



## FICHA TÉCNICA DE LA ASIGNATURA

<b>Datos de la asignatura</b>	
<b>Nombre completo</b>	Inteligencia Artificial Aplicada a Ciberseguridad
<b>Código</b>	DOI-MCS-522
<b>Impartido en</b>	Máster en Ciberseguridad [Primer Curso]
<b>Nivel</b>	Master
<b>Cuatrimestre</b>	Semestral
<b>Créditos</b>	4,5 ECTS
<b>Carácter</b>	Optativa
<b>Departamento / Área</b>	Departamento de Organización Industrial
<b>Responsable</b>	Rafael Palacios
<b>Descriptor</b>	<p>El objetivo de la asignatura es conocer cómo a partir de la aplicación de técnicas de Inteligencia Artificial (IA) sobre casos de uso de ciberseguridad, se consigue un salto cualitativo y cuantitativo a nivel de detección y protección de los activos de información de una compañía gracias a la cualidad predictiva que éstas aportan. Aunque la IA puede ayudar a la defensa de dichos activos de información, también puede ser utilizada como mecanismo de ataque sobre los mismos, siendo una herramienta cada vez más empleada por los ciberatacantes. De esta forma, se presentarán los mecanismos tanto de defensa como de ataque mediante IA cercanos al estado del arte, realizando un repaso a los principales escenarios de ciberseguridad como son la detección de malware, análisis de fraude y análisis de comportamientos, además de otros cada vez con más futuro como son las fake news o fake faces.</p>

<b>Datos del profesorado</b>	
<b>Profesor</b>	
<b>Nombre</b>	Hugo Gascón Polanco
<b>Departamento / Área</b>	Departamento de Organización Industrial
<b>Correo electrónico</b>	hgascon@icai.comillas.edu
<b>Profesor</b>	
<b>Nombre</b>	Juan Pablo Fuentes Brea
<b>Departamento / Área</b>	Departamento de Organización Industrial
<b>Correo electrónico</b>	jpgfuentes@icai.comillas.edu

## DATOS ESPECÍFICOS DE LA ASIGNATURA

<b>Contextualización de la asignatura</b>
<b>Prerequisitos</b>



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

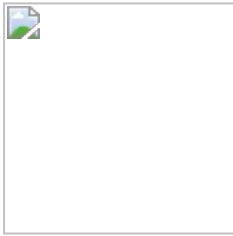
- Problemas y algoritmos
- Herramientas y librerías
- Sistemas ML en producción

##### 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

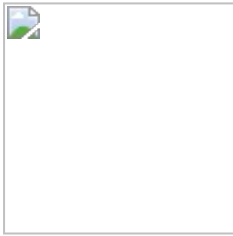
## METODOLOGÍA DOCENTE

### 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



## GUÍA DOCENTE 2019 - 2020

suma deberá ser como mínimo de 5.0 para superar la asignatura. Los porcentajes de ambas partes serán las siguientes:

$$\text{Nota final} = 0.8 * (\text{nota teoría}) + 0.2 * (\text{nota prácticas})$$

### 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