MEMORIA PARA A SOLICITUDE DO Máster de Formación Permanente en Ciberinteligencia y Ciberoperaciones en Sectores Estratégicos para la Seguridad Nacional

Máster de Formación Permanente en Ciberintelixencia e Ciberoperacións en Sectores Estratéxicos para a Seguridade Nacional

☒Nova Solicitude	☐Reedición	Num. Edición:
☐Programa modular	☐Interuniversitario	

CURSO ACADÉMICO: 2025/26

Promotor/a do título: José Carlos López Ardao
Teléfono de contacto:
Correo electrónico de contacto: jardao@det.uvigo.es

Centro organizador: Centro de Posgrao e Formación Permanente
Data de aprobación no centro: Faga click para engadir unha data
Teléfono de contacto: 986 130 304
Correo electrónico de contacto: cpfp@uvigo.es

1. DATOS XERAIS

1.1. DATOS BÁSICOS

NÚMERO DE CRÉDITOS QUE TEN QUE SUPERAR O ESTUDANTE: 60 ECTS Nº DE CRÉDITOS TEÓRICOS: 60 ECTS Nº DE CRÉDITOS PRÁCTICOS: 0 ECTS Nº DE CRÉDITOS DE PRÁCTICAS EXTERNAS: 0 H ☐ Prácticas externas obrigatorias Nº DE CRÉDITOS TRABALLO FIN DE MESTRADO: 15 ECTS (mínimo 6 ECTS)
NÚMERO DE CRÉDITOS QUE OFERTA O TÍTULO: 60 ECTS Nº DE CRÉDITOS OBLIGATORIOS: 60 ECTS Nº DE CRÉDITOS OPTATIVOS: 0 ECTS ESPECIALIDADES (no caso de ofertarse): 1) 2) 3) 4)
ÁMBITO DE COÑECEMENTO: Enxeñería Telemática
DATA DE INICIO: 01/09/2025
DATA DE REMATE: 26/06/2026
DATA PARA A DEFENSA DO TFM: Faga click para engadir unha data
MODALIDADE: Síncrona virtual
Nº DE HORAS SÍNCRONAS PRESENCIAIS: 0H Nº DE HORAS SÍNCRONAS VIRTUAIS: 360H Nº DE HORAS DE PRÁCTICAS EXTERNAS: 0H
NÚMERO DE PRAZAS: Mínimo 20 Máximo 30
COORDINADOR/A ACADÉMICO: José Carlos López Ardao
LUGAR (CENTRO) DE IMPARTICIÓN (modalidade presencial): PLATAFORMAS VIRTUAIS TELEDOCENCIA: Campus Remoto e MooVi
LINGUAXE DE IMPARTICIÓN: Castelán
WEB DO TÍTULO: http://eafp.uvigo.gal/gl/campus-aberto/titulos-propios/
DENOMINACIÓN DO TÍTULO EN CASTELÁN: Máster de Formación Permanente en Ciberinteligencia y Ciberoperaciones en Sectores Estratégicos para la Seguridad Nacional

DENOMINACIÓN DO TÍTULO EN INGLÉS: Master in Cyberintelligence and Cyberoperations in Strategic Sectors for National Security

1.2. TITULOS DO PROGRAMA MODULAR

Título de experto/especialista ou curso avanzado de posgrao	ECTS
Título de experto/especialista ou curso avanzado de posgrao	ECTS
Título de experto/especialista ou curso avanzado de posgrao	ECTS
Título de experto/especialista ou curso avanzado de posgrao	ECTS
Título de experto/especialista ou curso avanzado de posgrao	ECTS
Título de experto/especialista ou curso avanzado de posgrao	ECTS
Título de experto/especialista ou curso avanzado de posgrao	ECTS

1.3. COLABORACIÓNS EXTERNAS

☐ Interuniversitario	Universidades colaboradoras: 1) 2) 3)
☒ Convenios con entidades non universitarias	Outras entidades: 1)INDRA Sistemas S.A. 2) 3)
☐ Subvencións externas	Entidades que subvencionan: 1) 2) 3)
☐ Contratos de patrocinio	Entidades que patrocinan o título: 1) 2) 3)

REPRESENTANTE ENTIDAD EXTERNA COLABORADORA: Carlos Ceballos Romero ENTIDAD/INSTITUCIÓN: INDRA Sistemas S.A. TELÉFONO: CORREO-E: caceballos@indra.es
REPRESENTANTE ENTIDAD EXTERNA COLABORADORA: ENTIDAD/INSTITUCIÓN: TELÉFONO: CORREO-E:

Engadir as filas necesarias para cada unha das universidades ou entidades colaboradoras

2. XUSTIFICACIÓN DO TÍTULO

2.1. BREVE DESCRICIÓN DO TÍTULO

El Máster ofrece una formación avanzada y especializada en el ámbito de la ciberinteligencia y las ciberoperaciones aplicadas a sectores estratégicos clave y al entorno de la defensa y la seguridad nacional. El máster aborda las técnicas, metodologías y herramientas necesarias para la obtención y análisis de inteligencia en el ciberespacio, así como la planificación y ejecución de operaciones en entornos digitales complejos.

Además, el máster aborda de manera integral el marco normativo nacional e internacional aplicable a las operaciones en el ciberespacio, así como la gestión de riesgos y la seguridad de la información en infraestructuras críticas y sistemas militares.

Por último, en el Máster se presta especial atención al papel de la inteligencia artificial como herramienta multiplicadora en el ámbito de la ciberinteligencia y las ciberoperaciones, tanto ofensivas como defensivas, facilitando la automatización de procesos, el análisis avanzado de datos y la mejora en la toma de decisiones operativas y estratégicas. El programa combina un enfoque técnico, táctico y operativo, alineado con las necesidades actuales y futuras de las Fuerzas Armadas y otros organismos clave en los sectores estratégicos de la Seguridad Nacional

2.2. OBXECTIVOS DO TÍTULO

Los objetivos específicos del máster son:

1. **Formar especialistas en ciberinteligencia aplicada a sectores estratégico y a la seguridad nacional**, capacitados para obtener, analizar y explotar información procedente del ciberespacio con fines operativos, estratégicos y de toma de decisiones.
2. **Dotar a los alumnos de las competencias necesarias para planificar, ejecutar y evaluar ciberoperaciones** en escenarios de conflicto híbrido, operaciones conjuntas y misiones de carácter defensivo, ofensivo e informacional.
3. **Conocer y aplicar el marco normativo y doctrinal vigente** en materia de ciberdefensa, ciberseguridad y protección de infraestructuras críticas, tanto a nivel nacional como internacional (OTAN y UE).
4. **Capacitar en la identificación, evaluación y gestión de riesgos en entornos digitales estratégicos**, aplicando metodologías adaptadas a la seguridad nacional.
5. **Integrar la ciberinteligencia y las ciberoperaciones en el ciclo de planeamiento de la defensa en sectores estratégicos**, comprendiendo su papel clave en la obtención de superioridad informacional y en la conducción de operaciones multidominio.
6. **Desarrollar competencias avanzadas en la protección de la seguridad de la información y de los sistemas en sectores estratégicos**, aplicando técnicas y procedimientos específicos para entornos clasificados y redes operacionales.

7. **Explorar el potencial de la inteligencia artificial en el ámbito de la ciberinteligencia y las ciberoperaciones**, potenciando su aplicación en el análisis predictivo, la automatización de procesos, la correlación de datos masivos y la detección de amenazas emergentes.
8. **Fomentar una visión estratégica e integral de la ciberdefensa**, alineada con los objetivos de la política de seguridad nacional y los compromisos internacionales en materia de seguridad colectiva.
9. **Potenciar el trabajo multidisciplinar y la colaboración interinstitucional**, facilitando la interacción entre profesionales de las Fuerzas Armadas, cuerpos de seguridad, organismos de inteligencia e industria relacionada con la defensa y los sectores estratégicos.

2.3. XUSTIFICACIÓN SOCIAL

En un contexto global marcado por la creciente digitalización de los sectores estratégicos y la consolidación del ciberespacio como un nuevo dominio operativo, las amenazas híbridas, las campañas de desinformación, el ciberespionaje y las ciberoperaciones ofensivas se han convertido en instrumentos habituales dentro de la confrontación entre Estados y otros actores no estatales. Esta realidad afecta directamente a la seguridad nacional, poniendo en riesgo la integridad de infraestructuras críticas en sectores estratégicos, la capacidad operativa de las Fuerzas Armadas y la soberanía tecnológica de los países.

El dominio del ciberespacio es hoy un factor clave en la proyección de poder y en la defensa de los intereses nacionales. Por ello, resulta imprescindible contar con profesionales altamente cualificados en ciberinteligencia y ciberoperaciones, capaces de anticipar amenazas, conducir operaciones en el entorno digital y garantizar la superioridad informacional en escenarios de conflicto multidominio. Esta necesidad es especialmente relevante en sectores estratégicos como la defensa, la energía, las telecomunicaciones o el transporte, donde la continuidad operativa es esencial para la estabilidad del Estado.

Además, el rápido avance de la inteligencia artificial y su aplicación en el ámbito de la ciberdefensa multiplica tanto las oportunidades como los riesgos, lo que exige una formación específica en el uso ético y eficaz de estas tecnologías dentro del marco normativo y doctrinal vigente, alineado con los compromisos internacionales de España en materia de seguridad y defensa (OTAN, UE, ONU).

En este contexto, el Máster responde a una demanda crítica de las Fuerzas Armadas, las empresas de sectores estratégicos, los organismos de seguridad y los centros de inteligencia, proporcionando un programa formativo especializado que combina un enfoque técnico, operativo y estratégico. Su objetivo es formar a una nueva generación de profesionales capaces de afrontar los desafíos del ciberespacio y garantizar la seguridad y la defensa en sectores estratégicos en el entorno digital del siglo XXI.

2.4. PERFIL DE EGRESO:

Los egresados del Máster estarán capacitados para desempeñar funciones de alta especialización en el ámbito de la ciberdefensa, la ciberseguridad estratégica y la ciberinteligencia aplicada en sectores estratégicos para la Seguridad Nacional. Con una formación integral que combina conocimientos técnicos, operativos, doctrinales y normativos, estos profesionales estarán preparados para incorporarse a diversos entornos institucionales, operativos y estratégicos, tanto en el ámbito militar como en organismos de seguridad y defensa en sectores estratégicos.

Perfiles profesionales específicos

1. **Analistas en ciberinteligencia y ciberoperaciones** dentro de unidades de ciberdefensa de las Fuerzas Armadas, cuerpos de seguridad y organismos vinculados a la seguridad nacional.
2. **Analistas de ciberinteligencia en centros de inteligencia y unidades de obtención de información**, con capacidad para explotar fuentes digitales, detectar amenazas emergentes y producir inteligencia accionable para el planeamiento y la toma de decisiones militares.
3. **Responsables de seguridad de la información y protección de infraestructuras críticas** en entornos de defensa y sectores estratégicos, gestionando el ciclo de vida de la información sensible y garantizando la continuidad operativa de sistemas clave.
4. **Especialistas en gestión de riesgos en ciberespacio y entornos militares**, capaces de evaluar amenazas, vulnerabilidades y riesgos en sistemas de mando y control, redes operacionales y plataformas tecnológicas de defensa en sectores estratégicos.
5. **Especialistas en aplicación de inteligencia artificial a ciberinteligencia y ciberoperaciones**, con capacidad para diseñar y emplear herramientas basadas en IA para la automatización de procesos, el análisis predictivo y la detección de amenazas avanzadas.
6. **Profesionales preparados para la colaboración interinstitucional e internacional**, capacitados para trabajar en entornos multinacionales (OTAN, UE) o en operaciones conjuntas de carácter híbrido, cibernético e informacional.

2.5. COMPETENCIAS:

CÓDIGO	COMPETENCIA
CG1	**Capacidad de análisis crítico y estratégico para interpretar el entorno geopolítico, tecnológico y de seguridad global, con especial énfasis en las amenazas híbridas y cibernéticas que afectan a la seguridad nacional en sus sectores estratégicos**
CG2	**Habilidad para integrar conocimientos multidisciplinares (técnicos, operativos, normativos y estratégicos) y aplicarlos en la resolución de problemas complejos relacionados con la ciberinteligencia y las ciberoperaciones en sectores estratégicos**
CG3	**Capacidad de trabajo en entornos de alta presión y toma de decisiones en situaciones críticas, propias de operaciones militares y de gestión de crisis cibernéticas en sectores estratégicos**
CG4	**Dominio de las metodologías de obtención, análisis y difusión de inteligencia aplicadas al ciberespacio, adaptadas a las necesidades operativas y estratégicas de los organismos de seguridad nacional**
CG5	**Capacidad para redactar un informe técnico-científico sólido, estructurado, y con rigor metodológico, en el campo de las ciberoperaciones y de la ciberinteligencia técnica, táctica operativa o estratégica, y con aplicabilidad en sectores estratégicos para la Seguridad Nacional**
CE1	**Desarrollar ciberinteligencia operativa, táctica y estratégica, identificando amenazas, analizando patrones de actividad en el ciberespacio y generando productos de inteligencia útiles para la toma de decisiones en sectores estratégicos.**

CE2	**Planificar y ejecutar ciberoperaciones, tanto defensivas como ofensivas, en el ámbito de la seguridad nacional en sectores estratégicos, integrándolas en operaciones conjuntas y en el planeamiento multidominio.**
CE3	**Aplicar marcos normativos nacionales e internacionales en el ámbito de la ciberdefensa y las operaciones en el ciberespacio, asegurando el cumplimiento de la legalidad.**
CE4	**Identificar, evaluar y gestionar riesgos y vulnerabilidades en infraestructuras críticas y sistemas en sectores estratégicos y de la seguridad nacional, aplicando metodologías adaptadas a los entornos de defensa.**
CE5	**Garantizar la seguridad de la información en el ciclo de vida de los datos en entornos clasificados, sistemas de mando y control, y redes en sectores estratégicos y de la seguridad nacional**
CE6	**Aplicar técnicas avanzadas de ciberseguridad y protección activa de sistemas, detectando y neutralizando amenazas persistentes avanzadas (APT) y ataques complejos en redes operativas.**
CE7	**Emplear inteligencia artificial y herramientas de análisis avanzado para la automatización de procesos de obtención y análisis de ciberinteligencia, para la detección de patrones anómalos o amenazas emergentes, así como para el planeamiento de ciberoperaciones ofensivas**
CE8	**Integrar la ciberinteligencia en el ciclo de inteligencia completo en sectores estratégicos, asegurando su alineamiento con las necesidades operativas y estratégicas de estos**
CE9	**Diseñar y ejecutar ejercicios y simulaciones de ciberdefensa y ciberinteligencia, como herramienta de entrenamiento y evaluación de la preparación operativa de unidades y equipos de respuesta.**
CE10	**Contribuir al desarrollo de procedimientos de ciberinteligencia y ciberoperaciones, participando en la evolución conceptual y tecnológica de la ciberdefensa en el marco de la seguridad nacional e internacional en sus sectores estratégicos**

Utilizar os seguintes códigos: CB (Competencia Básica), CG (Competencia Xeral), CT (Competencia Transversal), CE (Competencia Específica)

2.6. XUSTIFICACIÓN DA PROPOSTA NA UVIGO

En la Universidad de Vigo se está impartiendo actualmente un Máster Universitario en Ciberseguridad (MUNICS) de 90 ECTS en la Escola de Enxeñería de Telecomunicación, pero se trata de una formación muy amplia y genérica en el ámbito de la ciberseguridad, y muy especialmente en todos los aspectos relacionados con la ciberdefensa.

En cambio, la propuesta formativa de este Máster de Formación Permanente se centra de forma muy concreta y específica en el ámbito de la ciberinteligencia, la seguridad de la información, la normativa y las ciberoperaciones en sectores estratégicos para la Seguridad Nacional, con especial hincapié en la aplicación de la Inteligencia Artificial y la automatización de los procesos relacionados.

En este sentido, si bien este Máster incluye en su plan de estudios una parte imprescindible de contenidos relacionada con la ciberdefensa y la ciberseguridad que también se imparten en MUNICS, esta parte representa sólo en torno al 20% del total de los contenidos, siendo además su enfoque muy específico. El resto de los contenidos, que representan aproximadamente el 80%, se centran en la ciberinteligencia, técnicas de análisis estructurado, análisis de redes sociales, inteligencia artificial aplicada a las ciberoperaciones y normativas específicas, contenidos que no son impartidos en ninguna materia de MUNICS.

Cabe mencionar que los contenidos y estructura de este Máster de Formación Permanente han sido diseñados de forma conjunta con la empresa Indra Sistemas S.A., interesada en una formación de Máster de estas características, muy orientada hacia sectores estratégicos de la Seguridad Nacional y con un peso significativo en ciberinteligencia y en la aplicación de la IA a las ciberoperaciones, formación que no existe ni en la UVIGO ni en todo el ámbito Nacional.

3. DESTINATARIOS:

3.1. PERFIL DE INGRESO

PERFIL DE INGRESO: Ingeniería de Telecomunicación, Ingeniería Informática
REQUIRIMENTOS DE ACCESO AO TÍTULO DE MESTRADO : Titulados de Grado o Máster en Ingeniería de Telecomunicación, Ingeniería Informática
REQUERIMENTOS DE ACCESO AOS TÍTULOS MODULARES : Ter en conta os requisitos mínimos do artigo 27 do regulamento

3.2. PREINSCRIPCIÓN E MATRÍCULA

DATA DE INICIO PREINSCRICIÓN: Faga click para engadir unha data
DATA DE REMATE PREINSCRICIÓN: Faga click para engadir unha data
DOCUMENTACIÓN REQUIRIDA: 1) 2) 3) 4) 5) 6)
PROBAS DE ADMISIÓN (se procede):

CRITERIOS DE ADMISIÓN:	PONDERACIÓN (%):
1) Titulación	60
2) Formación complementaria en redes, ciberseguridad e Inteligencia Artificial	30
3) Entrevista Personal	10
4)	
5)	
6)	
7)	

DATA DE INICIO MATRÍCULA: Faga click para engadir unha data
DATA DE REMATE MATRÍCULA: Faga click para engadir unha data

3.3. PREZOS PÚBLICOS:

TER EN CONTA OS ***PREZOS MÁXIMOS POR CRÉDITO ESTABLECIDOS POLO CONSELLO SOCIAL***

Nas tarifas é preciso respectar o 10 % de redución sobre a tarifa xeral para a comunidade Alumni e do 15% para as persoas desempregadas e a comunidade universitaria

PREZO DO TÍTULO DE MESTRADO		
Xeral: 5400 €	Comunidade Universitaria e desempregados/as: 4590€	Comunidade Alumni: 4860€
☐Axudas ao estudo	NUMERO DE AXUDAS:	CONTÍA:

PREZO DO TÍTULO MODULAR:		
Xeral: €	Comunidade Universitaria e desempregados/as: €	Comunidade Alumni: €
☐Axudas ao estudo:	NUMERO DE AXUDAS:	CONTÍA:

PREZO DO TÍTULO MODULAR:		
Xeral: €	Comunidade Universitaria e desempregados/as: €	Comunidade Alumni: €
☐Axudas ao estudo	NUMERO DE AXUDAS:	CONTÍA:

PREZO DO TÍTULO MODULAR:		
Xeral: €	Comunidade Universitaria e desempregados/as: €	Comunidade Alumni: €
☐Axudas ao estudo	NUMERO DE AXUDAS:	CONTÍA:

PREZO DO TÍTULO MODULAR:		
Xeral: €	Comunidade Universitaria e desempregados/as: €	Comunidade Alumni: €
☐Axudas ao estudo	NUMERO DE AXUDAS:	CONTÍA:

4. COORDINACIÓN

4.1. COMISIÓN ACADÉMICA DO MÁSTER (CAM)

COORDINADOR/A DO MÁSTER:	
NOME: José Carlos López Ardao	NIF:
CATEGORÍA: TU	DEPARTAMENTO: Enxeñería Telemática
CORREO-E: jardao@det.uvigo.es	Nº TELÉFONO:

PDI Doutor/a con vinculación permanente á Universidade de Vigo

SECRETARIO/A DO MÁSTER:	
NOME: Raúl F. Rodríguez Rubio	NIF:
CATEGORÍA/PROFESIÓN: TU	DEPARTAMENTO: Enxeñería Telemática
CORREO-E: rrubio@det.uvigo.es	Nº TELÉFONO:

MEMBROS DA COMISIÓN ACADÉMICA:	
NOME: Alberto Gil Solla	NIF:
CATEGORÍA/PROFESIÓN: CU	DEPARTAMENTO: Enxeñería Telemática
CORREO-E: agil@det.uvigo.es	Nº TELÉFONO:
NOME: Andrés Suárez González	NIF:
CATEGORÍA/PROFESIÓN: TU	DEPARTAMENTO: Enxeñería Telemática
CORREO-E: asuarez@det.uvigo.es	Nº TELÉFONO:
NOME:	NIF:
CATEGORÍA/PROFESIÓN:	DEPARTAMENTO/EMPRESA:
CORREO-E:	Nº TELÉFONO:
NOME:	NIF:
CATEGORÍA/PROFESIÓN:	DEPARTAMENTO/EMPRESA:
CORREO-E:	Nº TELÉFONO:
NOME:	NIF:
CATEGORÍA/PROFESIÓN:	DEPARTAMENTO/EMPRESA:
CORREO-E:	Nº TELÉFONO:

5. PROGRAMA ACADÉMICO

5.1. MATERIAS DO PRIMER CUADRIMESTRE/SEMESTRE:

MÓDULO/ESPECIALIDADE	Obrigatoria	NOME DA MATERIA	ECTS
	☒	Malware, Ciberamenazas e Inteligencia Artificial (MCIA)	7,5
	☒	Introducción a la Inteligencia de Ciberamenazas (IIC)	7,5
	☒	Ciberoperaciones Ofensivas (COO)	7,5
	☒	Técnicas de Ciberinteligencia (TCI)	7,5
	☐	Haga clic o pulse aquí para escribir texto.	
	☐	Haga clic o pulse aquí para escribir texto.	
	☐	Haga clic o pulse aquí para escribir texto.	
	☐	Haga clic o pulse aquí para escribir texto.	
	☐	Haga clic o pulse aquí para escribir texto.	
	☐	Haga clic o pulse aquí para escribir texto.	
	☐	Haga clic o pulse aquí para escribir texto.	
	☐	Haga clic o pulse aquí para escribir texto.	
	☐	Haga clic o pulse aquí para escribir texto.	
	☐	Haga clic o pulse aquí para escribir texto.	
	☐	Haga clic o pulse aquí para escribir texto.	
	☐	Haga clic o pulse aquí para escribir texto.	
	☐	Haga clic o pulse aquí para escribir texto.	
	☐	Haga clic o pulse aquí para escribir texto.	
	☐	Haga clic o pulse aquí para escribir texto.	
	☐	Haga clic o pulse aquí para escribir texto.	
		TOTAL ECTS OFERTADOS:	**30**

Os ECTS totales actualizaranse automaticamente (pódese forzar a actualización facendo click con botón dereito no total e premendo a opción "*Actualizar_campos*")

5.2. MATERIAS DO SEGUNDO CUADRIMESTRE/SEMESTRE

MÓDULO/ESPECIALIDADE	Obrigatoria	NOME DA MATERIA	ECTS
	☒	Gestión de Seguridad de la Información e Infraestructuras Criíticas (GSI)	7,5
	☒	Ciberoperaciones Defensivas (COD)	7,5
	☒	Trabajo Fin de Máster (TFM)	15
	☐	Haga clic o pulse aquí para escribir texto.	
	☐	Haga clic o pulse aquí para escribir texto.	
	☐	Haga clic o pulse aquí para escribir texto.	
	☐	Haga clic o pulse aquí para escribir texto.	
	☐	Haga clic o pulse aquí para escribir texto.	
	☐	Haga clic o pulse aquí para escribir texto.	
	☐	Haga clic o pulse aquí para escribir texto.	
	☐	Haga clic o pulse aquí para escribir texto.	
	☐	Haga clic o pulse aquí para escribir texto.	
	☐	Haga clic o pulse aquí para escribir texto.	
	☐	Haga clic o pulse aquí para escribir texto.	
	☐	Haga clic o pulse aquí para escribir texto.	
	☐	Haga clic o pulse aquí para escribir texto.	
	☐	Haga clic o pulse aquí para escribir texto.	
	☐	Haga clic o pulse aquí para escribir texto.	
	☐	Haga clic o pulse aquí para escribir texto.	
	☐	Haga clic o pulse aquí para escribir texto.	
		TOTAL ECTS OFERTADOS:	**30**

Os ECTS totales actualizaranse automaticamente (pódese forzar a actualización facendo click con botón dereito no total e premendo a opción *"Actualizar_campos"*)

Engadir apartados 5.3 e 5.4 para terceiro e cuarto trimestre no caso de mestrados de 90 ou 120 ECTS

5.3. PRÁCTICAS EN EMPRESAS:

As prácticas en empresa seguirán o regulamento Regulamento de prácticas académicas externas do estudantado da UVigo

Xustificación da necesidade das prácticas e o seu valor docente

Listaxe de empresas nas que se desenvolverán as prácticas

5.4. SISTEMAS DE APOIO E ORIENTACIÓN DOS ESTUDANTES

Procedementos de apoio e orientación aos estudantes unha vez matriculados

5.5. CALENDARIO E HORARIO

La impartición de las sesiones síncronas virtuales de las materias se divide en tres bimestres:

- **Bimestre 1**: del 1 de septiembre al 31 de octubre: lunes a jueves de 16 a 19h.
- **Bimestre 2**: del 3 de noviembre al 22 de diciembre, y del 8 al 16 de enero: lunes a jueves de 16 a 19h.
- **Bimestre 3**: del 19 de enero al 27 de marzo: : lunes y jueves de 16 a 19h. y martes y miércoles de 16 a 18h.

El cuarto bimestre, entre abril y junio, se dedica a la realización del TFM

5.6. CALENDARIO DE AVALIACIÓN

La primera oportunidad de evaluación de todas las materias es obligatoriamente mediante el mecanismo de evaluación continua, que consiste en la realización de tareas y pruebas intermedias durante el bimestre de impartición de cada materia.

La segunda oportunidad debe realizarse durante el mes de Junio, y consistirá en la entrega de un conjunto de tareas propuestas, dentro del plazo señalado en el mes de Junio, y en la realización de un único examen oral de en torno a 1 hora de duración, en fecha acordada entre profesorado y alumno, sobre el contenido teórico de toda la materia, así como sobre las tareas entregadas.

5.7. RECOÑECEMENTO DE CRÉDITOS

No se contempla

5.8. CONDICIÓNS DE TERMINACIÓN

El alumno debe obtener una calificación mínima de APROBADO en todas las materias, incluyendo el TFM.

6. PERSOAL DOCENTE

6.1. PERSOAL DA UNIVERSIDADE DE VIGO

(De acordo con artigo 22 do regulamento, polo menos, o 25% dos ECTS do título deben ser impartidos por profesorado da UVigo)

NOME	APELIDOS	Doutor/a	Área de coñecemento	Perfil/méritos en relación co titulo
Jose Carlos	López Ardao	☒	Enxeñería Telemática	
Raúl F.	Rodríguez Rubio	☒	Enxeñería Telemática	
Alberto	Gil Solla	☒	Enxeñería Telemática	
Andrés	Suárez González	☒	Enxeñería Telemática	
Sergio	Herrería Alonso	☒	Enxeñería Telemática	
Miguel	Rodríguez Pérez	☒	Enxeñería Telemática	
Carlos	Rivas Costa	☒	Enxeñería Telemática	
Manuel	Caeiro Rodríguez	☒	Enxeñería Telemática	
Yolanda	Blanco Fernández	☒	Enxeñería Telemática	
		☐		
		☐		
		☐		
		☐		
		☐		
		☐		
		☐		
		☐		

6.2. PERSOAL DOCENTE DOUTRAS UNIVERSIDADES

NOME	APELIDOS	Doutor/a	Área de coñecemento	Perfil/méritos en relación co titulo
		☐		
		☐		
		☐		
		☐		
		☐		
		☐		
		☐		
		☐		
		☐		
		☐		
		☐		
		☐		
		☐		
		☐		
		☐		
		☐		
		☐		
		☐		

6.3. PERSOAL DOCENTE EXTERNO

NOME	APELIDOS	Doutor/a	Empresa/institución	Perfil/méritos en relación co titulo
José Luis	Rivas López	☐	Laboratorio de Informática Forense europeo (LIFe)	
Miguel	Rodelgo Lacruz	☒	CUD Marín	
Gabriel	González Fernández	☐	Deicom Technologies	
		☐		
		☐		
		☐		
		☐		
		☐		
		☐		
		☐		
		☐		
		☐		
		☐		
		☐		
		☐		
		☐		
		☐		
		☐		
		☐		

7. PREVISIÓN ECONÓMICA

7.1. Previsión de Ingresos

A previsión dos ingresos debe cubrirse na pestana ingresos do ficheiro Excel "Prevision_economica_mestrado_propio"

7.2. Previsión de Gastos

A previsión dos gastos debe cubrirse nas pestanas de Gastos de coordinación, Axudas, Pagos docentes Uvigo, Pagos docentes externos, Recurso e desprazamentos do ficheiro "Prevision_economica_mestrado_propio"

7.3. Orzamento

A táboa actualizarase automaticamente ao cubrir o ficheiro Excel "Previsión_economica_mestrado_propio" (pódese forzar a actualización facendo click con botón dereito na táboa e premendo a opción "*Actualizar_vínculo*")

INGRESOS DO TÍTULO:	91.800,00 €

GASTOS DO TÍTULO	
Coordinación	1.800,00 €
Axudas ao estudo	0,00 €
Pago docentes UVIGO	79.200,00 €
Pago docentes externos	10.800,00 €
Recursos	0,00 €
Desprazamentos	0,00 €
TOTAL	91.800,00 €

Xustificación da contía indicada en outros gastos ou outros aspectos a xustificar da previsión económica

8. RESULTADOS PREVISTOS:

Taxa de rendemento: 100 %
Taxa de éxito: 80 %
Duración media dos estudos: meses
Xustificación das taxas anteriores

9. COMENTARIOS E OBSERVACIÓNS:

Comentarios ou observacións non recollidos noutros apartados da proposta

10.APROBACIÓN DO CENTRO ORGANIZADOR:

O consello da Facultade, Escola, Instituto, Departamento con motivo da súa reunión do pasado día
Faga click para engadir unha data

Acordou INFORMAR FAVORABLEMENTE a memoria de solicitude do Título de Máster de Formación Permanente en Ciberinteligencia y Ciberoperaciones en Sectores Estratégicos para la Seguridad Nacional

a implantar no curso académico 2025/26, nos termos que se expresan na documentación que se acompaña a este acordo.

Así mesmo, póñense ao dispor deste título propio os seguintes medios e infraestruturas:

Especificar as aulas, laboratorios, salas ou outras infraestruturas

Sinatura electrónica do Decano/a ou Director/a

11.SINATURA ELECTRÓNICA DOS MEMBROS DA CAM:

Fdo. José Carlos López Ardao Coordinador/a do mestrado	Fdo. Raúl F. Rodríguez Rubio Secretario/a do mestrado
Fdo. Alberto Gil Solla Membro da CAM	Fdo. Andrés Suárez González Membro da CAM
Fdo. Membro da CAM	Fdo. Membro da CAM
Fdo. Membro da CAM	Fdo. Membro da CAM

12.ANEXOS:

Esta proposta acompáñase dos seguintes documentos en formato electrónico:

☒ Fichas das materias en formato Word (modelo Ficha_materia_mestrado_propio.doc)

☒ Ficheiro Excel da proposta económica (Prevision_economica_mestrado_propio.xlsx)

☒ Ficheiro en formato Excel da planificación docente (Planificacion_docente_mestrado_propio.xlsx)

☐ Curriculum abreviado dos profesores externos

☐ Convenios de colaboración con outras entidades

☐ Contratos de patrocinio

☐ Outros: especificar

Modificación da proposta

O/A coordinador/a deberá solicitar ao Servizo de Posgrao calquera modificación da presente proposta para a súa aprobación pola Comisión de Estudos Propios.

Cancelación de mestrado

O/A coordinador/a é responsable de comunicar, tanto aos estudantes inscritos no curso como ao Servizo de Posgrao de Universidade de Vigo, a cancelación do mesmo con, polo menos, quince días naturais de antelación á data de comezo.

Tratamento de datos persoais

1. Responsable do tratamento:

A Universidade de Vigo é a responsable do tratamento dos datos de carácter persoal e cumpre cos principios de transparencia e información conforme aos artigos 12 e 13 do Regulamento (UE) 2016/679, do Parlamento Europeo e do Consello, de 27 de abril, relativo á protección das persoas físicas no que respecta ao tratamento de datos persoais e á libre circulación destes datos e polo que se derroga a Directiva 95/46/CE (RXPD) e co disposto no artigo 11 da Lei orgánica 3/2018, de 5 de decembro, de protección de datos persoais e garantía dos dereitos dixitais (LOPDGDD).

2. Finalidades:

Os datos persoais facilitados serán tratados coas seguintes finalidades:

- Encargado da docencia dos títulos propios
- Alta do profesorado nas plataformas administrativas e de xestión da Universidade de Vigo
- Alta do profesorado nas plataformas de teledocencia da Universidade de Vigo
- Certificacións de docencia

3. Lexitimación:

A Universidade de Vigo está lexitimada para o tratamento da información persoal de acordo cos principios de licitude sinalados no artigo 6 do RXPD, e especialmente en cumprimento de obrigas legais, dunha misión realizada en

interese público ou no exercicio de poderes públicos. O tratamento está amparado, principalmente, na Lei orgánica 6/2001, de 21 de decembro, de universidades para a prestación do servizo de educación superior que ten encomendada, así como en toda a súa normativa de desenvolvemento. Así mesmo, a Universidade está lexitimada pola Lei 6/2013, de 13 de xuño, do sistema universitario de Galicia, os Estatutos da Universidade de Vigo e a súa normativa de desenvolvemento.

4. Cesións:

Os datos so serán cedidos nos casos previstos legalmente cando sexa necesario para o cumprimento dunha obriga legal aplicable ao responsable do tratamento.

Os datos serán cedidos a outras administracións e organismos públicos para o exercicio das competencias que lles sexan propias e compatibles coas finalidades enunciadas.

5. Prazos de conservación:

Estes datos conservaranse durante o tempo necesario para cumprir coas finalidades para as que se recolleron e para determinar as posibles responsabilidades que se puideran derivar do tratamento dos datos. Será de aplicación o disposto na normativa de arquivo e documentación.

6. Dereitos:

Vostede ten dereito a solicitar ao responsable do tratamento, en calquera momento, o acceso, rectificación ou supresión dos seus datos persoais e a limitación do seu tratamento. Tamén terá dereito a oporse ao devandito tratamento, así como a solicitar, salvo casos de interese público e/ou exercicio de poderes públicos, a portabilidade dos seus datos.

Os devanditos dereitos poderanse exercer mediante solicitude dirixida ao reitor e presentada electronicamente a través da sede electrónica da Universidade de Vigo https://sede.uvigo.gal/ (preferentemente empregando o procedemento específico SXER – Exercicio de dereitos sobre protección de datos) ou ben presencialmente ante as Oficinas de Asistencia en Materia de Rexistro da Universidade de Vigo, ou en calquera dos rexistros e oficinas indicados no artigo 16 da Lei 39/2015, de 1 de outubro, do procedemento administrativo común das administracións públicas e remitida á Secretaría Xeral da Universidade de Vigo, Campus universitario Lagoas-Marcosende, 36310 Vigo (Pontevedra).

7. Máis información:

Pode consultar máis información sobre a protección de datos na Universidade de Vigo en https://www.uvigo.gal/proteccion-datos