FICHA DE TALLER

- **Datos generales:**

Título:	**Taller de Ciberseguridad Aplicada**					
Instructor o docente:	Luis Antonio Zafra Labrador					
Duración total de taller:	10 sesiones virtuales de 2 hrs. C/U					
Área:	☐	Formación para la docencia	☐	Formación para la gestión universitaria	☐	Otra
Modalidad de impartición:	☐	Presencial	☒	A distancia	☐	Híbrida
Fechas:	22 de septiembre al 03 de octubre.					

Descripción:

Durante el primer semestre de 2023, México registró más de 14 mil millones de intentos de ciberataques, lo que subraya la urgencia de implementar medidas efectivas de ciberseguridad para proteger información sensible. Las instituciones gubernamentales son objetivos atractivos para los cibercriminales debido a la falta de inversión en ciberseguridad en comparación con el sector privado. Esto pone en riesgo no solo la información pública, sino también la confianza ciudadana

Destinatarios:

- Profesionales responsables de la infraestructura de Tecnologías de Información y Comunicación de la UNAM.

Objetivo(s) o competencia(s):

- Los participantes reconocerán prácticas esenciales para habilitarse en técnicas ofensivas como defensivas en ciberseguridad, con un enfoque en la protección de la infraestructura crítica utilizando software libre.

Metodología y Actividades:

- Aprendizaje activo: combinando teoría con práctica guiada en entornos simulados.
- Enfoque basado en casos: resolución de escenarios reales aplicables al contexto universitario.
- Software libre: uso exclusivo de herramientas abiertas (Kali Linux, Wazuh, OpenVAS, MISP, etc.)
- Trabajo colaborativo: análisis y ejercicios por equipos sobre simulación de ataques y defensa.
- Orientación práctica: laboratorio virtual o entorno controlado tipo "CTF" (Capture The Flag) para consolidar aprendizajes.
- Análisis de caso: incidente de ransomware en infraestructura académica.
- Debate dirigido: ¿hasta dónde debe llegar la vigilancia en redes universitarias?

Mecanismo y criterios de evaluación:

- Autoevaluación inicial: breve cuestionario para conocer conocimientos previos y expectativas.
- Caso práctico en grupo: **i**ncidente de ransomware en infraestructura académica.
- Ejercicio colaborativo: diseño de un plan de respuesta a incidentes.
- Quiz final: validación de conceptos clave con herramienta interactiva.
- Autoevaluación final: comparación con la inicial para medir el progreso.
- Feedback: formulario o QR para valorar la sesión.

Criterios:

- Ejercicios prácticos en grupo
- Trabajo colaborativo (casos/plan de respuesta)
- Informe técnico
- Evaluación final escrita.

- **Temario:**

No. De sesión	Fecha	Hora	Temas a abordar
Sesión 1	22 de septiembre	18:00 – 20:00 hrs.	1. Fundamentos de Ciberseguridad (2 horas) 1. 1. Conceptos clave: amenazas, vulnerabilidades, riesgos, ataques 1. 2. Panorama actual de amenazas: tendencias y desafíos 1. 3. Situación actual de la ciberseguridad en México 1. 4. Marcos de referencia en ciberseguridad: 1. 4. 1. NIST Cybersecurity Framework 1. 4. 2. ISO/IEC 27001 1. 5. Importancia de la ciberseguridad en el contexto universitario
Sesión 2	23 de septiembre	18:00 – 20:00 hrs.	2. Técnicas Ofensivas (6 horas) 2. 1. Reconocimiento y recopilación de información (OSINT, footprinting, scanning) 2. 2. Explotación de vulnerabilidades (inyección SQL, XSS, buffer overflow)
Sesión 3	24 de septiembre	18:00 – 20:00 hrs.	2. 3. Ataques de denegación de servicio (DoS, DDoS)
Sesión 4	25 de septiembre	18:00 – 20:00 hrs.	2. 4. Ingeniería social y phishing 2. 5. Malware y ransomware
Sesión 5	26 de septiembre	18:00 – 20:00 hrs.	3. Técnicas Defensivas (6 horas) 3. 1. Seguridad perimetral (firewalls, IDS/IPS, VPNs) 3. 2. Seguridad de redes (segmentación, VLANs, NAC)
Sesión 6	29 de septiembre	18:00 – 20:00 hrs.	3. 3. Seguridad de endpoints (antivirus, EDR, control de aplicaciones) 3. 4. Gestión de vulnerabilidades (escaneo, parcheo, mitigación) 3. 5. Seguridad de aplicaciones (OWASP Top 10, pruebas de seguridad
Sesión 7	30 de septiembre	18:00 – 20:00 hrs.	3. 6. Hardening de sistemas operativos basados en GNU/Linux y Windows 3. 7. Hardening a bases de Bases de datos 3. 8. Hardening a Servidores de aplicación 3. 9. Hardening a Servidores web
Sesión 8	01 de Octubre	18:00 – 20:00 hrs.	4. Respuesta a Incidentes e Informática y Ciber inteligencia (4 horas) 4. 1. Plan de respuesta a incidentes: preparación, detección, contención, erradicación, recuperación, lecciones aprendidas 4. 2. Ciber Inteligencia: de los Indicadores al Entendimiento de la Amenaza
Sesión 9	02 de Octubre	18:00 – 20:00 hrs.	5. Gestión de Riesgos y Continuidad del Negocio (2 horas) 5. 1. Análisis y evaluación de riesgos 5. 2. Planes de continuidad del negocio y recuperación ante desastres 5. 3. Concienciación y capacitación en ciberseguridad

Sesión 10	03 de Octubre	18:00 – 20:00 hrs.	Ejercicio de Escritorio (Table Top) Incident Respond

Bibliografía

- NIST SP 800-61 Rev.2 – Computer Security Incident Handling Guide
- ISO/IEC 27001:2022 – Sistemas de gestión de seguridad de la información
- OWASP Top 10: Vulnerabilidades más críticas en aplicaciones web
- Blue Team Field Manual – Alan White & Ben Clark
- Hacking: The Art of Exploitation – Jon Erickson
- Practical Vulnerability Management – Andrew Magnusson
- Documentación oficial de herramientas: Kali Linux, OpenVAS, Wazuh, MISP, OSINT Framework