UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Metodología de técnicas OWASP para aplicaciones web java

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:

Ingeniero de Sistemas

AUTOR:

Chang del Carpio, Diego Antonio (orcid.org/0000-0002-3265-8400)

ASESORES:

Dr. Hilario Falcon, Francisco Manuel (orcid.org/0000-0003-3153-9343)

Dra. Vasquez Valencia, Yesenia Del Rosario (orcid.org/0000-0003-4682-2280)

LÍNEA DE INVESTIGACIÓN:

Auditoría de Sistemas y Seguridad de la Información

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:

Desarrollo económico, empleo y emprendimiento

LIMA – PERÚ

2023

DEDICATORIA

Este proyecto va dedicado especialmente a todas las personas que me han ayudado a seguir desarrollando la tesis y me dijeron que no me de por vencido para terminar la tesis la cual parecía imposible y terminar la carrera con todo mi esfuerzo.

AGRADECIMIENTO

A mis padres por haberme forjado como la persona que soy en la actualidad; muchos de mis logros se los debo a ustedes entre los que se incluyen este. Me formaron con reglas y con algunas libertades, pero al final me motivaron a alcanzar mis logros.

Gracias madre y padre.

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICOS Y FIGURAS

RESUMEN

El trabajo de investigación se titula “Metodología de buenas prácticas del top ten de OWASP en aplicaciones web java”. Partió de la necesidad que identificaron las empresas por medio de análisis en las aplicaciones web Java, obteniendo como resultados a las pruebas, problemas de seguridad y vulnerabilidad.

Por ello, se planteó el objetivo de identificar por medio de las consecuencias al mal uso de la programación en las aplicaciones web java. Se utilizó el uso de la metodología del Top Ten OWASP en la auditoría, adicionando tecnologías como Java, para la prevención seguridad las aplicaciones web Java.

Palabras Clave: Seguridad, análisis, aplicación web, vulnerabilidad, Java.

ABSTRACT

The research work is entitled "Methodology of good practices of the OWASP top ten in Java web applications". It started from the need identified by the companies through the analysis of Java web applications, obtaining security and vulnerability problems as a result of the tests.

Therefore, the objective was to identify the consequences of the misuse of programming in Java web applications. The use of the Top Ten OWASP methodology was used in the audit, adding technologies such as Java, for the prevention of Java web application security.

Keywords: Security, analytics, web application, vulnerability, Java.

I. INTRODUCCIÓN

En esta sección explicó temas de la realidad problemática, con las aplicaciones web Java, donde se observó que las aplicaciones web escritas en Java tienen deficiencias en el código desarrollado por el programador debido a la falta de conocimiento en el uso de la metodología de código seguro de OWASP, la cual ayuda a los programadores a poder tener controles técnicos de seguridad en aplicaciones web. Asimismo, a modo justificación teórica, es importante señalar el uso de los aspectos de seguridad como buenas prácticas de programación haciendo uso de la metodología OWASP, teniendo como resultado un nivel mayor de seguridad en las aplicaciones web debido a que esta metodología ayuda a medir los principales riesgos y amenazas de seguridad de las aplicaciones web para minimizarlos.

Esta investigación tuvo como propósito determinar la metodología de buenas prácticas del Top Ten de OWASP hacía aumento de la optimización, desarrollo de crecimiento, incremento en el conocimiento y avances del nivel de seguridad en los ataques que se dan en las aplicaciones web Java en las empresas. Finalmente, trazó como hipótesis referente a los indicadores nombrados correlativamente la metodología de buenas prácticas del Top Ten de OWASP para las aplicaciones web Java, considerando que tiene una influencia particular en la seguridad cibernética.

Se ha observado actualmente en estudios previos y antecedentes como la metodología de buenas prácticas del top ten de OWASP ayuda a entender la existencia de varios problemas causados por una programación incorrecta dentro de las aplicaciones web. Esto se debe al desarrollo de aplicaciones web por parte de los programadores sin el conocimiento de las buenas prácticas del Top Ten de OWASP. Por lo tanto, el código inseguro está abierto a ataques que se manifiestan en seguridad y controles cuestionables. Además, hoy en día las organizaciones están necesitando obtener una mejor seguridad en su programación, debido a que los hackers están haciendo ataques de mayor nivel a las empresas por medio de las nuevas tecnologías que salen y la falta de actualización tecnológica de métodos de programación que hacen que las aplicaciones queden vulnerables.

En consecuencia, Romero (2019) nos menciona que en recientes estudios tienen confirmado que la seguridad de la red es el objetivo del 75 por

ciento de los ataques cibernéticos, lo que deja en riesgo a dos tercios de todos los sistemas en línea. Los ataques contra tales aplicaciones incluyen SQL Injection, Parameter Tampering, Directory Traversal, Cross-site Request Forgery (CSFR), Denial-of-Service (DoS), Cookie Poisoning, Cross-site Scripting (XSS), Session Fixation. Este problema está muy extendido y las observaciones nacionales indican la necesidad de aplicaciones web para evitar tales obstáculos.

Debido a la gran cantidad de aplicaciones Web que se desarrollan en Java y a la Falta de conocimientos de Buenas Prácticas de Programación de Código Seguro para evitar vulnerabilidades presentes en aplicaciones web ha surgido instituciones como EC Council que han desarrollado Certificaciones de Seguridad basado en buenas prácticas de programación de código seguro en aplicaciones Java. Por lo tanto, finaliza el autor Banda (2022) refiriéndose, el ciclo del progreso de un software contiene una estructura de procesos y actividades relacionadas con el desarrollo y mantenimiento del software que garantiza seguridad, eficiencia, estabilidad y fiabilidad de uso. Dentro de las etapas de este ciclo se encuentra el desarrollo, prueba, entrega, implantación, verificación y monitoreo. Las cuales se encuentran agrupadas dentro de Desarrollo (análisis, diseño y construcción), Pruebas (test y correcciones de errores) y Entrega (control de cambios).

Esta investigación brindará a la comunidad una contribución técnica sobre el conocimiento acerca del uso de la metodología de buenas prácticas del Top Ten de OWASP en las aplicaciones web (Java).

Finalmente, la justificación tecnológica está orientado a proveer información para las empresas que les permita reducir las amenazas y aumentar el nivel de seguridad establecido para las aplicaciones web usado la metodología de Buenas Prácticas del Top Ten de OWASP, que constituye el problema de seguridad más recurrente debido a la falta de modelos de programación segura en el ciclo de vida del desarrollo de software en las organizaciones. (Menendez, 2022).

El problema de investigación general y específico surgió de una conflictiva realidad. La investigación tenía un problema general que necesitaba ser abordado: ¿Cómo influye la metodología de buenas prácticas del Top Ten de

OWASP en el nivel de seguridad para las aplicaciones web Java? Los problemas específicos de la investigación fueron los siguientes:

PE1: ¿Cómo influye la metodología de buenas prácticas del Top Ten de OWASP en la optimización en aplicaciones web Java?

PE2: ¿Cómo influye la metodología de buenas prácticas del Top Ten de OWASP en el crecimiento de aplicaciones web Java?

PE3: ¿Cómo influye la metodología de buenas prácticas del Top Ten de OWASP en el conocimiento para la programación de aplicaciones web seguras en Java?

PE4: ¿Cómo influye la metodología de buenas prácticas del Top Ten de OWASP en el nivel de seguridad para aplicaciones web Java?

El objetivo general fue determinar la influencia de metodología de buenas prácticas del Top Ten de OWASP para aumento de la optimización, desarrollo de crecimiento, incremento en el conocimiento y avances del nivel de seguridad en las aplicaciones web Java. Los objetivos específicos fueron los siguientes:

OE1: Determinar la influencia de la metodología de buenas prácticas del Top Ten de OWASP para el aumento de la optimización de aplicaciones web Java.

OE2: Determinar la influencia de la metodología de buenas prácticas del Top Ten de OWASP para el desarrollo de crecimiento de aplicaciones web Java.

OE3: Determinar la influencia de la metodología de buenas prácticas del Top Ten de OWASP para el incremento en el conocimiento de aplicaciones web Java.

OE4: Determinar la influencia de la metodología de buenas prácticas del Top Ten de OWASP para avances del nivel de seguridad de aplicaciones web Java.

Por ello, la hipótesis general planteada fue: “El uso de la metodología de buenas prácticas del Top Ten de OWASP aumentará la optimización, desarrollará un crecimiento, incrementará el conocimiento y mejorará el nivel de seguridad para aplicaciones web Java de las empresas” (Sierra Huerta, Tania. 2022). Al respecto, Sierra (2022) indica que las metodologías de desarrollo de software poseen un ambiente controlado que hace una mejora en la construcción de requerimientos de las aplicaciones, por lo que presenta mejoras en el desarrollo de aplicaciones web (p. 20). Finalmente, todo esto se cumple por buenas prácticas siguiendo la recopilación del Top Ten de OWASP.

La hipótesis específica 1 fue: “El uso de la metodología de buenas prácticas del Top Ten de OWASP aumentará la optimización en las aplicaciones web”. Zambrano y Andrade (2019) detalla que para las aplicaciones web Java

existen capas las cuales son cliente, intermedia, web, negocio y datos sirven para una mejor implementación en la aplicación web Java (p. 12). Según OWASP, se puede confiar en el desarrollo, adquisición y mantenimiento de aplicaciones y APIs debido a las mejoras realizadas en su desarrollo.

La hipótesis específica 2 fue: “El uso de la metodología de buenas prácticas del Top Ten de OWASP desarrollará un crecimiento en las aplicaciones web Java”. Al respecto, Carvaca (2022) realizó una investigación en la que mitigar las aplicaciones web con vulnerabilidades permiten disminuir riesgo de amenaza al generar un incidente de seguridad en la que conlleva a la interrupción de los procesos y genera una conciencia de seguridad al estudio en las aplicaciones web con buenas prácticas (p. 24). Según el CWE/SANS Top 25 permite enlistar los principales errores de software más peligrosos brindando una extensa descripción para cada consecuencia común, probabilidad de explotación, entre otros; en cambio el OWASP Top 10 incluye mucho más CWE orientados a aplicaciones web (p. 26).

La hipótesis específica 3 fue: “El uso de la metodología de buenas prácticas del Top Ten de OWASP incrementará el conocimiento de las aplicaciones web”. Por ello, Zapata (2019) detalla que la metodología OWASP usada por desarrolladores de software necesitan un código seguro e imprescindible de vulnerabilidades; tester de software, requieren pauta básica al efectuar diversos experimentos para seguridad y expertos en seguridad que necesitan garantizar la seguridad antes de lanzar una aplicación segura en una organización (p. 26). Además, estos deben contar con la metodología OWASP que es desarrollado principalmente por los tres módulos en que se basan la cuales son guía para el desarrollo, guía de código para revisión y guía de pruebas hacia una eficaz implementación de aplicaciones web.

La hipótesis específica 4 fue: “El uso de la metodología de buenas prácticas del Top Ten de OWASP mejorará el nivel de seguridad en las aplicaciones web Java”. Al respecto, Hernández (2020) menciona para identificar versiones de sistemas operativos, servicios y aplicaciones, obtener vulnerabilidades de seguridad comparándolas con bases de datos vulnerables y clasificar el riesgo en niveles bajo, medio y alto según la escala. (p.48).

II. MARCO TEÓRICO

En este presente capítulo explica sumario en lecciones conexas revelan similitudes hacia el trabajo de investigación, encontraron múltiples investigaciones a nivel nacional e internacional como libros, artículos, patentes, tesis, en el que prioriza medidas de manera que influye, optimiza, crecimientos vistos en revisiones a el crecimiento, conocimiento y nivel de seguridad con los beneficios, herramientas e instrumentos, así como las teorías de la metodología OWASP, utilizada en la investigación. Hacia una amplia indagación de investigaciones a diversas bases de datos, repositorios, revistas indexadas, entre otras.

En el ámbito nacional, Castro (2022) detalló en primer lugar; los ataques de inyección SQL, NoSQL, LDAP se conocen mediante el envío de datos, los cuales no aplican al sistema que está esperando por un usuario, por si en la mayoría de los casos por un comando o sentencia. En realidad, Castro (2022) indicó que los datos nocivos implementados por el atacante que negando al intérprete pudieron lograr ejecutar comandos que permiten la fuerza bruta en datos. Finalmente, Castro (2022) concluyó que los entes externos peligrosamente colocados para dar a conocer archivos internos dentro de los almacenadores en servidores los mismo que presentan desactualización frecuente, por eso se logró lanzar código de forma remota.

En el ámbito nacional, Calvo (2022) mencionó que la herramienta de OWASP es de código libre el cual debe descubrir y lidiar los orígenes que hacen que sea ambiente incierto. Además Calvo (2022) presentó compilación de indagación, a análisis de ratificación de ingresos en prácticas de parte del usuario.

En el ámbito nacional, Chinguel (2022) mencionó que hay diversos tipos de inyección, gracias a la inyección se puede comprobar porque los datos enviados por el usuario se registran como un comando o consulta, zafando al intérprete que procesa la tarea con las principales inyecciones ayudando al atacante el leer, crear, modificar o eliminar de manera arbitraria, los datos presentados en una aplicación. Además, Chinguel (2022) demostró que también Cross Site Scripting (XSS), permite secuestro en sesiones, modificación de sitios web, adecuar la elaboración de ataques de phishing. Finalmente, Chinguel (2022) demostró una sugerencia hacia las organizaciones que hacen uso

recurrente de tecnologías de información (TI) y que están dirigidas a riesgos de seguridad de la información en sus servidores web, innovando en la creencia de patrones favoritos de ataques propuestos.

En el ámbito nacional, Suárez y Yagual (2022) mencionó organización de una estructura que prueba la seguridad de la aplicación web la misma que se parte en dos: pasiva y activa; pasiva menciona que la aplicación interactúa directamente la lógica de entradas y salidas, la activa con el estudio de pruebas pasivas es más vulnerable a las pruebas de seguridad activas. Asimismo Suárez y Yagual (2022) plantea 11 categorías y 91 controles de los cuales hace uso la metodología OWASP. Finalmente, Suárez y Yagual (2022) en la metodología el objetivo se necesita personal capacitado en seguridad informática (hacker éticos) que son orientados a la búsqueda de vulnerabilidades por medio de herramientas y técnicas que utilizan los atacantes.

En el ámbito nacional, Bocanegra (2021) mencionó los problemas de vulnerabilidad XSS y Cross-Site Request Forgery (CSRF) en aplicaciones web, estas vulnerabilidades se encuentran entre las 10 vulnerabilidades más graves, lo que demuestra cómo los atacantes pueden entrar en el desarrollo web, presentando el flujo de datos de información de las mismas. Asimismo, Bocanegra (2021) estudió la problemática de los primeros diez riesgos de seguridad de aplicaciones web más relevantes, la vulnerabilidad de XSS, en el cual se observan muchas aplicaciones web demostrando ausencia de seguridad adecuada en la omisión de la validación de entrada al proceso de desarrollo. Finalmente, Bocanegra (2021) el método aceptado en las investigaciones fue aprobado por experimentación de proyectos web Java porque se elaboraron artificialmente con errores XSS, debido a que algunos proyectos web Java fueron de código abierto. Concluyendo de esta manera, se acordó que el método no solo mejoró la efectividad de detección del defecto XSS.

En el ámbito nacional, Castillo (2021) informó que por las única razón en la que se confía en esta metodología OWASP es porque los procesos a realizar son únicos y las vulnerabilidad es una debilidades en programadores. En resumen, Castillo (2021) mencionó así que los procedimientos que se tratan pueden llegar a referencia con razón en la seguridad informática y conociendo el código fuente.

En el ámbito nacional, Díaz (2021) mencionó que las más críticas vulnerabilidades gracias a las investigaciones anteriormente estudiadas es la metodología OWASP, debido a que es de relevante en el contorno de seguridad en el progreso de software. Asimismo, Díaz (2021) estudió el artículo publicado por OWASP el cual consideró soluciones específicas por medio de metodologías, técnicas y buenas prácticas para desarrollar modelos de términos orientados a seguridad del software, organizándolo por períodos.

En el ámbito nacional, Mendoza (2020) mencionó que los atacantes pueden, latentemente, utilizar diferentes rumbos a través de su estudio para perjudicar su dependencia u distribución, uno de estos vías simbolizan una inseguridad que puede o no ser competentemente difícil como para alcanzar el esmero. Además, Mendoza (2020) indicó que OWASP forma parte de una comunidad sin fines de lucro que ofrece seguridad en aplicaciones web empleando buenas prácticas hacia el periodo de edificación para adelantos hacia seguridad informática, hacia perfilado a referencias. Finalmente, Mendoza (2020) concluyó que en la comunidad de OWASP elaborada con programadores y patrocinadores orientados a la estabilidad en las aplicaciones web demuestran que garantiza mecanismos de su entorno ampara datos dentro de las aplicaciones o sistemas web.

En el ámbito nacional, Bernal (2019) realizó pruebas de seguridad de la información y tomo un proceso en la seguridad con Inyección SQL, Prueba XSS por medio de análisis estático basado en la técnica que evalúa un sistema y por medio de pruebas de penetración de caja negra, caja blanca y caja gris, las cuales son usadas en la metodología OWASP por medio de pruebas de intrusión, ethical hacking y el modelo de madurez. En conclusión, Bernal (2019) determinó que la metodología OWASP en sus proyectos puede incluir los proyectos de desarrollo y documentación en Testing Guide, Top Ten, Metodología de calificación de riesgo, estándar de comprobación de aplicaciones en seguridad usando WebScarab, filtros en validación, WebGoat, DotNet.

En el ámbito nacional, Chalabe (2019) mencionó que el programa abierto de aplicaciones de seguridad web OWASP, es una organización sin lucro en sus orígenes desde los años 2001 hasta la actualidad, como zonas de apoyo y comprobación de programas que denominan a los ataques XSS en uno de los ataque más frecuentes en las aplicaciones web. Finalmente, Chalabe (2019)

indicó que se han elaborado nuevos proyectos o programas en los que ayudan a medir fallos y amenazas en las aplicaciones web.

En el ámbito nacional, Oriundo (2019) mencionó que las aplicaciones web permiten obtener contenido, mediante creación de páginas personalizadas según un usuario, en la que esta interactúa la gestión de la compañía con la gestión de clientes, a través de una página web, las mismas que suelen encontrarse dentro de la arquitectura cliente servidor para resolver las solicitudes. Asimismo, Oriundo (2019) indicó que por ejemplo las organizaciones suelen optar por la gestión de recados, el registro de repertorio y despacho, que las prácticas comerciales suelen usar como servidores de Java EE y base de datos. Finalmente, Oriundo (2019) concluyó que los entornos ágiles son pruebas que van dirigidas al planteo de desarrollo de fases en la que estas abogan por que las prácticas y desarrollo estén completamente integradas a poder modificar la estructura de las compañías.

En el ámbito nacional, Sosa (2018) mencionó que la metodología que se utilizó fue la Programación Extrema (XP) por su condición que fue creada en las pequeñas aplicaciones, sobre todo que cambiado y reforzado por medio del antivirus que es reforzado y cambiado para encontrar mejoras necesarias por las evolución inmutable de los Malwares. Finalmente Sosa (2018) concluyó que luego del análisis del software Antivirus tiene la capacidad de encontrar enormes capacidades de revelar enormes cantidades de Malwares en las pruebas dinámicas halladas en tiempo real mediante las estrategias en la seguridad de protección de una aplicación web.

De acuerdo con el libro electrónico presentado en Colombia, Henao (2022) realizó un estudio del grado de riesgo cibernético que un evento adverso podría ocasionar un impacto; esta es la que contempla el impacto de los riesgos subyacentes en la categorización y comprobación es a través de una matriz de inconstante probabilidad en la que menciona el tipo de tecnología que debe ser esta coherente con las aplicaciones web, debido a su accesibilidad diaria en la vida de los individuos que accedan a Internet. Adicionalmente, Henao (2022) utiliza como metodología técnica a OWASP porque esta se dedica a mantener aplicaciones y API que sean confiables, en ofrecer una serie de recursos para incrementar la seguridad de las aplicaciones web y publica periódicamente un Top 10 con las contingencias más críticas, con la implementación a

repercusiones en una serie de recomendaciones para evitar riesgos. Finalmente, Henao (2022) recomienda seguir el orden de criticidad del Top 10 para 2021 de mayor a menor la cual es importante para obtener mejores resultados en los niveles de seguridad.

De acuerdo con la tesis presentado en Ecuador, Valle (2022) mencionó que la metodología OWASP instiga ser un estándar de verificación de seguridad, lo que esta produce la seguridad en una aplicación. Además, Valle (2022) aplicó su formulación en distintas situaciones en un proceso rápido y directo en demostrar la seguridad de páginas o aplicaciones web. Finalmente, Valle (2022) concluyó que después de realizar pruebas manuales que conllevó tiempo extra, es así que las pruebas acatadas por pruebas de revisión de código fuente pretenden programadores altamente capacitados para hacer la difícil tarea de buscar las vulnerabilidades.

De acuerdo con la tesis presentado en Ecuador, Zambrano (2022) indicó que para sistemas informáticos existen análisis de vulnerabilidades el cual es identificado por problemas a tratar en caso exista debilidades e impacto en la seguridad. Además, Zambrano (2022) utilizó para investigaciones del tema se utilizan libros, guías, y páginas web expertas. En conclusión, Zambrano (2022) concluyó que la investigación se hace para la obtención de solución a los problemas presentados.

De acuerdo con la tesis presentado en Ecuador, Fonseca (2021) estudió a las aplicaciones cliente/servidor que utilizan el protocolo HTTP para relacionarlas con los usuarios u otros sistemas aplicando seguridad, siendo así el resultado del avance logrado por las tecnologías de desarrollo de software, yendo al servidor web que es el elemento fundamental con aplicación en políticas de seguridad, para valerse de un sistema web seguro. Finalmente, Fonseca (2021) mencionó que una aplicación web en la parte de seguridad se divide en autenticidad, confidencialidad, disponibilidad, integridad, y trazabilidad.

De acuerdo con la tesis presentado en España, Medina (2021) estudió el modelo OWASP SAMM es un patrón sólido dirigido y proyectado a la protección en el desarrollo para edificación del software, en la que compone un marco de trabajo (framework) cuyo objetivo hacer que corporaciones puedan fundar e iniciar una táctica para desarrollo con seguridad basadas en técnicas usadas en ciclo de vida del software. Además, Medina (2021) mencionó que el patrón se ha

proyectado con un ángulo direccionado a inseguridad que aprueba a las compañías, iniciar como adaptar las buenas prácticas en función de requerimientos basado en su estado y respecto al peligro. Finalmente, Medina (2021) cabe mencionar las cinco funciones definidas en SAMM las cuales son gobierno, diseño, implementación, verificación y operación que estas se adicionan para cada práctica con un objetivo de alcance de cierto nivel de madurez que tener realizan operaciones más rígidas y métricas más rigurosas.

De acuerdo con la tesis presentado en Colombia, Luque (2021) mencionó que debes tener en cuenta en los ataques de inyección, primero agentes que amenaza otras fuentes en documentos que puede ser una resultante de inyección, movibles en el entorno, servicios web internos y externos y consumidores, errores de inyección comunes desarrollan el proceso de dirigir al atacante de datos hostiles a un usuario; luego la debilidad de seguridad se presentan con mayor frecuencia los atacantes de inyección particularmente en el código originario, y se encuentran consultas SQL, NoSQL, LDAP y Xpath, del sistema operativo comandos, SMTP en los encabezados, consultas ORM, por último el impacto de los ataques de inyección por lo que la inyección tiene un efecto negativo con pautas que estas generan una gran pérdida de datos, como también alteración o extensión de datos no licenciados, pérdida de asignación responsable o desestimación de acceso. Finalmente, Luque (2021) en resumidas cuentas una aplicación es vulnerable a inyección cuando la aplicación no válida, filtra y limpia los datos del intérprete, siendo así las consultas dinámicas o llamadas no parametrizadas estas se utilizan juntamente por el intérprete, pretendiendo esta minimizar el riesgo de tener un ataque inyección que esta se presenta en los datos de consultas alejados pero juntos por medio de consultas y comandos, y acceder a la validación de entrada desde el servidor en la “lista blanca”, que esta es conocida como una no defensa completa ya que existen en el presente aplicaciones que requieren caracteres especiales.

De acuerdo con la tesis presentado en Colombia, Santiago (2021) recomendó que antes de empezar la metodología OWASP tenemos que tener en cuenta que las aplicaciones de verificación de seguridad en entorno web, tiene por principio la verificación positiva del código efectuado en el estudio de aplicaciones web; esta se basa a que hay diferentes tipos de lenguajes de programación como los HTML, CSS, JavaScript, Java, entre otras que son vitales

para la innovación de aplicaciones web, la misma que permite hacer una estructura básica que es, servidor web con navegador es igual aplicación web. Además, Santiago (2021) menciona que esta técnica implementada es gracias a las disposiciones tomada en todo aspecto de seguridad de aplicaciones web, estas permiten justificar vulnerabilidades existentes y riesgos que presenta las distintas áreas donde se realiza el análisis que los especialistas en seguridad están en constante realización de auditorías las cuales muestran la mayor incidencia de ser atacados por ciberdelincuentes. Finalmente, Santiago (2021) menciona que los procesos de estudio de estas aplicaciones son relevantes a efectuar una revisión en sucesos que permiten divisar registros de incoherencias que presentan al evadir aplicaciones las mismas que con el tiempo se vuelven menos seguras.

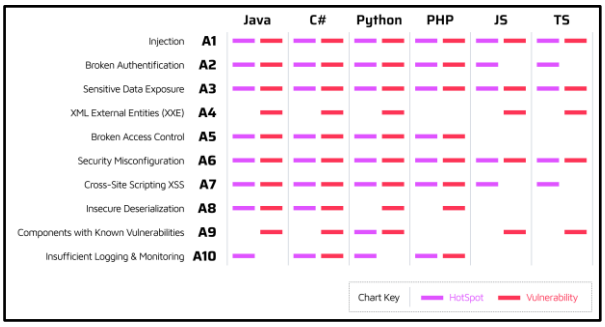


Figura 1: OWASP en lenguajes de programación

Fuente: SonarQube, 2021. https://www.sonarsource.com/solutions/security/owasp/

De acuerdo con el articulo científico presentado en India, Aliero (2020) mencionó que existen nuevas vulnerabilidades en el entorno cibernético de nivel alto en las aplicaciones, cuyo estándar realiza un seguimiento de vulnerabilidades que exhiben mayor inseguridad para que cualquier empresa adapte aplicaciones web. Finalmente, Aliero (2020) concluyó que está para crear conocimiento entre las personas a fin de sujetar el riesgo de ser perseguido en resultados a vulnerabilidades nuevas mediante informes mensuales y anuales que muestran las principales debilidades del Top 10.

De acuerdo con el articulo científico presentado en España, Mateo (2020), el análisis interactivo, la capacidad de monitorear y analizar el código mientras se ejecuta, se ha establecido como una herramienta primordial en la investigación de seguridad, nos permite el análisis de seguridad preciso basado en el tiempo de ejecución de información. Las herramientas IAST son de caja blanca y son una evolución de las herramientas SAST. Ellas permiten análisis de

código, pero estas se hacen en tiempo real y debe integrarse de forma interactiva con la herramienta DAST. Además, Mateo (2020) menciona que estas herramientas son las que se diferencian, debido a que su ejecución es de manera directa al servidor y se integra con la aplicación. Finalmente, Mateo (2020) concluye que los monitoreos del comportamiento de las aplicaciones en todas sus capas de flujo del estudio y el flujo de datos hacen viables escenarios de polémicas que estas deben ser observadas cuidadosamente.

De acuerdo con la tesis presentada en Colombia, Osorio (2020) realizó una revisión a la guía de pruebas de OWASP y obtuvo una herramienta en el progreso del software en el ciclo de vida, estas recomendaciones en seguridad, están diseñadas, codificadas o implementadas para reducir el nivel de riesgo frente a amenazas directas en las aplicaciones o servicios. Finalmente, Osorio (2020) concluye en las recomendaciones concebidas a partir de resultados en pruebas y recomendaciones de uso de métodos OWASP como referencia para el refuerzo de aplicaciones web.

De acuerdo con la tesis presentada en Ecuador, Tasan (2020) aplicó metodología de seguridad, determinando las vulnerabilidades con el objetivo de verificar los procedimientos para ello existen distintas las metodologías como: National Institute of Standards and Technology (NIST SP 800-115), Open Source Security Testing Methodology Manual (OSSTMM), Penetration Testing Execution Standard (PTES), Information Systems Security Assessment Framework (ISSAF) y Open Web Application Security Project (OWASP), lo cual, permitió enfocarse en la ciberseguridad en las distintas aplicaciones web, en la que se plasma los resultados del nivel de seguridad en porcentaje de cada metodología, después de ser evaluadas.

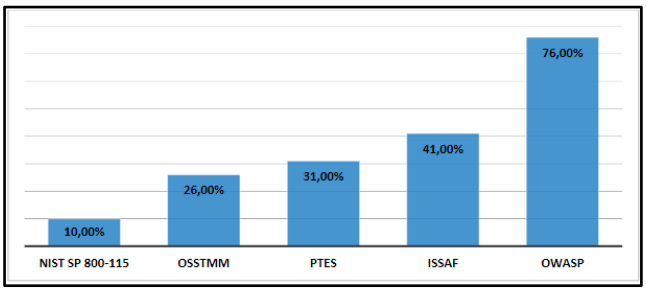


Figura 2: Porcentaje de Seguridad de las Metodologías

Fuente: Tasan, 2020

Finalmente Tasan (2020) realizó un estudio a la metodología OWASP de las vulnerabilidades del Top 10 de aplicaciones web, donde se propone a las

organizaciones formarlas en el uso de TICs por resultados presentes en vulnerabilidades de seguridad establecidas a las aplicaciones web. Estas 10 vulnerabilidades se plasman en la Figura 3.

1	• Inyección
2	• Pérdida de Autenticación
3	• Exposición de datos sensibles
4	• Entidades Externas XML (XXE)
5	• Pérdida de Control de Acceso
6	• Configuración de Seguridad Incorrecta
7	• Secuencia de Comandos en Sitios Cruzados (XSS)
8	• Deserialización Insegura
9	• Componentes con vulnerabilidades conocidas
10	• Registro y Monitoreo Insuficientes

Figura 3: Top Ten OWASP

Fuente: OWASP, 2017

De acuerdo con la tesis presentado en España, Varela (2020) propuso los datos de análisis en tres puntos: económico, técnico y de mercado. A continuación, Varela (2020) indicó en la vista viable de economía existen tres recursos humanos, software y hardware en la que como objetivo de realización a las aplicaciones web, existen múltiples softwares con código abierto adecuadas para esta realización. Seguidamente, Valera (2020) reveló en la vista viable de técnica tener en cuenta la experiencia previa del desarrollador de tecnologías, reduciendo así el riesgo si cabe. Asimismo, Varela (2020) presentó en la vista de mercado se centra más en las actividades diarias de los usuarios, las que gestionan actividades de aplicaciones en software de la cual se va a conseguir en las tareas centradas en análisis según el resultado de informes, ya que esto se debe al mercado principalmente rígido a las pequeñas y medianas empresas. Finalmente, Varela (2020) recomendó que hay que tener una planificación y análisis de costos en el desenvolvimiento de la protección de software por medio de costo y tiempo consiguiendo así un resultado óptimo.

De acuerdo con la tesis presentado en Colombia, Moreno (2019) mencionó que en su proyecto, esté realizó el estudio de una aproximación al objeto en punto a el dominio técnico en la marcha a los conceptos de su huella social que hace la búsqueda de varios conocimientos. Sin embargo, Moreno (2019) por otra parte suele mencionar que la inyección SQL es una vulnerabilidad más catastrófica que afectan a las compañías, generando un aprovechamiento de todo el dato íntimo allegado a una aplicación con base de datos en que esta incluye datos como nombre de usuario, credenciales, nombre, direcciones,

teléfono, tarjetas de créditos, entre otros datos de suma relevancia en la que la vulnerabilidad se genera por medio de SQL, el cual atacantes aprovechan la sintaxis y capacidad del propio SQL, para así ser una funcionalidad hacia el sistema operativo disponible en la base de datos. Finalmente, Moreno (2019) concluyó que no son necesariamente cláusulas cuya estructura están siendo determinadas de modo deliberado por el atacante y estas pueden acarrear consecuencias no deseadas hacia el propietario y los usuarios que cumplen los objetivos del vector de ataque.

De acuerdo con la tesis presentado en España, Ortega (2018) se sostiene que todas las organizaciones que ofrecen servicios en internet deben garantizar una cuidadosa protección de su información y recursos. En este sentido, Ortega (2018) señaló la importancia de asegurar los sistemas críticos, ya que las aplicaciones web son susceptibles a tres tipos de ataques: anónimos, de integridad y de denegación de servicios. En resumen, Ortega (2018) terminó de ver que la seguridad y configuración de las aplicaciones en los principales servidores que van hacia el mercado, deben ser distinguidos por el control de acceso de recursos de las aplicaciones que permiten restringir el acceso según el rol permitido.

III. METODOLOGÍA

3.1 Tipo y diseño de investigación

3.1.1 Tipo de investigación

El tipo de investigación cuantitativo fue aplicada. Al respecto, Arias (2020) explicó que el tipo de investigación aplicada proporciona el tipo fundamental, debido a su conjetura responsabilizada en descifrar inconvenientes eficaces en base a aciertos, innovaciones y salidas por lo que trató en una aplicación a fondo (p. 43). Dicho de otra manera, su ejecución indaga resolver problemas de un proyecto que investiga y compendia información para alcanzar desconocido conocimiento por parte del investigador, la cual fue aplicada para buscar desconocidos enfoques en solventar temas de metodologías técnicas como OWASP.

El trabajo actual de investigación fundamentó un estudio de diferentes informaciones obtenidas por fundamentos de metodologías en enfoque cuantitativo, esto nos lleva a utilizar materias estadísticas para recolección optima.

Hernández y Mendoza (2018), una investigación cuantitativa comprende la recolección en informes usando materias de análisis en variable de estudio, por lo que requiere concretar el resultado de la hipótesis y la variable (p. 226). También, la investigación incorpora particularidades iniciando en la proyección de la hipótesis, el concepto de las variables de manera conceptual y operacional.

Después los estudios cuantitativos, obtiene la aprobación y reafirmación en sucesos situados en la investigación, indagando vínculos casuales de órdenes hacia componentes. Por consiguiente, para esta investigación se requiere lograr que el problema sea formulado con claridad y que permita la posibilidad de realizar pruebas, todo esto debe validarse en las teorías de estudio (Gonzáles, 2021, p. 5). Es por ello, que se realizará un estudio cuantitativo donde buscaremos reafirmar las teorías comenzando por las hipótesis de la investigación.

Ochoa, Nava y Fusil (2020) precisaron un enfoque cuantitativo basado en la intuición probabilística del realismo universal, la medida sutil, inspeccionada y neutral, consintiendo al experto realizar deducciones profundas de los informes, el desarrollo afirmativo inferencial racional, encaminado al suceso aplicando

valores consistentes y continuos (p. 5). En conclusión, este diseño se lleva a cabo siguiendo lo anteriormente desarrollado.

3.1.2 Diseño de investigación

- El diseño para la presente investigación fue experimental. Arias (2020) explicó que los diseños experimentales son un procedimiento cuya característica primordial es verificar cuantitativamente la casualidad de la variable, por ello involucra el empleo con variable independiente sobre variable dependiente, así requerimos plan gestión donde instituir períodos en el tema de interposición o carácter en nivelación establecido por medidas de jerarquías (p. 46). Además, Arias (2020) recomendó que en los esquemas señalados a la variable independiente simboliza el método, elemento, situaciones, interposición donde el analista opera, inspecciona los resultados variables dependiente. Resumiendo, observamos la variable determinante aplicada por indagación.
- El tipo de diseño de investigación tocó preexperimental. Arias (2020) explicó que al trabajar con este estudio resulta necesidad de validez interna y externa. Para esta investigación se eligió estudio de una sola mención, ya que se debe realizar antes y después pruebas para el uso de la aplicación.

Figura 4: Diseño preexperimental

$$G = O1\ X\ O2$$

Donde:

- G = Grupo de sujetos
- X = Aplicación del tratamiento en grupo experimental de variable independiente
- O1 = Medición de la variable dependiente (Pre test)
- O2 = Medición de la variable dependiente (Post test)

(Arias, 2020, p.47)

3.2 Variables y operacionalización

La variable en estudio subsistió la influencia metodología de técnicas OWASP en aplicaciones web java. Presenta una matriz de operacionalización de variables en el anexo. Otro modo, delimita cada fase:

Definición conceptual: Las metodología de técnicas de OWASP en proceso de aplicaciones web java que hace uso de código abierto hacia mejora y protección de la web; se recomienda codificación segura, detección de riesgos y evaluación de proceso, en las cuales se consideran las 10 amenazas más frecuentes que pueden sufrir las aplicaciones web (Sierra Huertas, Tania. 2022).

Definición operacional: La influencia de la metodología técnicas OWASP aumenta la optimización, desarrollando crecimiento e incrementa en el conocimiento y avances de niveles de seguridad en las aplicaciones web Java (Sierra Huertas, Tania. 2022).

Dimensiones:

- Optimización (Sierra Huertas, Tania. 2022).
- Crecimiento (Carvaca Orrala, Ana Luisa. 2022).
- Conocimiento (Zapata, Juliana, et al. 2019).
- Nivel de seguridad (Zambrano, Grace Marcela y Andrade, María. 2019).

Indicadores:

- Aumento de la optimización (Sierra Huertas, Tania. 2022).
- Desarrollo de crecimiento (Carvaca Orrala, Ana Luisa. 2022).
- Incremento en el conocimiento (Zapata, Juliana, et al. 2019).
- Avances del nivel de seguridad (Zambrano, Grace Marcela y Andrade, María. 2019).

Instrumento:

- Guía de Observación

Escala de medición:

- Escala Ordinal

3.3 Población, muestra, muestreo, unidad de análisis

3.3.1 Población

La población seleccionada en la investigación está orientada a empresas que desarrollan aplicaciones web basada en Java, para poder adquirir conocimiento en buenas prácticas del Top Ten de OWASP que se pueden desarrollar a través de servicios de Ethical Hacking en empresas hacia la búsqueda de vulnerabilidades de sus aplicaciones web y por último el aprendizaje para los programadores y especialistas en el ámbito metodológico de buenas prácticas del Top Ten de OWASP.

Criterios de inclusión: Para la muestra serán los siguientes: Empresas que desarrollan aplicaciones web basada en Java a nivel nacional.

Criterios de exclusión: Aquellas empresas que desarrollan aplicaciones web en otros lenguajes de programación como .Net, PHP, Python y otros diferentes a Java.

3.3.2 Muestra

La muestra estará compuesta por empresas peruanas que desarrollan aplicaciones web basada en Java como empresas pequeñas, medianas y grandes, utilizando criterios de inclusión y exclusión específicos. Por ello, la muestra de estudio conformado por 50 empresas que se encargan de desarrollar aplicaciones web con java para la prueba piloto. Asimismo, se considerará el consentimiento informado de los participantes debidamente firmados. En síntesis, se va emplear el cálculo de la muestra para el estudio de investigación, tal como se evidencia:

Fórmula para muestra:

$$\alpha = \frac{K}{K-1}\left[1 - \frac{\sum S_i^2}{S_t^2}\right]$$

Donde:

K: El número de ítems

S_i^2: Sumatoria de Varianzas de los Ítems

S_t^2: Varianza de la suma de los Ítems

α: Coeficiente de Alfa de Cronbach

$$\alpha = \frac{16}{16-1}\left[1 - \frac{15.202}{44.76}\right]$$

$$\alpha = 0.7044$$

Se determina que para la prueba piloto del estudio se realiza como muestra 17 empresas que se encargan del desarrollo de aplicaciones web.

3.3.3 Muestreo

La técnica de muestreo que se desarrollará es muestreo estratificado. De modo que se identificarán las vulnerabilidades presentes en las empresas con aplicaciones web basadas en java. Esto admitirá adquirir una muestra representativa de empresas 50 empresas.

La ejecución de esta técnica de muestreo consentirá extender la representatividad de la muestra y conseguir resultas a nivel nacional. Además,

al utilizar un enfoque estratificado, se lograrán comparar en análisis entre las diferentes empresas, lo que adquiere descubrimiento y admitirá conclusiones más compactas.

En resumen, para el presente estudio se seleccionará la muestra más conveniente de empresas nacionales con desarrollo de aplicaciones web basadas en java, utilizando los criterios de inclusión y exclusión específicos.

3.3.4 Unidad de análisis

En el marco de este proyecto de investigación, se ha elegido a empresas que trabajan desarrollan aplicaciones web basadas en java. Esta elección se fundamenta en el potencial del campo de estudio en cuestión.

3.4 Técnicas e instrumentos de recolección de datos

3.4.1 Técnica

Esta sección desarrollará utilizando herramientas en análisis de vulnerabilidades de aplicaciones web para la identificación de brechas de seguridad basados en las buenas prácticas del Top Ten de OWASP. Algunas de las herramientas a utilizar serán: Burp Suite Professional y OWASP ZAP.

La recolección de datos de vulnerabilidades presentes en estas empresas, permitirá identificar las brechas de seguridad más frecuentes en organizaciones nacionales permitiendo compararlas con las estadísticas de OWASP a nivel internacional, permitiéndonos conocer la falta de conocimiento en las Buenas prácticas del Top Ten de OWASP, lo que permitirá poder hacer recomendaciones de buenas prácticas de código seguro para la mitigación de las brechas de las vulnerabilidades presentes en las aplicaciones web en java.

Useche (2019), la guía de observación es una método estructurado para recopilar información sobre la variable específica que se está investigando. Se considera que esta técnica es crucial para obtener datos precisos que reflejen la realidad. Esta se lleva a cabo en una entrevista, en la que de manera de interés a la investigación es utilizada para ser observación de la investigación por medio de los aspectos a observar de forma general e identifica una variable y los elementos a observar del mismo.

3.4.2 Instrumento

Asimismo, se tomó particularidades del instrumento para la recopilación de información para calcular la variable donde se usó un cuestionario acerca de la

"Influencia de la Metodología de Buenas Prácticas del Top Ten de OWASP en Aplicaciones web Java".

Tabla 1: Ficha técnica

Nombre de la Prueba:	Guía de Observación de Auditoría sobre la Influencia de la Metodología de Buenas Prácticas Del Top Ten de OWASP en Aplicaciones Web Java
Autor:	Diego Antonio Chang del Carpio
Procedencia:	Propio realizado por el investigador
Administración:	Directa
Tiempo de aplicación:	15 minutos
Ámbito de aplicación:	Está enfocado hacia el área de programación o de desarrollo de aplicaciones web
Significación:	Explicar Cómo está compuesta la escala a nivel de (dimensiones, áreas, ítems por área, explicación breve de cuál es el objetivo de medición)

3.4.3 Validez

La validación se desarrolló con el propósito de la adquisición de una guía de observación, con el propósito de adquirir un formulario de preguntas que permite recolectar los datos que posteriormente se van a evaluar. Al respecto, Arias (2020) menciono que la validación no es necesaria cuando la guía de observación es validada estadísticamente por expertos, debido a que la información sociodemográfica de las empresas.

3.4.4 Confiabilidad

Previamente a este paso, se desarrolló una prueba piloto a 17 empleados de distintas empresas, cuyos datos recolectados se analizaron con el uso de la estadística Alfa de Cronbach para precisar su confiabilidad. De manera relacionada, Ñaupas et al. (2018), estas herramientas muestran confiabilidad si no muestran cambios en los datos medidos y los resultados no cambian en el tiempo ni se adaptan a diferentes temas de investigación. Esta cualidad garantiza la fiabilidad de la prueba. Esta consideración fue esencial en la elaboración de la investigación, ya que los instrumentos se basaron en autores cuyas obras verifican de manera adecuada la variable que se pretende medir.

Tabla 2: Estadística de confiabilidad Influencia de la metodología de buenas prácticas del Top Ten de OWASP en aplicaciones web java

Estadísticas de fiabilidad

Alfa de Cronbach	N de elementos
,701	16

En la tabla 2, se puede observar el resultado de la prueba de Alfa de Cronbach aplicada a la variable "Influencia de la Metodología de Buenas Prácticas del Top Ten de OWASP en Aplicaciones web Java" es 0.701. Como la consistencia interna es de 0.701 se encuentra entre el rango de 0.70 y 0.80. Entonces el instrumento es Aceptable para pasar la prueba de confiabilidad y se valida su uso para la presente investigación.

3.5 Procedimientos

Este procedimiento consiente fundar una consigna entre las técnicas para su mejoría, respaldado en la calidad asociada a ellos. Enseguida, incluyen grupos estadísticos suministrando procesamiento y disminuyendo equidad resultante (Medina et al., 2019).

Por otra parte, la selección en la muestra final utilizara 50 empresas que deseen ser evaluadas de manera gratuita como parte de la investigación. Además de poseer aplicaciones web. Esto fue examinado con herramientas de escaneo de vulnerabilidades de aplicaciones web permitiendo resultados que sean documentados y permitan obtener los logros deseados.

La metodología de Buenas Prácticas del Top Ten de OWASP permite a las empresas desarrollar y contribuir a la mejora del ciclo de vida del software. Así que la medida de las indicaciones del aumento de la optimización, desarrollo de crecimiento, incremento en el conocimiento y avances del nivel de seguridad se ejecutó a través de evaluaciones y presentación de resultados. En conclusión, el desarrollo de las pruebas favoreció a las aplicaciones web y permitió la expansión y mejora del ciclo de vida del desarrollo de código, es así que podemos listar las actividades a desarrollar a continuación:

En primer lugar, desarrollar las actividades en cronograma mencionando cada uno de los puntos a desarrollar, para que más adelante se pueda recopilar e identificar aplicaciones web basadas en Java, para poder desarrollar las evaluaciones basado en la metodología de buenas prácticas del Top Ten de OWASP, con respecto a ello seguir con la tarea de analizar las vulnerabilidades

utilizando herramientas de escaneo de vulnerabilidades web como Burp Suite y OWASP Suite buscando los puntos más débiles de las aplicaciones web y poder modelar las amenazas identificadas para poder presentar recomendaciones acordes a las vulnerabilidades encontradas, con este resultado se va a elaborar informes donde se cumple el objetivo final que da resultados a la simulación de los ataques para implementar mejoras y refuerzos en los sistemas de seguridad y finalmente, empleo la aplicación de la metodología de Buenas Prácticas del Top Ten de OWASP, entrega de resultados que permitan a las organizaciones aumentar la optimización, el crecimiento, e incremento en el conocimiento y avance del nivel de seguridad.

3.6 Método de análisis de datos

Este periodo examina como puntualiza una técnica observada, adecuada para proyecto de investigación.

Esta parte se basa en la observación de los resultados de las pruebas efectuadas a las empresas y en recopilación de las vulnerabilidades encontradas basadas en la metodología de Buenas Prácticas del Top Ten de OWASP que permita poder identificar las vulnerabilidades presentes en las aplicaciones web desarrolladas en Java.

Hernández y Mendoza (2018) determinaron una escala Likert, método perfeccionado por Rensis Likert en 1932, aún todavía conocido radicando un vínculo con piezas mostradas a manera de informaciones con criterios reconocidos por partícipes (p. 245). De esta forma, Rodríguez y Reguant (2020) afirmaron que Cronbach planteó el coeficiente alfa en 1951 concluye dar fiabilidad en estadística como un instrumento de escala de actitudes, debido a que se expresa la consistencia entre los ítems del cuestionario se debe tener una interpretación adecuada y utilización del mismo, es así que la escala tipo Likert, en sus resultados, cuando dan cinco o más categorías de respuesta y cuando prevalece un número conveniente de sujetos.

Hernández y Mendoza (2018) determinaron que la observación es un método en forma sistemática, efectiva y confiable, el cual observan comportamientos y situaciones en diferentes categorías y subcategorías. Esta técnica de recolección de información no obstructiva está dirigido a conductas y procesos del cual se puede adaptar por medio de eventos tal como ocurren por

la evaluación de hechos, conductas y no mediciones indirectas las cuales estas son complejas para categorizar las conductas observadas, este método de análisis del dato resulta ser costosa y difícil de interpretarse.

Además, se emplean herramientas estadísticas como SPSS y Microsoft Excel para procesar, recopilar y analizar los datos obtenidos. Se opta por utilizar gráfica debido a su estructura dimensional, que emplea rectángulos con bases iguales y alturas proporcionales a la frecuencia.

3.7 Aspectos éticos

En la resolución de consejo universitario N° 0340-2021 de la Universidad César Vallejo se determinó que el Código de Ética de Investigación es necesario para conocidos que anhelan cumplir una investigación científica en la UCV. Se han aplicado los siguientes principios éticos:

Se evita cualquier tipo de lesión o daño de acuerdo con el principio de "no hacer trampa". Asimismo, se fomentan las actividades filantrópicas para el bienestar de los sujetos de investigación, enfocándose en comprender sus beneficios y mejorar la recuperación de acuerdo con el principio de "filantropía". Se valoran y respetan la libertad y las elecciones individuales de los participantes, esto les habilita para tomar decisiones informadas y proceder de condición autónoma, en consonancia con el principio de "autonomía". Además, debe asegurarse de que todos los participantes de la investigación reciban un trato justo y equitativo, y que compartan completamente los riesgos, beneficios y costos relevantes, y se adhieran al principio de "equidad".

Asimismo cumplió del Colegio de Ingenieros del Perú el código de ética relacionados con artículos 13 y 15. Desde el artículo 13° observamos conducta y comportamiento profesional del ingeniero, cuyos propósitos sean ideales y afines a la Institución; también, verificó con el artículo 15° donde se aprendió acerca de legalidad profesional, solidaridad, considero, justicia, inclusión sindical, integridad, responsabilidad y dignidad profesional, considerando las partes mismas en investigación (Colegio de Ingenieros, 1999, p. 2-3).

Dado al acatamiento a principios bioéticos de la Unesco (Organización de las Naciones Unidas para la Cultura, las Ciencias y la Educación) adaptó "Declaración Universal de Bioética y Derechos Humanos". Del mismo modo, estos especialistas de la UNESCO (2003) indicaron del artículo 23 el cual ha implantar bioética promoviendo nociones relacionadas en esta "Declaración"

percibiendo alto valor ético del avance científico y tecnológico que los estados incumben desvelarse por entablar absolutas condiciones de iniciación y escuadra tocantes en todos los niveles de la bioética, fomentando un impulso de programas informativos y expansivos al conocimiento de bioética y que sean evaluaciones y encaminadas por multitudes específicas, esencialmente investigadores e integrantes al comité de ética o público (p. 7).

De esta misma forma, aquellos elementos primordiales en la elaboración de la investigación con estudio en metodología técnica de OWASP; para ello, los profesionales y especialistas en el área de TI fueron vitales; además, se demostró que la metodología provocó a certificar que la revisión de seguridad de un proyecto web forma conveniente, aseverando que examinamos todos los puntos clave para descubrir cualquier fallo de seguridad categorizado en riesgo que proponen una serie de acciones, en las que estas son implantadas por profesionales, para proteger sus desarrollos.

De este modo, este trabajo de investigación desempeñó las bases éticas profesionales y las nociones de la bioética. De la misma forma, se acató la autenticidad de los exámenes y autenticidad de los datos distribuido a los partícipes. En definitiva, desempeña la actuación concreta en el cuadro lógico respectivo.

IV. RESULTADOS

Este capítulo describe los resultados obtenidos en la investigación basándose en los indicadores con respecto al aumento de optimización, desarrollo de crecimiento, incremento en el conocimiento, mejora en el nivel de seguridad evaluando la influencia de la metodología de Buenas prácticas del Top Ten de OWASP en aplicaciones Web Java entre distintas empresas.

4.1. Hipótesis específica 1

$HE1_0$: El uso de la metodología de buenas prácticas del Top Ten de OWASP no aumentó la optimización en las aplicaciones web.

$HE1_1$: El uso de la metodología de buenas prácticas del Top Ten de OWASP aumentó la optimización en las aplicaciones web.

Datos estadísticos del aumento de optimización

Para este indicador se realizó un análisis con un grupo de 50 empresas que se dedican al desarrollo de aplicaciones web, mediante la realización de la metodología técnica de OWASP en aplicaciones web java. A continuación, según el enfoque se detallan cuadros estadísticos basado en una guía de observación de pre y post, donde se consiguió medir el aumento de optimización al finalizar del enfoque de la metodología técnica de OWASP en aplicaciones web java.

Indicador del aumento de optimización

En la tabla 3 se muestra las medias de ambas pruebas realizadas en el pre y post prueba aplicado en este estudio del aumento de optimización.

Tabla 3: Indicador estadístico del aumento de optimización en las aplicaciones web

	Media	
	Estadístico	Desv. Error
Aumento de Optimización - Post	3,22	,096
Aumento de Optimización - Pre	3,04	,090

En la tabla 3 se visualiza la mejora en el nivel de seguridad hacia las aplicaciones web donde las empresas que se encargan de desarrollar aplicaciones web, donde en la guía de observación en el aumento de optimización (antes de usar la metodología OWASP) se obtuvo una media de 3.04 y la guía de observación en el nivel de seguridad (después de usar la metodología OWASP) con una media 3.22, donde se muestra un incremento en el aumento de optimización de

0.18 después de emplear la metodología OWASP. El porcentaje de aumento de optimización se calcula de la siguiente manera:

AO = Aumento de optimización

NPOST = Aumento de optimización post-test

NPRE = Aumento de optimización pre-test

$$AO = \frac{[APOST - APRE]}{APRE} * 100\%$$

$$AO = \frac{[3.22 - 3.04]}{3.04} * 100\%$$

$$AO = 5.921\%$$

Prueba de normalidad

En la prueba de normalidad se aplicó el método de Shapiro-Wilk, ya que la muestra para el indicador tuvo 50 empresas que se encargaron de estudiar o aplicar la metodología técnica de OWASP y con ello lograron obtener el uso de código seguro dentro de su aplicación web. A continuación, se detallarán los resultados para ambas pruebas del pre y post (antes y después) donde se puede visualizar en la tabla 3.

Nivel de significancia: 5%

Regla de decisión:

- Si p ≤ 0.05; Se rechaza la hipótesis nula (**$HO1_0$**)
- Si p > 0.05; Se acepta la hipótesis nula (**$HO1_0$**)

Decisión de estadística

Dado que el valor de p obtenido es igual a 0.000 y es menor que el nivel de significancia α establecido en 0.05, hay evidencia concluyente para rechazar la hipótesis nula. Este hallazgo respalda la afirmación de que los datos siguen una distribución no normal.

Tabla 4: Prueba de Shapiro-Wilk de la hipótesis específica 1

	Shapiro-Wilk		
	Estadístico	gl	Sig.
Aumento de Optimización - Pre	,789	50	,000
Aumento de Optimización - Post	,784	50	,000

Donde:

Aumento de Optimización Pre-Test

La tabla 4 muestra que los resultados después de aplicar la prueba de normalidad a partir de los datos medidos en el aumento de optimización pre-test, se obtuvo que el nivel es menor a 0.05, lo que indica que la muestra no se ajusta a la distribución normal.

Aumento de Optimización Post-Test

La tabla 4 muestra que los resultados después de aplicar la prueba de normalidad a partir de los datos medidos en el aumento de optimización post-test, se obtuvo que el nivel es menor a 0.05, lo que indica que la muestra no se ajusta a la distribución no normal.

Prueba de Wilcoxon

En la tabla 5 se muestra la prueba de Wilcoxon de manera detallada.

Tabla 5: Prueba de rangos con signo de Wilcoxon – Aumento de optimización hacia la metodología técnica de OWASP

Rangos				
		N	Rango promedio	Suma de rangos
Aumento de Optimización - Pre - Aumento de Optimización - Post	Rangos negativos	9[a]	5,00	45,00
	Rangos positivos	0[b]	,00	,00
	Empates	41[c]		
	Total	50		
a. Aumento de Optimización - Pre < Aumento de Optimización - Post				
b. Aumento de Optimización - Pre > Aumento de Optimización - Post				
c. Aumento de Optimización - Pre = Aumento de Optimización - Post				

En la tabla 6 se muestra la estadística de prueba Z sobre el aumento de optimización en el uso de la metodología técnica de OWASP.

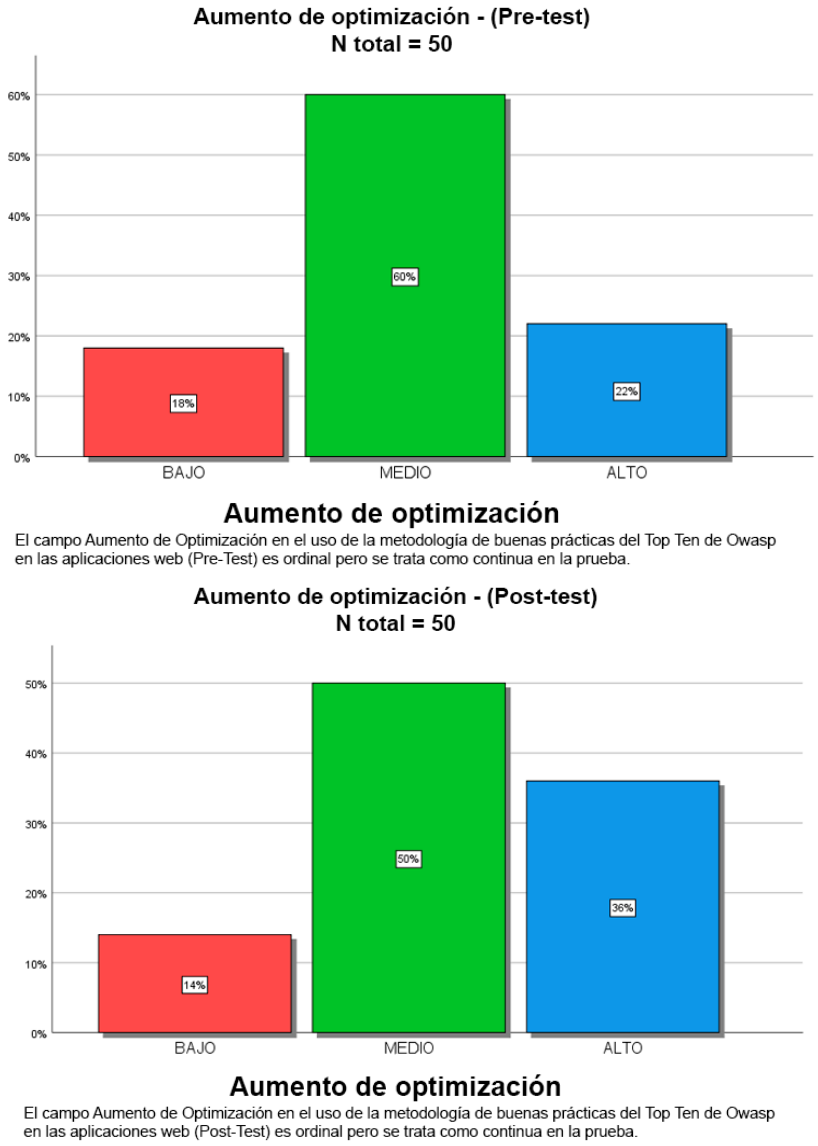
Tabla 6: Estadística de prueba Z – Aumento de optimización en la metodología OWASP

Estadísticos de prueba[a]	
	Aumento de Optimización - Pre - Aumento de Optimización - Post
Z	-3,000[b]
Sig. asintótica(bilateral)	,003
a. Prueba de rangos con signo de Wilcoxon	
b. Se basa en rangos positivos.	

Luego de realizar el análisis de los datos mediante el SPSS en la zona Z de la tabla 6, se consiguió -3.000, la cual se encontró en la región de rechazo y se

obtuvo un valor de p = 0.003 < 0.05, por lo tanto, se rechaza la $HE1_0$ y se acepta la $HE1_1$; por lo tanto, se aceptó que “El uso de la metodología de técnicas OWASP aumentará la optimización en las aplicaciones web Java” con un incremento de desarrollo de crecimiento del 5.921%.

Figura 5: Aumento de optimización en el uso de la metodología de buenas prácticas del Top Ten de OWASP en las aplicaciones web (Pre-Test vs Post-Test)



Según los resultados presentados en la tabla, existe evidencia estadística que respalda el rechazo de la hipótesis nula, lo que permite concluir que la implementación de la metodología de técnicas de OWASP para aplicaciones web java mejora de manera significativa el aumento de la optimización. Además, se puede observar en la figura un incremento en el aumento de la optimización, pasando de un nivel regular a uno considerado como bueno.

4.2. Hipótesis específica 2

$HE2_0$: El uso de la metodología de buenas prácticas del Top Ten de OWASP no desarrolló un crecimiento en las aplicaciones web Java.

$HE2_1$: El uso de la metodología de buenas prácticas del Top Ten de OWASP desarrolló un crecimiento en las aplicaciones web Java.

Datos estadísticos del desarrollo de crecimiento

Para este indicador se realizó un análisis con un grupo de 50 empresas que se dedican al desarrollo de aplicaciones web, mediante la realización de la metodología técnica de OWASP en aplicaciones web java. A continuación, según el enfoque se detallan cuadros estadísticos basado en una guía de observación de pre y post, donde se consiguió medir el aumento de optimización al finalizar del enfoque de la metodología técnica de OWASP en aplicaciones web java.

Indicador del desarrollo de crecimiento

En la tabla 7 se muestra las medias de ambas pruebas realizadas en el pre y post prueba aplicado en este estudio del indicador del desarrollo de crecimiento.

Tabla 7: Indicador estadístico del desarrollo de crecimiento en las aplicaciones web

	Media	
	Estadístico	Desv. Error
Desarrollo de Crecimiento - Post	3,14	,107
Desarrollo de Crecimiento - Pre	3,08	,102

En la tabla 7 se visualiza la mejora en el desarrollo de crecimiento hacia las aplicaciones web donde las empresas que se encargan de desarrollar aplicaciones web, donde en la guía de observación en el nivel de seguridad (antes de usar la metodología OWASP) se obtuvo una media de 3.08 y la guía de observación en el nivel de seguridad (después de usar la metodología OWASP) con una media 3.36, donde se muestra un incremento en la mejora en el nivel de seguridad de 0.28 después de emplear la metodología OWASP. El porcentaje de incremento del desarrollo de crecimiento se calcula de la siguiente manera:

DC = Desarrollo de crecimiento

NPOST = Desarrollo de crecimiento post-test

NPRE = Desarrollo de crecimiento pre-test

$$DC = \frac{[DPOST - DPRE]}{DPRE} * 100\%$$

$$DC = \frac{[3.14 - 3.08]}{3.08} * 100\%$$

$$DC = 1.948\%$$

Prueba de normalidad

En la prueba de normalidad se aplicó el método de Shapiro-Wilk, ya que la muestra para el indicador tuvo 50 empresas que se encargaron de estudiar o aplicar la metodología técnica de OWASP y con ello lograron obtener el uso de código seguro dentro de su aplicación web. A continuación, se detallarán los resultados para ambas pruebas del pre y post (antes y después) donde se puede visualizar en la tabla 7.

Nivel de significancia: 5%

Regla de decisión:

- Si p ≤ 0.05; Se rechaza la hipótesis nula (**$HO2_0$**)
- Si p > 0.05; Se acepta la hipótesis nula (**$HO2_0$**)

Decisión de estadística

Dado que el valor de p obtenido es igual a 0.000 y es menor que el nivel de significancia α establecido en 0.05, hay evidencia concluyente para rechazar la hipótesis nula. Este hallazgo respalda la afirmación de que los datos siguen una distribución no normal.

Tabla 8: Prueba de Shapiro-Wilk de la hipótesis específica 2

	Shapiro-Wilk		
	Estadístico	gl	Sig.
Desarrollo de Crecimiento - Pre	,802	50	,000
Desarrollo de Crecimiento - Post	,807	50	,000

Donde:

Desarrollo de Crecimiento Pre-Test

La tabla 8 muestra que los resultados después de aplicar la prueba de normalidad a partir de los datos medidos en el desarrollo del crecimiento pre-test, se obtuvo que el nivel es menor a 0.05, lo que indica que la muestra no se ajusta a la distribución normal.

Desarrollo de Crecimiento Post-Test

La tabla 8 muestra que los resultados después de aplicar la prueba de normalidad a partir de los datos medidos en el desarrollo del crecimiento post-test, se obtuvo que el nivel es menor a 0.05, lo que indica que la muestra no se ajusta a la distribución normal.

Prueba de Wilcoxon

En la tabla 9 se muestra la prueba de Wilcoxon de manera detallada.

Tabla 9: Prueba de rangos con signo de Wilcoxon – Desarrollo de crecimiento hacia la metodología técnica de OWASP

Rangos				
		N	Rango promedio	Suma de rangos
Desarrollo de Crecimiento Pre - Desarrollo de Crecimiento Post	Rangos negativos	3[a]	2,00	6,00
	Rangos positivos	0[b]	,00	,00
	Empates	47[c]		
	Total	50		
a. Desarrollo de Crecimiento - Pre < Desarrollo de Crecimiento - Post				
b. Desarrollo de Crecimiento - Pre > Desarrollo de Crecimiento - Post				
c. Desarrollo de Crecimiento - Pre = Desarrollo de Crecimiento - Post				

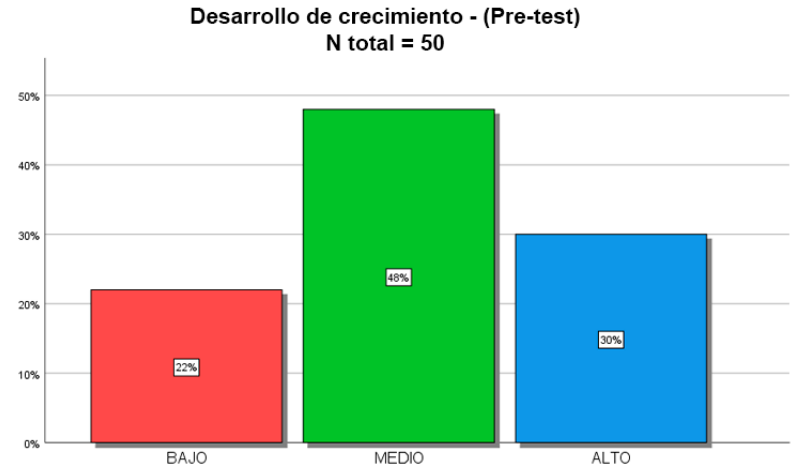
En la tabla 10 se muestra la estadística de prueba Z sobre el desarrollo de crecimiento en el uso de la metodología técnica de OWASP.

Tabla 10: Estadística de prueba Z – Desarrollo de Crecimiento en la metodología OWASP

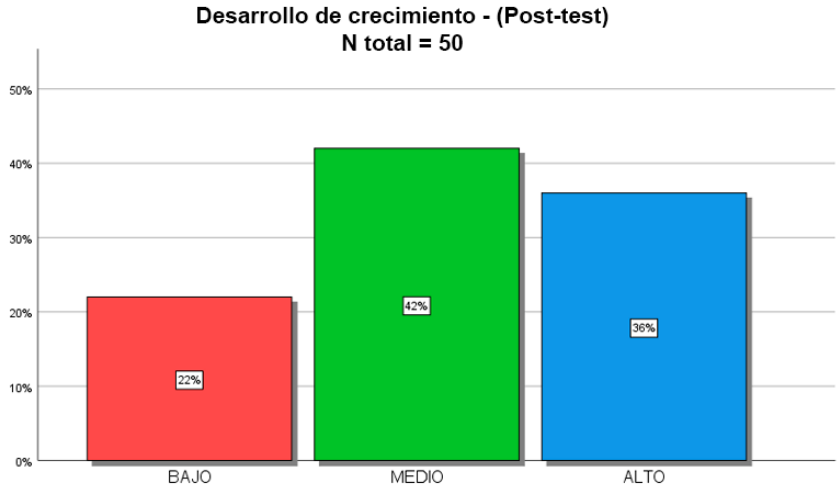
Estadísticos de prueba[a]	
	Desarrollo de Crecimiento Pre - Desarrollo de Crecimiento Post
Z	-1,732[b]
Sig. asintótica(bilateral)	,083
a. Prueba de rangos con signo de Wilcoxon	
b. Se basa en rangos positivos.	

Luego de realizar el análisis de los datos mediante el SPSS en la zona Z de la tabla 11, se consiguió -1.732, la cual se encontró en la región de rechazo y se obtuvo un valor de $p = 0.083 > 0.05$, por lo tanto, se acepta la $HE2_0$ y se rechaza la $HE2_1$; por lo tanto, se aceptó que “El uso de la metodología de buenas prácticas del Top Ten de OWASP no desarrollará un crecimiento en las aplicaciones web Java” debido a que tiene un incremento de desarrollo de crecimiento del 1.948%.

Figura 6: Desarrollo de crecimiento en el uso de la metodología de buenas prácticas del Top Ten de OWASP en las aplicaciones web (Pre-Test vs Post-Test)



El campo Desarrollo de Crecimiento en el uso de la metodología de buenas prácticas del Top Ten de Owasp en las aplicaciones web (Pre-Test) es ordinal pero se trata como continua en la prueba.



El campo Desarrollo de Crecimiento en el uso de la metodología de buenas prácticas del Top Ten de Owasp en las aplicaciones web (Post-Test) es ordinal pero se trata como continua en la prueba.

Según los resultados presentados en la tabla, existe evidencia estadística que respalda el rechazo de la hipótesis nula, lo que permite concluir que la implementación de la metodología de técnicas de OWASP para aplicaciones web java mejora de manera significativa el desarrollo de crecimiento. Además, se puede observar en la figura un incremento en el desarrollo de crecimiento, pasando de un nivel regular a uno considerado como bueno.

4.3. Hipótesis específica 3

HE3$_0$: El uso de la metodología de buenas prácticas del Top Ten de OWASP no incrementó el conocimiento de las aplicaciones web.

HE3$_1$: El uso de la metodología de buenas prácticas del Top Ten de OWASP incrementó el conocimiento de las aplicaciones web.

Datos estadísticos del incremento en el conocimiento

Para este indicador se realizó un análisis con un grupo de 50 empresas que se dedican al desarrollo de aplicaciones web, mediante la realización de la metodología técnica de OWASP en aplicaciones web java. A continuación, según el enfoque se detallan cuadros estadísticos basado en una guía de observación de pre y post, donde se consiguió medir el aumento de optimización al finalizar del enfoque de la metodología técnica de OWASP en aplicaciones web java.

Indicador del incremento en el conocimiento

En la tabla 11 se muestra las medias de ambas pruebas realizadas en el pre y post prueba aplicado en este estudio del indicador del conocimiento.

Tabla 11: Indicador estadístico del incremento del conocimiento en las aplicaciones web

	Media	
	Estadístico	Desv. Error
Incremento del Conocimiento - Post	3,26	,085
Incremento del Conocimiento - Pre	3,12	,089

En la tabla 11 se visualiza la mejora en el incremento del conocimiento hacia las aplicaciones web donde las empresas que se encargan de desarrollar aplicaciones web, donde en la guía de observación en el nivel de seguridad (antes de usar la metodología OWASP) se obtuvo una media de 3.12 y la guía de observación en el nivel de seguridad (después de usar la metodología OWASP) con una media 3.26, donde se muestra un incremento en la mejora en el nivel de seguridad de 0.14 después de emplear la metodología OWASP. El porcentaje del incremento del conocimiento se calcula de la siguiente manera:

IC = Incremento del conocimiento

IPOST = Incremento del conocimiento post-test

IPRE = Incremento del conocimiento pre-test

$$IC = \frac{[IPOST - IPRE]}{IPRE} * 100\%$$

$$IC = \frac{[3.26 - 3.12]}{3.12} * 100\%$$

$$IC = 4.487\%$$

Prueba de normalidad

En la prueba de normalidad se aplicó el método de Shapiro-Wilk, ya que la muestra para el indicador tuvo 50 empresas que se encargaron de estudiar o aplicar la metodología técnica de OWASP y con ello lograron obtener el uso de código seguro dentro de su aplicación web. A continuación, se detallarán los resultados para ambas pruebas del pre y post (antes y después) donde se puede visualizar en la tabla 11.

Nivel de significancia: 5%

Regla de decisión:

- Si p ≤ 0.05; Se rechaza la hipótesis nula (**$HO3_0$**)
- Si p > 0.05; Se acepta la hipótesis nula (**$HO3_0$**)

Decisión de estadística

Dado que el valor de p obtenido es igual a 0.000 y es menor que el nivel de significancia α establecido en 0.05, hay evidencia concluyente para rechazar la hipótesis nula. Este hallazgo respalda la afirmación de que los datos siguen una distribución no normal.

Tabla 12 Prueba de Shapiro-Wilk de la hipótesis específica 3

	Shapiro-Wilk		
	Estadístico	gl	Sig.
Incremento del Conocimiento - Pre	,755	50	,000
Incremento del Conocimiento - Post	,777	50	,000

Donde:

Incremento del Conocimiento Pre-Test

La tabla 12 muestra que los resultados después de aplicar la prueba de normalidad a partir de los datos medidos en el incremento del conocimiento pre-test, se obtuvo que el nivel es menor a 0.05, lo que indica que la muestra no se ajusta a la distribución normal.

Incremento del Conocimiento Post-Test

La tabla 12 muestra que los resultados después de aplicar la prueba de normalidad a partir de los datos medidos en el incremento del conocimiento post-test, se obtuvo que el nivel es menor a 0.05, lo que indica que la muestra no se ajusta a la distribución normal.

Prueba de Wilcoxon

En la tabla 13 se muestra la prueba de Wilcoxon de manera detallada.

Tabla 13: Prueba de rangos con signo de Wilcoxon – Incremento del conocimiento hacia la metodología técnica de OWASP

Rangos				
		N	Rango promedio	Suma de rangos
Incremento del Conocimiento Pre - Incremento del Conocimiento Post	Rangos negativos	7[a]	4,00	28,00
	Rangos positivos	0[b]	,00	,00
	Empates	43[c]		
	Total	50		
a. Incremento del Conocimiento Pre-Test < Incremento del Conocimiento Post-Test				
b. Incremento del Conocimiento Pre-Test > Incremento del Conocimiento Post-Test				
c. Incremento del Conocimiento Pre-Test = Incremento del Conocimiento Post-Test				

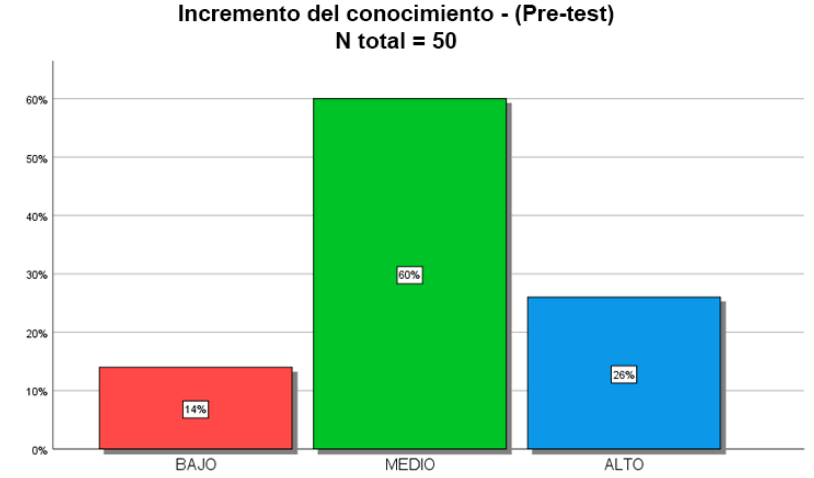
En la tabla 14 se muestra la estadística de prueba Z sobre el incremento del conocimiento en el uso de la metodología técnica de OWASP.

Tabla 14: Estadística de prueba Z – Incremento del Conocimiento en la metodología OWASP

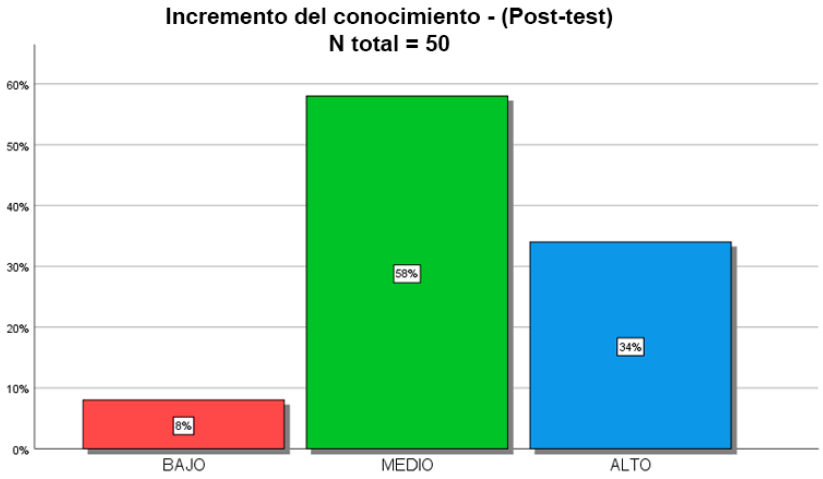
Estadísticos de prueba[a]	
	Incremento del Conocimiento Pre-Test - Incremento del Conocimiento Post-Test
Z	-2,646[b]
Sig. asintótica(bilateral)	,008
a. Prueba de rangos con signo de Wilcoxon	
b. Se basa en rangos negativos.	

Luego de realizar el análisis de los datos mediante el SPSS en la zona Z de la tabla 14, se consiguió -3.156, la cual se encontró en la región de rechazo y se obtuvo un valor de $p = 0.008 < 0.05$, por lo tanto, se rechaza la $HE3_0$ y se acepta la $HE3_1$; por lo tanto, se aceptó que "El uso de la metodología de técnicas OWASP incrementará el conocimiento de las aplicaciones web Java" con un incremento de mejora en el incremento del conocimiento del 4.487%.

Figura 7: Incremento del conocimiento en el uso de la metodología de buenas prácticas del Top Ten de OWASP en las aplicaciones web (Pre-Test vs Post-Test)



El campo Incremento del Conocimiento en el uso de la metodología de buenas prácticas del Top Ten de Owasp en las aplicaciones web (Pre-Test) es ordinal pero se trata como continua en la prueba.



El campo Incremento del Conocimiento en el uso de la metodología de buenas prácticas del Top Ten de Owasp en las aplicaciones web (Post-Test) es ordinal pero se trata como continua en la prueba.

Según los resultados presentados en la tabla, existe evidencia estadística que respalda el rechazo de la hipótesis nula, lo que permite concluir que la implementación de la metodología de técnicas de OWASP para aplicaciones web java mejora de manera significativa el incremento del conocimiento. Además, se puede observar en la figura un incremento en el incremento del conocimiento, pasando de un nivel regular a uno considerado como bueno.

4.4. Hipótesis específica 4

$HO4_0$: El uso de la metodología de buenas prácticas del Top Ten de OWASP no mejoró el nivel de seguridad en las aplicaciones web Java.

$HE4_1$: El uso de la metodología de buenas prácticas del Top Ten de OWASP mejoró el nivel de seguridad en las aplicaciones web Java.

confirma que los datos siguen una distribución normal.

Datos estadísticos de la mejora en el nivel de seguridad

Para este indicador se realizó un análisis con un grupo de 50 empresas que se dedican al desarrollo de aplicaciones web, mediante la realización de la metodología técnica de OWASP en aplicaciones web java. A continuación, según el enfoque se detallan cuadros estadísticos basado en una guía de observación de pre y post, donde se consiguió medir el aumento de optimización al finalizar del enfoque de la metodología técnica de OWASP en aplicaciones web java.

Indicador de la mejora en el nivel de seguridad

En la tabla 15 se muestra las medias de ambas pruebas realizadas en el pre y post prueba aplicado en este estudio del indicador del nivel de seguridad.

Tabla 15: Indicador estadístico del nivel de seguridad en las aplicaciones web

	Media	
	Estadístico	Desv. Error
Mejora en el Nivel de seguridad - Post	3,42	,091
Mejora en el Nivel de seguridad - Pre	3,26	,094

En la tabla 15 se visualiza la mejora en el nivel de seguridad hacia las aplicaciones web donde las empresas que se encargan de desarrollar aplicaciones web, donde en la guía de observación en el nivel de seguridad (antes de usar la metodología OWASP) se obtuvo una media de 3.26 y la guía de observación en el nivel de seguridad (después de usar la metodología OWASP) con una media 3.42, donde se muestra un incremento en la mejora en el nivel de seguridad de 0.16 después de emplear la metodología OWASP. El porcentaje de incremento de la mejora en el nivel de seguridad se calcula de la siguiente manera:

MN = Mejora en el nivel de seguridad

NPOST = Nivel de seguridad post-test

NPRE = Nivel de seguridad pre-test

$$MN = \frac{[NPOST - NPRE]}{NPRE} * 100\%$$

$$MN = \frac{[3.42 - 3.26]}{3.26} * 100\%$$

$$MN = 4.907\%$$

Prueba de normalidad

En la prueba de normalidad se aplicó el método de Shapiro-Wilk, ya que la muestra para el indicador tuvo 50 empresas que se encargaron de estudiar o aplicar la metodología técnica de OWASP y con ello lograron obtener el uso de código seguro dentro de su aplicación web. A continuación, se detallarán los resultados para ambas pruebas del pre y post (antes y después) donde se puede visualizar en la tabla 15.

Nivel de significancia: 5%

Regla de decisión:

- Si p ≤ 0.05; Se rechaza la hipótesis nula (**$HO3_0$**)
- Si p > 0.05; Se acepta la hipótesis nula (**$HO3_0$**)

Decisión de estadística

Dado que el valor de p obtenido es igual a 0.000 y es menor que el nivel de significancia α establecido en 0.05, hay evidencia concluyente para rechazar la hipótesis nula. Este hallazgo respalda la afirmación de que los datos siguen una distribución no normal.

Tabla 16 Prueba de Shapiro-Wilk de la hipótesis específica 4

	Shapiro-Wilk		
	Estadístico	gl	Sig.
Mejora en el Nivel de seguridad - Pre	,781	50	,000
Mejora en el Nivel de seguridad - Post	,679	50	,000

Donde:

Mejora en el Nivel de seguridad Pre-Test

La tabla 16 muestra que los resultados después de aplicar la prueba de normalidad a partir de los datos medidos en la mejora en el nivel de seguridad pre-test, se obtuvo que el nivel es menor a 0.05, lo que indica que la muestra no se ajusta a la distribución normal.

Mejora en el Nivel de seguridad Post-Test

La tabla 16 muestra que los resultados después de aplicar la prueba de normalidad a partir de los datos medidos en la mejora en el nivel de seguridad post-test, se obtuvo que el nivel es menor a 0.05, lo que indica que la muestra no se ajusta a la distribución normal.

Prueba de Wilcoxon

En la tabla 17 se muestra la prueba de Wilcoxon de manera detallada.

Tabla 17: Prueba de rangos con signo de Wilcoxon – Mejora en el nivel de seguridad hacia la metodología técnica de OWASP

Rangos				
		N	Rango promedio	Suma de rangos
Mejora en el Nivel de seguridad - Pre - Mejora en el Nivel de seguridad - Post	Rangos negativos	7[a]	4,00	28,00
	Rangos positivos	0[b]	,00	,00
	Empates	43[c]		
	Total	50		
a. Mejora en el Nivel de seguridad - Pre < Mejora en el Nivel de seguridad - Post				
b. Mejora en el Nivel de seguridad - Pre > Mejora en el Nivel de seguridad - Post				
c. Mejora en el Nivel de seguridad - Pre = Mejora en el Nivel de seguridad - Post				

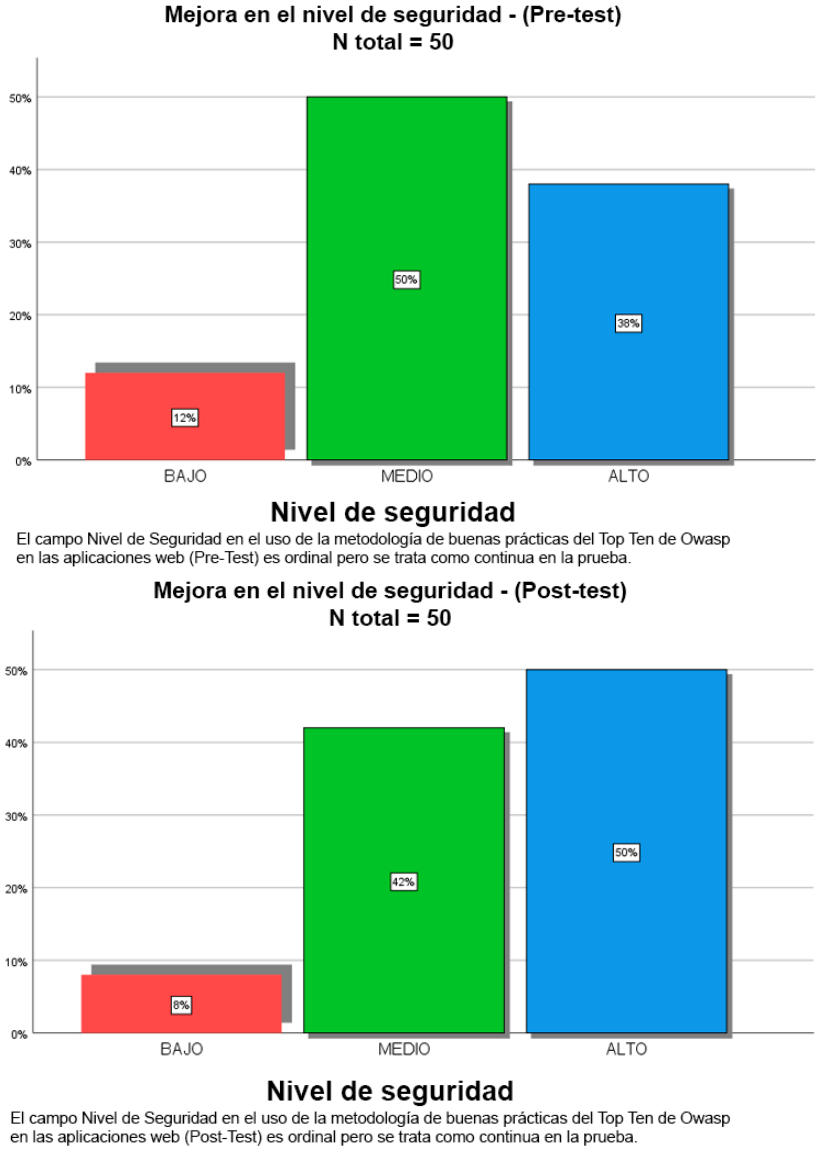
En la tabla 18 se muestra la estadística de prueba Z sobre la mejora en el nivel de seguridad en el uso de la metodología técnica de OWASP.

Tabla 18: Estadística de prueba Z – Mejora en el nivel de seguridad en la metodología OWASP

Estadísticos de prueba[a]	
	Mejora en el Nivel de seguridad - Pre - Mejora en el Nivel de seguridad - Post
Z	-2,530[b]
Sig. asintótica(bilateral)	,011
a. Prueba de rangos con signo de Wilcoxon	
b. Se basa en rangos positivos.	

Luego de realizar el análisis de los datos mediante el SPSS en la zona Z de la tabla 18, se consiguió -2.530, la cual se encontró en la región de rechazo y se obtuvo un valor de $p = 0.011 < 0.05$, por lo tanto, se rechaza la $HE4_0$ y se acepta la $HE4_1$; por lo tanto, se aceptó que "El uso de la metodología de buenas prácticas del Top Ten de OWASP mejorará el nivel de seguridad en las aplicaciones web Java" con un incremento de mejora en el nivel de seguridad del 4.907%.

Figura 8: Nivel de Seguridad en el uso de la metodología de buenas prácticas del Top Ten de OWASP en las aplicaciones web (Pre-Test vs Post-Test)



Según los resultados presentados en la tabla, existe evidencia estadística que respalda el rechazo de la hipótesis nula, lo que permite concluir que la implementación de la metodología de técnicas de OWASP para aplicaciones web java mejora de manera significativa el nivel de seguridad. Además, se puede observar en la figura una mejora en el nivel de seguridad, pasando de un nivel regular a uno considerado como bueno.

4.5. Prueba de hipótesis general

Dado que se acepta las condiciones determinadas en las hipótesis 1, 2, 3 y 4. Finalmente, se aceptó la hipótesis general: “El uso de la metodología de buenas prácticas del Top Ten de OWASP aumentará la optimización, desarrollará un

crecimiento, incrementará el conocimiento y mejorará el nivel de seguridad para aplicaciones web Java de las empresas".

4.6. Resumen de las hipótesis

A continuación, se muestra en la tabla 19 indicando un resumen de los resultados de la comparación de las hipótesis planteadas en este estudio:

Tabla 19: Resumen de los resultados de las hipótesis de la investigación

Cód.	Hipótesis	Resultado (Aceptado o Rechazada)
HE1	El uso de la metodología de buenas prácticas del Top Ten de OWASP aumentará la optimización en las aplicaciones web	Aceptada
HE2	El uso de la metodología de buenas prácticas del Top Ten de OWASP desarrollará un crecimiento en las aplicaciones web Java	Rechazada
HE3	El uso de la metodología de buenas prácticas del Top Ten de OWASP incrementará el conocimiento de las aplicaciones web	Aceptada
HE4	El uso de la metodología de buenas prácticas del Top Ten de OWASP mejorará el nivel de seguridad en las aplicaciones web Java	Aceptada
HG	El uso de la metodología de buenas prácticas del Top Ten de OWASP aumentará la optimización, desarrollará un crecimiento, incrementará el conocimiento y mejorará el nivel de seguridad para aplicaciones web Java de las empresas	Aceptada

Como se detalla en la Tabla 19, los resultados demuestran la aceptación de las hipótesis actualmente propuestas. Esto conduce al logro de los objetivos generales y específicos, lo que resulta en un aumento significativo en el nivel de optimización hasta un 5.921%. Además, los desarrolladores de aplicaciones web que implementaron las 10 mejores prácticas principales de OWASP lograron un aumento del 1.948 % en el conocimiento, un aumento del 4.487 % en el conocimiento y una mejora del 4.907 % en la seguridad.

V. DISCUSIÓN

En general, la metodología técnica de OWASP favoreció al ser aplicado para fomentar el uso de las buenas prácticas del código seguro en la programación de aplicaciones web java, ya que de esta manera se logró el objetivo de aumentar la optimización, desarrollar el crecimiento, incrementar en el conocimiento y mejorar en el nivel de seguridad hacia los programadores de aplicaciones en las empresas. Se obtuvo como resultado lo siguiente: el aumento de optimización en 5.921%, el desarrollo de crecimiento en 1.948%, el incremento del conocimiento en 4.487%, la mejora en el nivel de seguridad en 4.907%, en lo que concierne a la aplicación de la metodología técnica de OWASP. De esta manera, se demostró que la metodología técnica de OWASP en aplicaciones web java es una metodología que fomenta el desarrollo en el código seguro por medio de librerías de desarrolladas hacia las aplicaciones web java y que tiene buenos resultados para la variable descrita.

Se encontró que la implementación de la metodología OWASP en aplicaciones web java aumento en la optimización. Según Castro (2022) subraya que es de suma importancia el uso de la metodología técnica de OWASP debido a que esta ayuda mitigar los ataques de inyección que son enviados como datos nocivos implementados que permiten su ejecución por medio de la fuerza bruta la cual es peligrosamente colocada dentro de los servidores de las empresas que hay alojan su aplicación web.

Estos resultados fueron estudiados por Calvo (2022) indica que la metodología OWASP aumenta la optimización de 5.921% con una muestra de 50 empresas que se dedican al desarrollo de aplicaciones web, debido a que es libre de uso y que cualquier programador está libre de usarla y gracias a ello es vital para poder conseguir código seguro en el transcurso de desarrollo de las aplicaciones web. De modo que Calvo (2022) muestra que si no se hace uso de ello presentamos complicaciones en la ratificación de ingresos en las prácticas de uso de la aplicaciones web.

Además, los resultados de las pruebas del estudio muestran que en una escala de 1 a 4, el valor promedio pre-prueba de es 3,04 y el valor promedio post-prueba es 3,22, lo que proporciona una mejora de optimización del 5,921%. Al respecto, Chinguel (2019) debido a que en la metodología OWASP se pueden

hacer exámenes por medio de comandos que estas se desarrollan con el objetivo de obtener una mayor seguridad. Por lo tanto, Chinguel (2022) menciona hay que tener un adecuado estudio de los ataques de inyección y phishing que debemos informar a los del área de tecnología de información (TI) y con ello evitar riesgos de seguridad en los servidores web.

Estos resultados fueron estudiados por Suárez y Yagual (2022), quienes mencionaron que la tasa de crecimiento de las aplicaciones web seguras en una muestra de 50 empresas fue de 1.948%, ya que consta de dos partes: pasiva y activa. Por ello, Suárez y Yagual (2022) da a conocer que estas actúan por medio de pruebas las cuales son parte fundamental del objetivo de la metodología OWASP, en la que todo personal capacitado en seguridad informática necesita emplear por medio de herramientas y técnicas.

Además, los resultados de la prueba de encuesta mostraron que en una escala de 1 a 4, la puntuación pre-prueba de 3.12 y post-prueba de 3.26, lo que arroja una tasa de crecimiento del 1,948%. Por lo tanto, por medio de Bocanegra (2021) se puedo dar a conocer que si no se desarrolla el crecimiento en los desarrolladores de las aplicaciones web puede genera problemas en el código seguro porque surge en transcurso del desarrollo web por parte de los atacantes y esta a su vez hace que los proyectos web java tengan errores y vulnerabilidades. Asimismo, Bocanegra (2021) presenta un proyecto por medio del resultado de estudio en la metodología y da a conocer un método que hace mejoras en la efectividad de detecciones.

Estos resultados fueron estudiados por Castillo (2021) sugiere que la razón de uso y confianza de la metodología OWASP en el incremento de conocimiento es 4.487% con una muestra de 50 empresas la cuales dan por qué el código debe ser más seguro. Concluye, Castillo (2021) según la prueba la metodología OWASP mejora implementado una invulnerabilidad por parte de los programadores en la seguridad del código fuente y dar un código seguro con uso de las buenas prácticas.

De esta forma, los resultados de la prueba de investigación arrojaron una media de pre-prueba de 3.12 y post-prueba de 3.26 en una escala de 1 al 4 obteniendo un incremento del conocimiento de 4.487%. Por lo que, Díaz (2021)

en su estudio con respecto a nuestro análisis también su halló una mejoría por parte del uso de la metodología OWASP, y es así que incremento el conocimiento de los desarrolladores. De esta manera, Díaz (2021) considera que el uso de las buenas prácticas orientadas a seguridad se muestra en el nivel de seguridad del software.

Estos resultados fueron estudiados por Bernal (2019) indica que por medio de las pruebas realizadas el nivel de seguridad es 4.907% con una muestra de 50 empresas que establecen en que el código seguro de las aplicaciones web de las cuales se han realizado en la prueba de ethical hacking deben tener medidas baja, media y alta. Además Bernal (2019) incluye que la documentación de la metodología OWASP se califica como un estándar de comprobación de aplicaciones web en la parte de seguridad.

De modo que, los resultados de la prueba de investigación dieron una media de pre-prueba de 3.26 y post-prueba de 3.42 en una escala de 1 al 4 obteniendo un mejora en el nivel de seguridad de 4.907%. Sin embargo, Chalabe (2019) indica que es fundamental el nivel de seguridad en las aplicaciones web con el uso de las buenas prácticas del Top Ten de OWASP. De esta manera, Chalabe (2019) presenta que en la actualidad existe la zona de apoyo y comprobación por parte de programas que siguen el estándar de la metodología de OWASP. Finalmente, Chalabe (2019) indica que para nuevos proyectos esta genera medida de fallos en las amenazas.

VI. CONCLUSIONES

Las conclusiones de la investigación fueron las presentes:

1. Se logró aumentar la optimización en un 5.921%, debido a que la metodología técnica de OWASP logró avivar el desarrollo de las buenas prácticas en los programadores o desarrolladores de aplicaciones web, además de la posibilidad de aprender la metodología acorde a las necesidades que se presentan.
2. En cuanto al desarrollo de crecimiento se logró incrementar un 1.948%, puesto que la metodología brinda información específica en cuanto al código seguro en el desarrollo de las aplicaciones web.
3. Se obtuvo un incrementó de conocimiento a los programadores de aplicaciones web java con un 4.487%, demostrando que ellos pueden mejorar su aprendizaje en el uso de desarrollo seguro con principios y buenas prácticas.
4. Con respecto al nivel de seguridad se logró mejorar en 4.907%, ya que el resultado direcciona un dato que indica que los desarrolladores perciben un nivel de seguridad en la implementación de código seguro dando beneficios directos en combatir la codificación sucia para obtener una codificación limpia por medio de las buenas prácticas de la metodología.
5. De acuerdo a los resultados obtenidos se puede concluir que el uso de la metodología técnica de OWASP fomenta el desarrollo de código seguro en las aplicaciones web por medio del uso de las Buenas Prácticas del Top Ten, esta a su vez ayuda a mejorar la calidad del ciclo de vida de la aplicación web y conseguir un nivel de seguridad optimo continuo a lo presentado en la Metodología de código seguro de OWASP.

VII. RECOMENDACIONES

Las recomendaciones para futuras investigaciones son las siguientes:

1. Desarrollar una metodología con características similares a las de este estudio, que va encaminado a los desarrolladores de aplicaciones web en la que se implementa código seguro que satisfacen los requerimientos.
2. Incorporar unas librerías de código seguro explicando detalladamente su función y la lógica de cómo debe ser implementado para solucionar las brechas de vulnerabilidades que puede presentar la aplicación web java.
3. Agregar una técnica de aprendizaje la cual sea de conocimiento hacia los programadores, esto será de guía a mejorar el nivel de seguridad y conseguir óptimos resultados.
4. Añadir una clasificación de los temas o de las vulnerabilidades más comunes que presentan los desarrolladores para que por medio de la metodología se pueda dar a conocer los pasos a implementar la metodología en la aplicación web java.
5. Adaptar la metodología no solo a desarrolladores de java sino también a programadores de .net (siendo otro lenguaje de programación) muy usado en lo que respecta a aplicaciones web.
6. Evaluar los criterios del SMART que van a ser ampliado en el estudio: Específico, Medible, Procesable, Realista y Oportuno. Estos criterios compensarían al estudio con el objetivo de reunir información para ser evaluada en base a los requisitos de seguridad.

REFERENCIAS

ACOSTA SANTANA, José Javier, et al. Pentesting en entornos controlados. Tesis (Ingeniería). España: Universidad de La Laguna. 2022. Pág. 56. Disponible en: https://riull.ull.es/xmlui/bitstream/handle/915/28744/Pentesting%20en%20entornos%20controlados.pdf

ALIERO, Muhammad Saidu, et al. WEB APPLICATION FIREWALL. International Journal Of All Research Writings, 2020, vol. 3, no 4, p. 26-43. Disponible en: http://www.ijciras.com/PublishedPaper/IJCIRAS1243.pdf

ARIAS GONZÁLES, José Luis. Proyecto de tesis: guía para la elaboración. Arequipa: Hecho el Depósito Legal en la Biblioteca Nacional del Perú N° 2020-05577. 2020. Pág. 75. [Fecha de consulta: 20 de mayo de 2023] ISBN: 978-612-00-5416-1

BANDA TORPOCO, Ricardo Manuel. Automatización pruebas de calidad de código para las aplicaciones web con herramientas de código abierto. Tesis (Ingeniero Empresarial y de Sistemas). Lima: Universidad San Ignacio de Loyola. Pág. 67. 2022. Disponible en: https://repositorio.usil.edu.pe/server/api/core/bitstreams/71014249-7c5a-4971-b2e0-f9435209da2d/content

BRAVO MULLO, Silvia Jeaneth. Contribuciones para la Detección de Ataques Distribuidos de Denegación de Servicio (DDoS) en la Capa de Aplicación. Tesis (Doctor en Ingeniería de Sistemas e Informática). Lima: Universidad Mayor de San Marcos. 2019. Pág. 162. Disponible en: https://cybertesis.unmsm.edu.pe/bitstream/handle/20.500.12672/18699/Bravo_ms.pdf

BERGILLOS PEDRAZA, Sergi. La seguridad como punto de partida del desarrollo web. Tesis (Ingeniería Informática). Cataluña: Universidad de Girona. 2021. Pág. 154. Disponible en: https://dugi-doc.udg.edu/bitstream/handle/10256/22561/Memoria_SergiBergillosPedraza_01-09-21.pdf

BERNAL YONG, Wendy; ECHEVARRÍA ANGELES, Norhelia. Modelo de niveles de seguridad para pruebas de intrusión en aplicaciones web para pymes en el Perú. Tesis (Ingeniero de Sistemas de Información). Lima: Universidad Peruana de Ciencias Aplicadas. 2019. Pág. 176. Disponible

en: https://repositorioacademico.upc.edu.pe/bitstream/handle/10757/625792/Bernal_yw.pdf

BOCANEGRA CHÁVEZ, Cristian Alexander. Comparación De Técnicas De Detección De Vulnerabilidades De Ataques De Cross Site Scripting En Aplicaciones Web De Microempresas. Tesis (Ingeniero de Sistemas). Pimentel: Universidad Señor de Sipán. 2021. Pág. 159. Disponible en: https://repositorio.uss.edu.pe/bitstream/handle/20.500.12802/8545/Bocanegra%20Ch%c3%a1vez%20Cristian%20Alexander.pdf

BURBANO ANGULO, Carolina Alexandra. Propuesta metodológica para realizar pruebas de penetración en ambientes virtuales. Tesis (Ingeniero de sistemas y computación). Esmeraldas: Pontificia Universidad Católica del Ecuador. 2019. Pág. 59. Disponible en: https://repositorio.pucese.edu.ec/bitstream/123456789/1890/1/BURBANO%20ANGULO%20CAROLINA%20ALEXANDRA.pdf

CALVO CACHA, Jhunior Leonel. Aplicación De Pentesting Y La Seguridad Informática En Los Equipos Tecnológicos De La Universidad Nacional Santiago Antúnez De Mayolo, 2022. Tesis (Ingeniero de Sistemas e Informática). Huaraz: Universidad Nacional Santiago Antúnez de Mayolo. 2022. Pág. 131. Disponible en: https://repositorio.unasam.edu.pe/bitstream/handle/UNASAM/5336/T033_71533965_T.pdf

CASTRO FERNANDEZ, Levi Ronald. Análisis Comparativo De Algoritmos De Aprendizaje Automático Para Identificar Ataques De Inyección SQL A Base De Datos En Aplicaciones Web. Tesis (Ingeniero de Sistemas). Pimentel: Universidad Señor de Sipán. 2022. Pág. 151. Disponible en: https://repositorio.uss.edu.pe/bitstream/handle/20.500.12802/9320/Castro%20Fern%c3%a1ndez%2c%20Levi%20Ronald.pdf

CARVACA ORROLA, Ana Luisa. Análisis de seguridad controlado en aplicaciones web de una institución financiera utilizando herramientas de ciberseguridad y buenas prácticas de OWASP. Tesis (Ingeniería en Tecnología de la Información). La Libertad: Universidad Estatal Península de Santa Elena. 2022. Pág. 138. Disponible en:

https://repositorio.upse.edu.ec/bitstream/46000/8646/1/UPSE-TTI-2022-0030.pdf

CASTILLO VERA, Olegario. Evaluación de metodologías de hacking ético para el diagnóstico de vulnerabilidades de la seguridad informática en una empresa de servicios logísticos. Tesis (Ingeniero de Sistemas). Pimentel: Universidad Señor de Sipán. 2021. Pág. 150. Disponible en: https://repositorio.uss.edu.pe/bitstream/handle/20.500.12802/9148/Castillo%20Vera%2c%20Olegario.pdf

CHALABE JIMENEZ, Nasser Segundo. Hacking web (Análisis de ataques SQL Inyección, XSS). Tesis (Seguridad Informática). Cartagena: Universidad Nacional Abierta y a Distancia – UNAD. 2019. Pág. 83. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/31471/nschalabej.pdf

CHANGO SAAVEDRA, Roberto Javier; GUALPA SARABIA, Daniela Alexandra. Implementación de pruebas de hackeo ético para evaluar el sistema de seguridad informática en la empresa RHELEC Ingeniería CIA. LTDA. Tesis (Ingeniero Electrónico). Quito: Universidad Politécnica Salesiana. 2023. Pág. 70. Disponible en: https://dspace.ups.edu.ec/bitstream/123456789/24450/1/TTS1228.pdf

CHAVARRIA GONZALEZ, Víctor. Estudio de los ataques contra website. OWASP. Tesis (Ingeniería Telemática). Palma: Universidad de las Islas Baleares. 2020. Pág. 83. Disponible en: https://dspace.uib.es/xmlui/bitstream/handle/11201/151259/Memoria_EPSU0643.pdf

CHINGUEL TINEO, Segundo Florentino. Evaluación de rendimiento de algoritmos en la identificación de ataques a sitios web utilizando logs de servidor. Tesis (Ingeniero de Sistemas). Pimentel: Universidad Señor de Sipán. 2022. Pág. 95. Disponible en: https://repositorio.uss.edu.pe/bitstream/handle/20.500.12802/9214/Chinguel%20Tineo%20Segundo%20Florentino.pdf

DÍAZ CASTAÑEDA, Rudy Slaytonw. Modelo De Procesos Para El Desarrollo De Software Con Características De Seguridad Para Vulnerabilidades Más Recurrentes. Tesis (Ingeniero de Sistemas). Pimentel: Universidad Señor de Sipán. 2021. Pág. 140. Disponible en:

https://repositorio.uss.edu.pe/bitstream/handle/20.500.12802/9221/Díaz Castañeda Rudy Slaytonw.pdf

DEL PERÚ, Colegio de Ingenieros. Código de Ética del CIP. Código de ética del CIP, 1999, vol. 26.

ESQUIVEL CABEZAS, Harold Alfredo; LOZANO OLIVARES, Jesus Henry. Análisis de seguridad para el sitio web de la clínica veterinaria de occidente aplicando metodología de pentets owasp. Tesis (Especialista en Seguridad Informática). Ibagué: Universidad Nacional Abierta y a Distancia. 2020. Pág. 93. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/36704/haesquivelc.pdf

FERNÁNDEZ GAYOL, Pilar. Estudio de los principales tipos de ataques por inyección de código a aplicaciones web y sistema para determinar si un código fuente es vulnerable a SQL Injection. Tesis (Ingeniería Informática). Madrid: Universidad Politécnica de Madrid. 2022. Pág. 65. Disponible en: https://oa.upm.es/71140/1/TFG_PILAR_FERNANDEZ_GAYOL.pdf

FERNÁNDEZ MIRANDA, Henry Armando. Análisis de la seguridad del sitio web del ministerio del trabajo aplicando pruebas de pentesting en la sede principal de la ciudad de bogotá. Tesis (Especialista en Seguridad Informática). Bogotá: Universidad Nacional Abierta y a Distancia. 2019. Pág. 87. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/27059/hafernandezm.pdf

FONSECA CHANGOLUISA, Elvis Martin. Comparativo de las principales tecnologías orientadas al desarrollo de aplicaciones web dinámicas seguras. Tesis (Maestría en Seguridad Telemática). Riobamba: Escuela Superior Politécnica de Chimborazo. 2021. Pág. 74. Disponible en: http://dspace.espoch.edu.ec/bitstream/123456789/14931/1/20T01460.pdf

FREIRE SILVA, Jorge Enrique. Metodología para mitigar vulnerabilidades de almacenamiento mediante inteligencia de fuentes abiertas (OSINT) en la EEASA. Tesis (Magister en Ciberseguridad). Ambato: Pontificia

Universidad Católica del Ecuador. 2022. Pág. 120. Disponible en: https://repositorio.pucesa.edu.ec/bitstream/123456789/3528/1/77818.pdf

GAMBOA SAFLA, Diego Leonardo. Vulnerabilidades en aplicaciones web utilizando la metodología de “proyecto abierto de seguridad de aplicaciones web”. Tesis (Magister en Ciberseguridad). Ambato: Pontificia Universidad Católica del Ecuador. 2021. Pág. 202. Disponible en: https://repositorio.pucesa.edu.ec/bitstream/123456789/3175/1/77336.pdf

GARCÍA, Ricardo E., et al. Análisis de Herramientas para el Testeo de Vulnerabilidades de Aplicaciones Web [en línea]. Santiago Puebla: Montiel & Soriano Editores S.A. de C.V. 2021. p. 46 - 51. [Fecha de consulta 18 de mayo de 2023]. Disponible en: https://conacic.siycise.org/public/docs/LIBRO_CONACIC_2021_APORTACIONES.pdf#page=47

GONZÁLES, José Luis Arias. Guía para elaborar el planteamiento del problema de una tesis: el método del hexágono. Revista Arbitrada: Orinoco, Pensamiento y Praxis, 2021, no 13, p. 58-69. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=7798562
ISSN 2244-8314/

HENAO, Brayan Andrés, [et al]. Ciberseguridad: los datos tienen la respuesta. [en línea]. Cali: Universidad Icesi. 2022. [Fecha de consulta: 27 de abril de 2023]. Disponible en: https://doi.org/10.18046/EUI/ee.4.2022. ISBN: 978-628-7538-78-8

HERNÁNDEZ MECHATE, Edderson Jair. Vulnerabilidades Informáticas En El Portal Web De La Universidad Andina Del Cusco. Tesis (Ingeniero de Sistemas). Cusco: Universidad Andina del Cusco. 2020. Pág. 119. Disponible en: https://repositorio.uandina.edu.pe/bitstream/handle/20.500.12557/3555/Edderson_Tesis_bachiller_2020.pdf

HERNÁNDEZ SAMPIERI, R.; MENDOZA TORRES, C. P. Recolección y análisis de los datos en la ruta cualitativa. Metodología de la investigación. Las rutas cuantitativa, cualitativa y mixta, 2018, p. 440-520. Disponible en: http://www.biblioteca.cij.gob.mx/Archivos/Materiales_de_consulta/Drogas_de_Abuso/Articulos/SampieriLasRutas.pdf
ISBN: 978-1-4562-6096-5

K, Nagendran et al. Web Application Penetration Testing [en línea]. Vol. 8. Blue Eyes Intelligence Engineering and Sciences Engineering and Sciences Publication – BEIESP. 2019. [Fecha de consulta: 22 de abril de 2023]. Disponible en: http://dx.doi.org/10.35940/ijitee.J9173.0881019. ISSN: 2278-3075

LUQUE TOVAR, Angela Lizeth, et al. Diseño e implementación de un sistema de protección contra el ataque de inyección SQL, en un servidor vulnerable utilizando herramientas Open Access. Tesis (Ingeniero de Telecomunicaciones). Bogotá: Universidad Distrital Francisco José de Caldas. 2021. Pág. 95. Disponible en: https://repository.udistrital.edu.co/bitstream/handle/11349/29053/LuqueTovarAngelaLizeth%2cBravoBuilesCristianBernardo2021.pdf

MATEO TUDELA, Francesc, et al. On Combining Static, Dynamic and Interactive Analysis Security Testing Tools to Improve OWASP Top Ten Security Vulnerability Detection in Web Applications. Applied Sciences [en línea]. vol. 10. no 9119: 24. 2020. [Fecha de consulta 26 de abril de 2023]. Disponible en: https://doi.org/10.3390/app10249119

MEDINA CASAS, Rafael. Madurez del ciclo de vida del desarrollo de software seguro: OWASP Software Assurance Maturity Model (SAMM). Tesis (Maestría Universitario en Ciberseguridad y Privacidad). Cataluña: Universidad Abierta de Cataluña. 2021. Pág. 135. Disponible en: https://openaccess.uoc.edu/bitstream/10609/132728/6/rmedinacasTFM0621memoria.pdf

MEDINA LEÓN, Alberto, et al. Procedimiento para la gestión por procesos: métodos y herramientas de apoyo. Ingeniare. Revista chilena de ingeniería, 2019, vol. 27, no 2, p. 328-342. [Fecha de consulta 15 de mayo de 2023]. Disponible en: https://www.scielo.cl/pdf/ingeniare/v27n2/0718-3305-ingeniare-27-02-00328.pdf

MENDOZA MINCHAN, Houston Wily; SANDOVAL URBINA, Rodrigo Andre. Sistema web basado en OWASP para el proceso de cobranza en el Instituto de Educación Superior Tecnológico Privado Santa Rosa. Tesis (Ingeniero de Sistemas). Lima: Universidad César Vallejo. 2020. Pág. 182. Disponible en: https://repositorio.ucv.edu.pe/handle/20.500.12692/54534

MENENDEZ ARANTE, Silvia Clara. Auditoría de Seguridad Informática [en línea]. Madrid: Grupo RA-MA Editorial. 2022. [Fecha de consulta: 13 de abril de 2023]. Disponible en: https://www.digitaliapublishing.com/a/116389
ISBN: 978-84-1897-193-8

METODOLOGÍA de la investigación por Humberto Ñaupas [et al.] 5a. Bogotá: Editorial de la U. 2018. Pág. 560. Disponible en: http://www.biblioteca.cij.gob.mx/Archivos/Materiales_de_consulta/Drogas_de_Abuso/Articulos/MetodologiaInvestigacionNaupas.pdf
ISBN: 978-958-762-876-0

MORENO MARÍN, John Edison, et al. Modelo base de conocimiento para auditorías de seguridad en Servicios Web con SQL Injection. Tesis (Ingeniero de Software). Bogotá: Universidad Distrital Francisco José de Caldas. 2019. Pág. 104. Disponible en: https://repository.udistrital.edu.co/bitstream/handle/11349/23088/MorenoMarinJohnEdison2019.pdf

OCHOA, Roselva; NAVA, Ninoska; FUSIL, Damaris. Comprensión epistemológica del tesista sobre investigaciones cuantitativas, cualitativas y mixtas. Orbis: revista de Ciencias Humanas, 2020, vol. 15, no 45, p. 13-22. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=7407375
ISSN 1856-1594

OSPINA SANTANDER, Elizabeth; ROLDAN LIZCANO, Melany. Evaluación de una versión modificada de la prueba Shapiro-Wilk Generalizada con estimación Shrinkage de la matriz de covarianzas: caso de alta dimensión con muestras pequeñas. 2022. Disponible en: https://bibliotecadigital.univalle.edu.co/bitstream/handle/10893/24333/3752%20O83eva.pdf

ORIUNDO MALLCO, Eliauim. Modelo De Framework De Código Abierto Java Para El Desarrollo Rápido De Aplicaciones Web Empresariales Basadas En Componentes De Negocio Para Entornos Agiles, 2019. Tesis (Ingeniero de Sistemas). Ayacucho: Universidad Nacional De San Cristóbal De Huamanga. 2019. Pág. 141 Disponible en:

http://repositorio.unsch.edu.pe/bitstream/UNSCH/3616/1/TESIS%20SIS85_Ori.pdf

ORTEGA CANDEL, José Manuel. Seguridad en aplicaciones web java [en línea]. Madrid: Grupo RA-MA Editorial. 2018. [fecha de consulta: 13 de abril de 2023]. Disponible en: https://www.digitaliapublishing.com/a/110101 ISBN: 978-84-9964-732-6

ORTIZ PADILLA, Gerardo Antonio. Análisis de técnicas para pruebas de ethical hacking-pentesting en sitios web. Tesis (Ingeniero de sistemas). Cañar: Universidad Católica de Cuenca. 2021. Pág 37. Disponible en: https://dspace.ucacue.edu.ec/bitstream/ucacue/12756/1/Articulo%20de%20Ethical%20Hacking-Pentesting.pdf

OSORIO GUTIÉRREZ, Diego Andrés, et al. Plan y Pruebas de Seguridad de un Sistema de Gestión Documental Tomando como Referencia la Guía de Pruebas de OWASP. Bogotá: Universidad Distrital Francisco José de Caldas. 2020. Pág. 104. Disponible en: https://repository.udistrital.edu.co/bitstream/handle/11349/25722/OsorioGutierrezDiegoAndres2020.pdf

PEREIRA, Karina de Fatima Portela de Oliveira, et al. Attention to oropharingeal dysfunction in home care: speech therapy management. Appearance and content validation study of a guidance manual. Revista CEFAC, 2018, vol. 20, no 5, p. 640-647. Disponible en: https://www.scielo.br/j/rcefac/a/MZsrs3CwdtgMMWp4xWDKMsy/

RAMÍREZ MÁRQUEZ, Jimmy Fernando. Análisis, desarrollo e implementación de un sistema de seguridad para el fortalecimiento de vulnerabilidades e integridad de aplicaciones web académicas. Tesis (Magíster en seguridad telemática). Riobamba: Escuela Superior Politécnica de Chimborazo. 2022. Pág. 81. Disponible en: http://dspace.espoch.edu.ec/bitstream/123456789/15708/1/20T01508.pdf

RIO HERNÁNDEZ, Oscar. Detección y explotación de vulnerabilidades del top 10 de OWASP y protección contra éstas. Tesis (Ingeniería de Informática). Cataluña: Universidad Politécnica de Cataluña. 2022. Pág. 75. Disponible en: https://upcommons.upc.edu/bitstream/handle/2117/375146/169364.pdf

ROBAYO GARCÍA, Luz Angela. Vulnerabilidades Informáticas en Implementaciones con el CMS Wordpress. Tesis (Especialista en Seguridad Informática). Bogotá: Universidad Nacional Abierta y a Distancia. 2021. Pág. 78. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/40343/larobayog.pdf

RODRÍGUEZ-RODRÍGUEZ, Julio; REGUANT-ÁLVAREZ, Mercedes. Calcular la fiabilidad de un cuestionario o escala mediante el SPSS: el coeficiente alfa de Cronbach. REIRE Revista d'Innovació i Recerca en Educació, 2020, vol. 13, no 2, p. 1–13-1–13. Disponible en: https://revistes.ub.edu/index.php/REIRE/article/view/reire2020.13.230048/31484
ISSN: 2013-2255

ROMERO ALIAGA, Juan José. Trabajo de investigación de mejores prácticas en desarrollo de sistemas web contra ataque de inyección. Tesis (Maestro en Ingeniería de Seguridad Informática). Lima: Universidad Tecnológica del Perú. 2019. Pág. 106. Disponible en: https://repositorio.utp.edu.pe/bitstream/handle/20.500.12867/2078/Juan%20Romero_Trabajo%20de%20Investigacion_Maestria_2019.pdf

SALAZAR, Pablo Gutiérrez. El libro blanco del hacker [en línea]. 2ª ed. Madrid: Grupo RA-MA Editorial. 2019. Pág. 300. [Fecha de consulta: 13 de abril de 2023]. Disponible en: https://www.digitaliapublishing.com/a/110151/
ISBN: 978-84-9964-840-8

SANTIAGO GARCÍA, Omar Camilo, et al. 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. Tesis (Especialista en Seguridad Informática). Villavicencio: Universidad Nacional Abierta y a Distancia. 2021. Pág. 72. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/43494/ocsantiagog.pdf

SEGUNDO, Chalabe Jiménez Nasser, et al. Hacking web (Análisis de ataques SQL Inyección, XSS). Tesis (Seguridad Informática). Cartagena: Universidad Nacional Abierta y a Distancia – UNAD. 2019. Pág. 83.

Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/31471/nschalabej.pdf

SIERRA HUERTAS, Tania, et al. La seguridad informática en el desarrollo de aplicaciones web mediante el uso de la metodología OWASP. Tesis (Seguridad Informática). Cartagena: Universidad Nacional Abierta y a Distancia – UNAD. 2022. Pág. 84. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/54049/ta52sie605.pdf

SOSA FERNANDEZ, Julissa Tatiana. Metodología para la elección de fotware de seguridad informática. Tesis (Ingeniería de sistemas). Lima: Universidad César Vallejo. 2018. Pág. 90. Disponible en: https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/31944/Sosa_FJ.pdf

SUÁREZ, Ivan Coronel; YAGUAL, Daniel Quirumbay. Seguridad informática, metodologías, estándares y marco de gestión en un enfoque hacia las aplicaciones web. Revista Científica y Tecnológica UPSE. vol. 9. no 2, p. 97-108. 2022. Disponible en: https://doi.org/10.26423/rctu.v9i2.672 ISSN: 1390-7638

TASAN GARCÉS, Fabricio Andrés; MOROCHO BUÑAY, Miriam Elizabeth. Metodología OWASP en el desarrollo de un Website para voto electrónico. Caso práctico: Sistema de elecciones asociación de estudiantes TI-UNACH. Tesis (Ingeniería de Sistemas y Computación). Riobamba: Universidad Nacional de Chimborazo. 2020. Pág. 80. Disponible en: http://dspace.unach.edu.ec/bitstream/51000/7024/2/UNACH-RGF-01-04-02.14%20Informe%20Final%20del%20Proyecto%20de%20Investigaci%c3%b3n%20%28Tesis%20OWASP%20Voto%20electr%c3%b3nico%29.pdf

TOMALÁ LAÍNEZ, Steven Xavier. Estudio de técnicas de ciberseguridad aplicado al desarrollo de aplicaciones web mediante el uso de la herramienta damn vulnerable web application (DVWA). Tesis (Ingeniero en Tecnologías de la Información). Santa Elena: Universidad Estatal Península de Santa Elena. 2023. Pág. 223. Disponible en: https://repositorio.upse.edu.ec/handle/46000/9277

TORRES, Mariela; SALAZAR, Federico G.; PAZ, Karim. Métodos de recolección de datos para una investigación. 2019. Disponible en: http://148.202.167.116:8080/jspui/bitstream/123456789/2817/1/M%c3%a9todos%20de%20recolecci%c3%b3n%20de%20datos%20para%20una%20investigaci%c3%b3n.pdf

UNESCO, A. G. Declaración universal sobre bioética y derechos humanos. París: Octubre de, 2005. Disponible en: https://www2.congreso.gob.pe/sicr/cendocbib/con4_uibd.nsf/07761DB776BF854205257D160072F6D6/$FILE/9_Brochure+UNESCO_SP.pdf

USECHE, María Cristina, et al. Técnicas e instrumentos de recolección de datos cuali-cuantitativos. 2019. Disponible en: https://repositoryinst.uniguajira.edu.co/bitstream/handle/uniguajira/467/88.%20Tecnicas%20e%20instrumentos%20recolecci%c3%b3n%20de%20datos.pdf

VARELA LEMA, Anxo. Análise, deseño e implementación dunha Aplicación Web Java para a xestión de laboratorios de análises ambientais. Tesis (Ingeniería de Software). Coruña: Universidade da Coruña. 2020. Pág. 145. Disponible en: https://ruc.udc.es/dspace/bitstream/handle/2183/26155/A.Varela_Lema_2020_An%c3%a1lise_dese%c3%b1o_e_implementaci%c3%b3n_dunha_aplicaci%c3%b3n_Java.pdf

VALLE, Alejandro Javier. Análisis de seguridad de la plataforma de libre comercio electrónico de la empresa CorpoAmbato. 2022. Tesis (Ingeniero de Tecnologías de la Informaciíon y la Comunicación). Ambato: Pontificia Universidad Católica del Ecuador. 2022. Pág. 161. Disponible en: https://repositorio.pucesa.edu.ec/bitstream/123456789/3508/1/77566.pdf

WILLBERG, Mikael. Web application security testing with owasp top 10 framework. Bachelor's thesis (Information and Communications Technology). Turku: University of Applied Science. 2019. Pág. 33. Disponible en: https://www.theseus.fi/bitstream/handle/10024/170389/Willberg_Mikael.pdf

ZAMBRANO, Karen Barbarita Álava; VIDAL, Willians Eduardo Basurto; VERA, Roberth Ronaldo Tóala. Vulnerabilidades en los sistemas informáticos

owasp top 10: revisión bibliográfica. Journal Business Science, 2022, vol. 3, no 2, p. 1-8. Disponible en: https://revistas.uleam.edu.ec/index.php/business_science/article/view/221/308
ISSN electrónico 2737-615X

ZAMBRANO VÉLEZ, Grace Marcela y ANDRADE RODRÍGUEZ, María José. Diagnóstico de las vulnerabilidades informáticas en las aplicaciones web de la universidad central del ecuador. Tesis (Ingeniero en Sistemas Informáticos). Quito: Universidad Tecnológica Israel. 2019. Pág. 150. Disponible en: https://repositorio.uisrael.edu.ec/bitstream/47000/1946/1/UISRAEL-EC-SIS-378.242-2019-019.pdf

ZAPATA GARCÍA, Juliana. Uso de tecnologías de pruebas de penetración para validación de seguridad de aplicaciones web basado en el top 10 de vulnerabilidades de OWASP. Tesis (Especialista en Seguridad Informática). Sabaneta: Universidad Nacional Abierta y a Distancia. 2018. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/28466/1033648651.pdf

ANEXOS

Anexo 1: Matriz de operacionalización de variables

Tabla 20: Matriz de operacionalización de variables

VARIABLES	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL	DIMENSIÓN	INDICADOR	INSTRUMENTO	ESCALA DE MEDICIÓN
Influencia de las Metodología de Buenas Prácticas del Top Ten de OWASP en Aplicaciones web Java (Hernández Mechate, Edderson Jair. 2020)	La metodología de Buenas Prácticas del Top Ten de OWASP en desarrollo de aplicaciones web Java en la que son de código abierto para mejorar y protección de la web; se recomienda codificación segura, detección de riesgos y evaluación de proceso, en las cuales se consideran las 10 amenazas más frecuentes que pueden sufrir las aplicaciones web (Sierra Huertas, Tania. 2022)	La influencia de la metodología de Buenas Prácticas del Top Ten de OWASP aumenta mejoras, desarrollando crecimiento e incrementa en el conocimiento y avances de niveles de seguridad en las aplicaciones web Java (Sierra Huertas, Tania. 2022)	Optimización (Sierra Huertas, Tania. 2022)	Aumento de la optimización (Sierra Huertas, Tania. 2022)	Guía de Observación	Ordinal
			Crecimiento (Carvaca Orrala, Ana Luisa. 2022)	Desarrollo de Crecimiento (Carvaca Orrala, Ana Luisa. 2022)	Guía de Observación	Ordinal
			Conocimiento (Zapata, Juliana, et al. 2019)	Incremento en el Conocimiento (Zapata, Juliana, et al. 2019)	Guía de Observación	Ordinal
			Nivel de seguridad (Zambrano, Grace Marcela y Andrade, María. 2019)	Mejora en el Nivel de seguridad (Zambrano, Grace Marcela y Andrade, María. 2019)	Guía de Observación	Ordinal

Anexo 2: Matriz de consistencia

Tabla 21: Matriz de consistencia

PROBLEMAS	OBJETIVOS	HIPÓTESIS	VARIABLE	DIMENSIONES	INDICADORES
Principal	**General**	**General**			
¿Cómo influye la metodología de Buenas Prácticas del Top Ten de OWASP en la optimización, crecimiento, conocimiento y nivel de seguridad para las aplicaciones web Java?	Determinar la influencia de metodología de técnicas OWASP para el aumento de la optimización, desarrollo de crecimiento, incremento en el conocimiento y avances del nivel de seguridad en las aplicaciones web Java	El uso de la metodología de Buenas Prácticas del Top Ten de OWASP aumentará la optimización, desarrollará un crecimiento, incrementará el conocimiento y mejorará el nivel de seguridad para aplicaciones web Java de las empresas			
Específicos	**Específicos**	**Específicos**	**Variable**	**Dimensiones**	**Indicadores**
¿Cómo influye la metodología de buenas prácticas del Top Ten de OWASP en la optimización en aplicaciones web Java?	Determinar la influencia de la metodología de Buenas Prácticas del Top Ten de OWASP para el aumento de la optimización de aplicaciones web Java	El uso de la metodología de técnicas OWASP aumentará la optimización en las aplicaciones web Java (Zambrano, Grace Marcela y Andrade, María. 2019)	Influencia de la Metodología de Buenas Prácticas del Top Ten de OWASP en Aplicaciones web Java (Hernández Mechate, Edderson Jair. 2020)	Optimización (Sierra Huertas, Tania, et al. 2022)	Aumento de optimización (Sierra Huertas, Tania, et al. 2022)
¿Cómo influye la metodología de Buenas Prácticas del Top Ten de OWASP en el crecimiento de aplicaciones web Java?	Determinar la influencia de la metodología de Buenas Prácticas del Top Ten de OWASP para el desarrollo de crecimiento de aplicaciones web Java	El uso de la metodología de técnicas OWASP desarrollará un crecimiento en las aplicaciones web Java (Carvaca Orrala, Ana Luisa. 2022)		Crecimiento (Carvaca Orrala, Ana Luisa. 2022)	Desarrollo de Crecimiento (Carvaca Orrala, Ana Luisa. 2022)
¿Cómo influye la metodología de Buenas Prácticas del Top Ten de OWASP en el conocimiento para aplicaciones web Java?	Determinar la influencia de la metodología de Buenas Prácticas del Top Ten de OWASP para el incremento en el conocimiento de aplicaciones web Java	El uso de la metodología de técnicas OWASP incrementará el conocimiento de las aplicaciones web Java (Zapata, Juliana, et al. 2019)		Conocimiento (Zapata, Juliana, et al. 2019)	Incremento en el Conocimiento (Zapata, Juliana, et al. 2019)
¿Cómo influye la metodología de Buenas Prácticas del Top Ten de OWASP en el nivel de seguridad de implementación para aplicaciones web Java?	Determinar la influencia de la metodología de Buenas Prácticas del Top Ten de OWASP para el incremento en el conocimiento de aplicaciones web Java	El uso de la metodología de técnicas OWASP mejorará el nivel de seguridad en las aplicaciones web Java (Hernández Mechate, Edderson Jair. 2020)		Nivel de seguridad (Zambrano, Grace Marcela y Andrade, María. 2019)	Mejora en el Nivel de seguridad (Zambrano, Grace Marcela y Andrade, María. 2019)

Anexo 3: Instrumento de recolección de datos

GUÍA DE OBSERVACIÓN DE AUDITORÍA SOBRE LA INFLUENCIA DE LA METODOLOGÍA DE BUENAS PRÁCTICAS DEL TOP TEN DE OWASP EN APLICACIONES WEB JAVA					
Observador					
Aplicación		Aplicaciones Web desarrolladas en JAVA			
Fecha					
	Criterios	ALTO	MEDIO	BAJO	NULO
1	¿Tu comprensión respecto a las Buenas prácticas de Código Seguro que se utilizan en aplicaciones Web es?				
2	¿Cómo catalogarías tu conocimiento respecto a la seguridad que la ISO 27001 recomienda en el desarrollo de aplicaciones web?				
3	¿Cuál es tu nivel de conocimientos con respecto a una Auditoria de una aplicación web basado en OWASP?				
4	¿Cómo defines tu nivel de conocimiento con respecto al TOP TEN de OWASP utilizado en auditorias de Aplicaciones Web?				
5	¿En tu organización realizan evaluaciones de Auditorias de Vulnerabilidades de Aplicaciones Web basados en OWASP?. Donde : Alto : Se realiza antes de la puesta en Producción Medio : Se realiza una vez al Año Bajo : No se realizan Evaluaciones Nulo : Desconocemos del tema.				
6	¿Cuándo desarrollan una Aplicación Web, utilizan buenas prácticas de código seguro basado en OWASP? Alto: Se utiliza durante la etapa de diseño Medio : Se utiliza durante la etapa de Implementación de código Bajo : No se utiliza Nulo : Se desconoce				
7	¿Han sufrido ataques de Vulnerabilidades en Aplicaciones Web durante los dos últimos Años? Alto : No, No hemos sufrido ningún ataque Medio : SI, al menos 1 ataque Bajo : SI, más de 3 ataques Nulo : No sabemos si tenemos ataques				

8	¿La organización cuenta con Librerías de código seguro o código de buenas prácticas basados en OWASP? Alto : Si contamos con librerías de código seguro para aplicaciones Web basado en OWASP Medio : No contamos con librerías, pero utilizamos equipos de protección perimetral Bajo : No tenemos librerías o script de código seguro Nulo : Desconocemos el uso de librerías de código seguro				
9	¿El personal del área de desarrollo de aplicaciones web, ha llevado un curso de capacitación en la programación de aplicaciones web basado en buenas prácticas de OWASP? Alto : Si ha llevado un curso. Medio : No ha llevado un curso, pero conocen algo del tema. Bajo : No ha llevado un curso Nulo: Desconocen del tema				
10	¿La organización cuando identifica vulnerabilidades de Aplicaciones Web que hace? Alto : Lo soluciona con personal propio utilizando buenas prácticas del TOP TEN de OWASP Medio : Lo soluciona con una empresa tercera basado en el Top Ten de OWASP Bajo : No lo soluciona Nulo : No tiene la capacidad de identificar estas vulnerabilidades				
11	¿Cuánto tiempo después de un ataque han demorado en solucionar un problema basado en vulnerabilidades de aplicaciones web? Alto : Menos de 1 día Medio : Mas de 1 semana Bajo : Mas de un mes Nulo : No se puede solucionar				
12	¿La organización desarrolla capacitaciones de buenas prácticas de desarrollo seguro para aplicaciones web basadas en OWASP? Alto : Si , lo realiza cada 6 meses Medio : SI, lo realiza 1 vez al año Bajo : No lo realiza				

	Nulo : No forma parte de las políticas de seguridad de la empresa				
13	¿Luego de un incidente de seguridad basado en Aplicaciones Web, realizan una reunión de revisión de lo sucedido? Alto : Si, siempre Medio : Si, 2 después de 30 días Bajo : No se realiza Nulo : No existe un encargado de ciberseguridad en la organización				
14	¿Cuándo una vulnerabilidad de Aplicaciones Web es detectada por la organización, esta es analizada con el área de desarrollo? Alto : Si, se analiza y se ve los errores de código encontrados Medio : No, solo se envía las vulnerabilidades encontradas al área de desarrollo Bajo : No se realiza reunión e informe alguno Nulo : La organización no realiza evaluaciones de vulnerabilidades de aplicaciones Web				
15	¿La organización desarrolla reuniones de capacitación para revisar las nuevas versiones de buenas prácticas de Código Seguro basado en Top Ten de OWASP? Alto : Si, dentro de los 30 días de anunciada la nueva versión Medio : Si, dentro de los 6 meses de anunciado la nueva versión Bajo : No realiza capacitaciones Nulo : No llevan un control de las versiones utilizadas				
16	¿Estarías dispuesto a aprender Buenas prácticas de código seguro para programación de aplicaciones web basado en el Top Ten de OWASP? Alto : Si, completamente Medio : Si, la empresa lo requiere. Bajo : No estoy interesado Nulo : Considero que no es necesario				

Anexo 4: Proceso de Prueba Piloto

	V2 - Influencia de la Metodología de Buenas Prácticas del Top Ten de OWASP en Aplicaciones web Java															
	Aumento de optimización				Desarrollo de Crecimiento				Incremento del Conocimiento				Mejora en el Nivel de seguridad			
Items	p1	p2	p3	p4	p5	p6	p7	p8	p9	p10	p11	p12	p13	p14	p15	p16
1	3	3	3	3	2	3	3	3	3	4	3	1	2	4	3	4
2	3	1	1	1	1	1	3	1	1	1	3	1	2	2	2	3
3	3	2	2	2	2	2	4	3	3	3	3	2	2	2	2	4
4	2	3	2	2	2	1	1	1	1	2	2	2	1	2	1	2
5	3	3	3	2	2	2	4	3	2	3	4	2	4	4	2	4
6	3	2	2	3	3	3	4	3	3	4	3	2	4	4	2	4
7	2	4	4	1	2	2	3	1	1	2	4	1	2	1	3	1
8	3	2	3	1	2	2	4	2	3	2	4	4	1	1	4	3
9	4	3	4	4	4	2	3	1	1	2	3	4	1	3	3	1
10	4	3	4	1	1	2	1	1	4	1	3	1	1	2	4	4
11	2	2	2	2	3	4	3	4	1	3	1	2	3	4	4	4
12	1	2	2	1	4	3	2	1	3	3	2	2	2	3	1	3
13	3	2	1	1	2	1	2	1	1	3	3	2	1	2	2	3
14	4	3	3	4	2	3	4	2	1	2	3	3	3	3	1	3
15	3	3	4	1	4	2	4	4	3	3	3	4	2	2	2	3
16	2	3	4	1	2	4	1	4	1	1	4	4	1	3	3	2
17	2	2	4	3	4	2	4	3	3	2	1	1	1	4	2	2

Anexo 5: Prueba final de resultados - Pre

	V2 - Influencia de la Metodología de Buenas Prácticas del Top Ten de OWASP en Aplicaciones web Java															
	Aumento de Optimización				Desarrollo de Crecimiento				Incremento del Conocimiento				Mejora en el Nivel de seguridad			
Items	p1	p2	p3	p4	p5	p6	p7	p8	p9	p10	p11	p12	p13	p14	p15	p16
1	3	3	3	3	2	3	3	3	3	4	3	1	2	4	3	4
2	3	3	1	1	1	1	3	1	1	1	3	1	2	2	2	3
3	3	2	2	2	2	2	4	3	3	3	3	2	2	2	2	4
4	2	3	2	2	2	1	1	1	1	2	2	2	1	2	1	2
5	3	3	3	2	2	2	4	3	2	3	4	2	4	4	2	4
6	3	2	2	3	3	3	4	3	3	4	3	2	4	4	2	4
7	2	4	4	1	2	2	3	1	1	2	4	1	2	1	3	1
8	3	2	3	1	2	2	4	2	3	2	4	4	1	1	4	3
9	4	3	4	4	4	2	3	1	1	2	3	4	1	3	3	1
10	4	3	4	1	1	2	1	1	4	1	3	1	1	2	4	4
11	2	2	2	2	3	4	3	4	1	3	1	2	3	4	4	4
12	1	2	2	1	4	3	2	1	3	3	2	2	2	3	1	3
13	3	2	1	1	2	1	2	1	1	3	3	2	1	2	2	3
14	4	3	3	4	2	3	4	2	1	2	3	3	3	3	1	3
15	3	3	4	1	4	2	4	4	3	3	3	4	2	2	2	3
16	2	3	4	1	2	4	1	4	1	1	4	4	1	3	3	2
17	2	2	4	3	4	2	4	3	3	2	1	1	3	4	2	2
18	3	2	2	2	2	3	2	4	1	2	4	2	4	3	4	3
19	2	1	3	1	4	2	2	3	3	1	1	1	3	1	2	2
20	2	1	2	4	1	3	4	2	4	2	4	4	2	2	4	3
21	4	4	2	1	1	3	1	3	1	3	2	4	3	2	2	4
22	4	2	1	1	4	3	3	2	1	3	3	4	4	4	3	2
23	2	1	4	2	1	2	3	4	4	2	3	2	3	3	3	3
24	1	1	4	2	4	1	1	1	1	2	3	2	2	3	2	3
25	2	4	2	2	1	3	2	2	3	3	4	2	3	3	4	3
26	4	4	1	4	1	2	3	4	2	1	4	3	3	3	4	3
27	2	2	2	4	3	4	3	4	3	2	4	4	3	2	4	2
28	2	2	2	2	2	3	2	4	3	2	2	3	2	4	2	2
29	1	3	1	2	1	3	2	2	3	1	3	3	3	2	4	3
30	4	2	3	4	1	4	4	2	3	2	2	3	3	3	4	4
31	2	4	4	3	1	2	2	2	1	2	2	4	4	2	3	3
32	3	3	2	2	3	2	2	2	3	3	4	3	3	3	3	3
33	4	2	2	4	4	4	3	3	3	3	4	3	4	4	4	4
34	4	3	2	2	2	3	4	4	2	4	2	3	4	3	4	2
35	3	3	4	2	2	2	4	2	2	2	3	4	2	4	2	3
36	4	3	2	4	2	3	2	4	3	3	2	2	4	2	3	3
37	2	3	2	3	3	4	3	3	3	2	4	4	3	2	2	4

38	4	3	4	4	4	4	4	3	4	2	3	4	4	4	2	4
39	3	2	3	2	3	4	3	4	2	2	3	3	4	3	3	4
40	3	2	4	2	2	3	4	4	4	2	4	4	4	4	2	3
41	1	4	3	4	2	4	3	2	2	3	4	1	2	3	2	3
42	3	2	3	2	3	3	4	2	4	2	1	2	4	3	2	3
43	2	2	4	4	2	4	4	4	3	4	3	4	4	3	4	2
44	3	4	2	4	4	3	3	3	4	2	2	3	4	4	2	3
45	4	2	3	2	2	2	2	2	4	4	3	2	2	2	3	3
46	4	4	2	3	4	1	2	3	3	2	4	3	2	2	3	3
47	3	2	2	2	4	4	3	3	3	2	3	4	4	3	4	3
48	2	2	3	2	3	2	3	2	2	3	4	2	3	1	2	2
49	4	3	3	4	4	2	4	4	3	4	4	4	4	2	4	4
50	4	2	4	4	2	3	4	2	4	3	4	3	2	4	4	4

Anexo 6: Prueba final de resultados – Post

	V2 - Influencia de la Metodología de Buenas Prácticas del Top Ten de OWASP en Aplicaciones web Java															
	Aumento de Optimización				Desarrollo de Crecimiento				Incremento del Conocimiento				Mejora en el Nivel de seguridad			
Items	p1	p2	p3	p4	p5	p6	p7	p8	p9	p10	p11	p12	p13	p14	p15	p16
1	4	4	4	4	2	3	3	3	3	4	3	2	4	4	3	4
2	4	4	2	2	1	1	3	1	3	3	3	1	3	4	4	4
3	3	3	3	3	2	2	4	3	3	3	3	3	4	4	2	4
4	3	4	3	3	2	1	1	1	1	2	2	2	2	2	1	2
5	3	3	3	2	2	2	4	3	2	3	4	2	4	4	2	4
6	3	2	2	3	3	3	4	3	3	4	3	2	4	4	2	4
7	2	4	4	3	2	2	3	1	2	2	4	1	2	2	3	1
8	3	2	3	3	2	2	4	2	3	2	4	4	1	1	4	3
9	4	3	4	4	4	2	3	1	2	2	3	4	1	3	3	1
10	4	3	4	2	1	2	1	1	4	2	3	1	1	2	4	4
11	2	2	2	2	3	4	3	4	4	3	2	2	3	4	4	4
12	1	2	2	3	4	3	2	1	3	3	2	2	2	3	1	3
13	3	2	1	2	2	1	2	1	1	3	3	2	1	2	2	3
14	4	3	3	4	2	3	4	2	1	2	3	3	3	3	1	3
15	3	3	4	2	4	2	4	4	3	3	3	4	2	2	2	3
16	2	3	4	3	2	4	1	4	1	1	4	4	1	3	3	2
17	2	2	4	3	4	2	4	3	3	2	2	1	3	4	2	2
18	3	2	2	2	2	3	2	4	1	2	4	2	4	3	4	3
19	2	1	3	3	4	2	2	3	3	2	2	1	3	2	2	2
20	2	1	2	4	1	3	4	2	4	2	4	4	2	2	4	3
21	4	4	2	2	1	3	1	3	1	3	2	4	3	2	2	4
22	4	2	1	1	4	3	3	2	1	3	3	4	4	4	3	2
23	2	1	4	2	1	2	3	4	4	2	3	2	3	3	3	3
24	1	1	4	2	4	1	1	1	1	2	3	2	4	3	3	3
25	2	4	2	2	1	3	2	2	3	3	4	2	3	3	4	3
26	4	4	1	4	1	4	4	4	2	2	4	3	3	3	4	3
27	2	2	2	4	3	4	3	4	3	2	4	4	3	2	4	2
28	2	2	2	2	2	3	2	4	3	2	2	3	4	4	2	2
29	1	3	1	2	1	3	2	2	3	2	3	3	3	2	4	3
30	4	2	3	4	1	4	4	2	3	2	2	3	3	3	4	4
31	2	4	4	3	1	2	3	2	2	2	3	4	4	2	3	3
32	3	3	2	2	3	2	3	2	3	4	4	3	3	3	3	3
33	4	2	2	4	4	4	3	3	3	3	4	3	4	4	4	4
34	4	3	2	2	2	4	4	4	3	4	2	3	4	3	4	2
35	3	3	4	2	3	3	4	2	3	2	3	4	2	4	2	3
36	4	3	2	4	3	4	3	4	3	4	3	3	4	2	3	3
37	2	3	2	4	3	4	3	4	4	3	4	4	3	2	2	4

38	4	3	4	4	4	4	4	3	4	3	3	4	4	4	3	4
39	3	2	4	3	3	4	3	4	2	3	3	3	4	3	3	4
40	3	2	4	3	2	3	4	4	4	3	4	4	4	4	3	3
41	1	4	4	4	2	4	3	2	4	3	4	2	2	3	2	3
42	3	4	3	3	3	3	4	2	4	3	2	2	4	3	2	3
43	2	4	4	4	2	4	4	4	3	4	3	4	4	3	4	2
44	4	4	2	4	4	3	3	3	4	3	4	4	4	4	4	3
45	4	2	3	2	2	2	2	2	4	4	3	2	4	4	3	3
46	4	4	3	3	4	3	2	3	3	3	4	3	4	4	3	3
47	3	2	2	2	4	4	3	3	3	2	3	4	4	3	4	3
48	2	2	3	2	3	2	3	3	2	3	4	2	4	3	4	4
49	4	3	3	4	4	2	4	4	3	4	4	4	4	3	4	4
50	4	2	4	4	3	3	4	3	4	3	4	4	3	4	4	4

Anexo 7: Encuesta realizada por Google Form

Uso de las Buenas Practicas del TOP TEN de OWASP en Aplicaciones Web Java

Esta es una Guía de observación de auditoria sobre el uso de las buenas practicas del TOP TEN de OWASP en Aplicaciones Web JAVA

DATOS DEL ENCUESTADO (Observador)

Descripción (opcional)

Apellidos y Nombres *

Texto de respuesta corta

Email *

Texto de respuesta corta

Celular *

Texto de respuesta corta

País *

Texto de respuesta corta

Empresa donde trabaja *

Texto de respuesta corta

Estudios Realizados (profesión) *

Texto de respuesta corta

Anexo 8: Metodología de código seguro de OWASP

Diego Chang

Metodología de código seguro de OWASP

ÍNDICE

UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Declaratoria de Autenticidad del Asesor

Yo, HILARIO FALCON FRANCISCO MANUEL, docente de la FACULTAD DE INGENIERÍA Y ARQUITECTURA de la escuela profesional de INGENIERÍA DE SISTEMAS de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA NORTE, asesor de Tesis titulada: "Metodología de técnicas OWASP para aplicaciones web java", cuyo autor es CHANG DEL CARPIO DIEGO ANTONIO, constato que la investigación tiene un índice de similitud de 20.00%, verificable en el reporte de originalidad del programa Turnitin, el cual ha sido realizado sin filtros, ni exclusiones.

He revisado dicho reporte y concluyo que cada una de las coincidencias detectadas no constituyen plagio. A mi leal saber y entender la Tesis cumple con todas las normas para el uso de citas y referencias establecidas por la Universidad César Vallejo.

En tal sentido, asumo la responsabilidad que corresponda ante cualquier falsedad, ocultamiento u omisión tanto de los documentos como de información aportada, por lo cual me someto a lo dispuesto en las normas académicas vigentes de la Universidad César Vallejo.

LIMA, 30 de Noviembre del 2023

Apellidos y Nombres del Asesor:	**Firma**
HILARIO FALCON FRANCISCO MANUEL **DNI:** 10132075 **ORCID:** 0000-0003-3153-9343	Firmado electrónicamente por: FHILARIOF el 11-12-2023 16:45:04

Código documento Trilce: TRI - 0674127

INVESTIGA UCV