Universidad Nacional de Ingeniería (UNI)
Escuela Profesional de
Ciberseguridad
Sílabo 2024-II

1. CURSO

CY351. Seguridad de Sistemas Avanzada (Obligatorio)

2. INFORMACIÓN GENERAL

2.1 Curso	:	CY351. Seguridad de Sistemas Avanzada
2.2 Semestre	:	10^{mo} Semestre.
2.3 Créditos	:	3
2.4 horas	:	2 HT; 2 HP;
2.5 Duración del periodo	:	16 semanas
2.6 Condición	:	Obligatorio
2.7 Modalidad de aprendizaje	:	Presencial
2.8 Prerrequisitos	:	• CY231. Seguridad de Componentes. (9^{no} Sem) • CY251. Seguridad de Sistemas. (7^{mo} Sem)

3. PROFESORES

Atención previa coordinación con el profesor

4. INTRODUCCIÓN AL CURSO

Este curso avanzado amplía los conocimientos en seguridad de sistemas, profundizando en el análisis de riesgos, la mitigación de vulnerabilidades y el diseño de soluciones de seguridad robustas para sistemas complejos. Se examinan temas como seguridad en la nube, sistemas de control industrial, análisis forense avanzado y métodos formales de verificación.

5. OBJETIVOS

- Analizar y mitigar riesgos de seguridad en sistemas complejos, incluyendo entornos de nube e infraestructuras críticas.
- Aplicar técnicas avanzadas de análisis forense para investigar incidentes de seguridad.
- Diseñar e implementar soluciones de seguridad robustas utilizando métodos formales de verificación.

6. RESULTADOS DEL ESTUDIANTE

1) Analizar un problema computacional complejo y aplicar los principios computacionales y otras disciplinas relevantes para identificar soluciones. (Assessment)

5) Funcionar efectivamente como miembro o líder de un equipo involucrado en actividades apropiadas a la disciplina del programa. (Assessment)

6) Aplicar principios y prácticas de seguridad para mantener las operaciones en presencia de riesgos y amenazas. (Assessment)

7. TEMAS

Unidad 1: Pruebas del sistema (10 horas)	
Resultados esperados: 1,6	
Temas	**Objetivos de Aprendizaje (*Learning Outcomes*)**
• Requisitos de validación – Describe metodologías para mostrar que los requisitos cumplen con los objetivos. • Validación de la composición de los componentes. – Este tema cubre cómo probar un sistema en su conjunto. • Pruebas unitarias versus de sistema T – Este tema cubre en qué se diferencian las pruebas del sistema de las pruebas de componentes y conexiones. • Verificación formal de sistemas. – Este tema cubre lenguajes, demostradores de teoremas y descomposición jerárquica.	• Describe qué es una prueba de penetración y por qué es valiosa [Usar] • Analice cómo documentar una prueba que revele una vulnerabilidad [Usar] • Discuta la importancia de validar los requisitos [Usar]
Lecturas : [**PezzÃĺ2008**]	

Unidad 2: Arquitecturas de sistemas comunes (14 horas)	
Resultados esperados: 1,6	
Temas	**Objetivos de Aprendizaje (*Learning Outcomes*)**
• Máquinas virtuales – Cubre hipervisores, virtualización de discos y memoria y el uso de máquinas virtuales en seguridad. • Sistemas de control industriales – Este tema incluye SCADA • Internet de las cosas (IoT) – Este tema incluye ejemplos como refrigeradores y sensores. • Sistemas integrados – Este tema incluye ejemplos como sistemas en • Sistemas móviles – Este tema incluye ejemplos como computadoras portátiles y teléfonos inteligentes. • Sistemas autónomos – Este tema incluye ejemplos como robots y vehículos aéreos no tripulados que no requieren control humano. • Sistema de propósito general – Este tema incluye ejemplos como computadoras de escritorio, portátiles y mainframes.	• Analice la importancia de documentar la instalación y configuración adecuadas de un sistema [Usar] • Ser capaz de escribir documentación sobre intrusiones de red y host [Usar] • Ser capaz de explicar las implicaciones de seguridad de una documentación poco clara o incompleta del funcionamiento del sistema [Usar]
Lecturas : [**Stallings2018**]	

Unidad 3: Control de sistema (12 horas)	
Resultados esperados: 1,6	
Temas	**Objetivos de Aprendizaje (*Learning Outcomes*)**
• control de acceso – Este tema se centra en controlar el acceso a los recursos y la integridad de los controles, en lugar de controlar el acceso a los datos, lo que se trata en el área de conocimiento de Seguridad de datos. • Modelos de autorización – Cubre la gestión de la autorización en muchos sistemas y la distinción entre autenticación y autorización. • Detección de intrusiones – Cubre anomalías, uso indebido (basado en reglas, basado en firmas) y técnicas basadas en especificaciones. • Ataques – Este tema cubre modelos de ataque (como árboles y gráficos de ataque) y ataques específicos. • Defensas – Este tema incluye ejemplos como ASLR, salto de IP y tolerancia a intrusiones. • Auditoría – cubre el registro, el análisis de registros y la relación con la detección de intrusiones • malware – Ejemplos como virus informáticos, gusanos, ransomware y otras formas de malware. • Modelos de vulnerabilidades – Ejemplos como RISOS y PA; y enumeraciones como CVE y CWE. • Pruebas de penetración – Cubre la Metodología de Hipótesis de Fallas y otras formas (ISSAF, OSSTMM, GISTA, PTES, etc.). • forense – Este tema se centra en los requisitos del sistema para análisis forense. • Recuperación, resiliencia – Este tema incluye mecanismos de disponibilidad.	• Describir una lista de control de acceso [Usar] • Describir el control de acceso físico y lógico, compararlos y contrastarlos [Usar] • Distinga entre autorización y autenticación [Usar]
Lecturas : [**Bishop2002**]	

Unidad 4: Continuidad del negocio, recuperación ante desastres y gestión de incidentes (12 horas)	
Resultados esperados: 1,6	
Temas	**Objetivos de Aprendizaje (*Learning Outcomes*)**
• Respuesta a incidentes – incluye la creación y el uso de los planes IR, la organización de los planes, las ocasiones para revisar/reescribir los planes y el examen de los planes saneados. • Recuperación ante desastres – incluye la creación y el uso de los planes de recuperación ante desastres, la organización de los planes, las ocasiones para revisar/reescribir los planes y el examen de los planes saneados. – Se deben brindar oportunidades a los estudiantes para que escriban planes reales o basados en casos para adquirir algo de experiencia. • Continuidad del negocio – la creación y uso de los planos BC – organizacion de los planes – Ocasiones para revisar/reescribir planes. – y examen de planos sanitizados – Se deben brindar oportunidades a los estudiantes para que escriban planes reales o basados en casos para adquirir algo de experiencia.	• Explicar la planificación organizacional estratégica para la ciberseguridad y su relación con la planificación estratégica de TI y para toda la organización [Usar] • Identificar las partes interesadas clave de la organización y sus roles [Usar] • Describir los componentes principales de la planificación de la implementación del sistema de ciberseguridad [Usar]
Lecturas : [**NIST-SP800-61r2**]	

8. PLAN DE TRABAJO

8.1 Metodología

Se fomenta la participación individual y en equipo para exponer sus ideas, motivándolos con puntos adicionales en las diferentes etapas de la evaluación del curso.

8.2 Sesiones Teóricas

Las sesiones de teoría se llevan a cabo en clases magistrales donde se realizarán actividades que propicien un aprendizaje activo, con dinámicas que permitan a los estudiantes interiorizar los conceptos.

8.3 Sesiones Prácticas

Las sesiones prácticas se llevan en clase donde se desarrollan una serie de ejercicios y/o conceptos prácticos mediante planteamiento de problemas, la resolución de problemas, ejercicios puntuales y/o en contextos aplicativos.

9. SISTEMA DE EVALUACIÓN

********* EVALUATION MISSING ********

10. BIBLIOGRAFÍA BÁSICA