




16 DE FEBRERO DE 2026

## ACTIVIDAD 05

CARTOGRAFIANDO EL PENTESTING: ANÁLISIS COMPARATIVO DE  
METODOLOGÍAS DE SEGURIDAD INFORMÁTICA

CAROL ELIZABETH CORTES BELTRAN  
UNIVERSIDAD POLITECNICA DE SAN LUIS POTOSI  
Seguridad Informática



# Introducción

En el panorama tecnológico actual, caracterizado por la evolución constante de las ciberamenazas, las pruebas de penetración y la evaluación de la seguridad informática se han consolidado como pilares fundamentales de una gestión eficaz de riesgos. La necesidad de ir más allá de los controles preventivos ha convertido a estas prácticas en herramientas indispensables para validar la postura de seguridad de las organizaciones, permitiendo identificar vulnerabilidades, evaluar la efectividad de las defensas implementadas y simular escenarios de ataque realistas.

Para abordar esta compleja tarea, la industria y la academia han desarrollado diversos marcos de referencia y estándares que guían la ejecución de pruebas de seguridad. Estas metodologías, lejos de ser homogéneas, presentan enfoques, alcances y objetivos particulares: mientras algunas se centran en el análisis ofensivo y técnico, otras priorizan la evaluación formal de controles o el mapeo estratégico de las tácticas y técnicas empleadas por los adversarios.

El presente documento tiene como objetivo analizar y comparar de manera estructurada seis metodologías y marcos ampliamente reconocidos en el ámbito profesional: **MITRE ATT&CK, OWASP WSTG, NIST SP 800-115, OSSTMM, PTES e ISSAF**. A través de una tabla comparativa, se examinan sus características principales, fases, objetivos, escenarios de aplicación, orientación estratégica, organismos responsables, certificaciones asociadas y su vigencia en el contexto actual de la ciberseguridad.

Metodología	Descripción	Fases de implementación	Objetivo principal	Escenarios de uso	Orientación	Autores / organismos	Certificaciones asociadas	Versiones / vigencia
<b>MITRE ATT&amp;CK</b>	Plataforma de conocimiento que documenta y clasifica las tácticas y técnicas empleadas por actores de amenazas en ataques reales.	Reconocimiento inicial, Preparación de recursos, Punto de entrada, Activación de código, Mantenimiento de acceso, Obtención de mayores privilegios, Ocultamiento de actividades, Robo de credenciales, Exploración interna, Desplazamiento lateral, Sustracción de datos, Canales encubiertos, Filtración de información, Alteración de servicios.	Establecer un lenguaje común para identificar comportamientos adversarios, simular operaciones ofensivas, reforzar mecanismos de defensa y optimizar la capacidad de respuesta ante incidentes.	Búsqueda proactiva de amenazas, priorización de alertas en centros de operaciones, ejercicios de equipos rojos, evaluación de capacidades defensivas, alimentación de sistemas de telemetría.	Enfoque defensivo y analítico, con utilidad para planificar ejercicios ofensivos.	Corporación MITRE, en colaboración con la comunidad global de ciberseguridad.	Aunque no expide certificaciones, su dominio es esencial para profesionales en detección, respuesta y simulación de adversarios.	En constante evolución, con actualizaciones periódicas para entornos empresariales, dispositivos móviles y sistemas industriales.
<b>OWASP WSTG</b>	Iniciativa colaborativa que produce estándares, documentos y herramientas orientados a fortalecer la seguridad en el desarrollo de software y servicios web.	Análisis de requerimientos, Planeación de arquitectura, Codificación segura, Pruebas de integración, Despliegue y operación. Estudio preliminar de la documentación, Identificación de activos en red, Análisis de debilidades, Simulación de ingeniería social, Ejecución de pruebas técnicas, Interpretación de hallazgos, Elaboración de informes, Implementación de medidas correctivas.	Identificar y mitigar fallos de seguridad en aplicaciones web y servicios API, priorizando aquellas vulnerabilidades de mayor prevalencia.	Construcción de software con prácticas seguras, evaluaciones de seguridad en aplicaciones, pruebas de servicios API, análisis de código fuente.	Mixta, combinando actividades preventivas durante el desarrollo con pruebas ofensivas controladas.	Fundación OWASP, respaldada por una red internacional de especialistas.	Sus lineamientos son frecuentemente adoptados en programas de estudio para acreditaciones técnicas especializadas.	Revisión continua; la edición más reciente del Top 10 data de 2021, con nuevas versiones en preparación.
<b>NIST SP 800-115</b>	Documento de referencia del instituto de estándares estadounidense que establece lineamientos para llevar a cabo evaluaciones de seguridad y pruebas de intrusión.	Evaluación de factores humanos, Análisis de perímetros físicos, Examen de comunicaciones inalámbricas, Revisión de sistemas de telefonía, Inspección de redes de datos.	Ofrecer un enfoque sistemático para examinar la efectividad de los controles implementados y disminuir la probabilidad de incidentes.	Sector financiero, entidades gubernamentales, auditorías externas, revisiones de infraestructura tecnológica.	Orientación hacia la verificación y mejora de controles desde una perspectiva de cumplimiento.	Instituto Nacional de Estándares y Tecnología (NIST) de Estados Unidos.	Sus fundamentos son materia de estudio en programas de certificación en auditoría y seguridad de sistemas.	Conserva su validez como publicación oficial, siendo una fuente de consulta técnica habitual.
<b>OSSTMM</b>	Enfoque integral para examinar la seguridad operacional a través de indicadores verificables y reproducibles.	Obtención de información preliminar, Construcción de perfiles de amenaza, Exploración de vulnerabilidades, Fase de	Proporcionar una visión cuantificable y completa del estado de la seguridad en sus dimensiones	Revisiones integrales de seguridad corporativa, diagnósticos de infraestructura, análisis de	Evaluación basada en métricas y evidencias medibles.	Instituto de Seguridad y Metodologías Abiertas (ISECOM).	Existe una acreditación profesional específica para evaluadores que aplican esta metodología.	La iteración más difundida corresponde a la versión 3 del manual.

		explotación, Actividades posteriores al acceso, Documentación de resultados.	tecnológica, física y humana.	controles físicos y de interacción con personas.				
<b>PTES</b>	Conjunto de directrices que detallan las etapas necesarias para realizar pruebas de penetración de manera estructurada y profesional.	Obtención de información preliminar, Construcción de perfiles de amenaza, Exploración de vulnerabilidades, Fase de explotación, Actividades posteriores al acceso, Documentación de resultados.	Definir un procedimiento uniforme para la ejecución de pruebas de intrusión que garantice la calidad y completitud de los resultados.	Proyectos de evaluación de seguridad en entornos corporativos, análisis de redes internas, verificaciones técnicas de infraestructura.	Enfoque predominantemente ofensivo, con énfasis en la práctica profesional de pruebas de intrusión.	Grupo de especialistas independientes que conformaron el estándar PTES.	Aunque no está ligado a una certificación propia, su estructura es base para múltiples programas de formación en pruebas de penetración.	El material continúa disponible y es empleado como referencia metodológica actual.
<b>ISSAF</b>	Estructura metodológica que describe con detalle las fases, herramientas y productos esperados en evaluaciones de seguridad ofensivas.	Acopio de datos iniciales, Descubrimiento de topología de red, Localización de puntos débiles, Acceso a sistemas, Escalamiento de privilegios, Establecimiento de persistencia, Afectación de usuarios y sistemas remotos, Limpieza de rastros de la prueba.	Ejecutar evaluaciones de seguridad que reproduzcan fielmente las tácticas empleadas por atacantes en escenarios reales.	Valoraciones exhaustivas de seguridad empresarial, pruebas de penetración de alta complejidad, análisis minuciosos de redes y servidores.	Enfoque ofensivo detallado, con énfasis en la simulación realista de ataques.	Grupo Abierto de Seguridad de Sistemas de Información (OISSG).	No es habitual encontrar acreditaciones formales directamente vinculadas a este marco.	Apreciado por su rigor técnico, aunque sus actualizaciones son menos frecuentes en comparación con otros estándares.

## Conclusión

El análisis comparativo de metodologías de pentesting evidencia que no existe un enfoque único y universal, sino que cada marco responde a necesidades y contextos específicos dentro de la ciberseguridad. Mientras que MITRE ATT&CK se orienta a la defensa estratégica y la caza de amenazas, estándares como PTES e ISSAF guían la ejecución técnica de pruebas ofensivas. Por su parte, OWASP WSTG se especializa en aplicaciones web, y NIST SP 800-115 junto con OSSTMM aportan rigor formal y métrico para entornos corporativos y de auditoría.

En definitiva, la diversidad de enfoques —lejos de ser una limitación— representa una fortaleza, ya que permite a los profesionales seleccionar, combinar y adaptar las metodologías más adecuadas según el objetivo y el alcance de cada evaluación. Cartografiar estas herramientas resulta fundamental para construir programas de seguridad más completos y efectivos frente a un panorama de amenazas en constante evolución.

## Referencias

1. MITRE Corporation. (2024). *MITRE ATT&CK*®. <https://attack.mitre.org/>

2. OWASP Foundation. (2024). *Web Security Testing Guide (WSTG)*. <https://owasp.org/www-project-web-security-testing-guide/>
3. Scarfone, K., Souppaya, M., Cody, A., & Orebaugh, A. (2008). *Technical guide to information security testing and assessment* (NIST Special Publication 800-115). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-115>
4. ISECOM. (2022). *Open Source Security Testing Methodology Manual (OSSTMM)* (Versión 3). <https://www.isecom.org/OSSTMM.3.pdf>
5. The Penetration Testing Execution Standard Team. (2022). *Penetration Testing Execution Standard (PTES)*. <http://www.pentest-standard.org/>