16 DE FEBERO DE 2026

# CARTOGRAFIANDO EL PESTING

## ACT 05

CAVAZOS ZACARÍAS RODOLFO – 178823
UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ
CNO V: Seguridad Informática

## Introducción

En el actual entorno de transformación digital, la seguridad informática se ha consolidado como un pilar estratégico para garantizar la continuidad operativa y la protección de los activos de información. El incremento de amenazas avanzadas y ataques dirigidos ha hecho imprescindible la aplicación de pruebas de penetración y marcos metodológicos que permitan evaluar de manera estructurada la efectividad de los controles de seguridad. Estas metodologías no solo organizan el proceso técnico de evaluación, sino que establecen enfoques, fases y objetivos claros según el tipo de sistema y el contexto organizacional.

Existen distintos marcos con orientaciones específicas: algunos se centran en el análisis de técnicas reales de adversarios, como MITRE ATT&CK; otros se especializan en pruebas técnicas sobre aplicaciones web, como la guía de OWASP; y algunos proporcionan lineamientos formales para la evaluación de controles, como las publicaciones del National Institute of Standards and Technology. Comprender sus diferencias y alcances permite seleccionar la metodología más adecuada según el escenario, fortaleciendo el criterio profesional en la práctica del pentesting y la evaluación de seguridad.

| MITRE ATT&CK | |
|---|---|
| **Descripción** | Base de conocimiento que documenta tácticas y técnicas reales utilizadas por adversarios basadas en inteligencia de amenazas. |
| **Fases** | Reconocimiento → Initial Access → Execution → Persistence → Privilege Escalation → Defense Evasion → Credential Access → Lateral Movement → Impact |
| **Objetivo** | Identificar, mapear y analizar técnicas de ataque utilizadas por adversarios reales. |
| **Escenarios** | Red Team, Blue Team, Threat Hunting, SOC, análisis post-incidente. |
| **Orientación** | Evaluación y defensa (basado en comportamiento de ataque real). |
| **Organismo** | MITRE Corporation. |
| **URL** | https://attack.mitre.org |
| **Certificaciones** | No propia, pero usada en CEH, OSCP, CISSP, Security+. |
| **Vigencia** | Actualizaciones continuas (Enterprise ATT&CK v14+ en constante revisión). |

| OWASP WSTG | |
|---|---|
| **Descripción** | Guía metodológica para pruebas de seguridad en aplicaciones web. |
| **Fases** | Información → Configuración → Autenticación → Autorización → Gestión de sesión → Validación de entradas → Criptografía → Lógica de negocio → Cliente. |
| **Objetivo** | Identificar vulnerabilidades en aplicaciones web. |
| **Escenarios** | Auditorías web, pruebas en APIs, desarrollo seguro SDLC. |

| | |
|---|---|
| **Orientación** | Ataque técnico controlado (pentesting web). |
| **Organismo** | Open Web Application Security Project (OWASP). |
| **URL** | https://owasp.org/www-project-web-security-testing-guide/ |
| **Certificaciones** | OSCP, CEH, eWPT, certificaciones OWASP. |
| **Vigencia** | WSTG v4.2 (actualizada periódicamente). |

| NIST SP 800-115 | |
|---|---|
| **Descripción** | Guía técnica para pruebas de seguridad y evaluación de controles. |
| **Fases** | Planificación → Descubrimiento → Ataque → Reporte. |
| **Objetivo** | Evaluar controles de seguridad organizacionales. |
| **Escenarios** | Gobierno, auditorías formales, cumplimiento normativo. |
| **Orientación** | Evaluación y cumplimiento. |
| **Organismo** | NIST (EE.UU.). |
| **URL** | https://csrc.nist.gov/publications/detail/sp/800-115/final |
| **Certificaciones** | CISSP, CISA, CISM. |
| **Vigencia** | Publicado 2008, aún vigente como referencia normativa. |

| OSSTMM | |
|---|---|
| **Descripción** | Manual metodológico para pruebas de seguridad operacional cuantificables. |
| **Fases** | Recolección de información → Evaluación → Verificación → Análisis cuantitativo (RAV). |
| **Objetivo** | Medir la seguridad de forma objetiva y verificable. |
| **Escenarios** | Auditorías técnicas, infraestructura crítica, telecomunicaciones. |
| **Orientación** | Evaluación técnica estructurada. |
| **Organismo** | ISECOM. |
| **URL** | https://www.isecom.org/osstmm.html |
| **Certificaciones** | OPST, OPSA, OPSE. |
| **Vigencia** | Versión 3.0 (última versión estable). |

| PTES | |
|---|---|
| **Descripción** | Estándar que define fases completas del proceso de pentesting. |
| **Fases** | Pre-engagement → Intelligence Gathering → Threat Modeling → Vulnerability Analysis → Exploitation → Post-exploitation → Reporting. |
| **Objetivo** | Estandarizar la ejecución profesional del pentesting. |
| **Escenarios** | Empresas privadas, pruebas controladas, Red Team. |
| **Orientación** | Ataque estructurado. |
| **Organismo** | Comunidad PTES. |
| **URL** | http://www.pentest-standard.org |
| **Certificaciones** | OSCP, GPEN. |
| **Vigencia** | Última actualización 2014, aún ampliamente usado. |

| ISSAF | |
|---|---|
| **Descripción** | Marco integral para evaluación técnica y administrativa de seguridad. |
| **Fases** | Planeación → Evaluación técnica → Análisis → Reporte. |
| **Objetivo** | Evaluar seguridad de sistemas de información. |
| | |
| **Escenarios** | Auditorías organizacionales completas. |
| **Orientación** | Evaluación integral. |
| **Organismo** | OISSG. |
| **URL** | http://www.oissg.org/issaf |
| **Certificaciones** | No oficiales propias. |
| **Vigencia** | Marco menos actualizado pero aún referenciado académicamente. |

Conclusión

Las metodologías no compiten entre sí, sino que se complementan. Mientras PTES y OWASP están orientadas al ataque técnico controlado, NIST y OSSTMM buscan evaluación estructurada. MITRE ATT&CK funciona como marco de referencia estratégico para comprender el comportamiento adversario real.

Referencias bibliográficas: