14 DE FEBRERO DE 2026

# CNOV SEGURIDAD INFORMATICA

ACTIVIDAD 05

BRIAN SALVADOR ESPINOZA AGUILAR

175031

Universidad Politécnica de San Luis Potosí

# Introducción

Para entender la ciberseguridad moderna, no basta con conocer las herramientas; es fundamental dominar las metodologías que dictan cómo, cuándo y por qué se realizan las pruebas.

En el ecosistema digital actual, la evaluación de la seguridad ha dejado de ser una actividad caótica para convertirse en una disciplina altamente estructurada.

# Desarrollo

| MTRE ATT&CK | |
|---|---|
| **Descripción** | El marco MITRE ATT&CK es una base de conocimientos universalmente accesible y actualizada para modelar, detectar, prevenir y combatir las amenazas de ciberseguridad basadas en los comportamientos adversarios conocidos de los delincuentes cibernéticos |
| **Fases de implementación** | Emulación de adversario<br>Red Teaming.<br>Desarrollo de análisis de comportamiento.<br>Evaluación de brechas defensivas.<br>Evaluación de madurez de SOC.<br>Enriquecimiento de inteligencia de amenazas cibernéticas. |
| **Objetivo principal** | Proporcionar información sobre tacticas y tecnicas, utilizadas por ciberdelincuentes. |
| **Escenarios en los que se utiliza** | • Clasificación de alertas, detección de amenazas y respuesta.<br>• Caza amenazas.<br>• Equipo rojo/emulación de adversario.<br>• Análisis de brechas de seguridad y evaluaciones de madurez del centro de operaciones de seguridad |
| **Orientación** | Defensa |
| **Autores u organismos responsables** | MITRE Corporation, una organización sin fines de lucro, y es mantenido por MITRE con aportes de una comunidad global de profesionales de la ciberseguridad. |
| **Material original** | https://attack.mitre.org/ |
| **Certificaciones asociadas** | • SANS Institute (GIAC)<br>• CREST (Organización internacional de seguridad)<br>• Certificaciones de Offensive Security<br>• Certificaciones de Blue Team / SOC<br>• Certificaciones específicas de Threat Intelligence |
| **Versiones o actualizaciones vigentes** | Version 16 lanzada en Octubre 2024 |

| OWASP WSTG | |
|---|---|
| **Descripción** | Es una guía completa para probar la seguridad de aplicaciones web y servicios web. La WSTG proporciona un marco de mejores prácticas comúnmente utilizadas por testeadores de penetración externos y organizaciones que realizan pruebas internas. |
| **Fases de implementación** | • Planificación y Preparación.<br>• Reconocimiento Pasivo/Activo.<br>• Pruebas de Configuración y Gestión.<br>• Pruebas de Autenticación y Gestión de Sesiones.<br>• Pruebas de Autorización y Control de Acceso.<br>• Pruebas de Validación de Entrada (Inyecciones).<br>• Pruebas de Lógica de Negocio.<br>• Pruebas de APIs y Servicios Web.<br>• Pruebas del Lado del Cliente.<br>• Revisión y Reporte. |
| **Objetivo principal** | Identificar y corregir vulnerabilidades en aplicaciones web. |
| **Escenarios en los que se utiliza** | • Pentesting Ético Formal<br>• Bug Bounty Programs<br>• Desarrollo Seguro (DevSecOps)<br>• Auditorías de Cumplimiento<br>• Respuesta a Incidentes |
| **Orientación** | Evaluación |
| **Autores u organismos responsables** | OWASP WSTG fue creado por y para la comunidad de seguridad. |
| **Material original** | https://owasp-org.translate.goog/www-project-web-security-testing-guide/?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc |
| **Certificaciones asociadas** | • OSWE (Offensive Security Web Expert)<br>• GWAPT (GIAC Web Application Penetration Tester)<br>• Burp Suite Certified Practitioner de PortSwigger<br>• Certificaciones de eLearnSecurity |
| **Versiones o actualizaciones vigentes** | WSTG v4.2 (2021) |

| NIST SP 800-115 | |
|---|---|
| **Descripción** | Marco metodológico formal para la evaluación técnica de seguridad. |
| **Fases de implementación** | • Planificación.<br>• Descubrimiento.<br>• Ataque.<br>• Reporte |
| **Objetivo principal** | Asistir a organizaciones en la planificación y conducción de pruebas técnicas y exámenes de seguridad de la información. |
| **Escenarios en los que se utiliza** | • Sector Público Federal de EE.UU.<br>• Sectores Regulados.<br>• Organizaciones de Alta Madurez.<br>• Base para Programas de Evaluación Interna |
| **Orientación** | Evaluación |
| **Autores u organismos responsables** | Gobierno de Estados Unidos |
| **Material original** | https://www.nist.gov/privacy-framework/nist-sp-800-115 |
| **Certificaciones asociadas** | No hay certificaciones oficiales emitidas por NIST |
| **Versiones o actualizaciones vigentes** | Unica version lanzada en 2008 |
| **OSSTMM** | |
| **Descripción** | Es una metodología de pruebas de seguridad con una orientación radicalmente diferente a NIST, OWASP, su enfoque es científico, holístico y de evaluación cuantitativa. |
| **Fases de implementación** | • Seguridad Humana.<br>• Seguridad Física.<br>• Seguridad Inalámbrica (Wireless).<br>• Telecomunicaciones.<br>• Redes de Datos |
| **Objetivo principal** | Medir la seguridad operacional con precisión matemática. |
| **Escenarios en los que se utiliza** | • Grandes organizaciones con alta madurez<br>• Equipos de aseguramiento (no solo pentest)<br>• Telecomunicaciones<br>• Logística |
| **Orientación** | Evaluación |
| **Autores u organismos responsables** | ISECOM |
| **Material original** | https://www.isecom.org/OSSTMM.3.pdf |
| **Certificaciones asociadas** | • OPST (OSSTMM Professional Security Tester)<br>• OPSA (OSSTMM Professional Security Analyst)<br>• OPSE (OSSTMM Professional Security Expert) |
| **Versiones o actualizaciones vigentes** | OSSTMM 3 (2016) |

| PTES | |
|---|---|
| **Descripción** | Es un estándar técnico/operacional. Su propósito es unificar criterios, fases y metodologías en la ejecución de pruebas de penetración, eliminando la ambigüedad entre distintos proveedores y equipos internos. |
| **Fases de implementación** | • Pre-engagament (Pre-acuerdo / Pre-ataque).<br>• Intelligence Gathering (Recolección de información).<br>• Threat Modeling (Modelado de amenazas).<br>• Vulnerability Analysis (Análisis de vulnerabilidades).<br>• Exploitation (Explotación).<br>• Post-Exploitation (Post-explotación).<br>• Reporting (Reporte). |
| **Objetivo principal** | Establecer un estándar universal para la ejecución de pruebas de penetración. |
| **Escenarios en los que se utiliza** | • Pentesting externo (Red team / Seguridad perimetral).<br>• Pentesting interno (Red interna y Active Directory).<br>• Pentesting de aplicaciones web.<br>• Pentesting de infraestructura cloud (aws, azure, gcp).<br>• Pentesting de ingeniería social y físico. |
| **Orientación** | Ataque |
| **Autores u organismos responsables** | Comunidad de ciberseguridad. |
| **Material original** | https://www-pentest--standard-org.translate.goog/index.php/PTES_Technical_Guidelines?_x_tr_sch=http&_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc |
| **Certificaciones asociadas** | • Certified Lead Ethical Hacker (PECB).<br>• GPEN (GIAC Penetration Tester).<br>• OSCP. |
| **Versiones o actualizaciones vigentes** | No hay un sistema de versiones, pero se divide por componentes:<br>El Estándar (The Standard)<br>La Guía Técnica (Technical Guidelines) |

| ISSAF | |
|---|---|
| **Descripción** | Es una metodología extremadamente detallada y estructurada diseñada para que los profesionales de la ciberseguridad realicen auditorías de seguridad y pruebas de penetración de manera organizada y profesional. |
| **Fases de implementación** | • Planificación y Preparación.<br>• Evaluación (Assessment).<br>• Reporte y Limpieza. |
| **Objetivo principal** | Proporcionar un marco de trabajo estandarizado, exhaustivo y técnico para evaluar la seguridad de los sistemas de información de una organización de principio a fin. |
| **Escenarios en los que se utiliza** | • Auditorías de Cumplimiento (Compliance).<br>• Pentesting de "Caja Blanca" (White Box).<br>• Evaluación de Infraestructuras Críticas.<br>• Formación de Nuevos Auditores. |
| **Orientación** | Evaluación y ataque |
| **Autores u organismos responsables** | OISSG (Open Information Systems Security Group). |
| **Material original** | https://pymesec.org/issaf/ |
| **Certificaciones asociadas** | • CISA (Certified Information Systems Auditor) de ISACA.<br>• CISSP (Certified Information Systems Security Professional).<br>• CEH (Certified Ethical Hacker).<br>• OSCP (Offensive Security Certified Professional). |
| **Versiones o actualizaciones vigentes** | v0.2 (2000) |

# Conclusión

La evolución de las metodologías de seguridad informática demuestra que la protección de dispositivos y archivos digitales ha pasado de ser una serie de pruebas aisladas a convertirse en una disciplina científica y estratégica. Mientras que marcos históricos como el ISSAF sentaron las bases procedimentales y técnicas, estándares modernos como el PTES han desplazado el enfoque hacia el impacto real en el negocio y la post-explotación. Por otro lado, la especialización de OWASP en el ámbito web, la rigurosidad normativa de NIST y el enfoque métrico de OSSTMM ofrecen soluciones específicas para cada necesidad organizacional. Finalmente, la integración de MITRE ATT&CK como lenguaje universal de tácticas de ataque cierra el círculo, permitiendo que la evaluación de seguridad no solo detecte fallos, sino que anticipe comportamientos de adversarios reales.

# Referencias


- IBM. (2025, November 26). Mitre Attack. *IBM*. https://www.ibm.com/mx-es/think/topics/mitre attack
- Kippeotechnologies, & Kippeotechnologies. (2025, July 25). *Del estándar a la práctica: cómo aplicamos la guía OWASP para pruebas de seguridad web reales*. Attack Surface Discovery. http://kippeo.com/del-estandar-a-la-practica-como-aplicamos-la-guia-owasp-para-pruebas-de-seguridad-web-reales/
- Admin. (2024, October 5). *Guía NIST SP 800-115*. Tu Consultor TI. https://www.tuconsultorti.com/ciberseguridad/guia-nist-sp-800-115/
- Admin. (2024b, October 5). *Guía OSSTMM*. Tu Consultor TI. https://www.tuconsultorti.com/ciberseguridad/guia-osstmm/
- *Pre-engagement - the Penetration Testing Execution standard*. (n.d.). http://www.pentest-standard.org/index.php/Pre-engagement
- *Metodología ISSAF | H4CKdotCL*. (n.d.). H4CKdotCL. https://book.h4ck.cl/metodologia-y-fases-de-hacking-etico/metodologias/metodologia-issaf