ANX-PR/CL/001-01
GUÍA DE APRENDIZAJE

ASIGNATURA

613000132 - Seguridad Y Privacidad De Los Datos

PLAN DE ESTUDIOS

61AH - Máster Universitario En Aprendizaje Automático Y Datos Masivos

CURSO ACADÉMICO Y SEMESTRE

2023/24 - Segundo semestre

Índice

Guía de Aprendizaje

1. Datos descriptivos

1.1. Datos de la asignatura

Nombre de la asignatura	613000132 - Seguridad y Privacidad de los Datos
No de créditos	3 ECTS
Carácter	Obligatoria
Curso	Primer curso
Semestre	Segundo semestre
Período de impartición	Febrero-Junio
Idioma de impartición	Castellano
Titulación	61AH - Máster Universitario en Aprendizaje Automático y Datos Masivos
Centro responsable de la titulación	61 - Escuela Tecnica Superior De Ingenieria De Sistemas Informaticos
Curso académico	2023-24

2. Profesorado

2.1. Profesorado implicado en la docencia

Nombre	Despacho	Correo electrónico	Horario de tutorías *
Jorge Blasco Alis (Coordinador/a)	1229	jorge.blasco.alis@upm.es	Sin horario. Sin horario. Concertar por email

* Las horas de tutoría son orientativas y pueden sufrir modificaciones. Se deberá confirmar los horarios de tutorías con el profesorado.

3. Competencias y resultados de aprendizaje

3.1. Competencias

CB10 - Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo.

CB6 - Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación

CB7 - Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio

CB8 - Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios

CB9 - Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades

CE09 - Entender y valorar las implicaciones éticas, legales y sociales de la inteligencia artificial, así como la seguridad y privacidad de los datos masivos.

CG1 - Capacidad para aplicar el método científico y saber organizar y planificar experimentos con rigor metodológico en el ámbito del aprendizaje automático y los datos masivos

CG2 - Participar en la aplicación de mecanismos de descripción, cuantificación, análisis, interpretación y evaluación de resultados experimentales del ámbito de los datos masivos y el aprendizaje automático

CG3 - Capacidad para reunir e interpretar datos masivos relevantes para emitir juicios que incluyan una reflexión sobre temas importantes de índole científico, social o ético en el ámbito del aprendizaje automático y los datos masivos

CG4 - Capacidad de aplicar iniciativa, integración, colaboración y potenciación de la discusión crítica en el ámbito del trabajo en equipo dentro del ámbito del aprendizaje automático y datos masivos

CG5 - Participar en la transmisión de la información generada, las ideas, los problemas y las soluciones de forma oral y escrita para un público tanto especializado como no especializado

CT1 - Creatividad

CT2 - Organización y planificación

CT3 - Gestión de la información

CT4 - Liderazgo de equipos

CT5 - Trabajo en contextos internacionales

K05 - El alumno analiza las distintas arquitecturas para el almacenamiento y procesado de datos masivos de altas prestaciones

S02 - El alumno planifica y ejecuta la gestión y el despliegue de infraestructuras de datos masivos

3.2. Resultados del aprendizaje

RA34 - · Dominar los principales criptosistemas y los algoritmos de cifrado actuales más característicos

RA35 - · Conocer y aplicar procedimientos de anonimización de datos personales y sensibles

RA36 - · Analizar riesgos de pérdida de privacidad y robo de información y diseñar las soluciones adecuadas.

RA33 - Conocer y evaluar las técnicas para proteger los sistemas informáticos frente a ataques y software malintencionado

4. Descripción de la asignatura y temario

4.1. Descripción de la asignatura

Esta asignatura aborda la intersección entre el aprendizaje automático y la ciberseguridad. La asignatura trata ambos temas desde dos perspectivas principales: la utilización del aprendizaje automático en el ámbito de la ciberseguridad y la incorporación de fundamentos de seguridad de la información en las propias tareas de aprendizaje automático. En particular, se tratarán diversos problemas en el ámbito de la ciberseguridad que pueden ser abordados mediante la utilización de técnicas de aprendizaje automático como la detección de intrusiones o malware. Además, la asignatura también revisará como los requisitos de seguridad y privacidad pueden afectar a las tareas de aprendizaje automático.

4.2. Temario de la asignatura

1. Seguridad de Sistemas de Información
    1.1. Conceptos de seguridad
    1.2. Criptografía
    1.3. Privacidad
    1.4. Ciberseguridad y Aprendizaje Automático
2. 2. Privacidad y Anonimización de la Información
    2.1. Anonimización
    2.2. Privacy Enhancing Technologies (PETs)
    2.3. Criptografía Homomórfica
3. Aprendizaje Automático en el Ámbito de la Ciberseguridad
    3.1. Dominios
    3.2. Aprendizaje Automático en Dominios Hostiles

5. Cronograma

5.1. Cronograma de la asignatura *

Sem	Actividad en aula	Actividad en laboratorio	Tele-enseñanza	Actividades de evaluación
1				
2				
3				
4				
5				
6	**Tema 1** Duración: 06:00 LM: Actividad del tipo Lección Magistral			
7	**Tema 2** Duración: 06:00 LM: Actividad del tipo Lección Magistral			
8	**Tema 3** Duración: 02:00 LM: Actividad del tipo Lección Magistral	**Tema 2 (Laboratorios)** Duración: 04:00 PL: Actividad del tipo Prácticas de Laboratorio		
9	**Tema 3** Duración: 06:00 LM: Actividad del tipo Lección Magistral			
10		**Tema 3** Duración: 04:00 PL: Actividad del tipo Prácticas de Laboratorio		**Presentación de progreso de la práctica.** PG: Técnica del tipo Presentación en Grupo Evaluación continua Presencial Duración: 02:00
11				
12				
13				
14				
15				
16				
17				**Trabajo Práctico** TG: Técnica del tipo Trabajo en Grupo Evaluación continua y sólo prueba final Presencial Duración: 00:00 **Examen escrito** EX: Técnica del tipo Examen Escrito Evaluación sólo prueba final Presencial Duración: 01:00

Para el cálculo de los valores totales, se estima que por cada crédito ECTS el alumno dedicará dependiendo del plan de estudios, entre 26 y 27 horas de trabajo presencial y no presencial.

6. Actividades y criterios de evaluación

6.1. Actividades de evaluación de la asignatura

6.1.1. Evaluación (progresiva)

Sem.	Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
10	Presentación de progreso de la práctica.	PG: Técnica del tipo Presentación en Grupo	Presencial	02:00	10%	0 / 10	CB9 CT1 CT2 CG5
17	Trabajo Práctico	TG: Técnica del tipo Trabajo en Grupo	Presencial	00:00	90%	5 / 10	S02 CT3 CB9 CG1 K05 CB10 CB7 CG3 CT5 CT1 CE09 CT2 CB6 CB8 CG2 CG5

6.1.2. Prueba evaluación global

Sem	Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
17	Trabajo Práctico	TG: Técnica del tipo Trabajo en Grupo	Presencial	00:00	90%	5 / 10	S02 CT3 CB9 CG1 K05 CB10 CB7 CG3 CT5 CT1 CE09 CT2 CB6 CB8 CG2

							CG5
17	Examen escrito	EX: Técnica del tipo Examen Escrito	Presencial	01:00	10%	5 / 10	CB9 CT1 CT2 CG5

6.1.3. Evaluación convocatoria extraordinaria

Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
Trabajo individual de análisis de una temática relacionada con la asignatura	TI: Técnica del tipo Trabajo Individual	Presencial	00:00	100%	5 / 10	CG4 CB9 CG1 S02 CT3 K05 CB10 CB7 CG3 CT5 CT1 CE09 CT4 CT2 CB6 CB8 CG2 CG5

6.2. Criterios de evaluación

La evaluación se llevará a cabo sobre una práctica obligatoria. La práctica consistirá en la ejecución de un caso práctico y la presentación de un informe correspondiente. Como parte de la evaluación continua se realizará una presentación sobre el trabajo realizado el último día de clase de la asignatura. La evaluación por prueba final incluye la realización de un examen con una nota mínima de 5.0. Para la convocatoria extraordinaria se deberá realizar un trabajo individual sobre un tema relacionado con la asignatura.

7. Recursos didácticos

7.1. Recursos didácticos de la asignatura

Nombre	Tipo	Observaciones
Dos and Don'ts of Machine Learning in Computer Security	Bibliografía	Arp, Daniel, et al. "Dos and Don'ts of Machine Learning in Computer Security." 31st USENIX Security Symposium (USENIX Security 22). 2022.
The security of machine learning	Bibliografía	Barreno, Marco, et al. "The security of machine learning." Machine Learning 81 (2010): 121-148.
Adversarial attacks and defenses in images, graphs and text: A review	Bibliografía	Xu, H., Ma, Y., Liu, H. C., Deb, D., Liu, H., Tang, J. L., & Jain, A. K. (2020). Adversarial attacks and defenses in images, graphs and text: A review. International Journal of Automation and Computing, 17, 151-178.
When machine learning meets privacy: A survey and outlook	Bibliografía	Liu, Bo, et al. "When machine learning meets privacy: A survey and outlook." ACM Computing Surveys (CSUR) 54.2 (2021): 1-36.
Moodle de la Asignatura	Recursos web	