Escola Aberta
de Formación Permanente
Universidade Vigo

FICHA MATERIA MÁSTER PROPIO

O nome da materia debe indicarse en galego, castelán e inglés mentres que o resto dos apartados deberanse cubrir no idioma en que se impartirá o título propio

NOME MATERIA (Galego): Traballo Fin de Máster		
NOME MATERIA (Castelán): Trabajo Fin de Máster		
NOME MATERIA (Inglés): Master's Thesis		
Módulo/Especialidade:		
Tipo: ☒Obrigatoria ☐Optativa		
ECTS TOTALES: 15	ECTS TEORICOS:	ECTS PRÁCTICOS: 15
Semestre/Cuadrimestre:Segundo		
Modalidade: Mixta		
COMPETENCIAS ASOCIADAS: CG2, CG5, CE2, CE3, CE8, CE10 Indicar códigos da táboa 2.3 da proposta		
Descrición general: El **Trabajo Fin de Máster (TFM)** constituye la culminación del programa y tiene como objetivo que el estudiante demuestre la integración y aplicación de los conocimientos adquiridos en el ámbito de la **ciberinteligencia, las ciberoperaciones y la seguridad en sectores estratégicos para la defensa nacional**. El TFM deberá abordar una problemática relevante en el campo de la **ciberdefensa, la ciberseguridad en infraestructuras críticas, la inteligencia operativa en el ciberespacio o la aplicación de inteligencia artificial en ciberoperaciones en sectores estratégicos para la Defensa Nacional**. El TFM será supervisado por un profesor del máster, opcionalmente cotutorizado por un experto externo, y culminará con una **defensa ante un tribunal académico.**		
Coordinador/a: José Carlos López Ardao Equipo docente: Todo el profesorado del Máster		

Resultados de aprendizaje:
Al finalizar la materia, el estudiante será capaz de:

1. **Aplicar los principios de ciberinteligencia y ciberoperaciones en un caso práctico o investigación aplicada**, alineado con las necesidades de la defensa nacional.
2. **Identificar y analizar amenazas cibernéticas en sectores estratégicos**, empleando metodologías de inteligencia estructurada y técnicas avanzadas de análisis de amenazas.
3. **Evaluar la viabilidad y efectividad de estrategias de ciberseguridad y ciberdefensa en infraestructuras críticas**, considerando marcos doctrinales y normativos (OTAN, UE, ENS, Ley PIC).
4. **Realizar una revisión del estado del arte y del marco doctrinal de la ciberinteligencia y las ciberoperaciones en sectores estratégicos para la seguridad nacional**, contrastando teorías, normativas y mejores prácticas.
5. **Integrar inteligencia artificial y automatización en el análisis de amenazas**, explorando su impacto en la detección, prevención y respuesta a ciberataques en entornos militares, gubernamentales o estratégicos para la seguridad nacional.
6. **Generar productos de inteligencia aplicados a la seguridad nacional y la defensa**, alineados con los requisitos operacionales de las Fuerzas Armadas, sectores estratégicos, organismos de inteligencia o agencias gubernamentales.
7. **Redactar un informe técnico-científico sólido y estructurado**, con rigor metodológico y aplicabilidad en el campo de la ciberinteligencia.
8. **Defender su trabajo ante un tribunal académico y profesional**, demostrando capacidad de análisis, argumentación y aplicabilidad en escenarios reales.
9. **Desarrollar habilidades de liderazgo, gestión de proyectos y planificación estratégica en el contexto de la ciberinteligencia y las ciberoperaciones en sectores estratégicos para la Defensa Nacional**

Programa académico:

Los contenidos del TFM se definen en las propuestas ofertadas por los profesores tutores. El tema de cada trabajo es específico. A modo orientativo, el TFM se podrá orientar hacia uno de los siguientes enfoques:

- **Investigación aplicada:** Estudio de amenazas emergentes, nuevas metodologías de obtención de inteligencia en el ciberespacio, guerra cognitiva, ciberoperaciones en conflicto híbrido, o doctrina de ciberdefensa en entornos multinacionales (OTAN, UE).
- **Desarrollo de capacidades técnicas:** Implementación de herramientas avanzadas para la detección de amenazas, automatización de ciberinteligencia, simulación de ciberoperaciones ofensivas y defensivas, o integración de plataformas SOAR/SIEM en operaciones militares.
- **Análisis estratégico y normativo:** Evaluación de políticas y normativas de ciberdefensa en sectores estratégicos, cooperación interinstitucional en ciberinteligencia, o planificación de ciberoperaciones conjuntas en entornos multidominio.

Metodoloxía docente:

Los TFM pueden realizarse de forma individual o grupal. El desarrollo del TFM se realizará entre los meses de abril y junio

Competencias asociadas	Actividades formativas SÍNCRONAS	Horas síncronas presenciais	Horas síncronas virtuais	Horas de traballo autónomo do estudante
	ECTS TOTALES = 0,00	0,00	0,00	0,00

Las horas síncronas estarán comprendidas entre 8 y 12 por ECTS en modalidade síncrona

Competencias asociadas	Actividades formativas ASÍNCRONAS	Horas titorización	Horas de traballo autónomo do estudante
	Desarrollo del trabajo		375
	ECTS TOTALES = 15,00	0,00	375,00

Las horas de titorización estarán comprendidas entre 4 e 8 por ECTS en modalidade asíncrona

Metodoloxía de avaliación:

La evaluación se hará mediante la presentación y defensa ante un Tribunal del trabajo realizado por el alumno o grupo de alumnos, bajo la tutoría de un profesor de la titulación, o un profesor o ingeniero experto ajeno a la Universidad, representado por un profesor de la titulación.

En la evaluación, el Tribunal tendrá en cuenta las opiniones o el informe razonado del profesor tutor, así como aspectos como la calidad de la presentación, la revisión del estado del arte, la calidad de la propuesta técnica, la novedad y relevancia de los resultados, la capacidad de iniciativa de los estudiantes, etc.

Competencias avaliadas	Probas de avaliación	% Ponderación
	Defensa pública	20
	Memoria	20
	Informe del tutor	20
	Novedad, calidad y relevancia	40
		100%

Plataformas de Teledocencia e titorización:

Toda la documentación y comunicación relacionada con el TFM se realiza a través de una materia en MooVi. La comunicación entre alumando y tutores podrá realizarse a través de Campus Remoto