National University of Engineering (UNI)
School of Cybersecurity
Syllabus 2024-II

1. COURSE

CY251. System Security (Mandatory)

2. GENERAL INFORMATION

2.1 Course	:	CY251. System Security
2.2 Semester	:	7^{th} Semester.
2.3 Credits	:	3
2.4 Horas	:	2 HT; 2 HP;
2.5 Duration of the period	:	16 weeks
2.6 Type of course	:	Mandatory
2.7 Learning modality	:	Face to face
2.8 Prerrequisites	:	CS2S1. Operating systems . (4^{th} Sem)

3. PROFESSORS

Meetings after coordination with the professor

4. INTRODUCTION TO THE COURSE

This course addresses the security of computer systems as a whole, considering the interaction between components, connections, and software. Concepts of system thinking, system management, access control, and security testing are explored to train students in analyzing and mitigating risks in complex systems.

5. GOALS

- Apply system thinking to the security analysis of computer systems.
- Understand and apply management, access control, and testing techniques to strengthen system security.
- Identify and evaluate vulnerabilities and threats to system security.

6. COMPETENCES

1) Analyze a complex computing problem and apply principles of computing and other relevant disciplines to identify solutions. (Usage)

5) Function effectively as a member or leader of a team engaged in activities appropriate to the program's discipline. (Assessment)

6) Apply security principles and practices to maintain operations in the presence of risks and threats. (Usage)

7. TOPICS

Unit 1: Pensamiento sistémico (8 hours)

Competences Expected: 1,6

Topics	Learning Outcomes
• ¿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]

Readings : [**Bishop2002**]

Unit 2: Gestión del sistema (10 hours)

Competences Expected: 1,6

Topics	Learning Outcomes
• 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]

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

Unit 3: Acceso al sistema (8 hours)	
Competences Expected: 6	
Topics	**Learning Outcomes**
• 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]
Readings : [**Gollmann2010**]	

Unit 4: Control de sistema (10 hours)

Competences Expected: 1,6

Topics	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]

Readings : [**Bishop2002**]

Unit 5: Retiro del sistema (12 hours)	
Competences Expected: 6	
Topics	**Learning Outcomes**
• 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]
Readings : [**NIST-SP800-88r1**]	

8. WORKPLAN

8.1 Methodology

Individual and team participation is encouraged to present their ideas, motivating them with additional points in the different stages of the course evaluation.

8.2 Theory Sessions

The theory sessions are held in master classes with activities including active learning and roleplay to allow students to internalize the concepts.

8.3 Practical Sessions

The practical sessions are held in class where a series of exercises and/or practical concepts are developed through problem solving, problem solving, specific exercises and/or in application contexts.

9. EVALUATION SYSTEM

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

10. BASIC BIBLIOGRAPHY