



# 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 <sup>mo</sup> 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           | : | <ul style="list-style-type: none"><li>• CY231. Seguridad de Componentes. (9<sup>no</sup> Sem)</li><li>• CY251. Seguridad de Sistemas. (7<sup>mo</sup> Sem)</li></ul> |

## 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) ()

5) ()

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

## 7. TEMAS

| Unidad 1: Pruebas del sistema (10 horas)  |   |
|---|---|
| Resultados esperados: 1,6   |   |
| Temas   | Objetivos de Aprendizaje  |
| <ul style="list-style-type: none"> <li>• Requisitos de validación <ul style="list-style-type: none"> <li>– Describe metodologías para mostrar que los requisitos cumplen con los objetivos.</li> </ul> </li> <li>• Validación de la composición de los componentes. <ul style="list-style-type: none"> <li>– Este tema cubre cómo probar un sistema en su conjunto.</li> </ul> </li> <li>• Pruebas unitarias versus de sistema T <ul style="list-style-type: none"> <li>– Este tema cubre en qué se diferencian las pruebas del sistema de las pruebas de componentes y conexiones.</li> </ul> </li> <li>• Verificación formal de sistemas. <ul style="list-style-type: none"> <li>– Este tema cubre lenguajes, demostradores de teoremas y descomposición jerárquica.</li> </ul> </li> </ul> | <ul style="list-style-type: none"> <li>• Describe qué es una prueba de penetración y por qué es valiosa [Usar]</li> <li>• Analice cómo documentar una prueba que revele una vulnerabilidad [Usar]</li> <li>• Discuta la importancia de validar los requisitos [Usar]</li> </ul> |
| Lecturas : [PezzÁ12008]   |   |

| Unidad 2: Arquitecturas de sistemas comunes (14 horas)   |   |
|--|---|
| Resultados esperados: 1,6  |   |
| Temas  | Objetivos de Aprendizaje  |
| <ul style="list-style-type: none"> <li>• Máquinas virtuales <ul style="list-style-type: none"> <li>– Cubre hipervisores, virtualización de discos y memoria y el uso de máquinas virtuales en seguridad.</li> </ul> </li> <li>• Sistemas de control industriales <ul style="list-style-type: none"> <li>– Este tema incluye SCADA</li> </ul> </li> <li>• Internet de las cosas (IoT) <ul style="list-style-type: none"> <li>– Este tema incluye ejemplos como refrigeradores y sensores.</li> </ul> </li> <li>• Sistemas integrados <ul style="list-style-type: none"> <li>– Este tema incluye ejemplos como sistemas en</li> </ul> </li> <li>• Sistemas móviles <ul style="list-style-type: none"> <li>– Este tema incluye ejemplos como computadoras portátiles y teléfonos inteligentes.</li> </ul> </li> <li>• Sistemas autónomos <ul style="list-style-type: none"> <li>– Este tema incluye ejemplos como robots y vehículos aéreos no tripulados que no requieren control humano.</li> </ul> </li> <li>• Sistema de propósito general <ul style="list-style-type: none"> <li>– Este tema incluye ejemplos como computadoras de escritorio, portátiles y mainframes.</li> </ul> </li> </ul> | <ul style="list-style-type: none"> <li>• Analice la importancia de documentar la instalación y configuración adecuadas de un sistema [Usar]</li> <li>• Ser capaz de escribir documentación sobre intrusiones de red y host [Usar]</li> <li>• Ser capaz de explicar las implicaciones de seguridad de una documentación poco clara o incompleta del funcionamiento del sistema [Usar]</li> </ul> |
| Lecturas : [Stallings2018]   |   |

| Unidad 3: Control de sistema (12 horas)  |   |
|--|---|
| Resultados esperados: 1,6  |   |
| Temas  | Objetivos de Aprendizaje  |
| <ul style="list-style-type: none"> <li>● control de acceso <ul style="list-style-type: none"> <li>– 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.</li> </ul> </li> <li>● Modelos de autorización <ul style="list-style-type: none"> <li>– Cubre la gestión de la autorización en muchos sistemas y la distinción entre autenticación y autorización.</li> </ul> </li> <li>● Detección de intrusiones <ul style="list-style-type: none"> <li>– Cubre anomalías, uso indebido (basado en reglas, basado en firmas) y técnicas basadas en especificaciones.</li> </ul> </li> <li>● Ataques <ul style="list-style-type: none"> <li>– Este tema cubre modelos de ataque (como árboles y gráficos de ataque) y ataques específicos.</li> </ul> </li> <li>● Defensas <ul style="list-style-type: none"> <li>– Este tema incluye ejemplos como ASLR, salto de IP y tolerancia a intrusiones.</li> </ul> </li> <li>● Auditoría <ul style="list-style-type: none"> <li>– cubre el registro, el análisis de registros y la relación con la detección de intrusiones</li> </ul> </li> <li>● malware <ul style="list-style-type: none"> <li>– Ejemplos como virus informáticos, gusanos, ransomware y otras formas de malware.</li> </ul> </li> <li>● Modelos de vulnerabilidades <ul style="list-style-type: none"> <li>– Ejemplos como RISOS y PA; y enumeraciones como CVE y CWE.</li> </ul> </li> <li>● Pruebas de penetración <ul style="list-style-type: none"> <li>– Cubre la Metodología de Hipótesis de Fallas y otras formas (ISSAF, OSSTMM, GISTA, PTES, etc.).</li> </ul> </li> <li>● forense <ul style="list-style-type: none"> <li>– Este tema se centra en los requisitos del sistema para análisis forense.</li> </ul> </li> <li>● Recuperación, resiliencia <ul style="list-style-type: none"> <li>– Este tema incluye mecanismos de disponibilidad.</li> </ul> </li> </ul> | <ul style="list-style-type: none"> <li>● Describir una lista de control de acceso [Usar]</li> <li>● Describir el control de acceso físico y lógico, compararlos y contrastarlos [Usar]</li> <li>● Distinga entre autorización y autenticación [Usar]</li> </ul> |
| <b>4 Lecturas : [Bishop2002]</b>   |   |

| Unidad 4: Continuidad del negocio, recuperación ante desastres y gestión de incidentes (12 horas)   |  |
|---|--|
| Resultados esperados: 1,6   |  |
| Temas   | Objetivos de Aprendizaje   |
| <ul style="list-style-type: none"> <li>• Respuesta a incidentes <ul style="list-style-type: none"> <li>– 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.</li> </ul> </li> <li>• Recuperación ante desastres <ul style="list-style-type: none"> <li>– 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.</li> <li>– Se deben brindar oportunidades a los estudiantes para que escriban planes reales o basados en casos para adquirir algo de experiencia.</li> </ul> </li> <li>• Continuidad del negocio <ul style="list-style-type: none"> <li>– la creación y uso de los planos BC</li> <li>– organización de los planes</li> <li>– Ocasiones para revisar/reescribir planes.</li> <li>– y examen de planos sanitizados</li> <li>– Se deben brindar oportunidades a los estudiantes para que escriban planes reales o basados en casos para adquirir algo de experiencia.</li> </ul> </li> </ul> | <ul style="list-style-type: none"> <li>• Explicar la planificación organizacional estratégica para la ciberseguridad y su relación con la planificación estratégica de TI y para toda la organización [Usar]</li> <li>• Identificar las partes interesadas clave de la organización y sus roles [Usar]</li> <li>• Describir los componentes principales de la planificación de la implementación del sistema de ciberseguridad [Usar]</li> </ul> |
| 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