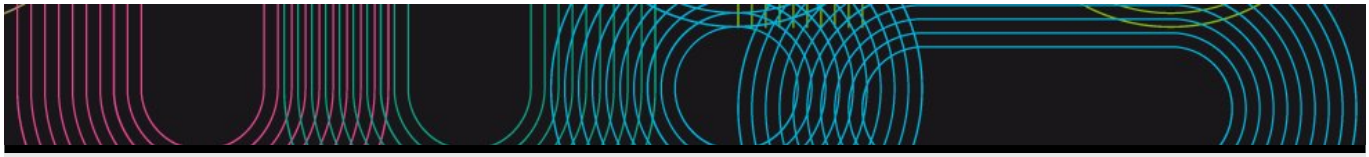

DATOS IDENTIFICATIVOS				
Privacidade e anonimidade				
Materia	Privacidade e anonimidade			
Código	V05M175V11110			
Titulación	Máster Universitario en Ciberseguridade			
Descritores	Creditos ECTS	Sinale	Curso	Cuadrimestre
	5	OB	1	1c
Lingua de impartición	#EnglishFriendly Castelán			
Departamento	Dpto. Externo Teoría do sinal e comunicacións			
Coordinador/a	Pérez González, Fernando			
Profesorado	Hernández Pereira, Elena María Pérez González, Fernando			
Correo-e	fperez@gts.uvigo.es			
Web	http://http://moovi.gal			
Descrición xeral	Nesta materia preséntanse as principais técnicas para proporcionar privacidade e anonimidade en redes, sistemas e aplicacións. Estúdanse conceptos e métodos de privacidade diferencial, técnicas de mellora da privacidade (PET), privacidade na xeolocalización, privacidade para aprendizaxe máquina e técnicas de anonimidade. Tamén se exploran as implicacións da privacidade desde o deseño e aspectos éticos e legais da privacidade.			

Resultados de Formación e Aprendizaxe
Código

Resultados previstos na materia	
Resultados previstos na materia	Resultados de Formación e Aprendizaxe

Contidos	
Tema	
Introdución. Ataques.	Introdución á privacidade e a anonimidade. Ataques de inferencia. Ataques de análises de tráfico. Rastrexo online.
Privacidad diferencial.	Privacidade diferencial. Mecanismos para a privacidade diferencial. Teoremas de composición.
Técnicas de mantemento e mellora da privacidade.	Primitivas con mantemento da privacidade: recuperación de información, intersección de conxuntos. Técnicas de mellora da privacidade con cifrado homomórfico e computación multipartita segura. Filtros de Bloom.
Anonimidade.	Conceptos básicos. K-anonimidade, l-diversidade e t-proximidade.
Aplicacións en privacidade e anonimidade.	Privacidade da xeolocalización. Comunicacións anónimas. Encamiñamento en cebola. Mixes. Autenticación anónima. Privacidade en aprendizaxe máquina.

Planificación			
	Horas na aula	Horas fóra da aula	Horas totais
Prácticas de laboratorio	19	38	57
Lección maxistral	19	38	57
Resolución de problemas	2	0	2
Exame de preguntas obxectivas	2	0	2
Informe de prácticas, prácticum e prácticas externas	0	3	3
Informe de prácticas, prácticum e prácticas externas	0	4	4

*Os datos que aparecen na táboa de planificación son de carácter orientador, considerando a heteroxeneidade do alumnado.

Metodoloxía docente	
	Descrición
Prácticas de laboratorio	Os estudantes desenvolverán no laboratorio prácticas de privacidade e anonimidade como aplicacións das técnicas presentadas nas leccións maxistrais. As prácticas ou proxectos serán supervisadas polos profesores.
Lección maxistral	Exposición sistemática dos contidos do curso: conceptos, resultados, algoritmos, exemplos e casos de uso.
Resolución de problemas	Resolución de problemas na aula por parte dos docentes.

Atención personalizada	
Metodoloxías	**Descrición**
Prácticas de laboratorio	Responderanse individualmente as cuestións relativas ás prácticas de laboratorio e ao desenvolvemento do proxecto. O horario de tutorías establecerase ao principio do curso e publicarase na páxina web da materia.
Lección maxistral	Dispensarase atención individual aos estudantes que precisen orientación para o estudo, explicación adicional sobre os contidos da disciplina, aclaración ou guía sobre a resolución de problemas. O horario de tutorías establecerase ao principio do curso e publicarase na páxina web da materia.
Resolución de problemas	Atenderanse individualmente as consultas sobre a resolución de problemas e exercicios expostos nas clases ou traballados de forma autónoma. O horario de tutorías establecerase ao principio do curso e publicarase na páxina web da materia.

Avaliación			
	Descrición	Cualificación	Resultados de Formación e Aprendizaxe
Exame de preguntas obxectivas	Exame escrito. Resolución de cuestións, problemas ou exercicios.	40	
Informe de prácticas, prácticum e prácticas externas	Informes sobre as prácticas correspondentes á primeira parte do curso realizadas individualmente ou por parellas.	30	
Informe de prácticas, prácticum e prácticas externas	Informes sobre as prácticas correspondentes á segunda parte do curso realizadas individualmente ou por parellas.	30	

Outros comentarios sobre a Avaliación

É necesario acadar un mínimo de 4.00 no exame escrito para poder aprobar a asignatura.

Nos informes de prácticas, será necesario indicar se se empregaron ferramentas de IA xenerativa e, de ser o caso, facer constar explícitamente qué elementos no informe foron producidos con elas. En caso de detección de plaxio ou de uso non xustificado das devantitas ferramentas, os profesores poderán cualificar o entregable con 0 puntos.

A cualificación das probas só fornece efecto no curso académico en que se obteñan.

Bibliografía. Fontes 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

Recomendacións