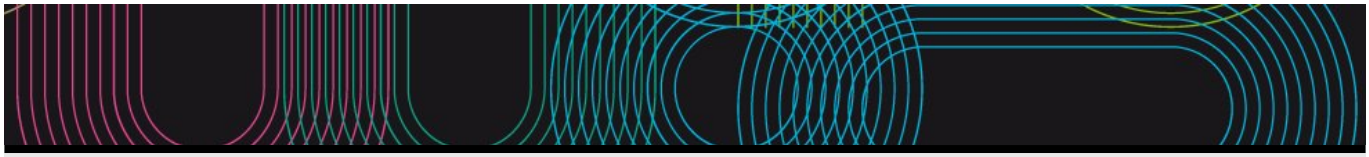

DATOS IDENTIFICATIVOS				
Privacidad y anonimidad				
Asignatura	Privacidad y anonimidad			
Código	V05M175V11110			
Titulacion	Máster Universitario en Ciberseguridad			
Descriptores	Creditos ECTS	Seleccione	Curso	Cuatrimestre
	5	OB	1	1c
Lengua Impartición	#EnglishFriendly Castellano			
Departamento	Dpto. Externo Teoría de la señal y comunicaciones			
Coordinador/a	Pérez González, Fernando			
Profesorado	Hernández Pereira, Elena María Pérez González, Fernando			
Correo-e	fperez@gts.uvigo.es			
Web	http://http://moovi.gal			
Descripción general	Esta asignatura se presentan las principales técnicas para proporcionar privacidad y anonimidad en redes, sistemas y aplicaciones. Se estudian conceptos y métodos de privacidad diferencial, técnicas de mejora de la privacidad (PET), privacidad en la geolocalización, privacidad para aprendizaje máquina y técnicas de anonimidad. También se exploran las implicaciones de la privacidad desde el diseño y aspectos éticos y legales de la privacidad.			

Resultados de Formación y Aprendizaje
Código

Resultados previstos en la materia	
Resultados previstos en la materia	Resultados de Formación y Aprendizaje

Contenidos	
Tema	
Introducción. Ataques.	Introducción a la privacidad y la anonimidad. Ataques de inferencia. Ataques de análisis de tráfico. Rastreo online.
Privacidad diferencial.	Privacidad diferencial. Mecanismos para la privacidad diferencial. Teoremas de composición.
Técnicas de mantenimiento y mejora de la privacidad.	Primitivas con mantenimiento de la privacidad: recuperación de información, intersección de conjuntos. Técnicas de mejora de la privacidad con cifrado homomórfico y computación multipartita segura. Filtros de Bloom.
Anonimidad.	Conceptos básicos. K-anonimidad, l-diversidad y t-proximidad.
Aplicaciones en privacidad y anonimidad.	Privacidad de la geolocalización. Comunicaciones anónimas. Encaminamiento en cebolla. Mixes. Autenticación anónima. Privacidad en aprendizaje máquina.

Planificación			
	Horas en clase	Horas fuera de clase	Horas totales
Prácticas de laboratorio	19	38	57
Lección magistral	19	38	57
Resolución de problemas	2	0	2
Examen de preguntas objetivas	2	0	2
Informe de prácticas, prácticum y prácticas externas	0	3	3

Informe de prácticas, prácticum y prácticas externas	0	4	4

*Los datos que aparecen en la tabla de planificación son de carácter orientativo, considerando la heterogeneidad de alumnado

Metodologías

	Descripción
Prácticas de laboratorio	Los estudiantes desarrollarán en el laboratorio prácticas de privacidad y anonimidad como aplicaciones de las técnicas presentadas en las lecciones magistrales. Las prácticas o proyectos serán supervisadas por los profesores.
Lección magistral	Exposición sistemática de los contenidos del curso: conceptos, resultados, algoritmos, ejemplos y casos de uso.
Resolución de problemas	Resolución de problemas en el aula por parte de los docentes.

Atención personalizada

Metodologías	Descripción
Prácticas de laboratorio	Se responderán individualmente las cuestiones relativas a las prácticas de laboratorio y al desarrollo del proyecto. El horario de tutorías se establecerá al principio del curso y se publicará en la página web de la asignatura.
Lección magistral	Se dispensará atención individual a los estudiantes que precisen orientación para el estudio, explicación adicional sobre los contenidos de la disciplina, aclaración o guía sobre la resolución de problemas. El horario de tutorías se establecerá al principio del curso y se publicará en la página web de la asignatura.
Resolución de problemas	Se atenderán individualmente las consultas sobre la resolución de problemas y ejercicios planteados en las clases o trabajados de forma autónoma. El horario de tutorías se establecerá al principio del curso y se publicará en la página web de la asignatura.

Evaluación

	Descripción	Calificación	Resultados de Formación y Aprendizaje
Examen de preguntas objetivas	Examen escrito. Resolución de cuestiones, problemas o ejercicios.	40	
Informe de prácticas, prácticum y prácticas externas	Informes sobre las prácticas correspondientes a la primera parte del curso realizadas individualmente o por parejas.	30	
Informe de prácticas, prácticum y prácticas externas	Informes sobre las prácticas correspondientes a la segunda parte del curso realizadas individualmente o por parejas.	30	

Otros comentarios sobre la Evaluación

Es necesario alcanzar un mínimo de 4.00 en el examen escrito para poder aprobar la asignatura.

En los informes de prácticas, será necesario indicar si se emplearon herramientas de IA generativa y, de ser así, hacer constar explícitamente qué elementos del informe fueron producidos con ellas. En caso de detección de plagio o de uso no justificado de dichas herramientas, los profesores podrán calificar el entregable con 0 puntos.

La calificación de las pruebas solo tendrá efecto en el curso académico en que se obtengan.

Fuentes de información

Bibliografía Básica

C. Dwork, **The Algorithmic Foundations of Differential Privacy**, Now Publishers Inc., 2013

J. Morris Chang, Di Zhuang, and G. Dumindu Samaraweer, **Privacy-preserving Machine Learning**, Manning Publications, 2023

Mark Craddock, Ed., **UN Handbook on Privacy-Preserving Computation Techniques**, GCATI, 2020

Bibliografía Complementaria

Katharine Jarmul, **Practical Data Privacy**, O'Reily Media, 2023

Nishant Bhajaria, **Data Privacy**, Manning Publications, 2022

PALISADE, **PALISADE HOMOMORPHIC ENCRYPTION SOFTWARE LIBRARY**,

Ilaria Chillotti, **TFHE Deep Dive**, https://www.zama.ai/post/tfhe-deep-dive-part-1,

Daniele Micciancio, and Oded Regev, **Lattice-based cryptography**, https://cseweb.ucsd.edu/%7Edaniele/papers/PostQuantum.pdf, Springer, 2009

Recomendaciones