COMILLAS
UNIVERSIDAD PONTIFICIA
ICAI ICADE CIHS

GUÍA DOCENTE
2024 - 2025

FICHA TÉCNICA DE LA ASIGNATURA

Datos de la asignatura	
Nombre completo	Inteligencia Artificial Aplicada a Ciberseguridad
Código	DOI-MCS-522
Créditos	4,5 ECTS
Carácter	Optativa
Departamento / Área	Departamento de Organización Industrial

Datos del profesorado	
Profesor	
Nombre	Juan Pablo Fuentes Brea
Departamento / Área	Departamento de Organización Industrial
Correo electrónico	jpfuentes@icai.comillas.edu

DATOS ESPECÍFICOS DE LA ASIGNATURA

Contextualización de la asignatura

Prerrequisitos

Conocimientos básicos de machine learning, ciberseguridad y lenguaje Python.

Competencias - Objetivos

BLOQUES TEMÁTICOS Y CONTENIDOS

Contenidos – Bloques Temáticos

Temario

Presentación de la asignatura

- Objetivos
- Temario
- Prácticas
- Evaluación
- Frameworks
- Contacto
- Bibliografía

Introducción a la IA aplicada a Ciberseguridad

- El contexto actual de la ciberseguridad y sus desafíos

- Inteligencia artificial aplicada a ciberseguridad
- Casos de uso para IA/ML en ciberseguridad
- Tendencias Futuras y Oportunidades

Algoritmos, Herramientas y Sistemas

- Problemas y algoritmos
- Herramientas y librerías
- Sistemas ML en producción

Threat Intelligence

- Threat Intelligence
- Plataformas para TI
- Caso de uso para IA

Detección de fraude

- Presentación de escenarios de fraude
- Detección de Fraude mediante Scoring estático
- Detección de Fraude mediante Scoring dinámico
- Introducción a Deep Learning

UEBA (User and Entity Behaviour Analytics)

- Presentación de escenarios UEBA
- Análisis temporal de actividades
- Modelos basados en autoencoders
- Modelos recurrentes
- Introducción a Pytorch

Adversarial ML

- Presentación de escenarios Adversarial ML
- Métodos de ataque
- Métodos de defensa
- Seguridad en el ciclo de vida de IA

Deepfakes

- Presentación de escenarios Deepfakes
- GANs
- Fake faces
- Fake news
- Fake speech

Optimización de ataques

- Presentación de escenarios de optimización
- Ciberataques de tipo Black-Box

- Reinforcement Learning
- Computación evolutiva

Futuras líneas de trabajo en Ciberseguridad & IA

- Escenarios futuros de IA aplicada a Ciberseguridad
- Nuevos perfiles necesarios: IA4sec
- Conclusiones finales

METODOLOGÍA DOCENTE

Aspectos metodológicos generales de la asignatura

EVALUACIÓN Y CRITERIOS DE CALIFICACIÓN

Calificaciones

El mecanismo de calificación de la asignatura estará compuesto por una parte teoría y otra práctica, cuya suma deberá ser como mínimo de 5.0 para superar la asignatura. Los porcentajes de ambas partes serán las siguientes:

Nota final = 0.8 * (nota teoría) + 0.2 * (nota prácticas)

BIBLIOGRAFÍA Y RECURSOS

Bibliografía Básica

Freeman and Chio. Machine Learning and Security. O'Reilly Media 2018

Duda, Hart and Stork. Pattern Classification. Wiley & Sons 2001

Shawe-Taylor & Cristianini. Kernel Methods for Pattern Analysis. Cambridge 2004

Gollmann. Computer Security. Wiley & Sons, 2011

Szor. The Art of Computer Virus Research and Defense. Addison-Wesley, 2005

Rieck. Machine Learning for Application-Layer Intrusion Detection, Lulu 2009