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

1. CURSO

CY251. Seguridad de Sistemas (Obligatorio)

2. INFORMACIÓN GENERAL

2.1 Curso	:	CY251. Seguridad de Sistemas
2.2 Semestre	:	7^{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	:	CS2S1. Sistemas Operativos. (4^{to} Sem)

3. PROFESORES

Atención previa coordinación con el profesor

4. INTRODUCCIÓN AL CURSO

Este curso aborda la seguridad de sistemas informáticos como un todo, considerando la interacción entre componentes, conexiones y software. Se exploran conceptos de pensamiento sistémico, gestión de sistemas, control de acceso y pruebas de seguridad, para capacitar a los estudiantes en el análisis y mitigación de riesgos en sistemas complejos.

5. OBJETIVOS

- Aplicar el pensamiento sistémico al análisis de la seguridad de sistemas informáticos.
- Comprender y aplicar técnicas de gestión, control de acceso y pruebas para fortalecer la seguridad de sistemas.
- Identificar y evaluar vulnerabilidades y amenazas a la seguridad de sistemas.

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: (8 horas)

Resultados esperados: 1,6

Temas	**Objetivos de Aprendizaje**
• ¿Qué es un sistema? – Analiza la definición de sistema y cómo depende del contexto. • ¿Qué es la ingeniería de sistemas? – Se centra en el valor de contar con buenos artefactos de ingeniería de sistemas para informar la gestión de riesgos de seguridad. • Enfoques holísticos – Cubre ver el sistema como un todo y no simplemente como una colección de componentes interconectados. Por ejemplo, considerar las consideraciones humanas, organizativas y ambientales del todo en lugar de ver cada componente y conexión individual y cómo afectan la visión del riesgo. • Seguridad de sistemas de propósito general. – Cubre las consideraciones de seguridad de la informática y de los sistemas en general. • Seguridad de sistemas de propósitos especiales. – Cubre consideraciones de seguridad derivadas de los fines a los que se destina el sistema. • Modelos de amenazas – Cubre qué problemas de seguridad pueden surgir y cómo pueden realizarse, detectarse y mitigarse. • Análisis de requisitos – Presenta la derivación y validación de requisitos a lo largo del ciclo de vida del sistema, incluso en diversas metodologías como la cascada y las metodologías de desarrollo ágil. • Principios fundamentales – El área de conocimiento de Seguridad del software cubre estos principios en detalle, pero también se aplican aquí. • Desarrollo para pruebas – Cubre el diseño de sistemas para facilitar y efectividad de las pruebas.	• Discuta la importancia de una política de seguridad [Usar] • Explique por qué diferentes sitios tienen diferentes políticas de seguridad [Usar] • Explique la relación entre un grupo de seguridad, la configuración del sistema y los procedimientos para mantener la seguridad del sistema [Usar]

Lecturas : [**Bishop2002**]

Unidad 2: Gestión del sistema (10 horas)

Resultados esperados: 1,6

Temas	**Objetivos de Aprendizaje**
• Modelos de políticas – incluye ejemplos como BellLaPadula, Clark-Wilson, Chinese Wall y Clinical Information Systems Security. • Composición de políticas – Este tema cubre la restricción. • Uso de la automatización – Este tema incluye minería de datos, aprendizaje automático y técnicas relacionadas, y sus beneficios y limitaciones. • Parches y ciclo de vida de la vulnerabilidad – Este tema incluye los problemas de seguridad que surgen al aplicar parches, como por ejemplo si se deben aplicar parches a un sistema y a un sistema en ejecución, así como cómo manejar los informes de vulnerabilidad. • Operación – Este tema incluye la seguridad en el funcionamiento y la importancia de las consideraciones de usabilidad. • Puesta en servicio y desmantelamiento – Este tema describe las consideraciones de seguridad al instalar y eliminar un sistema. • Amenaza interna – Este tema incluye ejemplos de amenazas internas, como la exfiltración de datos y el sabotaje, y cubre contramedidas. • Documentación – Este tema cubre la documentación de seguridad y garantía, así como las guías de instalación y de usuario centradas en el sistema en sí. • Sistemas y procedimientos – En este tema se analizan los procedimientos que se utilizan para gestionar sistemas.	• Discuta la importancia de una política de seguridad [Usar] • Explique por qué diferentes sitios tienen diferentes políticas de seguridad [Usar] • Explique la relación entre un grupo de seguridad, la configuración del sistema y los procedimientos para mantener la seguridad del sistema [Usar]

Lecturas : [**NIST-SP800-12r1**]

Unidad 3: Acceso al sistema (8 horas)	
Resultados esperados: 6	
Temas	**Objetivos de Aprendizaje**
• Métodos de autenticación – Los métodos de autenticación se refieren a la autenticación de persona a sistema o de sistema a sistema; los ejemplos incluyen contraseñas, datos biométricos, dongles e inicio de sesión único. • Identidad – ¿Cómo se representa la identidad ante el sistema? Este tema incluye roles, así como nombres, etc.	• Explique tres propiedades comúnmente utilizadas para la autenticación [Usar] • Explique la importancia de la autenticación multifactor [Usar] • Explique las ventajas de las frases de contraseña sobre las contraseñas [Usar]
Lecturas : [**Gollmann2010**]	

Unidad 4: Control de sistema (10 horas)	
Resultados esperados: 1,6	
Temas	**Objetivos de Aprendizaje**
• 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 5: Retiro del sistema (12 horas)	
Resultados esperados: 6	
Temas	**Objetivos de Aprendizaje**
• Desmantelamiento – Examina cómo retirar un sistema al final de su vida útil o antes puede afectar la seguridad de otros sistemas o de la organización que utilizó el sistema. – El estudiante debe comprender los efectos de eliminar un sistema, componentes o conexiones dentro de un sistema, sobre la seguridad del sistema en su conjunto. • Desecho – Incluye la limpieza de medios y otras formas de destrucción para evitar que se recupere información confidencial (como PII).	• Analice cómo los sistemas de detección de intrusos contribuyen a la seguridad [Usar] • Describir los límites del software antimalware, como los programas antivirus [Usar] • Analice los usos del monitoreo del sistema [Usar]
Lecturas : [**NIST-SP800-88r1**]	

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