



## 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 <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	:	CS2S1. Sistemas Operativos. (4 <sup>to</sup> 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) Analizar un problema computacional complejo y aplicar los principios computacionales y otras disciplinas relevantes para identificar soluciones. (Usage)
- 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. (Usage)

### 7. TEMAS

Unidad 1: Pensamiento sistémico (8 horas)	
Resultados esperados: 1,6	
Temas	Objetivos de Aprendizaje ( <i>Learning Outcomes</i> )
<ul style="list-style-type: none"> <li>• ¿Qué es un sistema? <ul style="list-style-type: none"> <li>– Analiza la definición de sistema y cómo depende del contexto.</li> </ul> </li> <li>• ¿Qué es la ingeniería de sistemas? <ul style="list-style-type: none"> <li>– Se centra en el valor de contar con buenos artefactos de ingeniería de sistemas para informar la gestión de riesgos de seguridad.</li> </ul> </li> <li>• Enfoques holísticos <ul style="list-style-type: none"> <li>– 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.</li> </ul> </li> <li>• Seguridad de sistemas de propósito general. <ul style="list-style-type: none"> <li>– Cubre las consideraciones de seguridad de la informática y de los sistemas en general.</li> </ul> </li> <li>• Seguridad de sistemas de propósitos especiales. <ul style="list-style-type: none"> <li>– Cubre consideraciones de seguridad derivadas de los fines a los que se destina el sistema.</li> </ul> </li> <li>• Modelos de amenazas <ul style="list-style-type: none"> <li>– Cubre qué problemas de seguridad pueden surgir y cómo pueden realizarse, detectarse y mitigarse.</li> </ul> </li> <li>• Análisis de requisitos <ul style="list-style-type: none"> <li>– 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.</li> </ul> </li> <li>• Principios fundamentales <ul style="list-style-type: none"> <li>– El área de conocimiento de Seguridad del software cubre estos principios en detalle, pero también se aplican aquí.</li> </ul> </li> <li>• Desarrollo para pruebas <ul style="list-style-type: none"> <li>– Cubre el diseño de sistemas para facilitar y efectividad de las pruebas.</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• Discuta la importancia de una política de seguridad [Usar]</li> <li>• Explique por qué diferentes sitios tienen diferentes políticas de seguridad [Usar]</li> <li>• Explique la relación entre un grupo de seguridad, la configuración del sistema y los procedimientos para mantener la seguridad del sistema [Usar]</li> </ul>
Lecturas : [Bishop2002]	

Unidad 2: Gestión del sistema (10 horas)	
Resultados esperados: 1,6	
Temas	Objetivos de Aprendizaje ( <i>Learning Outcomes</i> )
<ul style="list-style-type: none"> <li>• Modelos de políticas <ul style="list-style-type: none"> <li>– incluye ejemplos como BellLaPadula, Clark-Wilson, Chinese Wall y Clinical Information Systems Security.</li> </ul> </li> <li>• Composición de políticas <ul style="list-style-type: none"> <li>– Este tema cubre la restricción.</li> </ul> </li> <li>• Uso de la automatización <ul style="list-style-type: none"> <li>– Este tema incluye minería de datos, aprendizaje automático y técnicas relacionadas, y sus beneficios y limitaciones.</li> </ul> </li> <li>• Parches y ciclo de vida de la vulnerabilidad <ul style="list-style-type: none"> <li>– 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.</li> </ul> </li> <li>• Operación <ul style="list-style-type: none"> <li>– Este tema incluye la seguridad en el funcionamiento y la importancia de las consideraciones de usabilidad.</li> </ul> </li> <li>• Puesta en servicio y desmantelamiento <ul style="list-style-type: none"> <li>– Este tema describe las consideraciones de seguridad al instalar y eliminar un sistema.</li> </ul> </li> <li>• Amenaza interna <ul style="list-style-type: none"> <li>– Este tema incluye ejemplos de amenazas internas, como la exfiltración de datos y el sabotaje, y cubre contramedidas.</li> </ul> </li> <li>• Documentación <ul style="list-style-type: none"> <li>– Este tema cubre la documentación de seguridad y garantía, así como las guías de instalación y de usuario centradas en el sistema en sí.</li> </ul> </li> <li>• Sistemas y procedimientos <ul style="list-style-type: none"> <li>– En este tema se analizan los procedimientos que se utilizan para gestionar sistemas.</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• Discuta la importancia de una política de seguridad [Usar]</li> <li>• Explique por qué diferentes sitios tienen diferentes políticas de seguridad [Usar]</li> <li>• Explique la relación entre un grupo de seguridad, la configuración del sistema y los procedimientos para mantener la seguridad del sistema [Usar]</li> </ul>
Lecturas : [NIST-SP800-12r1]	

<b>Unidad 3: Acceso al sistema (8 horas)</b>	
<b>Resultados esperados: 6</b>	
<b>Temas</b>	<b>Objetivos de Aprendizaje (<i>Learning Outcomes</i>)</b>
<ul style="list-style-type: none"> <li>• Métodos de autenticación <ul style="list-style-type: none"> <li>– 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.</li> </ul> </li> <li>• Identidad <ul style="list-style-type: none"> <li>– ¿Cómo se representa la identidad ante el sistema? Este tema incluye roles, así como nombres, etc.</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• Explique tres propiedades comúnmente utilizadas para la autenticación [Usar]</li> <li>• Explique la importancia de la autenticación multifactor [Usar]</li> <li>• Explique las ventajas de las frases de contraseña sobre las contraseñas [Usar]</li> </ul>
<b>Lecturas : [Gollmann2010]</b>	

Unidad 4: Control de sistema (10 horas)	
Resultados esperados: 1,6	
Temas	Objetivos de Aprendizaje ( <i>Learning Outcomes</i> )
<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>
Lecturas : [Bishop2002]	

Unidad 5: Retiro del sistema (12 horas)	
Resultados esperados: 6	
Temas	Objetivos de Aprendizaje ( <i>Learning Outcomes</i> )
<ul style="list-style-type: none"> <li>• Desmantelamiento <ul style="list-style-type: none"> <li>– 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.</li> <li>– 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.</li> </ul> </li> <li>• Desecho <ul style="list-style-type: none"> <li>– Incluye la limpieza de medios y otras formas de destrucción para evitar que se recupere información confidencial (como PII).</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• Analice cómo los sistemas de detección de intrusos contribuyen a la seguridad [Usar]</li> <li>• Describir los límites del software antimalware, como los programas antivirus [Usar]</li> <li>• Analice los usos del monitoreo del sistema [Usar]</li> </ul>
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