Guía Docente					
Datos Identificativos				2024/25	
Asignatura (*)	Ciberseguridade Intelixente		Código	614544024	
Titulación	Máster Universitario en Intelixencia Artificial				
Descriptores					
Ciclo	Período	Curso	Tipo	Créditos	
Mestrado Oficial	1º cuadrimestre	Segundo	Optativa	3	
Idioma	Inglés				
Modalidade docente	Híbrida				
Prerrequisitos					
Departamento	Ciencias da Computación e Tecnoloxías da Información				
Coordinación	Garabato Míguez, Daniel	Correo electrónico	daniel.garabato@udc.es		
Profesorado	Garabato Míguez, Daniel	Correo electrónico	daniel.garabato@udc.es		
Web	udconline.udc.gal				
Descrición xeral	A materia introduce ao estudante no desenvolvemento de estratexias baseadas en Intelixencia Artificial para a defensa de sistemas informáticos e redes de comunicacións fronte a ataques maliciosos que pretenden o seu control ou acceso á información residente ou circulante neles. Capacitaráselle na prevención, detección, análise e eliminación de ameazas nun contexto de continua evolución. Revisaranse casos de uso tipo da Intelixencia Artificial en escenarios de ciberseguridade.				

Competencias / Resultados do título	
Código	Competencias / Resultados do título
A9	CE08 - capacidade para deseñar e desenvolver sistemas intelixentes seguros, en términos de integridade, confidencialidade e robustez
A20	CE19 - coñecemento de diferentes ámbitos de aplicación das tecnologías basadas en IA e a súa capacidade para ofrecer un valor engadido diferenciador
A21	CE20 - capacidade de combinar e adaptar diferentes técnicas, extrapolando coñecementos entre diferentes ámbitos de aplicación
A22	CE21 - coñecemento das técnicas que facilitan a organización e xestión de proxectos en IA en entornos reais, a xestión dos recursos e a planificación de tarefas dun xeito eficiente, tendo en conta conceptos de diseminación do coñecemento e ciencia aberta
A23	CE22 - coñecemento de técnicas que facilitan a seguridade dos datos, aplicacións e as comunicacións e as súas implicacións en diferentes ámbitos de aplicación da IA
A31	CE30 - Ser capaz de plantexar, modelar e resolver problemas que requiran a aplicación de métodos, técnicas e tecnoloxías de intelixencia artificial
B1	CG01 - Manter e extender os plantexamentos teóricos fundados para permitir a introducción e explotación de tecnoloxías novas e avanzadas no eido da Intelixencia Artificial
B2	CG02 - Abordar con éxito todas as etapas dun proxecto de Intelixencia Artificial
B4	CG04 - Elaborar axeitadamente e con certa orixinalidade composicións escritas ou argumentos motivados, redactar plans, proxectos de traballo, artigos científicos e formular hipóteses razoables no campo
B5	CG05 - Traballar en equipo, especialmente de carácter multidisciplinar, e ser hábiles na xestión do tempo, persoas e toma de decisións
B6	CB01 - Poseer e comprender coñecementos que aporten unha base ou oportunidade de ser orixináis no desenvolvemento e/ou aplicación de ideas, a miúdo nun contexto de investigación
B7	CB02 - Que os estudantes saiban aplicar os coñecementos adquiridos e posúan capacidade de resolución de problemas en entornos novos ou pouco coñecidos dentro de contextos máis amplos (ou multidisciplinares) relacioados coa su área de estudo
B9	CB04 - Que os estudantes saiban comunicar as súas conclusións e os coñecementos e razóns últimas que as sustentan a públicos especializados e non especializados dun xeito claro e sen ambigu?idades
B10	CB05 - Que os estudantes posúan as habilidades de aprendizaxe que lles permitan continuar estudando dun xeito que terá que ser en gran medida autodirixido ou autónomo
C5	CT05 - Entender a importancia da cultura emprendedora e coñecer os medios ao alcance das persoas emprendedoras
C8	CT08 - Valorar a importancia que ten a investigación, a innovación e o desenrolo tecnolóxico no avance socioeconómico e cultural da sociedade

C9	CT09 - Ter a capacidade de xestionar tempos e recursos: desenvolver plans, priorizar actividades, identificar as críticas, establecer plazos e cumplilos

Resultados da aprendizaxe			
Resultados de aprendizaxe	Competencias / Resultados do título		
Coñecer técnicas e ferramentas para implementar solucións baseadas en IA que permitan a detección automatizada de vulnerabilidades, ataques, contidos e aplicacións fraudulentas	AM8 AM19 AM20 AM22 AM30	BM1 BM6 BM7 BM10	CM5 CM8
Coñecer, comprender e analizar casos reais de aplicación de técnicas de IA en diferentes ámbitos da ciberseguridade	AM8 AM19 AM20 AM21 AM22 AM30	BM2 BM4 BM5 BM6 BM7 BM9 BM10	CM5 CM8 CM9
Coñecer técnicas que faciliten a seguridade por deseño e que permitan unha administración segura de sistemas e redes de comunicacións, permitan a xestión de riscos e posibiliten unha recuperación rápida ante eventos de ciberseguridade	AM8 AM20 AM21 AM22 AM30	BM1 BM2 BM4 BM5 BM7 BM9	CM8 CM9
Comprender a importancia do concepto de identidade e coñecer técnicas que permitan garantir o acceso aos datos e a súa privacidade	AM8 AM21 AM22 AM30	BM1 BM2 BM6 BM7 BM9 BM10	CM8

Contidos	
Temas	Subtemas
Teoría	- Conceptos e introdución á ciberseguridade. - Modelos de detección de ameazas e prevención de ataques. - Detección de contidos e aplicacións fraudulentos. - Minería de datos en sistemas de xestión de eventos. - Control de identidade, biometrías e patróns de comportamento. - Detección de anomalías e agrupamento para a detección de ataques en comunicacións. - Xestión de riscos en IA, riscos críticos e perfís de normalidade, usos maliciosos e plans de continxencia e recuperación.
Práctica	- Uso de ferramentas propias de contornas de ciberseguridade - Aplicación de técnicas de IA para a resolución de problemáticas propias de ciberseguridade

Planificación				
Metodoloxías / probas	Competencias / Resultados	Horas lectivas (presenciais e virtuais)	Horas traballo autónomo	Horas totais

Sesión maxistral	A5 A9 A20 A21 A22 A23 B1 B2 B6 B10 C5 C8	10	10	20
Prácticas de laboratorio	A9 A20 A21 A22 A23 A31 B1 B2 B4 B5 B6 B7 B9 C9	5	15	20
Traballos tutelados	A9 A20 A21 A22 A23 A31 B1 B2 B4 B5 B6 B7 B9 C9	5	28	33
Proba obxectiva	A9 A20 A21 A22 A23 A31 B1 B2 B4 B6 B7 B9 B10	1	0	1
Atención personalizada		1	0	1
***Os datos que aparecen na táboa de planificación son de carácter orientativo, considerando a heteroxeneidade do alumnado**				

Metodoloxías	
Metodoloxías	**Descrición**
Sesión maxistral	Exposición oral complementada co uso de medios audiovisuais e a introdución dalgunhas preguntas dirixidas ao alumnado, coa finalidade de transmitir coñecementos e facilitar a aprendizaxe. Ademais do tempo de exposición oral por parte do profesor, esta actividade formativa require do alumnado a dedicación dun tempo para preparar e revisar por conta propia os materiais obxecto da clase.
Prácticas de laboratorio	Clases dedicadas a que o alumnado desenvolva traballos prácticos que impliquen abordar a resolución de problemas complexos, e a análise e deseño de solucións que constitúan un medio para a súa resolución. Esta actividade pode requirir do alumnado a presentación oral dos traballos realizados. Os traballos realizados polo alumnado poden realizarse, segundo o caso, de forma individual ou en grupos de traballo.
Traballos tutelados	Trátase de sesións nas que o obxectivo é que o alumnado adquira determinadas competencias en base á resolución de exercicios, estudo de casos e realización de proxectos que requiran da aplicación dos coñecementos e competencias desenvolvidas durante a materia. Estas sesións poden requirir do alumnado a presentación oral da súa solución aos problemas formulados. Os traballos realizados polo alumnado poden realizarse, segundo o caso, de forma individual ou en grupos de traballo.
Proba obxectiva	Exame no que se poderán avaliar tanto os aspectos teóricos como prácticos vistos ao longo do curso.

Atención personalizada	
Metodoloxías	**Descrición**
Sesión maxistral Prácticas de laboratorio Traballos tutelados	Levarase a cabo un seguimento das prácticas a desenvolver durante as horas reservadas no horario (sesións de laboratorio). Adicionalmente, para abordar aqueles problemas de especial dificultade, tamén se poderán empregar as franxas horarias dispoñibles para a atención do alumnado.

Avaliación			
Metodoloxías	**Competencias / Resultados**	**Descrición**	**Cualificación**
Prácticas de laboratorio	A9 A20 A21 A22 A23 A31 B1 B2 B4 B5 B6 B7 B9 C9	Avaliación das prácticas de laboratorio propostas mediante a entrega de memoria e/ou do código desenvolvido. A entrega destas prácticas é obrigatoria. Terán unha data de entrega e, opcionalmente, de defensa.	40

Proba obxectiva	A9 A20 A21 A22 A23 A31 B1 B2 B4 B6 B7 B9 B10	Proba escrita onde se avaliarán os contidos e competencias revisados nas sesións maxistrais e os aspectos teóricos da súa posta en práctica levada a cabo na sesión prácticas. O tipo de proba consistirá nun conxunto de preguntas tipo test ou cuestións de resposta curta sobre conceptos concretos. Realizarase na data oficial prevista no calendario da titulación.	25
Traballos tutelados	A9 A20 A21 A22 A23 A31 B1 B2 B4 B5 B6 B7 B9 C9	Avaliación da memoria do traballo (ou traballos) de investigación tutelado, de carácter teórico-práctico, asignado a cada alumno. Avaliarase a capacidade de síntese e a completitude e adecuada presentación das ideas e conceptos relativos ao tema escollido. A entrega destes traballos é obrigatoria. Terán unha data de entrega e, opcionalmente, de defensa.	35

Observacións avaliación
Para superar (e liberar) tanto os traballos prácticos coma os traballos tutelados requírese acadar un 40% da puntuación máxima prevista para estes elementos de avaliación. Non hai mínimo esixido para a proba obxectiva. Para superar a materia é preciso acadar os mínimos anteriores (nos traballos prácticos e tutelados) e sumar na nota final ponderada un mínimo de 5 puntos sobre 10. No caso de non obter o mínimo esixido para superar algunha das partes (traballos prácticos e /ou tutelados), o alumnado terá unha segunda oportunidade na que so entregará os elementos non superados. No caso de superar parte dos elementos avaliados, pero non acadar o mínimo preciso para aprobar a materia completa, a cualificación a incluír nas respectivas actas calcularase como o mínimo entre a media ponderada das partes superadas e 4.9. Terá a condición de "Presentado" quen entregue todas as prácticas e traballos obrigatorios ou se presente á proba obxectiva no período oficial de avaliación. As entregas das prácticas e traballos deben realizarse dentro do prazo establecido, e seguirán as especificacións indicadas no enunciado tanto para a presentación como para a defensa. Os profesores facilitarán, na medida do posible e dentro dos horarios establecidos para a materia, a asistencia aos grupos de teoría e prácticas que mellor se axusten ás necesidades dos alumnos que teñen a matrícula a tempo parcial, para os que tamén aplica a forma de avaliación aquí establecida. Os alumnos con dispensa académica de exención de asistencia deberán asistir a todas as probas de avaliación. Todos os aspectos relacionados con dispensa académica, dedicación ao estudo, permanencia, fraude académica e igualdade rexeranse de acordo coa normativa académica vixente da UDC. A docencia impartirase en inglés. A docencia expositiva será impartida pola UVigo e retransmitida para todo o alumnado. Haberá un grupo de docencia interactiva específico e presencial en cada universidade (USC-UDC-UVigo).

Fontes de información	
Bibliografía básica	- William Stallings (2018). Effective Cybersecurity: A Guide to Using Best Practices and Standards. Addison-Wesley Professional - Clarence Chio, David Freeman (2018). Machine Learning and Security: Protecting Systems with Data and Algorithms. O'Reilly - Chiheb Chebbi (2018). Mastering Machine Learning for Penetration Testing: Develop an extensive skill set to break self-learning systems using Python. Packt Publisinhg
Bibliografía complementaria	- Alessandro Parisi (2019). Hands-On Artificial Intelligence for Cybersecurity: Implement smart AI systems for preventing cyber attacks and detecting threats and network anomalies. Packt Publishing

Recomendacións
Materias que se recomenda ter cursado previamente
Aprendizaxe Automática I/614544012 Aprendizaxe Profunda/614544013 Aprendizaxe Automática II/614544014 Coñecemento e Razoamento con Incerteza/614544007
Materias que se recomenda cursar simultaneamente
Materias que continúan o temario
Observacións
Recomendase ao alumnado, para un aproveitamento óptimo da materia, un seguimento activo das clases así como participar nas distintas actividades e o uso da atención personalizada para a resolución das dúbidas ou cuestións que lle podan xurdir.

(*)A Guía docente é o documento onde se visualiza a proposta académica da UDC. Este documento é público e non se pode modificar, salvo casos excepcionais baixo a revisión do órgano competente dacordo coa normativa vixente que establece o proceso de elaboración de guías