

FICHA DE TALLER

➤ Datos generales:

Título:	Seguridad en aplicaciones móviles					
Instructor o docente:	Felipe de Jesús Vázquez Victoria					
Duración total de taller:	4 sesiones virtuales de 2 hrs. C/U, 1 sesión presencial de 3 hrs.					
Área:	<input type="checkbox"/>	Formación para la docencia	<input type="checkbox"/>	Formación para la gestión universitaria	<input checked="" type="checkbox"/>	Otra
Modalidad de impartición:	<input type="checkbox"/>	Presencial	<input type="checkbox"/>	A distancia	<input checked="" type="checkbox"/>	Híbrida
Fechas:	26 de septiembre, 2, 9, 14 y 21 de octubre					

➤ Descripción:

Destinatarios:

El taller de seguridad en aplicaciones móviles está diseñado para satisfacer las necesidades específicas de los profesionales en el ámbito de la tecnología de la información. Dirigido a encargados de áreas de TI, desarrolladores de software y personal operativo.

Objetivo(s) o competencia(s):

El taller ofrece estrategias avanzadas y conocimientos prácticos para proteger las aplicaciones móviles contra amenazas emergentes. Este programa es esencial para aquellos que buscan mantener la integridad y la confidencialidad de la información en un mundo cada vez más móvil y conectado.

Metodología y Actividades:

Se empleará un enfoque centrado en el instructor, donde el conocimiento y experiencia del docente guiarán el proceso de aprendizaje. El curso también abarcará análisis de casos prácticos y discusiones dirigidas, basándose en la participación y retroalimentación de los asistentes.

Mecanismo y criterios de evaluación:

Participación en clase. Kahoot al finalizar cada sesión

➤ **Temario:**

No. De sesión	Fecha	Hora	Temas a abordar
Sesión 1	26 de septiembre	16:00 – 18:00 hrs	1. Introducción a las aplicaciones móviles a) Crecimiento en las TICs b) Usos 2. Taxonomía de aplicaciones a) Arquitecturas b) Tipos de datos
Sesión 2	2 de octubre	16:00 – 18:00 hrs	3. APIs 4. Protocolo HTTP
Sesión 3	9 de octubre	16:00 – 18:00 hrs	5. Seguridad en aplicaciones móviles a) Metodologías y frameworks de análisis b) Principios de pentesting i. Black box ii. White box iii. Gray box iv. SAST v. DAST c) Fases de pentesting i. Preparación ii. Recopilación de información iii. Mapeo iv. Explotación v. Reporteo d) Métricas i. CVE ii. CWE e) Herramientas del mercado i. SAST ii. DAST f) OWASP Mobile Top 10 6. Preparación de ambiente para pentesting a) Instalación de herramientas b) Consideraciones
Sesión 4	14 de octubre	16:00 – 18:00 hrs	7. Demo - Análisis de aplicación con método SAST



Sesión 5			8. Demo - Análisis de aplicación con método DAST
	21 de octubre	16:00 – 19:00 hrs	9. Mejores prácticas del mercado 10. Conclusiones

➤ **Bibliografía**

- OWASP. (2023). *OWASP Mobile Top 10*. <https://owasp.org/www-project-mobiletop-10/>
- R. Fielding. (2014). Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content. Internet Engineering Task Force (IETF). <https://datatracker.ietf.org/doc/html/rfc7231#section-4>
- Mozilla. HTTP request methods. <https://developer.mozilla.org/enUS/docs/Web/HTTP/Methods>
- Imperva. Black Box Testing. <https://www.imperva.com/learn/applicationsecurity/black-box-testing/>
- Imperva. White Box Testing. <https://www.imperva.com/learn/applicationsecurity/white-box-testing/>
- Imperva. Gray Box Testing. <https://www.imperva.com/learn/applicationsecurity/gray-box-testing/>

➤ **Recursos y materiales requeridos**

- Equipo de cómputo
 - o 8 GB RAM
 - o Core i3 o equivalente
 - o Windows 10 / Windows 11 / MacOS (10 en adelante) / Ubuntu (18 en adelante) o equivalente
 - o Microsoft Teams (Personal, Educativo o Empresarial) o Zoom