

**UNIVERSIDAD POLITECNICA
DE SAN LUIS POTOSI**

**COMPARACIÓN DE METODOLOGIAS
DE SEGURIDAD INFORMATICA**

Metodología	Descripción breve	Fases principales	Objetivo principal	Escenarios de uso	Orientación	Autores	URL Oficial	Existencia de certificados	Versiones vigentes
MTRE ATT&CK	Base de conocimiento globalmente accesible de tácticas y técnicas adversarias basadas en observaciones del mundo real.	<ol style="list-style-type: none"> 1. Reconocimiento 2. Desarrollo de recursos 3. Acceso inicial 4. Ejecución 5. Persistencia 6. Escalación de privilegios 7. Evasión de defensa 8. Acceso de credenciales 9. Descubrimiento 10. Movimiento lateral 11. Colección 12. Comando y control 13. Exfiltración 14. Impacto 	Proporcionar una base de conocimiento estructurada, exhaustiva y accesible de las tácticas, técnicas y procedimientos (TTP) utilizados por los atacantes en el mundo real, facilitando la detección, defensa y comprensión de ciber amenazas.	<p>Las tácticas de y técnicas MTRE ATT&CK son comúnmente usadas en escenarios como:</p> <ul style="list-style-type: none"> • Detección y análisis • Conocimiento de amenazas • Emulación adversaria (Red Teaming) • Asesoramiento e ingeniería 	MTRE ATT&CK está orientada a recopilar, modelar, detectar y comprender el comportamiento de los cibercriminales basándose en casos reales.	MTRE Corporation	https://attack.mitre.org/	<p>Avaladas por MITRE Engenuity validando la capacidad de aplicar TTP's en entornos reales:</p> <ul style="list-style-type: none"> • ATT&CK Fundamentals • CTI • Metodología de emulación adversaria • Assessment SOC • Purple Teaming Methodology 	La versión más reciente es la ATT&CK V18.1 Subida el 28 de octubre de 2025 para el actual 15 de febrero de 2026.
OWASP WSTG	Guía completa para probar la seguridad de sitios y aplicaciones web	<ol style="list-style-type: none"> 1. Gestión de Configuración y Despliegue 2. Gestión de Identidad 3. Autenticación 4. Autorización 5. Gestión de Sesiones 6. Validación de Entrada 7. Manejo de Errores 8. Criptografía Débil 9. Lógica de Negocio 10. Del lado del Cliente 11. API 	Proporcionar un marco de trabajo estandarizado, completo y actualizado para evaluar la seguridad de aplicaciones y servicios web.	<ul style="list-style-type: none"> • Recolección de Información y Mapeo (WSTG-INFO) • Pruebas de Configuración y Despliegue (WSTG-CONF) • Pruebas de Identidad y Autenticación (WSTG-ATHN) • Pruebas de Autorización (WSTG-ATHZ) • Pruebas de Gestión de Sesiones (WSTG-SESS) • Pruebas de Validación de Entradas (WSTG-INP) • Pruebas de Lógica de Negocio y Errores (WSTG-BUSL / WSTG-ERR) 	Orientada a la recopilación de vulnerabilidades y guía sobre como hacer un testing sistemático de la seguridad de un sistema o aplicación web.	<p>Líderes destacados:</p> <p>Matteo Meucci (2007-2020).</p> <p>Andrew Muller (2013-2019).</p> <p>Eoin Keary (2005-2007)</p> <p>Daniel Cuthbert (2003-2005).</p> <p>Mantenedores principales actuales:</p> <p>Rick Mitchell.</p> <p>Elie Saad.</p> <p>Rejah Rehim.</p> <p>Victoria Drake.</p>	https://devguide.owasp.org/	<p>No existen certificaciones oficiales para validar el conocimiento adquirido sobre OWASP WSTG, sin embargo, existen certificaciones relacionadas que tienen base en OWASP:</p> <ul style="list-style-type: none"> • Certified OWASP Security Fundamentals • Certificación Mobile App Security (MASVS/ MASTG) 	Versión más reciente de OWASP WSTG: Versión 4.2 lanzada en 2020-12-03 para el actual 15 de febrero de 2026.
OSSTMM	Estándar abierto y científico para realizar auditorías técnicas de seguridad operativa, pentesting y análisis de vulnerabilidades.	<ol style="list-style-type: none"> A. Seguridad de la información B. Proceso de seguridad C. Tecnologías de internet y seguridad D. Comunicaciones y seguridad E. Seguridad inalámbrica F. Evaluación de la seguridad física 	Proporcionar un manual de funja como marco de trabajo para profesionales y organizaciones acerca de las fases a seguir en la ejecución de una auditoria de seguridad (Pentesting).	<ul style="list-style-type: none"> • Auditorias de seguridad física • Pruebas de seguridad en redes y telecomunicaciones • Ingeniería social y seguridad humana • Auditoria de seguridad operativa y cumplimiento • Hacking ético y pruebas de penetración 	se centra en métricas verificables, ofreciendo una visión integral, precisa y consistente de las vulnerabilidades y la efectividad de los controles de seguridad.	<p>Figura principal que creo la metodología a través de la ISECOM (Institute for Security and Open Methodologies):</p> <p>Pete Herzog.</p>	https://www.isecom.org/certification.html	<ul style="list-style-type: none"> • OSSTMM Professional Security Analyst • OSSTMM Professional Security Tester • OSSTMM Professional Security Expert • OSSTMM Wireless Security Expert • OSSTMM Certified Trust Analyst • Certified Security Awareness Instructor • Certified Hacker Analyst • Certified Hacker Analyst Trainer • Certified Cyber Trooper • Certified Junior Hacker 	La versión más reciente es la versión 3 (OSSTMM 3), lanzada oficialmente en 2010 por ISECOM, con actualizaciones menores como la v3.0.2. Esto para el actual 15 de febrero de 2026.

Metodología	Descripción breve	Fases principales	Objetivo principal	Escenarios de uso	Orientación	Autores	URL Oficial	Existencia de certificados	Versiones vigentes
PTES	Marco integral de referencia multifacético para pruebas de penetración o pentesting.	<ol style="list-style-type: none"> 1. Interacciones previas al compromiso 2. Recolección de inteligencia 3. Modelado de amenazas 4. Análisis de vulnerabilidades 5. Explotación 6. Post explotación 7. Reporte 	Proporcionar un marco completo, Estandarizado Y de alta calidad para llevar a cabo pruebas de penetración.	<ul style="list-style-type: none"> • Pruebas de infraestructura de red • Aplicaciones Web y API's • Pruebas de ingeniería social • Entornos de la nube • Inspección reglamentaria 	Enfocado a la evaluación de la seguridad de la infraestructura y de las redes de comunicación.	Creado por un colectivo anónimo de expertos de la industria, ningún nombre publico relacionado.	http://www.penteststandard.org/index.php/Main_Page	A la fecha no existen certificados oficiales que le den valor al conocimiento sobre PTES, sin embargo, se considera un estándar dentro de la industria para las pruebas de penetración pentest.	Penetration Testing Execution Standard (PTES) v1.0. Publicada el 16 de agosto de 2014 a las 8:14 P.M. Para el 15 de febrero de 2026
ISSAF	Marco de evaluación estructurado para la realización de pruebas de penetración pentest.	<ol style="list-style-type: none"> 1. Planificación y Preparación 2. Evaluación (Assessment) 3. Reporte, Limpieza y Destrucción de Artefactos 	proporcionar una metodología estructurada, detallada y completa para la realización de pruebas de penetración (pentesting) y evaluaciones de seguridad en sistemas de información.	<ul style="list-style-type: none"> • Pruebas de penetración (pentesting) • Evaluación de seguridad de aplicaciones web • Auditoria de seguridad 	Proporcionar una metodología que conecta los pasos de las pruebas de seguridad con herramientas específicas.	Desarrollada y liberada por OISSG (Open Information Systems Security Group)	form.com/oissg/	No se tiene conocimiento de certificados asociados, ya que la ISSAF existe como una metodología y marco de trabajo.	La versión mas reciente de la ISSAF es comúnmente conocida como Draft 0.2 o 0.2.1A publicada alrededor del 2005. Para el 15 de febrero de 2026.