Polo del Conocimiento

Pol. Con. (Edición núm. 110) Vol. 10, No 9
Septiembre 2025, pp. 552-567
ISSN: 2550 - 682X
DOI: https://doi.org/10.23857/pc.v10i9.10338

OWASP como estrategia de evaluación de seguridad para el desarrollo de plataformas web

OWASP as a security assessment strategy for the development of web platforms

OWASP como estratégia de avaliação de segurança para o desenvolvimento de plataformas web

Vladimir Celi-Alvarez [I]
vladimir.celi@unl.edu.ec
https://orcid.org/0009-0003-4231-5692

Cristian Narváez-Guillen [II]
cristian.narvaez@unl.edu.ec
https://orcid.org/0000-0002-9096-1010

Mario Enrique Cueva-Hurtado [III]
mecueva@unle.du.ec
https://orcid.org/0000-0001-8931-6375

Cesar Iñiguez-Chicaiza [IV]
cesar.f.iniguez@unl.edu.ec
https://orcid.org/0000-0002-4917-7080

Andrés Navas-Castellanos [V]
andres.navas@unl.edu.ec
https://orcid.org/0000-0001-5890-9709

Correspondencia: mecueva@unle.du.ec

Ciencias Técnicas y Aplicadas
Artículo de Investigación

*** Recibido:** 21 de julio de 2025 ***Aceptado:** 18 de agosto de 2025 *** Publicado:** 09 de septiembre de 2025

I. Estudiante, Universidad Nacional de Loja, Ecuador.
II. Docente Ocasional, Universidad Nacional de Loja, Ecuador.
III. Docente Titular Auxiliar 2, Universidad Nacional de Loja, Ecuador.
IV. Docente Ocasional, Universidad Nacional de Loja, Ecuador.
V. Docente Ocasional, Universidad Nacional de Loja, Ecuador.

Resumen

La seguridad en el desarrollo de aplicaciones web ha adquirido una relevancia creciente en el ámbito educativo, aunque su implementación continúa representando un desafío para los desarrolladores. En este contexto, el análisis de la implementación de plataformas web desde una perspectiva formativa constituye una estrategia efectiva para fortalecer las competencias en ciberseguridad de los estudiantes de la Carrera de Computación.

El objetivo de este artículo es evaluar el nivel de madurez de las aplicaciones web tradicionales utilizando una plataforma web que integra recursos OWASP, incrementando los requisitos de seguridad y las mejores prácticas para el desarrollo de proyectos de software académico. Para el desarrollo de la plataforma se aplicó una variación de la metodología XP, que incluye las etapas de planeación, diseño, codificación y pruebas. La plataforma fue construida utilizando Node.js, ReactJS, ViteJS, PostgreSQL y MongoDB. La evaluación del nivel de madurez en seguridad se realizó mediante cuestionarios basados en el modelo OWASP SAMM. Los resultados evidenciaron una mejora significativa en el cumplimiento de buenas prácticas del 8,05 % al 62,21 % en el promedio general; y del 11,02 % al 74,90 % en el área de diseño, incrementando la seguridad a lo largo del ciclo de vida del desarrollo de software.

Palabras clave: OWASP; ASVS OWASP; OWASP SAMM; plataformas Web; seguridad WEB.

Abstract

Security in web application development has become increasingly important in the educational field, although its implementation continues to represent a challenge for developers. In this context, analyzing the implementation of web platforms from a training perspective constitutes an effective strategy for strengthening the cybersecurity competencies of Computer Science students.

The objective of this article is to evaluate the maturity level of traditional web applications using a web platform that integrates OWASP resources, increasing security requirements and best practices for the development of academic software projects. A variation of the XP methodology was applied to develop the platform, which includes the planning, design, coding, and testing stages. The platform was built using Node.js, ReactJS, ViteJS, PostgreSQL, and MongoDB. The security maturity level was assessed using questionnaires based on the OWASP SAMM model. The results showed a significant improvement in compliance with best practices, from 8.05% to

62.21% in the overall average. and from 11.02% to 74.90% in the design area, increasing security throughout the software development lifecycle.

Keywords: OWASP; OWASP ASVS; OWASP SAMM; Web platforms; Web security.

Resumo

A segurança no desenvolvimento de aplicações web tem se tornado cada vez mais importante no âmbito educacional, embora sua implementação continue representando um desafio para os desenvolvedores. Nesse contexto, analisar a implementação de plataformas web sob a perspectiva de treinamento constitui uma estratégia eficaz para o fortalecimento das competências em segurança cibernética de estudantes de Ciência da Computação.

O objetivo deste artigo é avaliar o nível de maturidade de aplicações web tradicionais utilizando uma plataforma web que integra recursos da OWASP, aumentando os requisitos de segurança e as melhores práticas para o desenvolvimento de projetos de software acadêmicos. Uma variação da metodologia XP foi aplicada para o desenvolvimento da plataforma, que inclui as etapas de planejamento, design, codificação e testes. A plataforma foi construída utilizando Node.js, ReactJS, ViteJS, PostgreSQL e MongoDB. O nível de maturidade em segurança foi avaliado por meio de questionários baseados no modelo OWASP SAMM. Os resultados mostraram uma melhora significativa na conformidade com as melhores práticas, de 8,05% para 62,21% na média geral e de 11,02% para 74,90% na área de design, aumentando a segurança em todo o ciclo de vida do desenvolvimento de software.

Palavras-chave: OWASP; OWASP ASVS; OWASP SAMM; Plataformas web; Segurança web.

Introducción

En la actualidad, el desarrollo seguro de aplicaciones web constituye un desafío crítico para los desarrolladores, dado que la aplicación de prácticas inadecuadas continúa generando vulnerabilidades capaces de comprometer la integridad de los sistemas y la confidencialidad de los datos de los usuarios (Robayo-Bautista, 2021). A pesar del creciente interés en la ciberseguridad, ataques como **SQL Injection** y **Cross-Site Scripting (XSS)** mantienen una tendencia ascendente (Menejías García et al., 2021), lo que evidencia la necesidad imperiosa de reforzar las medidas de

protección a lo largo de todo el Ciclo de Vida del Desarrollo de Software (SDLC) (Humayun, et al., 2022).

Según Ferdiansyah et al., (2023), detalla un estudio realizado a empresas de América Latina realizado por la compañía (Microsoft Latinoamérica, 2021), reporta que durante la pandemia el 31% de las organizaciones registró un aumento en los ciberataques, especialmente en el sector bancario, además, se descubrió que el 24% de las empresas incrementó su presupuesto en seguridad cibernética, y un 17% cuenta con un seguro de riesgo cibernético. Es alarmante que el 27% de las empresas permita que los empleados usen sus propios dispositivos tecnológicos para trabajar de manera remota, ya que esto representa un riesgo al desconocer el estado de los equipos

En el contexto de Ecuador, un estudio realizado por (Rendón et al., 2020), reporta un total de 5049 delitos informáticos consumado. Destacando que tres tipologías concentran aproximadamente el 92% de todos los casos reportados, lo que evidencia una alta concentración de incidencias en modalidades específicas de ciberdelito. La suplantación de identidad es el delito informático más común en Ecuador, con 2162 (43%) del total de casos reportados de los delitos informáticos. Por otro lado, la falsificación y uso de documentos falsos ocupa el segundo lugar con 1448 casos (29%), seguido por la apropiación fraudulenta a través de medios electrónicos con 1033 casos (20%). Estos datos evidencian la necesidad de tomar medidas preventivas y fortalecer la ciberseguridad en el país para reducir la incidencia de delitos informáticos.

Las metodologías de desarrollo seguro ofrecen un enfoque integral al incorporar la seguridad desde las primeras etapas del SDLC (Janisar et al., 2024). Sin embargo, su implementación enfrenta barreras como la falta de conocimientos especializados, recursos limitados y la complejidad de su integración en procesos de desarrollo existentes (Roshaidie et al., 2020). La colaboración entre equipos de seguridad y desarrollo, junto con una cultura de seguridad reforzada, es clave para superar estos desafíos (Mhara & Abdulrahman, 2022). En este contexto, diversos estudios han revelado un incremento en los ciberataques en América Latina y Ecuador, evidenciando la urgencia de fortalecer la ciberseguridad y reducir la incidencia de delitos informáticos(Rendón et al., 2020; Aslan et al., 2023).

Los aplicativos web son una parte crítica de las operaciones diarias de las organizaciones, utilizados por personal administrativo (Niazi et al., 2020). No obstante, a menudo no se enfoca en los aspectos de seguridad de estas aplicaciones (Ali et al., 2024), lo que las hace vulnerables a posibles ataques y violaciones de datos. A medida que las amenazas cibernéticas continúan aumentando, es esencial

que las universidades desarrollen y mantengan medidas de seguridad robustas para proteger sus aplicaciones web (Morante Mosquera & Daysi Magdalena, 2019).

Diversos estudios han explorado metodologías orientadas a la incorporación de directrices de seguridad en el desarrollo de software (Arega et al., 2024). No obstante, el presente trabajo ofrece un aporte significativo al aplicar las guías establecidas por OWASP (2021), en el contexto de los Trabajos de Integración Curricular (TIC) del área de computación. A partir de ello, se plantea la siguiente pregunta de investigación: ¿En qué medida la implementación de una plataforma web basada en OWASP contribuye al fortalecimiento de los requisitos y las buenas prácticas de seguridad en los proyectos de software desarrollados como TIC?.

Este trabajo implementa directrices de (OWASP, 2020) SAMM v2.0 y de ASVS (Alam et al., 2023), desarrollando una plataforma web que facilita la evaluación y mejora de la seguridad en el desarrollo de software. Se evaluaron 14 proyectos de desarrollo de software realizados en TIC de la Carrera de Computación, con el propósito de fortalecer los requisitos y buenas prácticas de seguridad en proyectos estudiantiles.

Materiales y Métodos

Para desarrollar la plataforma web basada en OWASP, se aplicó la Metodología de desarrollo de software Híbrida (XP-SCRUM) (Gonzaga et al., 2019). Se recopilaron requisitos mediante encuestas y se diseñaron prototipos con Figma y diagramas con Enterprise Architecture. La codificación se realizó en Visual Studio Code, con GitHub para la gestión del código. Finalmente, la plataforma fue evaluada con 14 proyectos registrados, utilizando cuestionarios del proyecto SAMM OWASP (2020). Se utilizó como base el proyecto OWASPSAMM (2024), el cual determinó el nivel de madurez en seguridad con base en los cuestionarios planteados en la guía versión 2.0 SAMM OWASP (2020). Tanto el proyecto utilizado como la guía 2.0 SAMM se implementaron en la aplicación web, para la evaluación de seguridad de proyectos.

En la Figura 1, se ilustra el modelo entidad-relación de la plataforma web, el mismo que evidencia los detalles de configuración y comportamiento de las clases, tablas y sus interrelaciones de la aplicación web.

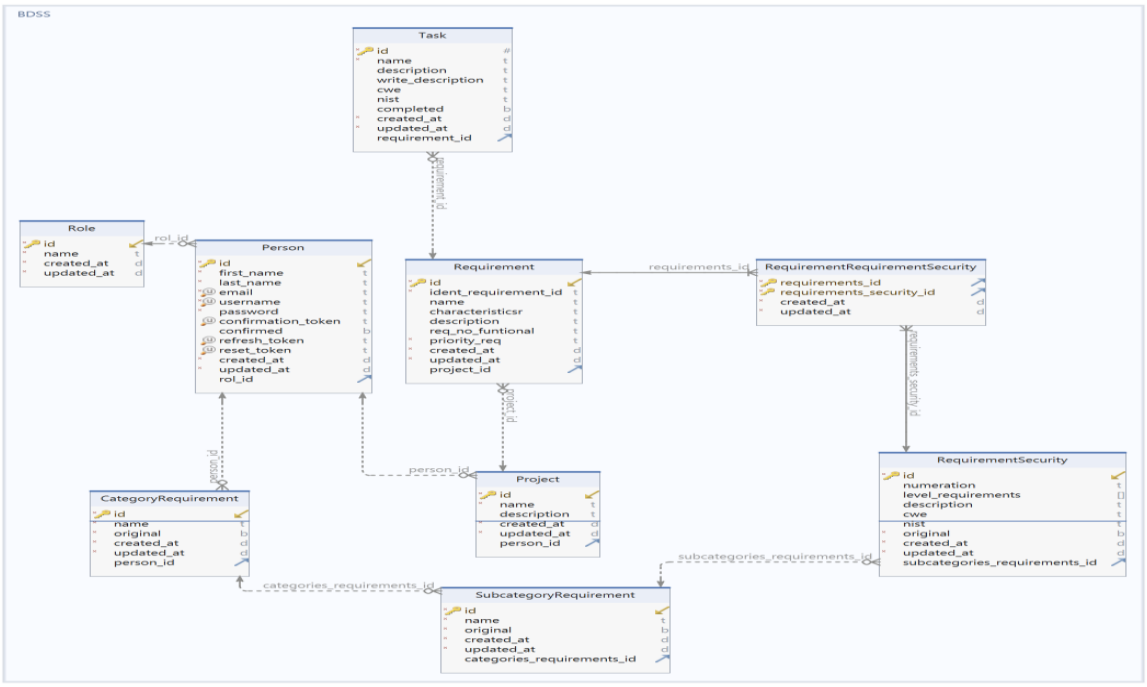

Figura 1. Modelo Relacional

En la Figura 2, se observa la arquitectura del sistema, el mismo que brinda una representación gráfica de las herramientas y tecnologías utilizadas en el sistema.

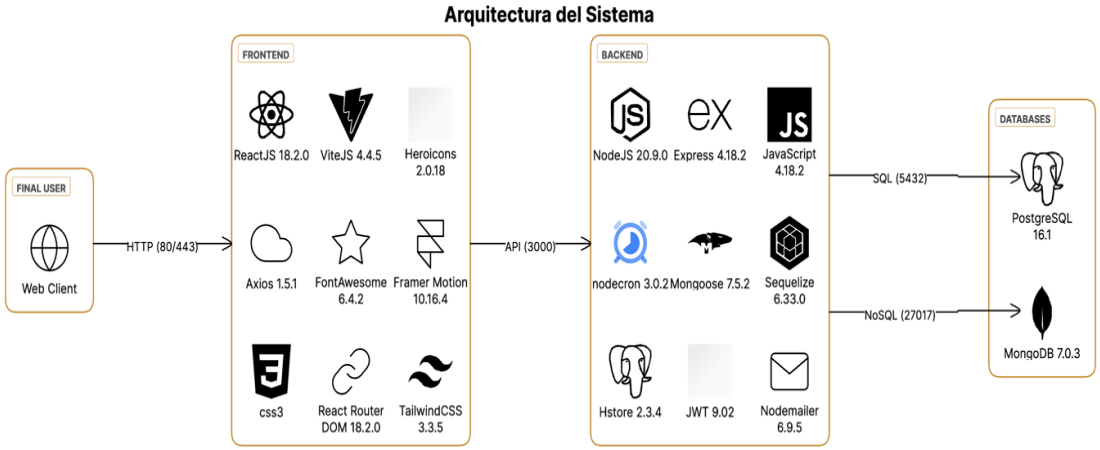

Figura 2. Arquitectura de la Plataforma Web

Resultados y discusión

Para el desarrollo de la plataforma se planificaron y validaron encuestas para identificar los requisitos de la plataforma web, con la participación de estudiantes y un experto en seguridad. En la fase de diseño, se definió la arquitectura del sistema y se crearon diagramas y prototipos de interfaz. Luego, durante la codificación, se implementaron iteraciones basadas en las historias de usuario y se revisó exhaustivamente el código tanto el back-end y front-end antes de las pruebas, los repositorios se encuentran en las siguientes direcciones: *https://github.com/vladimirCeli/Progresreqs-Backend* y *https://github.com/vladimirCeli/Progresreqs-Frontend* respectivamente. Finalmente, en la fase de se ejecutó la fase de pruebas dentro de la plataforma web, que consistió en evaluar los requisitos y buenas prácticas de seguridad en los proyectos de laboratorio pruebas, Se ejecutó la fase de pruebas dentro de la plataforma web, que consistió en evaluar los requisitos y buenas prácticas de seguridad en los proyectos de laboratorios de software de la Carrera de Computación, utilizando el modelo de madurez de aseguramiento de software de OWASP.

Los cálculos se llevaron a cabo como parte de un proceso integral que comprendió la aplicación de pruebas de seguridad en la plataforma web. Se empleó el cuestionario general de OWASP SAMM en dos momentos punto inicial y luego de implementar y parchear las tareas de seguridad identificadas en cada requisito de sus proyectos web como punto final. De formar similar, se siguió el procedimiento con el cuestionario enfocado en la fase de diseño. Estos permitiendo evaluar y mejorar la seguridad a nivel de requisitos y buenas prácticas de los proyectos web registrados en la plataforma. Sin embargo, OWASP SAMM no tiene una clasificación directa, para esta evaluación se ha adoptado el sistema de categorización de la herramienta SAMMWISE, que divide el desempeño en cuatro partes como se describe en la Tabla 1. Esta herramienta permitió categorizar las prácticas de acuerdo con su madurez y alinearlas con los principios de OWASP SAMM.

Tabla 1. *Categorías de madurez en base a principios de OWASSP SAMM*

Puntaje (%)	Rango	Descripción
0	Malo	Indica que la práctica no está implementada.
25	Regular	Refleja prácticas básicas y deficientes
50	Aceptable	Visualiza prácticas formalizadas, pero mejorables

100	Bueno	Muestra prácticas optimizadas e integradas en la organización.

Se examinaron 14 proyectos TICs desarrollados por estudiantes de Computación como se indica en la Tabla 2, en la cual se describe también los requisitos funcionales y no funcionales para su desarrollo.

Tabla 2. *Lista de proyectos TIC evaluados de la carrera de Computación de la UNL*

Identificador (IDP)	**Proyectos**	# de requisitos (funcionales y no funcionales)
1	SGPI	15
2	Kardex	10
3	Remenber	15
4	Web Shop	13
5	Sports Notes	15
6	Notflix	12
7	Prototipo web para intervención y estimulación psicopedagógica	16
8	System-bookings	7
9	QualityCCode	4
10	itechdata	22
11	aprendiendoJuntos	18
12	PWTEA	10
13	LCK	16
14	BiBlioPer	7

En la Tabla 3, se presentan los resultados del análisis de pruebas en la fase inicial de los 14 proyectos evaluados en la carrera de Computación. Los cálculos se presentan sobre una escala de 0 a 3, en concordancia con el modelo SAMM de (OWASP, 2020) y su herramienta de apoyo OWASPSAMM (2024), que estructuran la madurez en tres niveles. El nivel 1: prácticas iniciales, nivel 2: prácticas definidas e integradas, y nivel 3: prácticas optimizadas y en mejora continua. Esta categorización facilita evaluar a una organización para alcanzar prácticas óptimas de seguridad; de esta forma, la notación "/3" en columna puntuación general la porción del nivel máximo posible dentro de la escala de madurez.

La evaluación inicial general con OWASP SAMM (ICO): En base a los resultados recopilados en la Tabla 3, se realizó un análisis promedio de las 14 pruebas llevadas a cabo en la plataforma web, utilizando cada uno de los cuestionarios correspondientes. Se calcula ICO = (Total puntuación general / 14) = 3.38 /14 =0.2414. La evaluación resultante es 0.2414/3= 0.0804 (8.04%). Lo que indica un cumplimiento de 8.04% de requisitos y buenas prácticas de seguridad en proyecto de software tradicionales, este valor es categorizado como malo como se indica en la Tabla 1.

Tabla 3. *Resultados en cada sección de los cuestionarios que enmarca la fase inicial general de OWASP*

IDP	**Pruebas de seguridad**	**Estrategia y métricas**	**Política y cumplimiento**	**Educación y Orientación**	**Construcción segura**	**Despliegue seguro**	**Gestión de defectos**	**Gestión de incidentes**	**Gestión del entorno**	**Gestión operacional**	**Evaluación de amenazas**	**Requisitos de seguridad**	**Arquitectura de seguridad**	**Evaluación de la arquitectura**	**Pruebas basadas en los requisitos**	**Puntuación general**	**Porcentaje (%)**
1	0	0	0	1,125	1,5	0	0	0	1,75	2,125	0	0	1,75	0	0	0,55/3	18,33
2	0	0	0	0	0	0	0	0	0	0,875	0	0	0	0	0,75	0,11/3	3,67
3	1,125	0	1,25	1,375	1,5	1,5	1,25	1,5	1,375	1,375	1,375	1,5	1,25	1,375	1,375	1,27/3	42,33
4	0	0	0	0	0	0	0,75	0	0	0	0	0,75	0	0,75	0,75	0,20/3	6,67
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0/3	0,00
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0/3	0,00
7	0,75	0,875	0,75	0,75	0,75	1	1	0,75	0,75	0,75	0,75	0,75	0,75	0,75	0,75	0,79/3	26,33
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0/3	0,00
9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0/3	0,00
10	0	0	0	0	0	0,75	0	0	0,75	0	0	0,75	0,75	0	0	0,20/3	6,67
11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0/3	0,00
12	0	0	0	0	0	0	0	0	0	0	0,75	0	1,5	0,75	0	0,11/3	3,67

Pol. Con. (Edición núm. 110) Vol. 10, No 9, Septiembre 2025, pp. 552-567, ISSN: 2550 - 682X

13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0/3	0,00
14	0	0	0,75	0	0	0	0	0,75	0,75	0	0	0	0	0	0	0,15/3	5,00
Total Puntuación general																3.38	

La evaluación final cuestionario general OWASP SAMM (FCO): Al implementar mejoras en seguridad en los proyectos TICs; se procedió a calcular el promedio de las 14 pruebas llevadas a cabo en la plataforma web, utilizando cada uno de los cuestionarios correspondiente como lo ilustra la Tabla 4. Se calcula FC0= 26.13/14 =1.87. La evaluación final resultante es 1.87/3= 0.623 (62.3%). Es un notable crecimiento en la seguridad de aplicaciones web tradicionales y este valor es categorizado como Bueno como se indica en la Tabla 1.

Tabla 4. *Resultados en cada sección de los cuestionarios que enmarca la fase final de OWASP*

IDP	**Pruebas de seguridad**	**Estrategia y métricas**	**Política y cumplimiento**	**Educación y Orientación**	**Construcción segura**	**Despliegue seguro**	**Gestión de defectos**	**Gestión de incidentes**	**Gestión del entorno**	**Gestión operacional**	**Evaluación de amenazas**	**Requisitos de seguridad**	**Arquitectura de seguridad**	**Evaluación de la arquitectura**	**Pruebas basadas en los requisitos**	**Puntuación general**	**Porcentaje (%)**
1	2,25	2,25	1,625	2,25	2	2,375	2,25	2,125	2,25	1,875	1,625	1,375	2,25	1,875	2,5	2,06/3	68,67
2	0	2,5	2,5	0	2,75	2,5	2,75	2,5	2,75	2,5	2,75	2,75	2,5	0	2,75	2,10/3	70
3	2,5	2,5	0	0	2,75	2,5	3	1,875	2,125	1,375	2,75	1,625	1,375	0	2,5	1,79/3	60
4	2,75	2,25	2,25	2,5	2,5	2,5	2,5	2,75	2,75	2,75	2,75	2,75	3	2,75	2,75	2,63/3	88
5	3	2,75	3	2,75	2,25	2,5	2,5	2,25	2,5	2,75	2,75	3	2,5	2,75	2,5	2,65/3	88
6	0	1,75	1,5	0	1,75	1,75	1,75	1,5	0	0	1,5	2,75	2,25	2,5	2,5	1,43/3	48
7	2	2,5	2	2	2,5	2	1,75	2,25	2	1,75	1,75	1,75	2	2,25	2	2,03/3	68

8	0	0	1,625	0	0	0	1,25	0	1,375	0	1,5	2	2,5	0	0	0,76/3	25,33
9	2,5	2,75	3	0	0	3	3	3	2,75	3	3	3	3	3	0	2,33/3	78
10	2,125	2	2,125	1,75	1,875	1,875	2,25	2,25	2	1,875	2,25	2	2,25	2,25	2,25	2,08/3	69
11	2,75	1,75	2,25	2	2,5	2,25	2,5	2,25	2,25	1,75	2,5	2,25	2,5	2,25	2,25	2,27/3	76
12	2,25	0	0	0	0	0	0	2,25	0	0	2,75	1,375	0	2,5	2,5	0,91/3	30
13	1,5	1,625	1,375	1,625	2	2,125	1,75	2	1,75	1,625	1,75	1,25	2,75	2	1,125	1,75/3	58
14	1,375	0,75	1,25	1,375	1,5	1,375	1	1,625	1,75	1,25	1,25	1,25	1,625	1,5	1,25	1,34/3	45
Total Puntuación general																26.13	

Con la finalidad de evaluar la mejora en la madurez de las prácticas de OWASP (NMO), se calcula la diferencia entre FCO y ICO. NMO= FCO-ICO= 1.63. Este resultado refleja una mejora del 1.63/3 con un cumplimiento del 54.17 % en el nivel de madurez total de los proyectos registrados en la plataforma web. La métrica proporciona una visión más detallada de cómo las medidas de seguridad implementadas han contribuido a la mejora de la madurez de las prácticas en términos de seguridad en los proyectos web.

Evaluación inicial del diseño de seguridad (ICD): Al igual que en el primer cuestionario, se llevó a cabo el mismo proceso para el segundo cuestionario, que se centra en el diseño con enfoque en la infraestructura de seguridad, requisitos de seguridad y evaluación de amenazas. Se realizó un promedio de las 14 pruebas en la plataforma web como se describe en la Tabla 5. Se calcula ICD = 4.63/14 =0.33. La evaluación inicial resultante en el diseño es 0.33/3 = 11.02 (11.02%) de buenas prácticas en la seguridad.

Tabla 5. *Resultados en cada sección de los cuestionarios que enmarca la fase Inicial de Diseño*

IDP	Evaluación de amenazas	Requisitos de seguridad	Arquitectura de seguridad	Puntuación general	**Porcentaje (%)**
1	0	0	1,5	0,50/3	16,67
2	0	0	0	0/3	0
3	1,375	1,375	1,375	1,38/3	46

4	0,875	0,75	0,75	0,79/3	26
5	0	0	0	0/3	0
6	0,75	0	0	0,25/3	8
7	0,75	0,75	0,75	0,75/3	25
8	0	0	0	0/3	0
9	0	0	0	0/3	0
10	0	0,875	0,75	0,54/3	18
11	0	0	0	0/3	0
12	0	0	0	0/3	0
13	0	0	0	0/3	0
14	1,25	0	0	0,42/3	14
			Total Puntuación General= 4.63		

Evaluación Final del diseño de seguridad (FCD): Al implementar mejoras en el diseño como se muestra en la Tabla 6; se procede a calcular el promedio FCD=30.96/14 = 2.21. La evaluación final del diseño denota un cumplimiento de 2.21/3 = 0.737 (73.7%) de mejoramiento de buenas prácticas en seguridad en el diseño de aplicaciones web tradicionales.

Luego de evaluar la mejora en la madurez de las prácticas de diseño de seguridad (NMO), se realizó una diferencia entre FCD y ICD. NMO= FCD-ICD=2.21-0.33= 1.88. La mejora de 1.85/3, con un cumplimiento del 62.7%, en el nivel de madurez del diseño para los proyectos registrados en la plataforma web, revelando un avance significativo en la implementación de prácticas de seguridad. Este progreso se traduce en una mayor robustez y eficacia en las estrategias de arquitectura de seguridad, requisitos de seguridad y evaluación de amenazas incorporadas en los proyectos web.

Tabla 6. *Resultados en cada sección de los cuestionarios que enmarca la fase final de Diseño*

IDP	Evaluación de amenazas	Requisitos de seguridad	Arquitectura de seguridad	Puntuación general	**Porcentaje (%)**
1	2,25	2,25	2,25	2,25/3	75
2	2,5	2,75	2,75	2,67/3	89
3	2,75	2,75	2,5	2,67/3	89%
4	2,75	2,5	2,25	2,50/3	83
5	2,25	2,75	2,75	2,58/3	86
6	2,125	1,75	2	1,96/3	65
7	2,5	2,5	2,5	2,50/3	83
8	2,25	2,75	2,75	2,58/3	86
9	2,25	2,25	0	1,50/3	50

10	1,625	2,375	2	2/3	67
11	2,5	2,25	2,75	2,5/3	83
12	2,5	2	0	1,5/3	50
13	1,5	2,5	1,5	1,83/3	61
14	2,25	2,25	1,25	1,92/3	64
	Total Puntuación General= 30.96				

Los resultados obtenidos reflejan una mejora sustancial en la implementación de prácticas de seguridad en los proyectos evaluados. Inicialmente, la mayoría de los proyectos se encontraban en los niveles “Malo” o “Regular” según la categorización de OWASPSAMM (2024). Sin embargo, después de implementar mejoras en seguridad, los proyectos lograron avanzar niveles “Aceptable” y “Bueno”, lo que demuestra el impacto positivo de la aplicación de medidas correctivas. En particular, se destacan avances en la madurez en seguridad general con base en el modelo v2.0 SAMM OWASP (2020), registrando un incremento del 54.17 %, evidenciando una adopción más formalizada y efectiva de prácticas de seguridad en el desarrollo. La madurez en diseño de seguridad mejora del 62.7 %, lo que indica que los proyectos fortalecieron significativamente la seguridad desde su concepción y diseño.

Estos resultados resaltan la relevancia de aplicar buenas prácticas sobre la protección en el proceso de desarrollo de software. La adopción de metodologías basadas en el modelo SAMM v2.0 de OWASP (2020), mejoró la seguridad de los proyectos de forma efectiva y sostenible, garantizando la reducción de vulnerabilidades y aumentando la capacidad de resiliencia de las plataformas web tradicionales.

Conclusiones

El desarrollo de la plataforma web fortaleció los requisitos y buenas prácticas de seguridad en los 14 proyecto de software tradicionales, logrando un cumplimiento general inicial que pasó del 8.04% al 62.3 %. El análisis promedio de las 14 pruebas realizadas en la plataforma web revela un crecimiento notable en el porcentaje de cumplimiento general. Se inició con un promedio general inicial (ICO) del 8.04 %, categorizado como malo, mientras que al final del proceso (FC0), alcanzó un 62.3 %, categorizado como aceptable, indicando una mejora sustancial en la seguridad general de los proyectos web tradicionales registrados en la plataforma web.

Pol. Con. (Edición núm. 110) Vol. 10, No 9, Septiembre 2025, pp. 552-567, ISSN: 2550 - 682X

Con a la evaluación especifica en el cuestionario de diseño, el cumplimiento inicial promedio (ICD) fue del 11.02 % considerado como malo y después de implementar las acciones requeridas, se alcanzó un 73.7 %, categorizado como aceptable, en el cumplimiento final (FCD). Esto destaca la importancia de las estrategias de arquitectura de seguridad, requisitos de seguridad y evaluación de amenazas en la mejora del nivel de madurez en seguridad de requisitos en los proyectos registrados en la plataforma web.

Los resultados obtenidos en las pruebas no alcanzan el 100% debido a que los cuestionarios utilizados (OWASP SAMM) manejan un enfoque de madurez progresiva. Estos instrumentos están diseñados para reflejar el nivel real de implementación de prácticas de seguridad y destacar áreas de mejora. Por ello, más que buscar un puntaje perfecto, el valor principal está en identificar brechas, priorizar acciones y fomentar la mejora continua en la gestión de la seguridad del software.

Investigaciones futuras

Es necesario realizar investigaciones futuras ampliando la cobertura en seguridad de arquitecturas modernas con DSOMM, incluyendo entornos basados en contenedores y microservicios, con enfoque en la detección y mitigación de vulnerabilidades en la comunicación entre servicios y la gestión de permisos de usuarios. Adicionalmente, incorporar soporte para nuevas categorías de vulnerabilidades emergentes, tales como las relacionadas con el Internet de las Cosas (IoT), Inteligencia Artificial, y aplicaciones móviles.

Integrar la plataforma con herramientas de DevSecOps para automatizar la validación de requerimientos de seguridad en las etapas del SDLC, conectándola a pipelines CI/CD y generando reportes en tiempo real sobre el estado de seguridad de los proyectos.

Referencias

1. Alam, G., Mahmood, S., Alshayeb, M., Niazi, M., & Zafar, S. (2023). Maturity model for secure software testing. Journal of Software: Evolution and Process, e2593. https://doi.org/https://doi.org/10.1002/smr.2593
2. Ali, M., Uddin, M. S., Uddin, N., & Hasan, M. D. M. (2024). Impact of Security assessment for more secure software – A Tactics and Multi-Dimensional Perspective. Research Square (Research Square). https://doi.org/10.21203/rs.3.rs-3999692/v1

3. Arega, K. L., Beyene, A. M., & Yitagesu, S. (2024). Security Assurance in the Software Development Process: A Systematic Literature Review. Communications in computer and information science. https://doi.org/10.1007/978-3-031-59107-5_2
4. Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. En Electronics (Switzerland) (Vol. 12, Número 6). MDPI. https://doi.org/10.3390/electronics12061333
5. Ferdiansyah, D., Isnanto, R. R., & Suseno, J. E. (2023). Organizational indicators on startup software for implementing secure software development lifecycle (SSDL): A systematic literature review. AIP conference proceedings. https://doi.org/10.1063/5.0125388
6. Humayun, M., Niazi, M., Jhanjhi, N. Z., Mahmood, S., & Alshayeb, M. (2022). Toward a readiness model for secure software coding. Software Practice and Experience. https://doi.org/10.1002/spe.3175
7. Janisar, A. A., Shafee, K., Sarlan, A., Maiwada, U. D., & Salameh, A. A. (2024). Securing Software Development: A Holistic Exploration of Security Awareness in Software Development Teams. International Journal of Academic Research in Business and Social Sciences. https://doi.org/10.6007/ijarbss/v14-i1/20545
8. Marcos Klender Carrasco Gonzaga, Willian Javier Ocampo Pazos, Luis Javier Ulloa Meneses, & Jon Azcona Esteban. (2019). Metodología Híbrida de Desarrollo de Software combinando XP y SCRUM. Mikarimin. Revista Científica Multidisciplinaria, 5(2)(2), 109-116. https://www.revista.uniandes.edu.ec/ojs/index.php/mikarimin/article/view/1233
9. Menejías García, Roberto, Hidalgo Reyes, Noel Harrinso, Marín Díaz, Aymara, Trujillo Casañola, & Yaimí. (2021). Procedimiento para evaluar seguridad a productos de software. Revista Cubana de Ciencias Informáticas, 15(4), 333-349. http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2227-18992021000500333
10. Mhara, M. A. O. A., & Abdulrahman, A. (2022). Application and Software Security: Studying How to Secure Applications and Software from Vulnerabilities and Attacks. Stallion Journal for Multidisciplinary Associated Research Studies. https://doi.org/10.55544/sjmars.1.2.9
11. Microsoft Latinoamérica. (2021, marzo 2). Marsh y Microsoft: ingeniería social o phishing es el ciberataque que más aumentó en Latinoamérica a raíz de la pandemia - News Center

Latinoamérica. https://news.microsoft.com/es-xl/marsh-y-microsoft-ingenieria-social-o-phishing-es-el-ciberataque-que-mas-aumento-en-latinoamerica-a-raiz-de-la-pandemia/

12. Morante Mosquera, & Daysi Magdalena. (2019). Uso de los Modelos de Control Informático y su incidencia en la Seguridad de la Información en el Sistema de Control de Calificaciones de la Universidad Técnica de Babahoyo [Universidad Técnica de Babahoyo]. http://dspace.utb.edu.ec/handle/49000/5715
13. Niazi, M., Saeed, A. M., Alshayeb, M., Mahmood, S., & Zafar, S. (2020). A maturity model for secure requirements engineering. Computers & Security. https://doi.org/10.1016/j.cose.2020.101852
14. OWASP. (2020, febrero 11). OWASP SAMM. https://owaspsamm.org/resources/pdf/
15. OWASP. (2021). OWASP Application Security Verification Standard. https://owasp.org/www-project-application-security-verification-standard/
16. OWASPSAMM. (2024, marzo). GitHub - owaspsamm/sammwise: NextJS-based single-page application for completing and reviewing SAMM assessments. https://github.com/owaspsamm/sammwise
17. Rendón Zambrano Aura Dolores, Loor Campúes Fausto Daniel, & Zambrano Vera Wilmer Orley. (2020). DELITOS INFORMÁTICOS EN TIEMPOS DE COVID: REVISIÓN LITERARIA ECUADOR. https://www.espam.edu.ec/recursos/sitio/informativo/archivos/ponencias/vinculacion/i/s3/CIV52EIT24.pdf
18. Robayo-Bautista, E. C. (2021). Guía de principios y buenas prácticas para pruebas de seguridad de software en aplicaciones web para una empresa del sector privado. Universidad Católica de Colombia. https://hdl.handle.net/10983/25731
19. Roshaidie, M. D., Liang, W. P. H., Jun, C. G. K., Yew, K. H., & Fatimatuzzahra, F. (2020). Importance of Secure Software Development Processes and Tools for Developers. arXiv (Cornell University). https://doi.org/10.48550/arxiv.2012.15153