Programa de
TALLER DE SEGURIDAD INFORMÁTICA
(Tecnólogo en Informática)

1. NOMBRE DE LA UNIDAD CURRICULAR

Taller de Seguridad Informática

2. CRÉDITOS

8 créditos

3. OBJETIVOS DE LA UNIDAD CURRICULAR

- Integrar la Seguridad por Diseño (Shift Left): Implementar la seguridad en las fases tempranas del ciclo de vida del desarrollo de software (SDLC).
- Asegurar Arquitecturas Modernas: Dominar el hardening de contenedores (Docker) y orquestadores (Kubernetes)
- Introducción a la metodología de Hacking Ético: Aplicar las etapas de Reconocimiento, Explotación y Post-Explotación para validar la seguridad de los sistemas.
- Adoptar Roles de Seguridad (Red Team/Blue Team): Aplicar técnicas de ataque y defensa para validar la robustez de sistemas desarrollados por equipos pares.

4. METODOLOGÍA DE ENSEÑANZA

Componente	Horas de Clase (Semanales)	Horas Totales (15 Semanas)
Teórico (T)	2 hora	30 horas
Práctico / Laboratorio Asistido (P/L)	2 horas	30 horas
Dedicación No Presencial (Personal)	4 horas (estimado)	60 horas (estimado)
Total Estimado	8 horas	120 horas

Participación de los Estudiantes:

- Demostraciones Prácticas: El instructor realizará demostraciones en el laboratorio de herramientas (Nmap, Netcat, ZAP), ingeniería social y técnicas de ataque/defensa durante las horas de clase, para ilustrar los conceptos del dominio semanal.

- Presentaciones Grupales (Parcial 1): Los estudiantes realizarán presentaciones de 25 minutos en grupos, demostrando habilidades prácticas de investigación en seguridad.
- Proyecto de Riesgos (Evaluación Final): Realización de un proyecto de modelado y gestión de riesgos para una empresa ficticia.

5. TEMARIO

Tema	Descripción y subtemas
TEMA I: Fundamentos y Diseño Seguro	Seguridad por Diseño (Shift Left): Principios, Threat Modeling. Clean Code y Criptografía: Hashing seguro, Secrets.
TEMA II: Infraestructura y Redes	Diseño de Red Seguro: Segmentación, Firewalls (UFW). Seguridad de Contenedores: Imagen base segura, Mínimo Privilegio. Bases de Datos: Cifrado TDE y Nivel de Campo.
TEMA III: Pruebas y Automatización	Integración de Pipelines: Pasos de ejecución de pruebas estáticas (SAST/SCA). DAST: Uso de OWASP ZAP. Vulnerabilidades: Remediación avanzada de XSS/SQLi y BOLA.
TEMA IV: Metodología de Hacking Ético (Red Team)	Fase 1: Reconocimiento y Footprinting: Nmap (descubrimiento), Ingeniería Social. Fase 2: Explotación: Prueba de Inyección, Netcat, Web Shells. Fase 3: Post-Explotación: Persistencia, Monitoreo (Análisis de Logs). Detección: Uso de tcpdump y Monitoreo (SIEM).
TEMA V: Gestión de Riesgos y Continuidad (Blue Team)	Dominios: Gestión de Riesgos y BCDR. Modelado de Amenazas, Inventario de Activos y Planificación de la Continuidad del Negocio. Hardening: Aplicación de parches y respuesta a incidentes.

6. BIBLIOGRAFÍA

Tema	Básica	Complementaria
TEMA I a V	(1), (2)	(4), (5)
TEMA II, III		(3)

6.1 Básica

1. (ISC)². (Versión Reciente). CISSP Official Study Guide. (Referencia para Arquitectura y Gobernanza).
2. Stallings, W., Brown, L. (2018). Computer Security: Principles and Practice, 4th Edition. Pearson. (Referencia para Criptografía y Protocolos).

6.2 Complementaria

3. Vandana Verma Sehgal. Implementing DevSecOps in Practice. O'Reilly Media. (Referencia para Pipelines y Automatización).
4. OWASP Foundation. (Última versión). OWASP Top 10 y Proactive Controls.
5. Wei Lien Dang, Ajmal Kohgadai. DevSecOps in Kubernetes O'Reilly Media

7. CONOCIMIENTOS PREVIOS EXIGIDOS Y RECOMENDADOS

7.1 Conocimientos Previos Exigidos: Se requieren conocimientos de Administración de Infraestructura, Programación Avanzada, Bases de Datos y conocimientos básicos de Seguridad Informática.

7.2 Conocimientos Previos Recomendados:

- Experiencia en el desarrollo de aplicaciones web o API (Java/Python).
- Familiaridad con Docker y la línea de comandos.
- Conocimientos de redes de computadoras y sistemas operativos.

ANEXO A
Para todas las Carreras

A1) INSTITUTO

Comisión Nacional de Carrera del Tecnólogo en Informática (UTU-UTEC-UDELAR)

A2) CRONOGRAMA TENTATIVO

Semana	Temas (4 hs de clase)	Foco Práctico (3.0 hs)
Semana 1	TEMA I: DevSecOps Foundations, Clean Code, Cripto.	Teoría (Fundamentos de Diseño Seguro).
Semana 2	TEMA I: Seguridad por Diseño, Threat Modeling (Metodología STRIDE).	Teoría (Diseño y Riesgo).
Semana 3	TEMA II: Diseño de Red Seguro / Firewall Config.	Práctico: Taller de Configuración de Firewalls y Segmentación.
Semana 4	TEMA II: Seguridad de Contenedores y Cloud.	Práctico: Taller de Hardening de Dockerfile y Escaneo SCA/Vulnerabilidades.
Semana 5	TEMA II: Servidores y Bases de Datos Seguras.	Teoría (Hardening de DB/SO).
Semana 6	Presentación del Diseño de Sistema del Laboratorio (Inicio Proyecto Final).	
Semana 7	TEMA III: Automatización y Pipelines. SAST/SCA (Teoría).	Teoría (CI/CD y Pruebas).
Semana 8	EVALUACIÓN PARCIAL 1: Diseño y Simulación de Red Segura. (4 hs de clase, ambas sesiones).	Práctico: Cada grupo defiende su diseño de red, modelado de amenaza.
Semana 9	TEMA III: Implementación de Pipelines (SAST/SCA/DAST).	Práctico: Taller de integración de SonarLint/Dependency-Check en código.
Semana 10	TEMA IV (Fase 1 y 2): Reconocimiento y Escaneo. Nmap y ZAP (Análisis Activo).	Práctico: Red Team Reconocimiento.
Semana 11	TEMA IV (Fase 3): Explotación y Post-Explotación. Netcat, Web Shells, Persistencia.	Práctico: Pruebas de Concepto de Ataque.

Semana 12	Dinámica Red Team: Ataque a sistemas pares y Documentación de Fallos. Uso de herramientas de IA para ciberseguridad. (Ej. Pentestgpt)	
Semana 13	Dinámica Blue Team: Análisis de Logs y Remediación (Hardening y Parcheo de Código).	
Semana 14	TEMA V (Blue Team): Respuesta a Incidentes, Monitoreo (SIEM) y Hardening Final.	
Semana 15	EVALUACIÓN FINAL (Parcial 2): Defensa Red/Blue Team del Sistema y Remediación.	

A3) MODALIDAD DEL CURSO Y PROCEDIMIENTO DE EVALUACIÓN

Instancia de Evaluación	Peso Relativo	Criterio de Aprobación / Descripción
Parcial 1 (Semana 8)	35%	Diseño de Arquitectura Segura: Evaluación de la capacidad de modelar el riesgo. El grupo debe diseñar y defender (posiblemente con un simulador/diagrama) un diseño de red ,las reglas de firewall para el sistema del proyecto y el modelo de amenaza.
Evaluación Final (Semanas 12-15)	55%	Proyecto Red Team / Blue Team (Hack-and-Patch): Se evalúa la capacidad de Ataque (éxito en la explotación de fallos de pares) y Defensa (calidad del código remediado, hardening del servidor/contenedor y respuesta al incidente).
Participación y Asistencia	10%	Evaluación de la participación activa y asistencia.

Aprobación del Curso: Obtener un promedio ponderado mínimo de 60%. Es obligatorio participar en todas las evaluaciones.

A4) CALIDAD DE LIBRE

Esta asignatura no adhiere a la resolución del consejo sobre la condición de libre.

A5) CUPOS DE LA UNIDAD CURRICULAR

Cupos mínimos: no tiene
Cupos máximos: no tiene