



Guía docente				
Datos Identificativos				2023/24
Asignatura (*)	Ciberseguridad Inteligente	Código	614544024	
Titulación	Máster Universitario en Intelixencia Artificial			
Descriptorios				
Ciclo	Periodo	Curso	Tipo	Créditos
Máster Oficial	1º cuatrimestre	Segundo	Optativa	3
Idioma	Inglés			
Modalidad docente	Híbrida			
Prerrequisitos				
Departamento	Ciencias da Computación e Tecnoloxías da Información			
Coordinador/a	Garabato Míguez, Daniel	Correo electrónico	daniel.garabato@udc.es	
Profesorado	Garabato Míguez, Daniel	Correo electrónico	daniel.garabato@udc.es	
Web				
Descripción general	La asignatura introduce al estudiante en el desarrollo de estrategias basadas en Inteligencia Artificial para la defensa de sistemas informáticos y redes de comunicaciones frente a ataques maliciosos que pretenden su control o el acceso a la información residente o circulante en ellos. Se le capacitará en la prevención, detección, análisis y eliminación de amenazas en un contexto en continua evolución. Se revisarán casos de uso tipo de la Inteligencia artificial en escenarios de ciberseguridad.			

Competencias del título	
Código	Competencias del título
A5	CE04 - Conocer los fundamentos y técnicas básicas de la inteligencia artificial y su aplicación práctica
A9	CE08 - Capacidad para diseñar y desarrollar sistemas inteligentes seguros, en términos de integridad, confidencialidad y robustez
A20	CE19 - Conocimiento de diferentes ámbitos de aplicación de las tecnologías basadas en IA y su capacidad para ofrecer un valor añadido diferenciador
A21	CE20 - Capacidad de combinar y adaptar diferentes técnicas, extrapolando conocimientos entre diferentes ámbitos de aplicación
A22	CE21 - Conocimiento de las técnicas que facilitan la organización y gestión de proyectos en IA en entornos reales, la gestión de los recursos y la planificación de tareas de una manera eficiente, teniendo en cuenta conceptos de diseminación del conocimiento y ciencia abierta
A23	CE22 - Conocimiento de técnicas que facilitan la seguridad de los datos, aplicaciones y las comunicaciones y sus implicaciones en diferentes ámbitos de aplicación de la IA
A31	CE30 - Ser capaz de plantear, modelar y resolver problemas que requieran la aplicación de métodos, técnicas y tecnologías de inteligencia artificial
B1	CG01 - Mantener y extender planteamientos teóricos fundados para permitir la introducción y explotación de tecnologías nuevas y avanzadas en el campo de la Inteligencia Artificial
B2	CG02 - Abordar con éxito todas las etapas de un proyecto de Inteligencia Artificial
B4	CG04 - Elaborar adecuadamente y con cierta originalidad composiciones escritas o argumentos motivados, redactar planes, proyectos de trabajo, artículos científicos y formular hipótesis razonables en el campo
B5	CG05 - Trabajar en equipo, especialmente de carácter multidisciplinar, y ser hábiles en la gestión del tiempo, personas y toma de decisiones
B6	CB01 - 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
B7	CB02 - 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
B9	CB04 - 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
B10	CB05 - 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
C5	CT05 - Entender la importancia de la cultura emprendedora y conocer los medios al alcance de las personas emprendedoras



C8	CT08 - Valorar la importancia que tiene la investigación, la innovación y el desarrollo tecnológico en el avance socioeconómico y cultural de la sociedad
C9	CT09 - Tener la capacidad de gestionar tiempos y recursos: desarrollar planes, priorizar actividades, identificar las críticas, establecer plazos y cumplirlos

Resultados de aprendizaje			
Resultados de aprendizaje	Competencias del título		
Conocer técnicas y herramientas para implementar soluciones basadas en IA que permitan la detección automatizada de vulnerabilidades, ataques, contenidos y aplicaciones fraudulentas	AM4 AM8 AM19 AM20 AM22 AM30	BM1 BM6 BM7 BM10	CM5 CM8
Conocer, comprender y analizar casos reales de aplicación de técnicas de IA en diferentes ámbitos de la ciberseguridad	AM4 AM8 AM19 AM20 AM21 AM22 AM30	BM2 BM4 BM5 BM6 BM7 BM9 BM10	CM5 CM8 CM9
Conocer técnicas que faciliten la seguridad por diseño y que permitan una administración segura de sistemas y redes de comunicaciones, permitan la gestión de riesgos y posibiliten una recuperación rápida ante eventos de ciberseguridad	AM8 AM20 AM21 AM22 AM30	BM1 BM2 BM4 BM5 BM7 BM9	CM8 CM9
Comprender la importancia del concepto de identidad y conocer técnicas que permitan garantizar el acceso a los datos y su privacidad	AM4 AM8 AM21 AM22 AM30	BM1 BM2 BM6 BM7 BM9 BM10	CM8

Contenidos	
Tema	Subtema
Teoría	<ul style="list-style-type: none"> - Conceptos e introducción a la ciberseguridad - Modelos de detección de amenazas y prevención de ataques - Detección de contenidos y aplicaciones fraudulentos - Minería de datos en sistemas de gestión de eventos - Control de identidad, biometrías y patrones de comportamiento - Detección de anomalías y agrupamiento para la detección de ataques en comunicaciones - Gestión de riesgos en IA, riesgos críticos y perfiles de normalidad, usos maliciosos y planes de contingencia y recuperación
Práctica	<ul style="list-style-type: none"> - Utilización de herramientas propias de entornos de ciberseguridad - Aplicación de técnicas de IA para resolver problemáticas propias de la ciberseguridad

Planificación



Metodoloxías / probas	Competencias	Horas presenciais	Horas no presenciais / traballo autónomo	Horas totais
Sesión magistral	A5 A9 A20 A21 A22 A23 B1 B2 B6 B10 C5 C8	10	10	20
Prácticas de laboratorio	A5 A9 A20 A21 A22 A23 A31 B1 B2 B4 B5 B6 B7 B9 C9	5.25	15.75	21
Solución de problemas	A5 A9 A20 A21 A22 A23 A31 B1 B2 B4 B5 B6 B7 B9 C9	5.25	15.75	21
Prueba objetiva	A5 A9 A20 A21 A22 A23 A31 B1 B2 B4 B6 B7 B9 B10	2	10	12
Atención personalizada		1	0	1

(*Los datos que aparecen en la tabla de planificación són de carácter orientativo, considerando la heterogeneidad de los alumnos

Metodoloxías	
Metodoloxías	Descrición
Sesión magistral	Exposición oral complementada con el uso de medios audiovisuales y la introducción de algunas preguntas dirigidas al alumnado, con la finalidade de transmitir coñecimientos y facilitar el aprendizaxe. Ademais do tempo de exposición oral por parte do profesor, esta actividade formativa require que o alumnado dedique un certo tempo a preparar e revisar por su conta os materiais vistos en clase.
Prácticas de laboratorio	Clases dedicadas a que o alumnado desenvolva traballos prácticos que impliquen abordar a resolución de problemas complexos, así como o análise e deseño de solucións que constitúan un medio para a súa resolución. Esta actividade pode requirer que o alumnado realice unha presentación oral dos traballos realizados. Estes traballos podrán realizarse, según o caso, ben de forma individual ou en grupos de traballo.
Solución de problemas	Se trata de sesións en las que o obxectivo é que o alumnado adquira determinadas competencias en base a la resolución de exercicios, estudo de casos y realización de proxectos que requiren de la aplicación de los coñecimientos y competencias desarrolladas durante la asignatura. Esta actividade pode requirer que o alumnado realice unha presentación oral dos traballos realizados. Estes traballos podrán realizarse, según o caso, ben de forma individual ou en grupos de traballo.
Prueba objetiva	Examen en el que se podrá evaluar tanto los aspectos teóricos como prácticos vistos durante el curso.

Atención personalizada	
Metodoloxías	Descrición
Sesión magistral Prácticas de laboratorio Solución de problemas	Se levará a cabo un seguimento de las prácticas a desenvolver durante las horas reservadas en el horario (sesións de laboratorio). Adicionalmente, para abordar aqueles problemas de especial dificultad, tamén se podrán utilizar las franjas horarias disponibles para la atención del alumnado.

Evaluación			
Metodoloxías	Competencias	Descrición	Calificación
Prácticas de laboratorio	A5 A9 A20 A21 A22 A23 A31 B1 B2 B4 B5 B6 B7 B9 C9	Evaluación de traballos prácticos (E2)	40
Prueba objetiva	A5 A9 A20 A21 A22 A23 A31 B1 B2 B4 B6 B7 B9 B10	Examen final (E1)	20



Solución de problemas	A5 A9 A20 A21 A22 A23 A31 B1 B2 B4 B5 B6 B7 B9 C9	Evaluación de trabajos tutelados (E3)	40
-----------------------	---	---------------------------------------	----

Observaciones evaluación

Para superar (y liberar) tanto los trabajos prácticos como los trabajos tutelados es necesario alcanzar un 40% de la puntuación máxima prevista para estos elementos de evaluación. No hay mínimo exigido para la prueba objetiva.

Para superar la asignatura es necesario alcanzar los mínimos anteriores (en los trabajos prácticos y tutelados) y sumar en la nota final ponderada un mínimo de 5 puntos sobre 10.

En caso de no alcanzar el mínimo exigido para superar alguna de las partes (trabajos prácticos y/o tutelados), el alumnado tendrá una segunda oportunidad en la que sólo entregará los elementos no superados.

En caso de superar parte de los elementos evaluados, pero no se alcanzase el mínimo necesario para aprobar la asignatura completa, la calificación a incluir en las respectivas actas se calculará como el mínimo entre la media ponderada de las partes superadas y 4.9.

Tendrá condición de "Presentado" quien entregue todas las prácticas y trabajos obligatorios o se presente a la prueba objetiva en el período oficial de evaluación.

Las entregas de prácticas y trabajos deben realizarse dentro del plazo establecido, y seguirán las especificaciones indicadas en el enunciado, tanto para la presentación como para la defensa.

Los profesores facilitarán, en la medida de lo posible y dentro de los horarios establecidos para la asignatura, la asistencia a los grupos de teoría y prácticas que mejor se ajusten a las necesidades de los alumnos que tienen la matrícula a tiempo parcial, para los que también aplica la forma de evaluación aquí establecida. Los alumnos con dispensa académica de exención de asistencia deberán asistir a todas las pruebas de evaluación.

La realización fraudulenta de pruebas o actividades de evaluación, una vez comprobada, implicará directamente la calificación de "suspenso" (nota numérica 0) en la convocatoria en la que se cometa, tanto si la comisión de la falta se produce en la primera oportunidad como en la segunda.

La asignatura se impartirá en inglés. La docencia expositiva será impartida por la UVigo y retransmitida para todo el alumnado. Habrá un grupo de docencia interactiva específico y presencial en cada universidad (USC-UDC-UVigo).

Fuentes de información

Básica	- William Stallings (2018). Effective Cybersecurity: A Guide to Using Best Practices and Standards. Addison-Wesley Professional
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

Recomendaciones

Asignaturas que se recomienda haber cursado previamente

Asignaturas que se recomienda cursar simultáneamente

Asignaturas que continúan el temario

Otros comentarios

Se recomienda al alumnado, para un aprovechamiento óptimo de la asignatura, un seguimiento activo de las clases así como participar en las distintas actividades y el uso de la atención personalizada para la resolución de las dudas o cuestiones que le puedan surgir. Según se recoge en las distintas normativas de aplicación para la docencia universitaria en materia de perspectiva de género, en esta materia se usará lenguaje no sexista, se propiciará la intervención en clase de alumnos y alumnas, etc. Asimismo, se trabajará para identificar y modificar prejuicios y actitudes sexistas, fomentando valores de respeto e igualdad. En general, se intentará detectar situaciones de discriminación, por ejemplo, por razón de género y se propondrán acciones y medidas para corregirlas.



(*) La Guía Docente es el documento donde se visualiza la propuesta académica de la UDC. Este documento es público y no se puede modificar, salvo cosas excepcionales bajo la revisión del órgano competente de acuerdo a la normativa vigente que establece el proceso de elaboración de guías