



DATOS IDENTIFICATIVOS

Ciberseguridad inteligente

Asignatura	Ciberseguridad inteligente			
Código	O06M193V01306			
Titulación	Máster universitario en Inteligencia artificial			
Descriptores	Creditos ECTS	Seleccione	Curso	Cuatrimestre
	3	OP	2	1c
Lengua Impartición	Inglés			
Departamento				
Coordinador/a	Ribadas Pena, Francisco José			
Profesorado	A0075-Ax2tc-2 A0075-Ax2tc-2, A0075-Ax2tc-2 Ribadas Pena, Francisco José			
Correo-e	ribadas@uvigo.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 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.			

Resultados de Formación y Aprendizaje

Código	Descripción
A1	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
A2	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
A4	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
A5	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.
B1	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	Abordar con éxito todas las etapas de un proyecto de Inteligencia Artificial
B4	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	Trabajar en equipo, especialmente de carácter multidisciplinar, y ser hábiles en la gestión del tiempo, personas y toma de decisiones.
C8	Capacidad para diseñar y desarrollar sistemas inteligentes seguros, en términos de integridad, confidencialidad y robustez.
C19	Conocimiento de diferentes ámbitos de aplicación de las tecnologías basadas en IA y su capacidad para ofrecer un valor añadido diferenciador.
C20	Capacidad de combinar y adaptar diferentes técnicas, extrapolando conocimientos entre diferentes ámbitos de aplicación
C21	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.
C22	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.
C30	Ser capaz de plantear, modelar y resolver problemas que requieran la aplicación de métodos, técnicas y tecnologías de inteligencia artificial

D5	Entender la importancia de la cultura emprendedora y conocer los medios al alcance de las personas emprendedoras.
D8	Valorar la importancia que tiene la investigación, la innovación y el desarrollo tecnológico en el avance socioeconómico y cultural de la sociedad
D9	Tener la capacidad de gestionar tiempos y recursos: desarrollar planes, priorizar actividades, identificar las críticas, establecer plazos y cumplirlos.

Resultados previstos en la materia

Resultados previstos en la materia	Resultados de Formación y Aprendizaje
RA1: Conocer técnicas y herramientas para implementar soluciones basadas en IA que permitan la detección automatizada de vulnerabilidades, ataques, contenidos y aplicaciones fraudulentas	A1 A2 B1 B2 C8 C19 C21 C22 D8 D9
RA2: Conocer, comprender y analizar casos reales de aplicación de técnicas de IA en diferentes ámbitos de la ciberseguridad	A2 A5 B2 B5 C8 C20 C22 C30 D5 D8
RA3: 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.	A1 A2 B1 B4 C21 C22 C30 D5
RA4: Comprender la importancia del concepto de identidad y conocer técnicas que permitan garantizar el acceso a los datos y su privacidad.	A2 A4 B4 B5 C8 C20 C22 D8

Contenidos

Tema
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.

Planificación

	Horas en clase	Horas fuera de clase	Horas totales

Lección magistral	10	10	20
Prácticas de laboratorio	5	15	20
Trabajo tutelado	5	29	34
Examen de preguntas objetivas	1	0	1

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

Metodologías

Metodologías	Descripción
Lección magistral	<p>Exposición de los contenidos teóricos de la materia.</p> <p>Con el fin de facilitar la comprensión de la misma y aumentar el interés del alumno, se incluirán diversos ejemplos y ejercicios en los que se puede requerir la participación activa del alumno.</p> <p>Se promoverá una actitud activa, fomentando la realización de preguntas y proponiendo cuestiones abiertas para la reflexión del alumno.</p>
Prácticas de laboratorio	<p>Realización de problemas de carácter práctico que incluyen el empleo de herramientas específicas y la programación de software relacionado con los contenidos de la materia.</p> <p>EVALUACION CONTINUA Caracter: Obligatorio Asistencia: No obligatoria</p> <p>EVALUACION GLOBAL Caracter: Obligatorio</p>
Trabajo tutelado	<p>Conjunto de uno o más trabajos teórico-prácticos individuales, entregables y evaluables, sobre los aspectos teóricos presentados en la materia y trabajados en las actividades prácticas desarrolladas por los alumnos.</p> <p>Se trata de una tarea autónoma que contará con la tutorización puntual del profesorado. El resultado se plasmará en una o más memorias con la estructura que se determine.</p> <p>EVALUACION CONTINUA Caracter: Obligatorio Asistencia: No obligatoria</p> <p>EVALUACION GLOBAL Caracter: Obligatorio</p>

Atención personalizada

Metodologías	Descripción
Prácticas de laboratorio	El profesor tutorizará al alumno en el laboratorio para la realización de los proyectos que se evaluarán al final de la materia, respondiendo dudas individualmente.
Trabajo tutelado	Seguimiento del trabajo de los alumnos, resolución de dudas generales y puesta en común de problemas específicos de carácter teórico/práctico relacionados con la materia.

Evaluación

	Descripción	Calificación	Resultados de Formación y Aprendizaje			
Prácticas de laboratorio	<p>Evaluación de las prácticas de laboratorio propuestas mediante la entrega de memoria y/o del código desarrollado.</p> <p>La entrega de estas prácticas es obligatoria. Tendrán una fecha de entrega y, opcionalmente, de defensa.</p> <p>- PUNTUACION MINIMA: 4 puntos sobre 10 - RESULTADOS APRENDIZAJE EVALUADOS: RA1, RA2, RA3, RA4</p>	40	A1 A2 A5	B1 B2 B5	C8 C19 C20 C21 C22 C30	D5 D8 D9

Trabajo tutelado	Evaluación de la memoria del trabajo (o trabajos) de investigación tutelado, de caracates teórico-práctico, asignado a cada alumno. Se evaluará la capacidad de síntesis y la completitud y adecuada presentación de las ideas y conceptos relativos al tema escogido. La entrega de estos trabajos es obligatoria. Tendrán una fecha de entrega y, opcionalmente, de defensa.	40	A1 A4	B4 B5	C19 C20 C22 C30	D8 D9
	- PUNTUACION MINIMA: 4 puntos sobre 10 - RESULTADOS APRENDIZAJE EVALUADOS: RA1, RA2, RA3, RA4					
Examen de preguntas objetivas	Prueba escrita donde se evaluarán los contenidos y competencias revisados en las sesiones magistrales y los aspectos teóricos de su puesta en práctica llevada a cabo en las sesión prácticas. El tipo de prueba consistirá en un conjunto de preguntas tipo test o cuestiones de respuesta corta sobre conceptos concretos. Se realizará en la fecha oficial prevista en el calendario de la titulación.	20	A5	B1	C8 C19 C20 C21 C22 C30	
	- PUNTUACION MINIMA: no hay mínimo exigido - RESULTADOS APRENDIZAJE EVALUADOS: RA1, RA2, RA3, RA4					

Otros comentarios sobre la Evaluación

(1) SISTEMA DE EVALUACIÓN CONTÍNUA

PRUEBA 1: Prácticas de laboratorio

Descripción: Evaluación de la memoria de las prácticas de laboratorio entregadas en las fechas estipuladas.

Metodología(s): Prácticas de laboratorio

% Calificación: 40%

% Mínimo: 4 puntos sobre 10

Competencias evaluadas: A1,A2,A5,B1,B2,B5,C8,C19,C20,C21,C22,C30,D5,D8,D9

Resultados aprendizaje evaluados: RA1, RA2, RA3, RA4

PRUEBA 2: Trabajo tutelado

Descripción: Evaluación de la memoria del trabajo(s) entregados en las fechas estipuladas y de su presentación en clase.

Metodología(s): Trabajo tutelado

% Calificación: 40%

% Mínimo: 4 puntos sobre 10

Competencias evaluadas: A1,A4,B4,B5,C19,C20,C22,C30,D8,D9

Resultados aprendizaje evaluados: RA1, RA2, RA3, RA4

PRUEBA 3: Examen final

Descripción: Examen tipo test o de conceptos sobre los contenidos teóricos de la materia

Metodología(s): Examen de preguntas objetivas

% Calificación: 20%

% Mínimo: no hay mínimo

Competencias evaluadas: A5,B1,C8,C19,C20,C21,C22,C30

Resultados aprendizaje evaluados: RA1, RA2, RA3, RA4

ACLARACIONES ADICIONALES

- Para superar la materia es preciso alcanzar los mínimos indicados en las pruebas anteriores y sumar en la nota final ponderada un mínimo de 5 puntos sobre 10.
- En el caso de constatar un comportamiento no ético (copia, plagio) en alguna de las entregas realizadas (total o parcial), se anulará la totalidad de la contribución del correspondiente elemento de evaluación sobre la calificación final

(2) SISTEMA DE EVALUACIÓN GLOBAL

Procedimiento para la elección de la modalidad de evaluación global:

- Se asume por defecto la modalidad de *evaluación continua*.
- Los alumnos que opten por la *evaluación global* deberán comunicarlo via Moovi mediante los mecanismos que se habiliten y en el plazo estipulado, una vez superado el plazo de un mes desde el comienzo del cuatrimestre

PRUEBA 1: *Prácticas de laboratorio*

Descripción: Evaluación de la memoria de las prácticas de laboratorio entregadas en las fechas estipuladas.

Metodología(s): Prácticas de laboratorio

% Calificación: 40%

% Mínimo: 5 puntos sobre 10

Competencias evaluadas: A1,A2,A5,B1,B2,B5,C8,C19,C20,C21,C22,C30,D5,D8,D9

Resultados aprendizaje evaluados: RA1, RA2, RA3, RA4

PRUEBA 2: *Trabajo tutelado*

Descripción: Evaluación de la memoria del trabajo(s) entregados en las fechas estipuladas y de su presentación en clase.

Metodología(s): Trabajo tutelado

% Calificación: 40%

% Mínimo: 5 puntos sobre 10

Competencias evaluadas: A1,A4,B4,B5,C19,C20,C22,C30,D8,D9

Resultados aprendizaje evaluados: RA1, RA2, RA3, RA4

PRUEBA 3: *Examen final*

Descripción: Examen tipo test o de conceptos sobre los contenidos teóricos de la materia

Metodología(s): Examen de preguntas objetivas

% Calificación: 20%

% Mínimo: 5 puntos sobre 10

Competencias evaluadas: A5,B1,C8,C19,C20,C21,C22,C30

Resultados aprendizaje evaluados: RA1, RA2, RA3, RA4

ACLARACIONES ADICIONALES

- Para superar la materia es preciso alcanzar los mínimos indicados en las pruebas anteriores y sumar en la nota final ponderada un mínimo de 5 puntos sobre 10.
- En el caso de constatar un comportamiento no ético (copia, plagio) en alguna de las entregas realizadas (total o parcial), se anulará la totalidad de la contribución del correspondiente elemento de evaluación sobre la calificación final

(3) CRITERIOS DE EVALUACIÓN PARA CONVOCATORIA EXTRAORDINARIA Y FIN DE CARRERA

Se emplearán los sistemas de evaluación continua y global expuestos anteriormente.

En estas convocatorias, los alumnos sólo deberán realizar las pruebas en las cuales no hubieran obtenido la calificación mínima indicada.

(4) PROCESO DE CALIFICACIÓN DE ACTAS

En el caso de los alumnos que superen parte de los elementos evaluados, pero no alcancen el mínimo preciso para aprobar la materia completa, la calificación a incluir en las respectivas actas se calculará como el mínimo entre el promedio ponderado de las partes superadas y 4,9.

(5) FECHAS DE EVALUACIÓN

El calendario de pruebas de evaluación aprobado oficialmente por la Junta de Centro de la ESEI se encuentra publicado en la página web <http://www.esei.uvigo.es>

(6) EMPLEO DE DISPOSITIVOS MOVILES

Se recuerda a todo el alumnado la prohibición del uso de dispositivos móviles en ejercicios y prácticas, en cumplimiento del artículo 13.2.d) del Estatuto del Estudiante Universitario, relativo a los deberes del estudiantado universitario, que establece el deber de "Abstenerse de la utilización o cooperación en procedimientos fraudulentos en las pruebas de evaluación, en los trabajos que se realicen o en documentos oficiales de la universidad."

(7) CONSULTA/SOLICITUD DE TUTORÍAS

Las tutorías pueden consultarse a través de la página personal del profesorado, accesible a través de <https://esei.uvigo.es/docencia/profesorado/>

Fuentes de información

Bibliografía Básica

William Stallings, **Effective Cybersecurity: A Guide to Using Best Practices and Standards.**, 978-0134772806, 1, Addison-Wesley Professional, 2018

Bibliografía Complementaria

Alessandro Parisi, **Hands-On Artificial Intelligence for Cybersecurity: Implement smart AI systems for preventing cyber attacks and detecting threats and network anomalies.**, 978-1789804027, 1, Packt Publishing, 2019

Recomendaciones

Asignaturas que se recomienda haber cursado previamente

Aprendizaje automático I/O06M193V01105

Aprendizaje Automático II/O06M193V01207

Aprendizaje profundo/O06M193V01206

Conocimiento y razonamiento con incertidumbre/O06M193V01203

Otros comentarios

Materia coordinada por la Universidad de Vigo