



FICHA TÉCNICA DE LA ASIGNATURA

Datos de la asignatura	
Nombre completo	Machine Learning / Analítica Avanzada
Código	DOI-MCS-514
Impartido en	Máster en Ciberseguridad [Primer Curso]
Nivel	Master
Cuatrimestre	Semestral
Créditos	6,0 ECTS
Carácter	Obligatoria
Departamento / Área	Departamento de Organización Industrial
Responsable	Juan Pablo Fuentes Brea
Descriptor	El propósito de esta asignatura es brindar a los estudiantes una comprensión fundamental y una amplia experiencia práctica sobre cómo extraer conocimiento de un conjunto de datos aparentemente no estructurados, en busca de su aplicación sobre áreas como la Ciberseguridad. Al final del curso, los estudiantes: • Comprender los principios básicos detrás del aprendizaje automático. • Tener experiencia práctica con los algoritmos de aprendizaje automático más relevantes. • Disponer de criterios bien formados para elegir las técnicas más adecuadas para una determinada aplicación en el área de Ciberseguridad.

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
Los estudiantes deben estar familiarizados con álgebra lineal, probabilidad y estadística básicas, así como programación a nivel universitario. También se desea experiencia previa con el lenguaje de programación R y Python, aunque no es estrictamente necesario.

Competencias - Objetivos
Competencias
Generales
<i>Haber adquirido conocimientos avanzados y demostrado, en un contexto de investigación científica y tecnológica o altan CG1. especializado, una comprensión detallada y fundamentada de los aspectos teóricos y prácticos y de la metodología de trabajo en</i>



o más campos de estudio.

Saber aplicar e integrar sus conocimientos, la comprensión de estos, su fundamentación científica y sus capacidades de resolución de problemas en entornos nuevos y definidos de forma imprecisa, incluyendo contextos de carácter multidisciplinar tanto investigativos como profesionales altamente especializados.

Saber evaluar y seleccionar la teoría científica adecuada y la metodología precisa de sus campos de estudio para formular juicios a partir de información incompleta o limitada incluyendo, cuando sea preciso y pertinente, una reflexión sobre la responsabilidad social o ética ligada a la solución que se proponga en cada caso.

Ser capaces de predecir y controlar la evolución de situaciones complejas mediante el desarrollo de nuevas e innovadoras metodologías de trabajo adaptadas al ámbito científico/investigador, tecnológico o profesional concreto, en general multidisciplinarias en el que se desarrolle su actividad.

Saber transmitir de un modo claro y sin ambigüedades, a un público especializado o no, resultados procedentes de la investigación científica y tecnológica o del ámbito de la innovación más avanzada, así como los fundamentos más relevantes sobre los que sustentan.

Haber desarrollado la autonomía suficiente para participar en proyectos de investigación y colaboraciones científicas o tecnológicas dentro de su ámbito temático, en contextos interdisciplinares y, en su caso, con una alta componente de transferencia de conocimiento.

Ser capaces de asumir la responsabilidad de su propio desarrollo profesional y de su especialización en uno o más campos de estudio.

Específicas

Ser capaces de diseñar y entrenar sistemas que aprendan de manera automática, dominando tanto las técnicas de aprendizaje supervisado como no supervisado. Entender el potencial de aplicación de estos sistemas en la mejora de procesos industriales y en la relación con clientes, etc.

Resultados de Aprendizaje

Al final del curso, los alumnos deberían:

RA01. Conocer los principios básicos detrás del machine learning.

RA02. Adquirir una perspectiva general para la aplicación de las técnicas de machine learning en casos prácticos de Ciberseguridad.

RA03. Saber realizar predicciones, seleccionando las técnicas más adecuadas para cada aplicación.

BLOQUES TEMÁTICOS Y CONTENIDOS



Contenidos – Bloques Temáticos

Tema 0. Introducción

Introducción a Machine Learning

El proceso de aprendizaje

Tipos de técnicas de aprendizaje

Líneas de aplicación en Ciberseguridad

Tema 1. Modelos de regresión

El problema de la regresión

Linear regression.

Model selection and regularization

Polynomial regression

Splines

Generalized additive models

Multilayer perceptrons for regression

Radial basis function networks

Tema 2. Modelos de clasificación

El problema de la clasificación

Logistic regression

Discriminant analysis

K-nearest neighbors

Decision trees

Support vector machines

Multilayer perceptrons for classification

Tema 3. Series temporales

Stochastic processes

Exponential smoothing

Decomposition methods

ARIMA models

Dynamic regression models

Tema 4. Aprendizaje no supervisado



Dimensionality reduction methods

Probability density estimation

Clustering and vector quantization

Self-organizing feature maps

METODOLOGÍA DOCENTE

Aspectos metodológicos generales de la asignatura

Cada sesión combinará teoría y práctica. El profesor explicará los conceptos básicos de la materia y profundizará en los temas más importantes con ejemplos ilustrativos. Los estudiantes se agruparán en parejas para poner en práctica de forma colaborativa los métodos y técnicas propuestas.

Metodología Presencial: Actividades

Clase magistral: El profesor introducirá los conceptos fundamentales de cada unidad, junto con algunas recomendaciones prácticas, y repasará ejemplos trabajados para apoyar la explicación. Se fomentará la participación activa planteando preguntas abiertas para fomentar el debate y proponiendo ejercicios breves de aplicación para resolver en clase.

Sesión práctica: Bajo la supervisión del instructor, los estudiantes, divididos en pequeños grupos, aplicarán los conceptos y técnicas tratados en las clases magistrales y se familiarizarán con la aplicación práctica de los algoritmos más relevantes utilizando herramientas y bibliotecas de software.

Metodología No presencial: Actividades

Estudio personal del material del curso y resolución de los ejercicios propuestos.

Preparación de sesiones de laboratorio, análisis de resultados y redacción de informes.

RESUMEN HORAS DE TRABAJO DEL ALUMNO

Horas presenciales		
Clase magistral	Sesión práctica	Evaluación
28	28	4
Horas no presenciales		
Autoestudio	Preparación de sesiones e informes	
60	60	



Créditos ECTS:

6 (180 horas)

EVALUACIÓN Y CRITERIOS DE CALIFICACIÓN

Actividades de evaluación	Criterios de evaluación	Peso
Examen final	Comprensión de los conceptos teóricos. Aplicación de estos conceptos a la resolución de problemas. Análisis crítico de los resultados, interpretabilidad y justificación de los mismos.	50%
Sesión práctica	Aplicación de conceptos teóricos a la resolución de problemas reales. Capacidad para utilizar y desarrollar software de analítica de datos y aprendizaje automático. Actitud y esfuerzo: Se fomentará la iniciativa y el trabajo proactivo. Habilidades de comunicación en la defensa de los resultados.	50%

Calificaciones

Convocatoria Ordinaria

La calificación en la convocatoria ordinaria de la asignatura se obtendrá como:

Un 50% de la calificación del examen final

Un 50% de la calificación de las sesiones prácticas

Convocatoria Extraordinaria

La calificación en la convocatoria extraordinaria de la asignatura se obtendrá como:

Un 50% de la calificación del examen final de la convocatoria extraordinaria

Un 50% de la calificación de las sesiones prácticas

BIBLIOGRAFÍA Y RECURSOS



Bibliografía Básica

Slides preparadas por el profesor (disponibles en Moodlerooms).

G. James, D. Witten, T. Hastie, and R. Tibshirani, *An Introduction to Statistical Learning with Applications in R*, Springer, 2013.

Bibliografía Complementaria

M. Kuhn and K. Johnson, *Applied Predictive Modeling*, Springer, 2013.

T. Hastie, R. Tibshirani, and J. Friedman, *The Elements of Statistical Learning. Data Mining, Inference and Prediction*, 2nd Ed., Springer, 2009.

E. Alpaydin, *Introduction to Machine Learning*, 3rd Ed., MIT Press, 2014.

S. Marsland, *Machine Learning: An Algorithmic Perspective*, 2nd Ed., Chapman & Hall/CRC Machine Learning & Pattern Recognition, 2015.

T. Mitchell, *Machine Learning*, McGraw-Hill, 1997.

R. Duda, P. Hart, and D. Stork, *Pattern Classification*, 2nd Ed., Wiley-Interscience, 2000.

C. Bishop, *Pattern Recognition and Machine Learning*, Springer, 2007.

S. Haykin, *Neural Networks and Learning Machines*, Prentice Hall, 2009.

S. Haykin, *Neural Networks. A Comprehensive Foundation*, 2nd Ed., Pearson, 1999.

W. Wei, *Time Series Analysis. Univariate and Multivariate Methods*, 2nd Ed., Addison-Wesley, 2006.