP-ID-001	Envío de credenciales mediante un canal seguro y cifrado.	N.A	SI
OWASP-ID-002	Enumeración de usuarios.	N.A	NO

Número de Referencia	Nombre de prueba	Vulnerabilidades encontradas	Efectuada / No efectuada
OWASP-ID-003	Pruebas de diccionario.	Vulnerabilidad crítica mediante ataques de diccionario	SI
OWASP-ID-004	Pruebas de fuerza bruta.	N.A	NO
OWASP-ID-005	Eludir el sistema de autenticación.	N.A	NO
OWASP-ID-006	Verificar sistemas de recuperación o restauración de contraseñas que presenten vulnerabilidades.	Restauración de contraseñas vulnerable, fallo de WordPress y el sistema permite contraseñas con requisitos de seguridad mínimos.	SI
OWASP-ID-007	Evaluación de la gestión del caché del navegador y del proceso de cierre de sesión.	Fecha de caducidad de la cookie es para el año 2025 podría presentar un riesgo.	SI
OWASP-ID-008	Pruebas de CAPTCHA.	El sistema web cippuno.org.pe carece de un sistema de CAPTCHA	NO
OWASP-ID-009	Test para autenticación de factores múltiples.	N.A	NO
OWASP-ID-010	Prueba de situaciones adversas.	N.A	NO
OWASP-PA-001	Prueba de XSS Reflejado.	N.A	SI
OWASP-PA-002	Prueba de XSS Almacenado.	N.A	SI
OWASP-PA-003	Prueba de XSS basado en DOM.	N.A	SI
OWASP-PA-004	Prueba de XSS basado en Flash.	N.A	SI
OWASP-PA-005	Inyección SQL.	N.A	NO
OWASP-PA-006	Inyección LDAP.	N.A	NO
OWASP-PA-007	Inyección ORM.	N.A	NO
OWASP-PA-008	Inyección XML.	N.A	NO
OWASP-PA-009	Inyección SSI.	N.A	NO

Número de Referencia	Nombre de prueba	Vulnerabilidades encontradas	Efectuada / No efectuada
OWASP-PA-010	Inyección XPath.	N.A	NO
OWASP-AZ-001	Ruta Transversal.	N.A	NO
OWASP-AZ-002	Para Evitar Esquema de Autorización.	N.A	NO
OWASP-AZ-003	Prueba de escalada de privilegios.	N.A	NO
OWASP-GS-001	Prueba del Esquema de Gestión de Sesión.	N.A	NO
OWASP-GS-002	Prueba de atributos de Cookies.	N.A	NO
OWASP-GS-003	Prueba de Fijación de Sesión.	N.A	NO
OWASP-GS-004	Prueba de Variables de Sesión Expuestas.	N.A	NO
OWASP-VI-001	Ataques a través de Comodines SQL.	N.A	NO
OWASP-VI-002	Bloqueo de Cuentas de Usuarios.	N.A	NO
OWASP-SW-002	Prueba de REST/parámetros HTTP GET.	N.A	NO
OWASP-SW-002	Adjuntos SOAP maliciosos.	N.A	NO
OWASP-PX-002	Vulnerabilidades Ajax.	N.A	NO

Nota: Resultados obtenidos en base a la Guía de OWASP

4.5. OBJETIVO ESPECÍFICO 3

4.5.1. Valoración de Riesgos y Amenazas

En gran porcentaje de las instituciones u organizaciones manejan una gran cantidad de información, por ello se encuentran expuestos a muchos riesgos y uno de los activos calificados como alto, puede ser la pérdida de la información más relevante para la institución en estudio. El riesgo se puede definir como un evento potencialmente negativo, debido a que cualquier persona o entidad está expuesta a una variedad de riesgos internos y externos, incluidos su personal, su actividad,

la situación económica, la distribución de sus recursos financieros y la tecnología utilizada dentro de la institución.

Respecto a la amenaza, se basa en la posibilidad de que ocurra cualquier tipo de evento que pueda cause daño a la institución, ya sea material o inmaterial, a los componentes de un sistema web que utiliza el Colegio de Ingenieros del Perú, Consejo Departamental Puno, en el caso de la seguridad informática tiene como propósito garantizar la confidencialidad, integridad, disponibilidad y autenticidad de los datos e informaciones, también hay que ver en relación con las amenazas y los consecuentes daños que pueden causar dicho evento.

RIESGO = AMENAZA X VULNERABILIDAD

4.5.2. Valoración matriz de riesgos por impacto y probabilidad

MA	**:** Muy alto	**C**	**:** Crítico
A	**:** Alto	**I**	**:** Importante
M	**:** Medio	**A**	**:** Apreciable
B	**:** Bajo	**B**	**:** Bajo
MB	**:** Muy bajo	**MB**	**:** Depreciable

Tabla 32

Valoración matriz de riesgos por impacto y probabilidad

		Probabilidad				
		MB	**B**	**A**	**I**	**C**
Impacto	**MB**	1%	10%	35%	50%	60%
	B	10%	35%	50%	60%	70%
	M	35%	50%	60%	70%	80%
	A	50%	60%	70%	80%	90%
	MA	60%	70%	80%	90%	100%

Nota: Realizado en base a MAGERIT v3

Tabla 33

Valoración de Matriz de Riesgos

	Identificación de Riesgo	Análisis de Riesgo											
	Riesgo/Valoración	Impacto					Probabilidad					Resultados	Categoría
		MA	A	M	B	MB	C	I	A	B	MB		
R01	Debido a exposición de polvo, los equipos informáticos se encuentran expuestos a sufrir daños.		X						X			70%	AA
R02	El área donde se encuentran los equipos tecnológicos es compartida con el área de servidores.		X					X				80%	AI
R03	Debido a que no hay cortinas que protejan los equipos del sol, el ambiente y los equipos presentan altas temperaturas.				X		X					60%	BC
R04	Dentro de la institución no se cuenta con plan de actualizaciones de equipos.		X						X			70%	AA

	Identificación de Riesgo	Análisis de Riesgo											
	Riesgo/Valoración	Impacto					Probabilidad					Resultados	Categoría
		MA	A	M	B	MB	C	I	A	B	MB		
R05	No se controla el acceso de personal no autorizado en el área de tecnologías y sistemas.			X					X			60%	MA
R06	Los equipos de la institución no se encuentran actualizados.			X				X				70%	MI
R07	Los antivirus no se encuentran actualizados		X						X			70%	AA
R08	No se tienen configuradas los firewall en los servidores			X						X		50%	MB
R09	Dentro de la institución no se encuentra un lugar para almacenar los Backup del sistema y las copias de seguridad.		X					X				80%	AI
R010	Los usuarios finales pueden acceder a los puertos USB de las estaciones de trabajo.		X				X					90%	AC

Identificación de Riesgo		Análisis de Riesgo											
	Riesgo/Valoración	Impacto					Probabilidad					Resultados	Categoría
		MA	A	M	B	MB	C	I	A	B	MB		
R011	En ocasiones, el sistema está disponible para personas que no están involucradas en la operación.				X				X			50%	BA
R012	El sistema web del CIP-Puno está expuesto al posible robo de información.		X					X				80%	AI
R013	El sistema web del CIP-Puno está expuesto a posibles sabotajes.			X				X				70%	MI
R014	Falta de capacitación al personal que interactúa con el sistema web, sobre el manejo y cuidado de los equipos, herramientas con las que cuenta la institución.		X					X				80%	AI
R015	Falta de capacitación al personal que administra la red del CIP-Puno			X				X				70%	MI

Nota: Elaboración propia

4.6. DISCUSIÓN

Los resultados de la investigación se corroboraron con los antecedentes citados en el trabajo:

Se identificó las vulnerabilidades bajo el enfoque de la metodología OWASP en el sistema de información web del Colegio de Ingenieros del Perú, Consejo Departamental Puno. Tras someter el sistema web de la institución a pruebas de vulnerabilidad, se obtuvieron los siguientes resultados: directorios expuestos, una vulnerabilidad crítica a ataques de diccionario, un proceso inseguro de restauración de contraseñas y fallos en la plataforma WordPress. Respecto a la amenazas la evaluación reveló debilidades en el manejo de equipos informáticos y la falta de capacitaciones, así como la necesidad de implementar políticas de seguridad. El impacto estimado de estos riesgos en la disponibilidad del sistema web se sitúa entre el 80% y el 90%, lo que subraya la urgencia de adoptar medidas preventivas.

Los resultados encontrados tuvieron similitud con los hallazgos de Santiago, (2021) quien identificó que la metodología OWASP es un referente clave para mejorar la seguridad en aplicaciones web. Santiago resalta que OWASP permitió aplicar procedimientos que protegían la información frente a ataques cibernéticos, facilitando el seguimiento de incidentes y promoviendo la retroalimentación para la mejora continua. También enfatizó la importancia de que los desarrolladores conozcan las políticas de seguridad, las cuales deben actualizarse regularmente y cubrir aspectos como la privacidad de datos, la gestión de activos y la implementación de controles físicos, como CCTV y sensores, para proteger los equipos de trabajo. Asimismo, el autor destacó la necesidad de proteger la información almacenada en aplicaciones web, ya que estas plataformas son blanco constante de ciberdelincuentes que buscan explotar

vulnerabilidades para cometer delitos como suplantación de identidad, robo y secuestro de información, siendo este último uno de los mayores riesgos para las organizaciones en la actualidad.

Gallegos (2019) el cual identificó vulnerabilidades haciendo uso de herramientas como; sistema Operativo Kali Linux; Sqlmap para inyección Sql, BurpSuite para la pérdida de autenticación por fuerza bruta, y, Wireshark con la que pudo capturar datos sensibles, una vez ejecutadas pudo encontrar malas prácticas de programación que permitían, debilidades en la autenticación que facilitaban ataques de fuerza bruta, y riesgos en el tráfico de datos debido al uso de HTTP. Para mitigar estos riesgos, se implementaron restricciones de acceso, bloqueos temporales, y certificados SSL para asegurar el tráfico mediante HTTPS y evitar la exposición de datos sensibles. Resultados cercanos a los de Arboleda & Lopez (2022) los cuales llevaron a cabo un análisis técnico para identificar las vulnerabilidades, amenazas y riesgos más frecuentes en diversas aplicaciones web, y como resultado, se encontraron múltiples vulnerabilidades, entre las cuales destacan las más comunes que impactan a los sistemas informáticos, como la inyección SQL, fallos en la integridad del software y datos, componentes vulnerables y desactualizados, configuraciones de seguridad incorrectas y la pérdida de control de acceso derivada del desarrollo de las aplicaciones web, bajo los resultados del análisis, clasificaron a las vulnerabilidades en niveles de riesgo alto, medio y bajo, según el impacto se podrían tener casos de que un atacante intentara acceder al sitio web. Por otro lado Palacios (2021) obtuvo resultados luego de realizar un pentesting autorizado, legal y ético, que permitió identificar vulnerabilidades en el sistema web de Gestión administrativa de Devhuayra S.A.C. en Huancayo. La evaluación inicial, mediante un checklist, reveló la ausencia de políticas de respaldo, actualizaciones de software y un plan de respuesta ante incidentes de seguridad. Los resultados del Pentesting revelaron

varias vulnerabilidades durante las diferentes fases. En la fase de Reconocimiento, se detectaron dos vulnerabilidades: una de bajo riesgo, donde el sitio permitió la réplica de sus archivos utilizando la herramienta Httrack, y una de riesgo crítico, al no contar con un certificado SSL/TLS, identificado con Netcraft. En la fase de Escaneo, encontró seis vulnerabilidades: una importante relacionada con los puertos 80 y 443 vulnerables a ataques DDoS; puertos 110, 142, 993 y 995 con la vulnerabilidad Diffie-Hellman Key Exchange de tipo crítico; la vulnerabilidad CVE-2012-2122 en MySQL, de riesgo moderado; y la vulnerabilidad CVE-2012-020 en el protocolo RDF, también de riesgo moderado, todas identificadas mediante Nmap Scripting y Vuln. Además, Nikto detectó la falta de protección contra Cross Site Scripting, que representó una vulnerabilidad moderada, y algunos directorios del sistema web están indexados, siendo públicos y accesibles, lo que constituyó una vulnerabilidad de bajo riesgo. En la fase de explotación, identificó dos vulnerabilidades críticas: el formulario de inicio de sesión no estaba protegido contra inyección de código SQL, y las contraseñas de la base de datos no se encontraban encriptadas. Menciona Morocho & Tasan, (2020) que al realizar pruebas de penetración (pentesting) con Kali Linux, identificaron vulnerabilidades en los sitios web desarrollados, el que fue enfocado bajo OWASP demostró ser menos susceptible a ataques informáticos, alcanzando un 91.75% de seguridad, en comparación con el sitio desarrollado rápidamente, que solo logró un 19.15% de seguridad bajo el enfoque de OWASP, el sitio desarrollado vertiginosamente se centró únicamente en la funcionalidad, lo que resultó en un mayor número de vulnerabilidades.

Así mismo los resultados encontrados por Delgado (2020) en aplicaciones web y redes inalámbricas de ULEM Extensión en El Carmen, basado en OWASP y haciendo uso de la herramienta Nessus la cual le permitió verificar y evaluar la seguridad de las redes inalámbricas y sus respectivos puertos de internet, además verificó que se cumple

con un 90% de los estándares de seguridad, este cumplimiento se basó en la implementación de sistemas como puerto cautivo, firewall y antivirus, los cuales bloquearon los intentos sospechosos dentro de la universidad, además con base en las herramientas y hallazgos del análisis de seguridad, concluyó que la Extensión Universitaria fue protegida contra vulnerabilidades y riesgos informáticos. Por otro lado Gamboa (2021) luego de realizar las pruebas de vulnerabilidad en base a la guia presentada por OWASP v4.0 en sus resultados determinó que existen ciertas vulnerabilidades que representan una amenaza constante para la aplicación web y no alcanzan un nivel de seguridad aceptable. Además no pudo realizar todas las pruebas debido a limitaciones de programación, accesos restringidos y problemas de funcionalidad por ello que algunas pruebas no se pudieron ejecutar porque la aplicación web no cuenta con los mecanismos necesarios para su correcta realización.

V. CONCLUSIONES

PRIMERA: En cuanto al objetivo general, se completó satisfactoriamente el análisis de riesgos utilizando la metodología OWASP, lo que permitió identificar las debilidades, vulnerabilidades y riesgos que podían afectar al sistema web del Colegio de Ingenieros del Perú, Consejo Departamental Puno.

SEGUNDA: En el Colegio de Ingenieros del Perú, Consejo Departamental Puno, conforme al primer objetivo, se identificaron los activos de la institución, enfocándose específicamente en la Oficina de Tecnología y Sistemas. Se evaluaron las amenazas a las que estuvo expuesto el sistema web utilizando la metodología MAGERIT. Sin embargo, se determinó que la institución carece de políticas o medidas de seguridad informática, así como de directrices claras para la identificación, prevención y gestión de los riesgos informáticos asociados con sus actividades.

TERCERA: En el Colegio de Ingenieros del Perú, Consejo Departamental Puno, de acuerdo con el objetivo 2, se llevó a cabo un análisis utilizando las directrices de OWASP. Se identificaron varias debilidades en el sistema web, tales como directorios expuestos, vulnerabilidad crítica a ataques de diccionario, una restauración de contraseñas vulnerable y fallos en WordPress. Aunque el sistema presentó un nivel de seguridad del 75%, se necesitaba implementar mejoras significativas para fortalecer su protección.

CUARTA: En el Colegio de Ingenieros del Perú, Consejo Departamental Puno, de acuerdo con el objetivo 3, se evaluó el impacto de los riesgos y amenazas en relación con la seguridad existente. Esta evaluación permitió estimar el

posible daño que podría afectar la disponibilidad del sistema web, revelando debilidades en el manejo y cuidado de los equipos informáticos, así como la falta de capacitaciones y la necesidad de implementar políticas de seguridad. La valoración del impacto de estos riesgos se situó entre un 80% y un 90%, lo que sugirió que se debían de tomar medidas preventivas de manera urgente.

VI. RECOMENDACIONES

PRIMERA: A las organizaciones, es crucial establecer y formalizar políticas de seguridad informática claras y completas que cubran todos los aspectos de la protección de datos y sistemas. Estas políticas deben abordar la gestión de riesgos, la protección de información sensible, el acceso a sistemas y redes, y la respuesta a incidentes de seguridad. Las políticas deben ser revisadas y actualizadas regularmente para adaptarse a nuevas amenazas y cambios en la infraestructura.

SEGUNDA: A los desarrolladores de sistemas web si se planea implementar un sistema de pagos u otro tipo de sistema en el futuro, es esencial reforzar la seguridad del sistema web. Esto incluye la aplicación de controles adicionales de autenticación y autorización, la encriptación de datos sensibles durante la transmisión y almacenamiento, y la protección contra ataques comunes como inyecciones SQL, cross-site scripting (XSS) y cross-site request forgery (CSRF). Se recomienda realizar pruebas de penetración periódicas y revisiones de seguridad para garantizar que todas las nuevas funcionalidades cumplan con los estándares de seguridad.

TERCERA: A la institución asegurarse que se debe de llevar a cabo una recolección de información exhaustiva sobre todos los sistemas y procesos críticos de la organización. Realiza evaluaciones de seguridad detalladas basadas en las guías de OWASP para identificar vulnerabilidades y riesgos potenciales. Implementa un ciclo continuo de pruebas de seguridad, análisis de vulnerabilidades y revisión de configuraciones para mantener la seguridad de los sistemas a lo largo del tiempo. Documenta todos los hallazgos y

acciones correctivas para mejorar la seguridad y facilitar la toma de decisiones informadas.

CUARTA: A los trabajadores directos de la Oficina de Tecnología y Sistemas se implemente programas de capacitación y concienciación para todo el personal sobre las mejores prácticas de ciberseguridad. Esto debería incluir formación en la identificación de ataques comunes, como phishing y malware, en la protección de datos personales y organizacionales, promuevan una cultura de seguridad dentro de la organización mediante la realización de talleres, simulaciones de ataques y actualizaciones regulares sobre nuevas amenazas y vulnerabilidades.

VII. REFERENCIAS BIBLIOGRÁFICAS

Administración Electrónica . (2012). *MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* Madrid.

Aguilar, V. (2013). OWASP Top 10 2013: actualización de los riesgos más extendidos asociados a las aplicaciones web.

Akamai. (2022). *Las 10 principales vulnerabilidades según OWASP.*

Alarcon, C. (17 de Mayo de 2024). *Sistema web.* Obtenido de Data.: https://www.datatrust.pe/web/sistema-web/

Ángeles, M., & Cilleres, D. (2022). *El libro del Hacker.*

Araque, J. (2019). Guía para hacer una entrevista. *Germina* , 7-12.

Arboleda, V. C., & Lopez, G. (2022). *Aplicación de la Metodología OWASP – 2021 mediante Pentesting para la detección de vulnerabilidades en software de aplicación.* Guayaquil.

Balseca, F., Colina, A., & Espinoza, M. (2021). *Identificación de amenazas informáticas aplicando arquitecturas de Big Data.* Ecuador.

Bustamante, R. (2020). *Seguridad en Redes.*

Calvo, J. (2022). *Aplicación de pentesting y la seguridad informática en los equipos tecnológicos de la Universidad Nacional Santiago Antúnez de Mayolo, 2022.* Huaraz.

Campos, G., & Lule, E. (2012). La observación, un método para el estudio de la realidad. *Xihmai,* 45-60.

Castro, A. (2020). *Tipos de Vulnerabilidades y Amenazas informáticas.* Barcelona.

Castro, V., Herrera, R., & Villalobos, M. (2020). *Desarrollo de un software web para la generación de planes de gestión de riesgos de software.* Chile.

CEPAL. (2021). *Tecnologías digitales para un nuevo futuro.* Santiagp: LC/TS.2021/43.

Chancusing, J. D., & Guasumba, J. H. (2022). *Análisis de seguridad en smart home basado en la metodologia owasp asvs sobre un caso de estudio real.* Quito.

Chiluiza, L., & Enciso, L. (2023). *Detección y solución de vulnerabilidades con Greenbone Security Assistant.* Ecuador.

Cilleruelo, C. (27 de Mayo de 2024). *KeepCoding.* Obtenido de KeepCoding: https://keepcoding.io/blog/que-es-nessus/

Colegio de Ingenieros - Consejo Departamental de Puno. (2023). *Colegio de Ingenieros - Consejo Departamental de Puno*. Obtenido de Colegio de Ingenieros - Consejo Departamental de Puno: https://web.cippuno.org.pe/

Corredera, P. Á. (2023). *A04 Diseño Inseguro (by OWASP).*

Creswell, J. (2015). Investigación Cualitativa y Diseño Investigativo. En J. Creswell, *Investigación Cualitativa y Diseño Investigativo.*

Cújar, L. (2015). *A4 - Referencia Directa Insegura a Objetos.*

Delgado, J. (2020). *Análisis de seguridad mediante la metodología OWASP a redes inalámbricas en "Universidad Laica Eloy Alfaro de Manabí extención en el Carmen"".* El Carmen.

Duque , N., & Tamayo, A. (2019). *Hackers, Crackers y otros.*

Fabra, J. (2022). *Análisis de la vulnerabilidad Log4shell.* España.

Feito, L. (2007). *Vulnerabilidad.* Madrid.

Fernández, P., Vallejo, G., Livacic, P., & Tuero, E. (2014). Validez Estructurada para una investigación cuasi-experimental de calidad. Se cumplen 50 años de la presentación en sociedad de los diseños cuasi-experimentales. *SciELO Analytics*.

Gallegos, M. (2019). *Implementación de controles a una aplicación web mediante la metodología Owasp para el aseguramiento de su seguridad.* Machala.

Gamboa, D. (2021). *Vulnerabilidades en aplicaciones web utilizando la metodolgía de "Proyecto Abierto de Seguridad de Aplicaciones web".* Ecuador.

García, A. (2023). *Qué es IDOR (Insecure Direct Object Reference) y cómo solucionarlo.*

Gómez, Á. (2019). *Tipos de ataques e intrusos redes informaticas.*

González , H. R., & Montesino, R. (2018). Capacidades de las metodologías de pruebas de penetración para detectar vulnerabilidades frecuentes en aplicaciones web. *Revista Cubana de Ciencias Informáticas*.

Guevara, E. M., Delgado, J. R., & Mendoza, A. C. (2023). *Vulnerabilidades y amenazas en los activos de información: una revisión sistemática.* Perú.

Hacking Knowledge. (2023). *OWASP 04:2021 Diseño Inseguro.* Mexico.

IBM. (2022). *¿Qué son las amenazas internas?*

ISO 27001. (2020). *Guía Implementación ISO 27001*.

ISO 27001. (2022). *A9 Control de Acceso.* Barcelona.

Kaur, R. (2017). *Referencias Directas Inseguras a Objetos* .

León, E. G., & Gervacio, I. (2015). Seguridad de Prevención Cultura de prevención para TI Herramientas de detección. *Repositorio Universitario de la DGTIC*.

LimpiatuWeb. (2024). *Referencias de objetos directos inseguras (IDOR): Todo sobre este tipo de infección.*

LLanos, D. A., & Cerda, M. F. (2019). *Propuesta de medidas correctivas de un sistema web para la empresa marítima Cosmos Agencia Marítima S.A.C.* Lima.

Lotero , L., & Hurtado , R. G. (2015). *Vulnerabilidad de redes complejas y aplicaciones al transporte urbano: una revisión de la literatura.* Colombia.

Martínez, B. (2006). *La filosofía Hacking & Cracking.* Pachuca.

Marulanda, M. F., & Díaz, J. (2018). *Aplicación de la metodología de pruebas OWASP (open web application security project) para mejoramiento de la seguridad en el sistema e-commerce siembraviva.com.* Maninzales.

Ministerio de Hacienda y Administraciones Públicas. (2012). *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Método.* Madrid.

Miranda, A. H. (2022). *Fallos criptográficos: segunda mayor amenaza para la ciberseguridad* . São Paulo.

Morales, A. (2022). *Los diez riesgos de seguridad más importantes en aplicaciones web.*

Morocho, M., & Tasan, F. (2020). *Metodología OWASP en el desarrollo de un website para voto electrónico, caso práctico: Sistema de elecciones asociación de estudiantes TI-UNACH.* Riobamba - Ecuador.

Navarro, G. (2018). *Introducción a las vulnerabilidades.* Catalunya.

OWASP. (2021). *Owasp Top 10.*

Palacios, M. L. (2021). *Aplicación de Pentesting en el análisis de vulnerabilidades del sistema web de gestión administrativa de la Empresa DEVHUAYRA SAC Huancayo.* Huancayo.

Qawerk. (2023). *Vulnerabilidad de falla criptográfica: Explicación y ejemplos.* Ucrania.

Repullo, J. R., Donado, J., & Casas, J. (2003). La encuesta como técnica de investigación. Elaboración de cuestionarios y tratamiento estadístico de los datos (I). *Atención primaria Publicación oficial de la Sociedad Española de Familia y Comunitaria*, 527-538.

Rivera, N. R. (2011). La definición y medición de la vulnerabilidad social. Un enfoque normativo. *Investigaciones Geográficas (Mx).*

Rodríguez, M. J., & Peralta, I. (2013). *Gestión de Riesgos Magerit.*

Sampieri, R. (2006). *Metodología de la investigación.* McGraw-Hill.

Santandar Universidades. (2021). *Métodos de investigación: cualitativa y cuantitativa.*

Santander. (2023). *¿Qué es una vulnerabilidad informática?* Obtenido de ¿Qué es una vulnerabilidad informática?: https://www.bancosantander.es/glosario/vulnerabilidad-informatica#:~:text=En%20inform%C3%A1tica%2C%20una%20vulnerabilidad%20es,malintencionada%20para%20comprometer%20su%20seguridad.

Santiago, O. C. (2021). *Owasp como elemento estratégico en la identificación de vulnerabilidades y la validación de seguridad en el diseño, programación y operación de aplicaciones seguras en las organizaciones desarrolladoras de software en Colombia.* Colombia.

SeoEstudios. (2020). Qué es un script: cómo funciona, cómo crearlo o eliminarlo. *Qué es un script: cómo funciona, cómo crearlo o eliminarlo*.

Serra, J., Navarro , G., Castillo, S., Herrero, J., Robles, S., & García, J. (2021). *Seguridad Informática.*

Shivanandhan, M. (23 de 04 de 2023). *freeCodeCamp.* Obtenido de freeCodeCamp: https://www.freecodecamp.org/espanol/news/que-es-nmap-y-como-usarlo-un-tutorial-para-la-mejor-herramienta-de-escaneo-de-todos-los-tiempos/

Susatama, M. A. (2022). *Análisis de las técnicas más usadas en la ingeniería social.* Colombia.

Tarazona, C. (2007). *Amenazas Informáticas Seguridad de la Información.*

Tarlogic. (2022). *OWASP: Top 10 de vulnerabilidades en aplicaciones web* .

Taype, L. (2020). *"Propuesta de elaboración del manual de procedimientos en el proceso de evaluación de seguridad en una aplicación móvil android basado en la metodología OWASP para la empresa Entelgy 2020.* VILLA EL SALVADOR.

Tecana American University. (2023). *Los Niveles de Investigación.* Estados Unidos.

Villacis, W. E. (2022). *Análisis comparativo entre los sistemas operativos Windows Xp y Kali Linux para el ataque y prevención de su ciberseguridad.* Ecuador.

Walteros , E. A., Rivas, J. R., & Peralta , J. T. (2019). nálisis de los factores de seguridad informática, aplicando un test de vulnerabilidades mediante la metodología "OWASP v.4" a la aplicación portal web version 3.3.4 de la compañía "NOVASOFT-COLOMBIA". *Universidad Cooperativa de Colombia*, 4.

Weimann, G. (2017). *TERRORISMO e INTERNET.* España.

ANEXOS

ANEXO 1: Documento de Entrevista al encargado del sistema web del CIP-Puno

ENTREVISTA DIRIGIDA AL ENCARGADO DEL SISTEMA WEB DEL

COLEGIO DE INGENIEROS – CONSEJO DEPARTAMENTAL PUNO

Fecha: 23/04/2024

Nombre del entrevistado:

Presentación del Proyecto
El Colegio de Ingenieros – Consejo Departamental Puno, es el órgano profesional de estudios e investigación del Colegio de Ingenieros. Tiene por finalidad proveer al país de ingenieros ética y profesionalmente idóneos, para que a través de su participación efectiva y de una formación certificada, la Origen contribuya al desarrollo de la Nación.

Objetivo:
Conocer si la organización cuenta un plan de seguridad, como se realiza manejo de los de información en sistemas Web de la entidad.

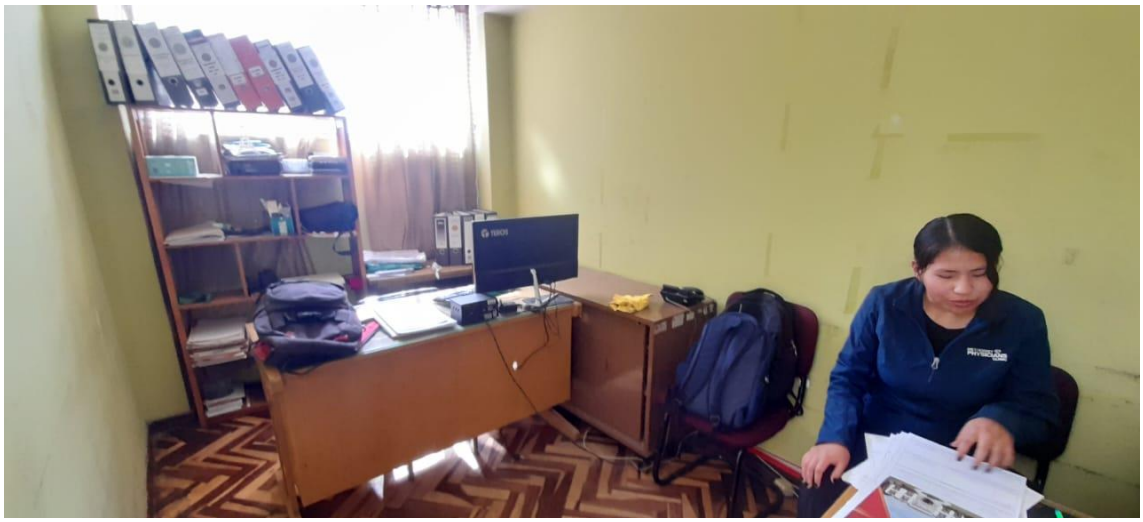
1. ¿Cuánto tiempo lleva operando el Colegio de Ingenieros en el Perú?
2. ¿Qué tipo de método de análisis de riesgos se realiza en la entidad?
3. ¿En la organización se ha registrado problemas con algún software malicioso?¿Cuáles?
4. ¿Otros usuarios pueden instalar y desinstalar software en los equipos informáticos que usted tiene a cargo?
5. ¿Cada cuánto tiempo se realizan los mantenimientos en los equipos informáticos?
6. ¿Se utiliza las políticas de seguridad para definir cómo debe y puede ser tratada la información frente a una amenaza?
7. ¿Existen problemas de manipulación (manejo no autorizado) de información en el Colegio de Ingenieros Consejo - Departamental Puno?
8. ¿Cada cuánto se realizan copias de seguridad de información en el Colegio de Ingenieros?
9. ¿Se han tenido problemas de seguridad donde se vea comprometida o alterada la información de la empresa o usuarios en los últimos años?
10. Cuándo un equipo informático tiene fallas. ¿Se soluciona rápidamente?
11. ¿De qué manera se encuentra protegido los sistemas Web del Colegio de Ingenieros?
12. Ante un posible ataque que se pueda dar por Hackers o personas malintencionadas. ¿Cuáles son las acciones que toman?

ANEXO 2: Instalación de equipos en la Oficina de Tecnología y Sistemas

ANEXO 3: Ambiente laboral del CIP-Puno Oficina de Tecnología y Sistemas

ANEXO 4: Equipos de trabajo del CIP-Puno Oficina de Tecnología y Sistemas

ANEXO 5: Evaluación de documentos brindados por el Jefe encargado



ANEXO 6: Entrevista al Jefe del CIP-Puno Oficina de Tecnología y Sistemas

ANEXO 7: Área de trabajo del CIP-Puno Oficina de Tecnología y Sistemas

ANEXO 8: Datos Complementarios de la Encuesta

Figura 44

Versión más usada por los usuarios

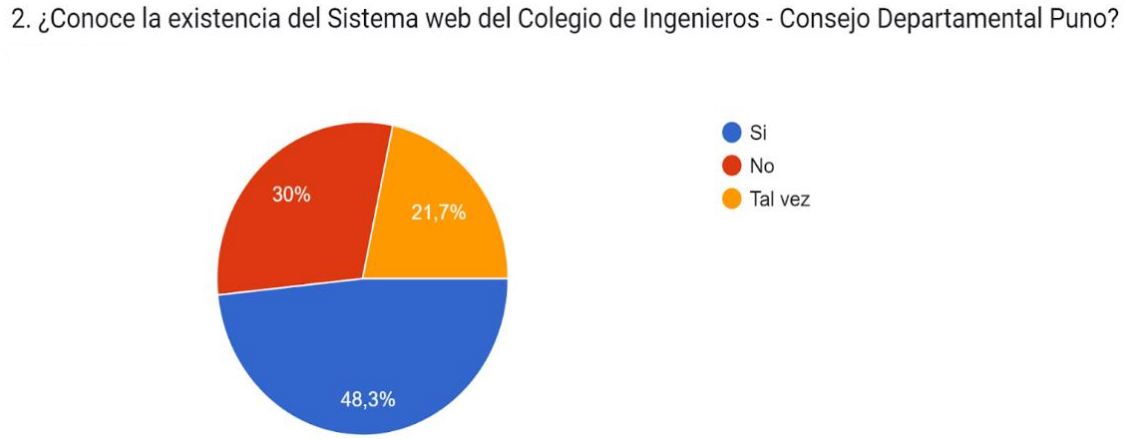
Nota: Realizado según datos de la encuesta

Interpretación

En la Figura 44 reflejó los resultados sobre las versiones de Windows utilizadas por los usuarios para navegar en el sistema web del Colegio de Ingenieros del Perú, Consejo Departamental Puno. Un 49.2% de los usuarios tenían instalada la versión de Windows 11 en sus ordenadores, un 36.1% tuvo instalada Windows 10 y por otro lado un 14.7% tenían instaladas otros sistemas operativos como: Linux, Debian, Garuda Linux, Fedora 39 y Kali Linux. El análisis de las preferencias de sistemas operativos entre los usuarios del Colegio de Ingenieros del Perú, Consejo Departamental Puno, reveló una comunidad tecnológicamente diversa. La prevalencia de Windows 11 refleja una tendencia hacia la adopción de nuevas tecnologías, mientras que el uso de Windows 10 demuestra una preferencia por la estabilidad y la familiaridad. La presencia de usuarios que emplean sistemas operativos de software libre indicó una segmentación en la que la personalización, la especialización y la privacidad son prioritarias, esto significó que deben mantener un enfoque inclusivo y versátil en sus sistemas de información para satisfacer las necesidades de todos sus usuarios.

Figura 45

Existencia del sistema web del CID - Puno



Nota: Realizado según datos de la encuesta

Interpretación

En la Figura 45 se reflejó los resultados, un 48.3% de los usuarios afirmaron que si conocían el sistema web, un 30% de usuarios indicaron que no lo conocían y finalmente un 21.7% tal vez lo conocían, lo que sugiere una falta de certeza o familiaridad parcial con el sistema. La percepción mixta sobre la existencia del sistema web del Colegio de Ingenieros del Perú, Consejo Departamental Puno resaltó la necesidad de fortalecer la difusión y la comunicación sobre la plataforma. Aunque casi la mitad de los usuarios conocían el sistema, existió un porcentaje significativo que no lo conocía o no estaba seguro de su existencia, lo que sugirió oportunidades para mejorar la visibilidad y la adopción del sistema.

Al abordar estas áreas, el Colegio puede maximizar el uso y la efectividad de su sistema web, asegurando que todos los miembros puedan beneficiarse de las herramientas y servicios que ofrece.

Figura 46

Navegador más utilizado por los usuarios de CIP-Puno

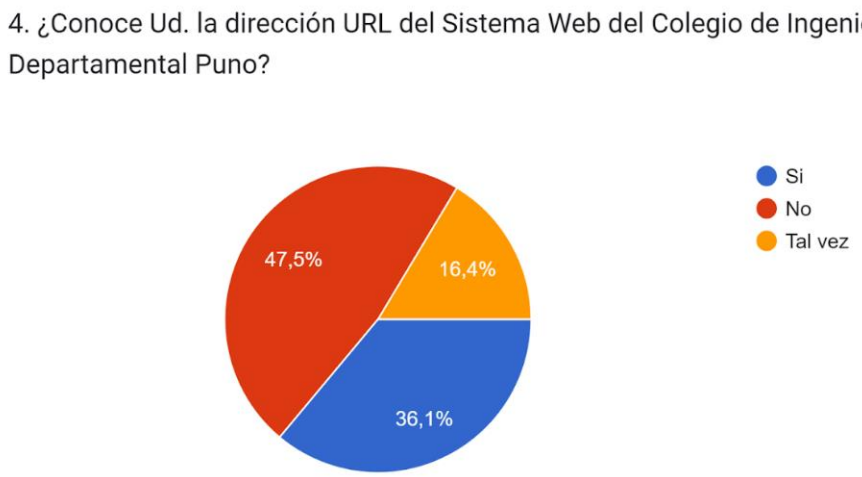
Nota: Realizado según datos de la encuesta

Interpretación

En la Figura 46 reveló las preferencias de los usuarios del Colegio de Ingenieros del Perú, Consejo Departamental Puno en cuanto a navegadores web, destacando a Google Chrome como el navegador más utilizado con un 63.9%. Le siguen Ópera con un 11.5%, Firefox con un 8.2%, Brave con un 6.6%, y finalmente Edge y Thor, que en conjunto representan el 4.9% de los usuarios. Esto pudo deberse a que las preferencias de los usuarios están influenciadas por la popularidad, funcionalidad, rendimiento, y las características específicas de cada navegador, con Chrome liderando debido a su integración y versatilidad. La preferencia predominante por Google Chrome entre los usuarios del Colegio de Ingenieros del Perú, Consejo Departamental Puno refleja tendencias globales en el uso de navegadores. Sin embargo, la presencia de navegadores como Ópera, Firefox, Brave, y Thor sugiere una conciencia creciente sobre la privacidad y la seguridad entre ciertos segmentos de usuarios. Estos datos indican la necesidad de un enfoque multifacético en el desarrollo y la optimización del sistema web, para garantizar que sea accesible y funcional para todos los usuarios, independientemente del navegador que elijan.

Figura 47

Conocimiento sobre la dirección URL



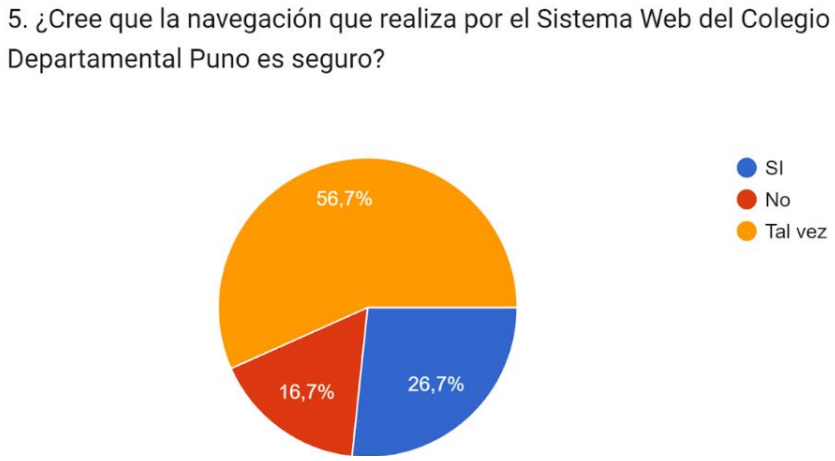
Nota: Realizado según datos de la encuesta

Interpretación

La Figura 47 presentó los resultados sobre el conocimiento de los usuarios del Colegio de Ingenieros del Perú, Consejo Departamental Puno respecto a la dirección URL del sistema web. Los datos revelan que; un 36.1% de los usuarios afirman que conocían la dirección URL del sistema web, un 47.5% indicaron que no conocen la URL mientras que un 16.4% no estaban seguros, señalando que tal vez conocen la dirección URL. La distribución del conocimiento sobre la dirección URL del sistema web entre los usuarios del Colegio de Ingenieros del Perú, Consejo Departamental Puno reveló áreas clave para mejorar la comunicación y la difusión. Con solo un 36.1% de usuarios que afirmaron conocer la URL, existe una clara oportunidad para aumentar la visibilidad y el uso del sistema web mediante estrategias de comunicación más efectivas y accesibles. Al abordar las necesidades de información y mejorar la capacitación, la institución puede garantizar que un mayor número de sus miembros esté preparado para aprovechar plenamente los recursos digitales disponibles.

Figura 48

Percepción de la seguridad en la navegación del sistema web



Nota: Realizado según datos de la encuesta

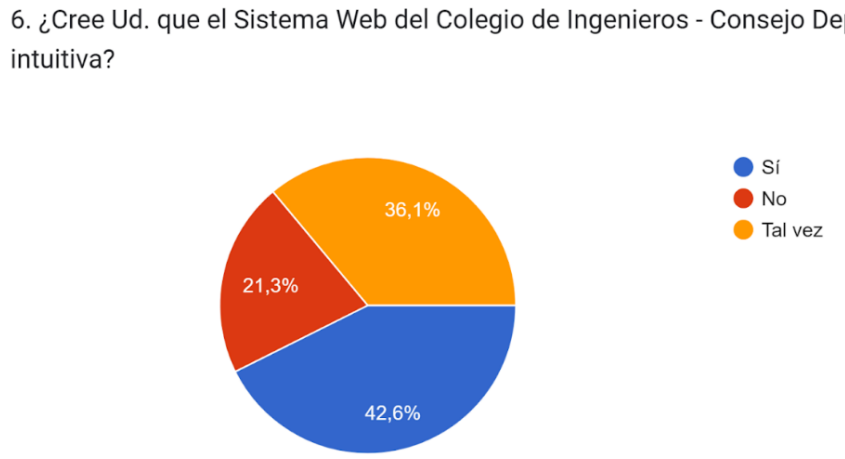
Interpretación

Según la Figura 48 presentó los resultados sobre la confianza de los usuarios al navegar por el sistema web del Colegio de Ingenieros del Perú, Consejo Departamental Puno. Los datos indicaron que, un 56.7% de los usuarios afirmaron que tal vez sea seguro, otro 26.5% creen que sí es seguro mientras que un 16.7% manifestaron que no estaban seguros de la seguridad del sistema. Los resultados reflejaron que, aunque una parte de los usuarios confiaban en la seguridad del sistema web del CIP-Puno, existía una mayoría que no estaban completamente seguros, lo que revela una oportunidad importante para mejorar la comunicación, la transparencia, y la educación en temas de seguridad. Al abordar estas áreas, la institución puede fortalecer la confianza de sus miembros en la plataforma digital.

Al abordar estas áreas, el Colegio de Ingenieros del Perú, Consejo Departamental Puno, puede fortalecer la confianza de sus miembros en la plataforma digital y mejorar la percepción general sobre la seguridad de su sistema web.

Figura 49

Percepción sobre la intuitividad del sistema web



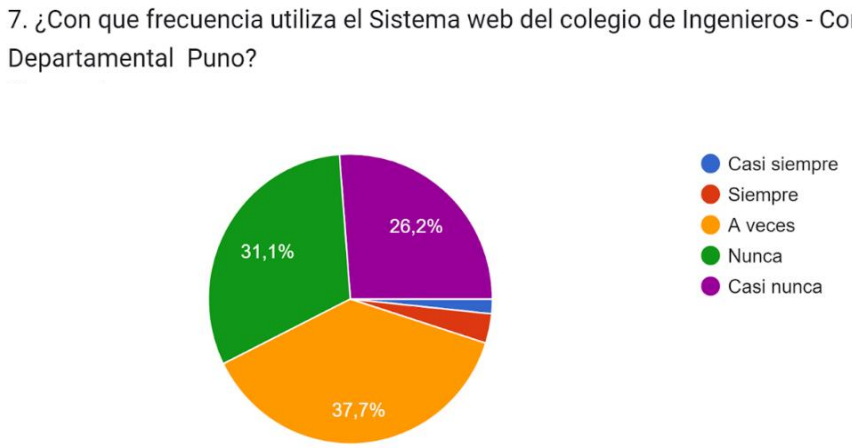
Nota: Realizado según datos de la encuesta

Interpretación

En la Figura 49 presenta los resultados sobre la percepción de la intuitividad del sistema web del Colegio de Ingenieros del Perú, Consejo Departamental Puno. Los datos indicaron que: un 42.2% de los usuarios consideraron que el sistema web era intuitivo, un 36.1% creían que el sistema web podía ser intuitivo mientras que un 21.3% opinaron que el sistema web no era intuitivo. Los resultados mostraron que mientras una parte significativa de los usuarios consideraron que el sistema web del CIP-Puno era intuitivo, existe una porción considerable que tiene dudas o considera que el sistema no era intuitivo. Implementar tutoriales interactivos, simplificar el diseño de la interfaz y mejorar la organización de los contenidos puede ayudar a que los usuarios comprendan y manejen el sistema de manera más eficiente. Al enfocar esfuerzos en estas áreas, el CIP-Puno puede asegurar que todos sus usuarios disfruten de una experiencia de uso más eficiente, agradable y satisfactorio, lo que fortalecerá la percepción general del sistema web como herramienta intuitiva y accesible.

Figura 50

Frecuencia de uso del sistema web



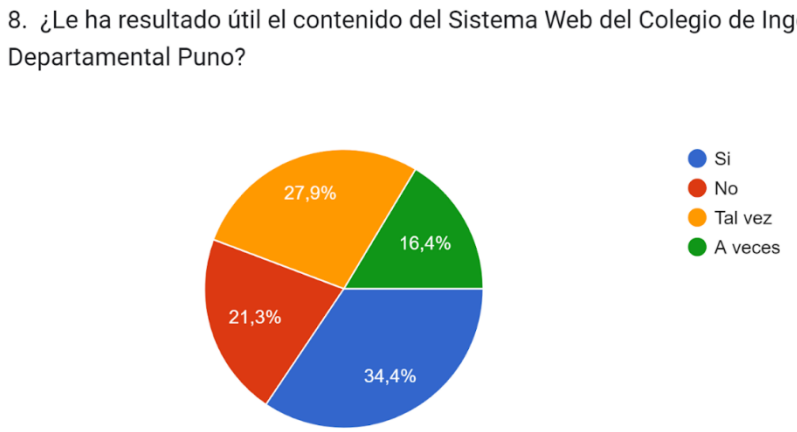
Nota: Realizado según datos de la encuesta

Interpretación

En la Figura 50 presentó los resultados sobre la frecuencia de uso del sistema web del Colegio de Ingenieros del Perú, Consejo Departamental Puno. Los datos mostraron que, un 37.7% de los usuarios indicaron que a veces utilizaban el sistema web, otro 31.1% afirman que nunca lo utilizaron y un total del 26.2% dicen que casi nunca lo utilizaron. Estos resultados mostraron una diversidad en la frecuencia de uso del sistema, con una combinación de uso ocasional, nulo y esporádico, Este panorama sugirió una oportunidad clara para mejorar la funcionalidad y accesibilidad del sistema web, con el objetivo de incrementar su adopción y fomentar un uso más regular y frecuente entre los miembros. Es posible que algunos usuarios no lo utilicen debido a problemas de usabilidad, falta de funcionalidades atractivas o desconocimiento de los servicios que la plataforma ofrece, frente a ello se podrían implementar estrategias como la mejora de la interfaz de usuario, la integración de nuevas funcionalidades, y la promoción de los beneficios del sistema, acompañada de campañas de capacitación para los usuarios.

Figura 51

Utilidad del contenido del sistema web



Nota: Realizado según datos de la encuesta

Interpretación

La Figura 51 presentó los resultados sobre la percepción de utilidad del contenido del sistema web del Colegio de Ingenieros del Perú, Consejo Departamental Puno. Los datos mostraron que; un 34.4% de los usuarios afirmaron que el contenido del sistema web sí les fue útil, otro 27.9% creían que tal vez les fue útil, un 21.3% opinaron que no les fue útil y finalmente un 16.4% consideran que a veces les fue útil. Estos resultados indicaron que, aunque una parte significativa de los usuarios encontraron que el contenido les fue útil, existe también una porción considerable que tiene dudas o que no lo encuentra útil. Esto señala una clara oportunidad para mejorar y adaptar el contenido del sistema a las necesidades y expectativas de los usuarios. La institución puede considerar realizar una revisión del contenido actual, con el fin de asegurar que sea relevante, actualizado y que responda a las inquietudes más importantes de sus miembros. Además, la creación de secciones personalizadas, la incorporación de tutoriales, guías interactivas, o la adición de funcionalidades que faciliten el acceso a la información crítica, podrían mejorar la percepción de utilidad del contenido.

Figura 52

Adecuación del diseño de la interfaz del sistema web

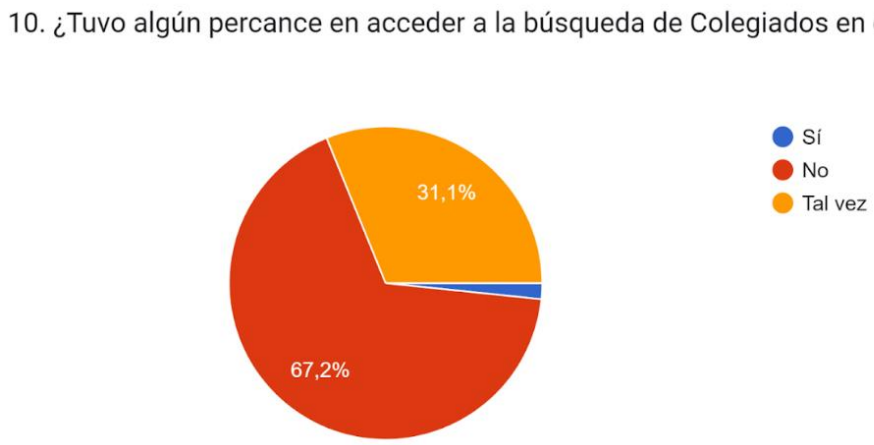
Nota: Realizado según datos de la encuesta

Interpretación

En la Figura 52 presentó los resultados sobre la percepción de los usuarios del Colegio de Ingenieros del Perú, Consejo Departamental Puno respecto a la adecuación del diseño del sistema web. Los datos revelaron que, un 55.7% de los usuarios consideraron que tal vez el sistema web era adecuado, otro 27.9% opinan que si era adecuado mientras que el 16.4% indican que no era adecuado. Estos resultados reflejaron una percepción mixta sobre la adecuación del diseño del sistema, con una mayoría de usuarios que están indecisos o que no lo encuentran completamente satisfactorio. Esto sugirió áreas potenciales de mejora en la estructura, organización y usabilidad del sistema. Para mejorar la percepción del diseño, la institución podría evaluar la experiencia del usuario y hacer ajustes que optimicen la navegación, la presentación visual y la claridad de los elementos interactivos del sitio. La modernización del diseño, la incorporación de elementos intuitivos y accesibles, y la mejora en la disposición de la información pueden aumentar la satisfacción de los usuarios, haciéndolo más atractivo y funcional.

Figura 53

Percances en el acceso a la búsqueda de colegiados



Nota: Realizado según datos de la encuesta

Interpretación

En la Figura 53 mostró los resultados sobre los percances que los usuarios han experimentado al acceder a la búsqueda de Colegiados en el sistema web del Colegio de Ingenieros del Perú, Consejo Departamental Puno. Los datos revelaron que un 67.2% de los usuarios indicaron que no tuvieron problemas al acceder a la búsqueda, un 31.1% afirman que tal vez experimentaron algún percance mientras que un 1.6% señalaron que tuvieron problemas. Estos resultados sugieren que la mayoría de los usuarios acceden sin inconvenientes a la función de búsqueda de Colegiados, lo que es positivo para la funcionalidad general del sistema. Sin embargo, el pequeño porcentaje de usuarios que ha enfrentado dificultades en esta área indica que hay espacio para mejoras. Para asegurar una experiencia de usuario fluida y sin percances, sería recomendable realizar una revisión técnica de la herramienta de búsqueda y su rendimiento, así como ofrecer soporte a aquellos usuarios que han experimentado problemas. Además, la implementación de mejoras en la interfaz de búsqueda o la optimización de la velocidad de respuesta del sistema podría ayudar a reducir la fricción para los usuarios que reportan inconvenientes.

Figura 54

Grado de satisfacción con la visita al sistema web

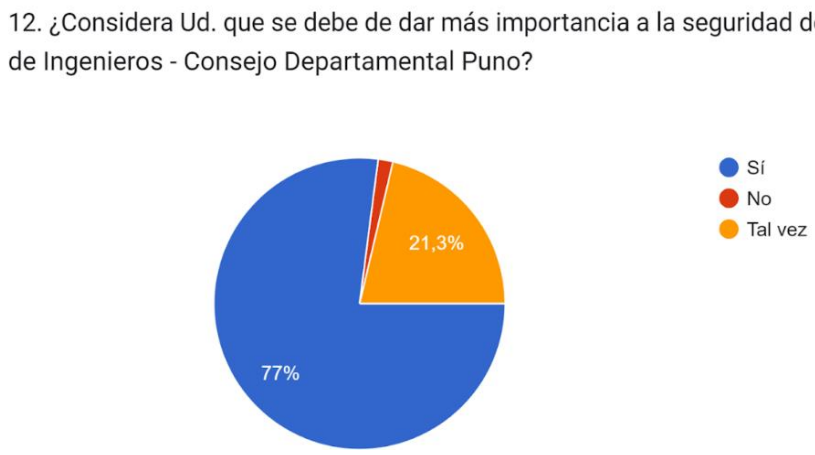
Nota: Realizado según datos de la encuesta

Interpretación

En la Figura 54 presentó los resultados sobre el grado de satisfacción de los usuarios con su visita al sistema web del Colegio de Ingenieros del Perú, Consejo Departamental Puno. Los datos revelaron que, un 59% de los usuarios se encontraron moderadamente satisfechos con su visita, el 21.3% indicaron estar muy satisfechos, el 13.1% no estaban satisfechos, el 4.9% se sentían poco satisfechos y 1.6% estaban extremadamente satisfechos. Estos resultados indican que, aunque la mayoría de los usuarios tenían una satisfacción moderada, existía un porcentaje menor que expresa niveles más altos o bajos de satisfacción. Esto sugiere la necesidad de realizar mejoras en áreas clave del sistema web para elevar la experiencia del usuario. Las acciones a considerar podrían incluir una optimización de la navegación, mejoras en el diseño y mayor funcionalidad, así como la implementación de un soporte técnico accesible para atender las inquietudes o dificultades que los usuarios puedan enfrentar durante su visita. Al abordar estos puntos, el CIP-Puno podría aumentar la satisfacción general y fomentar un uso más positivo y consistente del sistema web.

Figura 55

Importancia de la seguridad en el sistema web



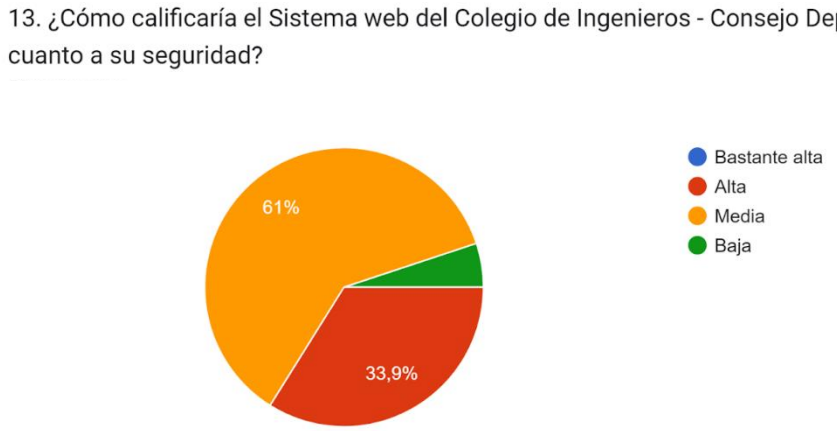
Nota: Realizado según datos de la encuesta

Interpretación

En la Figura 55 presentó los resultados sobre la opinión de los usuarios acerca de la importancia que se debe dar al sistema web del Colegio de Ingenieros del Perú. Consejo Departamental Puno. Los datos indicaron que, un 77% de los usuarios señalaron que sí se le debe dar más importancia, un 23% afirmaron que tal vez se debía considerar 1.6% creían que no es necesario darle más importancia. Estos resultados sugieren un consenso claro entre los usuarios sobre la necesidad de aumentar la atención y el enfoque en mejorar y optimizar el sistema web. La mayoría considera que se debe priorizar el desarrollo y perfeccionamiento del sistema, lo que resalta la relevancia de la plataforma digital en la relación del Colegio con sus miembros. Aunque una pequeña minoría no lo consideraba prioritario, el respaldo mayoritario es una señal para que el Consejo Departamental Puno enfoque sus esfuerzos en modernizar y reforzar el sistema web, haciéndolo más útil, accesible y funcional para todos los usuarios. Esto no solo mejorará la satisfacción y la confianza, sino que también permitirá un mejor aprovechamiento de las herramientas digitales disponibles.

Figura 56

Calificación de la seguridad del sistema web



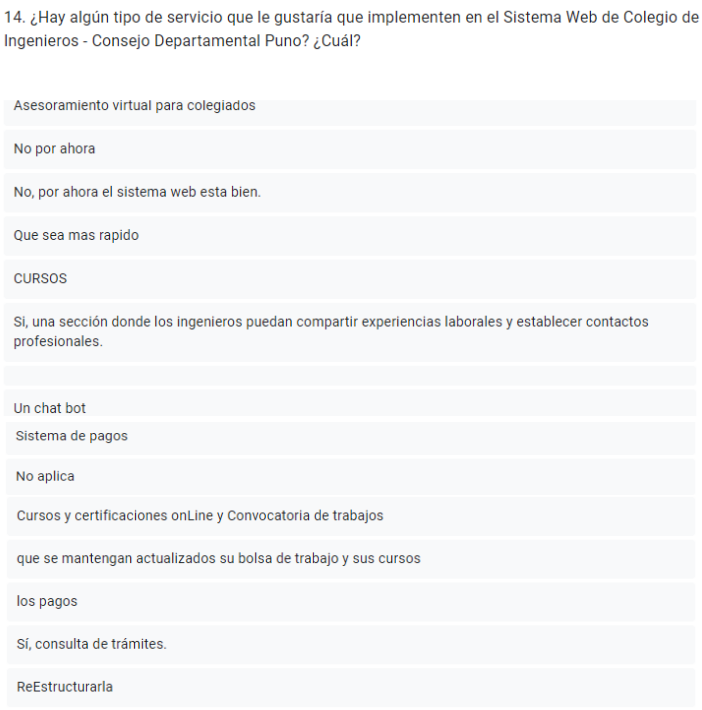
Nota: Realizado según datos de la encuesta

Interpretación

En la Figura 56 presentó la calificación de los usuarios respecto a la seguridad del sistema web del Colegio de Ingenieros del Perú, Consejo Departamental Puno. Los datos mostraron que, un 61% de los usuarios consideraron que la seguridad es media, un 33.9% opinan que la seguridad es alta y un 5.1% calificaron la seguridad como baja. Estos resultados sugirieron que la mayoría de los usuarios perciben la seguridad del sistema como adecuada pero no excepcional, lo que refleja una satisfacción general con las medidas actuales, aunque sin percibir características de seguridad más avanzadas. Aquellos que calificaron la seguridad como alta probablemente han tenido experiencias positivas o confían en las medidas implementadas, mientras que el pequeño porcentaje que la consideró baja pudieron haber enfrentado problemas menores o tener dudas sobre la protección de sus datos personales. Esto sugirió que, si bien las medidas de seguridad actuales son aceptables para la mayoría, existe una oportunidad para reforzar la seguridad del sistema mediante la implementación de protocolos más robustos, cifrado de datos más avanzado, y una mayor transparencia en la comunicación de las políticas de seguridad.

Figura 57

Servicios sugeridos para implementar en el sistema web



Nota: Realizado según datos de la encuesta

Interpretación

En la Figura 57 presentó los resultados sobre las sugerencias de los usuarios para implementar nuevos servicios en el sistema web del Colegio de Ingenieros del Perú, Consejo Departamental Puno. Los datos indican que, un 30% de los usuarios respondieron que no les gustaría que se implemente ningún servicio adicional mientras que el 70% restante sugirió implementar varios servicios, entre los cuales los más frecuentes fueron, un sistema de pago, chat bot, consulta de trámites, cursos, certificaciones online, matenimiento de bolsas de trabajo y una sección donde los colegiados puedan compartir experiencias.

Figura 58

Revisión de políticas de seguridad y privacidad al instalar software

Nota: Realizado según datos de la encuesta

Interpretación

En la Figura 58 presentó los resultados sobre la lectura de políticas de seguridad y privacidad por parte de los usuarios antes de instalar software o aplicaciones en sus ordenadores. Los datos mostraron que, un 45.5% de los usuarios afirmaron que a veces leen las políticas, 19.7% indicaron que no lo hacen, 13.1% señalan que nunca las leen, 13.1% responden que casi siempre las revisan y un 8.2% afirman que sí lo hacen. Estos resultados sugieren que la mayoría de los usuarios no siempre revisa las políticas de seguridad y privacidad antes de instalar software, lo que puede generar riesgos significativos en términos de seguridad, privacidad y experiencia del usuario. La falta de lectura de estas políticas puede llevar a los usuarios a aceptar condiciones inseguras o dar permisos excesivos sin ser conscientes de los riesgos involucrados. Esto destaca la importancia de fomentar una mayor conciencia sobre la revisión de estos documentos antes de proceder con instalaciones de software.

Figura 59

Confianza en la seguridad de las contraseñas

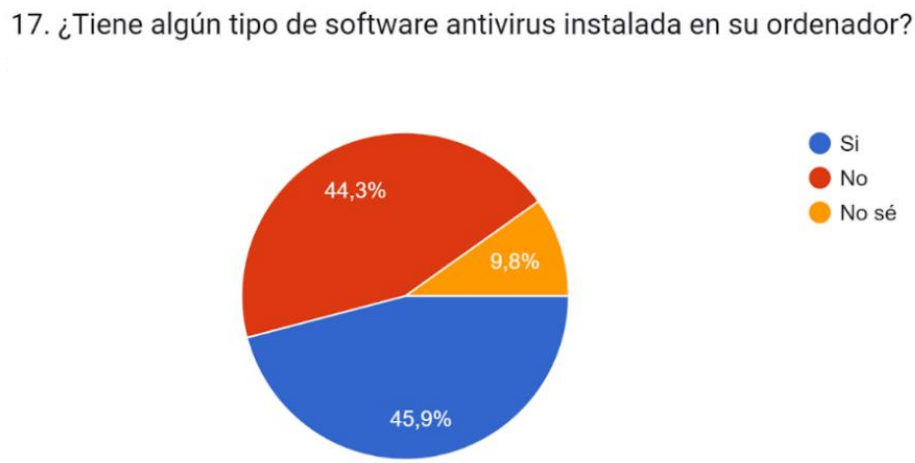
Nota: Realizado según datos de la encuesta

Interpretación

En la Figura 59 mostraron los resultados sobre la confianza de los usuarios en la seguridad de las contraseñas que crean para acceder a sistemas o sitios web. Los datos revelan que, un 45.9% de los usuarios califican la seguridad de sus contraseñas como media, 31.1% la consideran alta, 13.1% la califican como baja y un 9.8% la consideran bastante alta. Estos resultados indicaron que la mayoría de los usuarios perciben una seguridad media a alta en sus contraseñas, lo que refleja una confianza general moderada en sus prácticas de creación de contraseñas. Sin embargo, la variabilidad en la confianza sugiere que muchos usuarios todavía podrían estar expuestos a riesgos, como el uso de contraseñas débiles o reutilizadas. Esto pone de relieve la necesidad de mejorar las prácticas de seguridad, fomentando el uso de contraseñas robustas, la implementación de gestores de contraseñas. Promover estas buenas prácticas podría ayudar a proteger mejor las cuentas y los datos personales de los usuarios, reduciendo el riesgo de violaciones de seguridad o ciberataques.

Figura 60

Uso de software antivirus en el ordenado



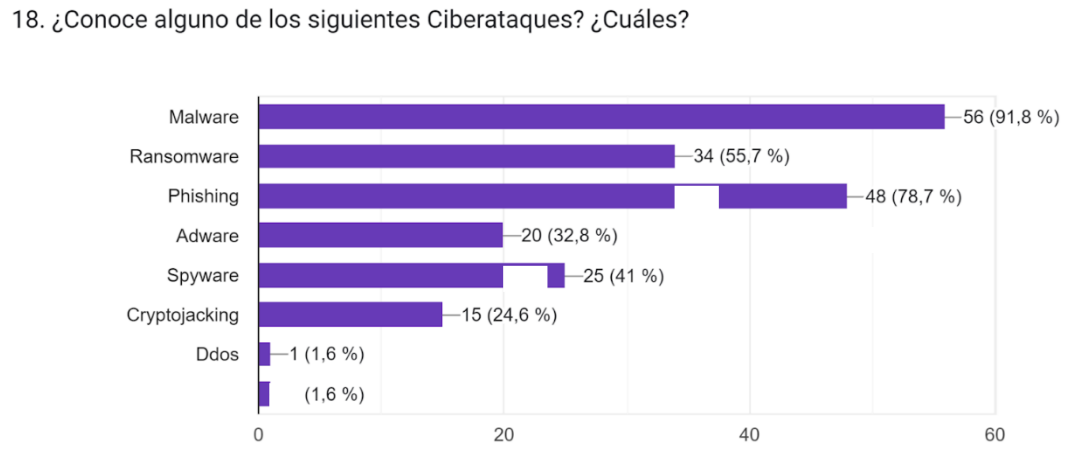
Nota: Realizado según datos de la encuesta

Interpretación

En la Figura 60 mostraron los resultados sobre la instalación de software antivirus en los ordenadores de los usuarios. Los datos indicaron que, un 45.9% de los usuarios sí tenían instalados softwares antivirus, 44.3% no tenían instalado softwares antivirus y un 9.8% no sabían si tienen o no software antivirus. Estos resultados revelan una distribución casi equilibrada entre quienes utilizan antivirus y quienes no lo utilizan, con un pequeño porcentaje de usuarios que no está seguro de su estado de protección. La ausencia de software antivirus, o la falta de claridad sobre su instalación, puede aumentar significativamente el riesgo de comprometer la seguridad del ordenador y los datos personales de los usuarios, lo que puede derivar en consecuencias graves como infecciones por malware, pérdida de información, o violaciones de privacidad. Para mitigar estos riesgos, es fundamental que los usuarios instalen y mantengan actualizado un software antivirus confiable y también que reciban educación sobre la importancia de proteger sus sistemas con herramientas de seguridad adecuadas.

Figura 61

Conocimiento de tipos de ciberataques



Nota: Realizado según datos de la encuesta

Interpretación

La Figura 61 reflejó los resultados sobre el conocimiento de ciberataques entre los usuarios. Los datos indican que, 91.8% conocen el Malware, 78.7% están familiarizados con Phishing, 55.7% conocen el Ransomware, 41% tienen conocimiento sobre Spyware, 32.8% conocen el Adware, 24.6% están informados sobre Cryptojacking, 1.6% conocen el ataque DDoS y 1.6% han oído hablar de otros tipos de ciberataques. Estos resultados muestran que los ciberataques más comunes, como el Malware y el Phishing, son ampliamente conocidos entre los usuarios, mientras que otros tipos, como DDoS y Cryptojacking, tienen menor reconocimiento.

El análisis de las figuras proporciona una visión integral sobre diversos aspectos del uso del sistema web del Colegio de Ingenieros del Perú, Consejo Departamental Puno, así como la percepción y prácticas de seguridad de los usuarios.

ANEXO 9: Declaración jurada de autenticidad de tesis

Universidad Nacional del Altiplano Puno | VRI Vicerrectorado de Investigación | Repositorio Institucional

DECLARACIÓN JURADA DE AUTENTICIDAD DE TESIS

Por el presente documento, Yo Mireya Yarumi Machaca Pampamallco,
identificado con DNI 72079976 en mi condición de egresado de:

☒ **Escuela Profesional,** ☐ **Programa de Segunda Especialidad,** ☐ **Programa de Maestría o Doctorado**
Ingeniería de Sistemas,
informo que he elaborado el/la ☒ **Tesis** o ☐ **Trabajo de Investigación** denominada:
"Análisis de riesgos del sistema de información web del Colegio de Ingenieros del Perú - Consejo Departamental Puno para identificar Vulnerabilidades y amenazas mediante la metodología OWASP - 2024"

Es un tema original.

Declaro que el presente trabajo de tesis es elaborado por mi persona y **no existe plagio/copia** de ninguna naturaleza, en especial de otro documento de investigación (tesis, revista, texto, congreso, o similar) presentado por persona natural o jurídica alguna ante instituciones académicas, profesionales, de investigación o similares, en el país o en el extranjero.

Dejo constancia que las citas de otros autores han sido debidamente identificadas en el trabajo de investigación, por lo que no asumiré como suyas las opiniones vertidas por terceros, ya sea de fuentes encontradas en medios escritos, digitales o Internet.

Asimismo, ratifico que soy plenamente consciente de todo el contenido de la tesis y asumo la responsabilidad de cualquier error u omisión en el documento, así como de las connotaciones éticas y legales involucradas.

En caso de incumplimiento de esta declaración, me someto a las disposiciones legales vigentes y a las sanciones correspondientes de igual forma me someto a las sanciones establecidas en las Directivas y otras normas internas, así como las que me alcancen del Código Civil y Normas Legales conexas por el incumplimiento del presente compromiso

Puno 21 de noviembre del 2024

FIRMA (obligatoria)

Huella

ANEXO 10: Autorización para el depósito de tesis en el Repositorio Institucional

Universidad Nacional del Altiplano Puno | VRI Vicerrectorado de Investigación | Repositorio Institucional

AUTORIZACIÓN PARA EL DEPÓSITO DE TESIS O TRABAJO DE INVESTIGACIÓN EN EL REPOSITORIO INSTITUCIONAL

Por el presente documento, Yo Miseya Yarumi Machaca Pampamallco,
identificado con DNI 72079976 en mi condición de egresado de:

☒ **Escuela Profesional,** ☐ **Programa de Segunda Especialidad,** ☐ **Programa de Maestría o Doctorado**

Ingeniería de Sistemas,

informo que he elaborado el/la ☒ **Tesis** o ☐ **Trabajo de Investigación** denominada:

" Análisis de riesgos del sistema de información web del Colegio de Ingenieros del Perú - Consejo Departamental Puno para identificar vulnerabilidades y amenazas mediante la metodología OWASP - 2024 "

para la obtención de ☐**Grado,** ☒ **Título Profesional** o ☐ **Segunda Especialidad.**

Por medio del presente documento, afirmo y garantizo ser el legítimo, único y exclusivo titular de todos los derechos de propiedad intelectual sobre los documentos arriba mencionados, las obras, los contenidos, los productos y/o las creaciones en general (en adelante, los "Contenidos") que serán incluidos en el repositorio institucional de la Universidad Nacional del Altiplano de Puno.

También, doy seguridad de que los contenidos entregados se encuentran libres de toda contraseña, restricción o medida tecnológica de protección, con la finalidad de permitir que se puedan leer, descargar, reproducir, distribuir, imprimir, buscar y enlazar los textos completos, sin limitación alguna.

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

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

Autorizo que los Contenidos sean puestos a disposición del público a través de la siguiente licencia:

Creative Commons Reconocimiento-NoComercial-CompartirIgual 4.0 Internacional. Para ver una copia de esta licencia, visita: https://creativecommons.org/licenses/by-nc-sa/4.0/

En señal de conformidad, suscribo el presente documento.

Puno 21 de noviembre del 2024

FIRMA (obligatoria) Huella