



Universidad Nacional de Ingeniería (UNI)

Escuela Profesional de
Inteligencia Artificial
Sílabo 2027-I

1. CURSO

AI364. Inteligencia Artificial para Ciberseguridad I (Obligatorio)

2. INFORMACIÓN GENERAL

- 2.1 Curso : AI364. Inteligencia Artificial para Ciberseguridad I
- 2.2 Semestre : 8^{vo} Semestre.
- 2.3 Créditos : 4
- 2.4 Horas : 2 HT; 4 HP;
- 2.5 Duración del periodo : 16 semanas
- 2.6 Condición : Obligatorio
- 2.7 Modalidad de aprendizaje : Presencial
 - AI264. Aprendizaje Profundo. (7^{mo} Sem)
- 2.8 Prerrequisitos :
 - AI265. Aprendizaje por Refuerzo. (7^{mo} Sem)

3. PROFESORES

Atención previa coordinación con el profesor

4. INTRODUCCIÓN AL CURSO

Este curso cubre técnicas avanzadas de IA aplicadas a ciberseguridad, incluyendo detección de amenazas mediante aprendizaje automático, generación de adversarios y defensas autónomas contra ataques modernos.

5. OBJETIVOS

- Implementar sistemas de detección de intrusos basados en IA
- Diseñar pruebas de estrés para modelos de seguridad
- Analizar implicaciones éticas del uso ofensivo de IA

6. RESULTADOS DEL ESTUDIANTE

AG-C02) Ética: Aplica principios éticos y se compromete con la ética profesional y las normas de la práctica profesional de la computación. (Usage)

AG-C09) Diseño y Desarrollo de Soluciones: Diseña, implementa y evalúa soluciones para problemas complejos de computación. (Assessment)

AG-C12) Usa enfoques sistémicos para seleccionar, desarrollar, aplica, integrar y administrar tecnologías seguras de computación para lograr los objetivos del usuario. (Assessment)

7. TEMAS

Unidad 1: Fundamentos de IA en Cybersecurity (12 horas)	
Resultados esperados: AG-C02	
Temas	Aprendizaje esperado (<i>Learning Outcomes</i>)
▪ Taxonomía de amenazas asistidas por IA ▪ Arquitecturas de modelos para análisis de malware ▪ Datasets de seguridad (CIC-IDS, NSL-KDD)	▪ Clasificar amenazas usando redes neuronales [Evaluar] ▪ Preprocesar logs de seguridad para modelos ML [Usar]
Lecturas : [apruzzese2023ai4cyber]	

Unidad 2: Ataques y Defensas (24 horas)	
Resultados esperados: AG-C02	
Temas	Aprendizaje esperado (<i>Learning Outcomes</i>)
▪ Adversarial examples en modelos de seguridad ▪ Generación automática de exploits (Fuzzing con RL) ▪ Sistemas de detección autoadaptativos	▪ Implementar ataques adversarios a modelos ML [Usar] ▪ Diseñar defensas metamórficas [Evaluar]
Lecturas : [goodfellow2014explaining], [anderson2020metamorphic]	

Unidad 3: Ética en Cybersecurity (8 horas)	
Resultados esperados: AG-C02	
Temas	Aprendizaje esperado (<i>Learning Outcomes</i>)
▪ Armas cibernéticas autónomas ▪ Responsabilidad en vulnerabilidades IA-generadas ▪ Regulaciones internacionales (AI Cyber Initiative)	▪ Evaluar riesgos de sistemas autónomos [Familiarizarse] ▪ Diseñar protocolos de rendición de cuentas [Usar]
Lecturas : [apruzzese2023ai4cyber]	

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