IMPRESO SOLICITUD PARA VERIFICACIÓN DE TÍTULOS OFICIALES

1. DATOS DE LA UNIVERSIDAD, CENTRO Y TÍTULO QUE PRESENTA LA SOLICITUD

De conformidad con el Real Decreto 822/2021, de 28 de septiembre, por el que se establece la organización de las enseñanzas universitarias y del procedimiento de aseguramiento de su calidad.

UNIVERSIDAD SOLICITANTE	CENTRO	CÓDIGO CENTRO
Universidad Internacional de La Rioja	Escuela Superior de Ingeniería y Tecnología	26004007

NIVEL	DENOMINACIÓN CORTA
Máster	Inteligencia Artificial Aplicada a la Ciberseguridad

DENOMINACIÓN ESPECÍFICA
Máster Universitario en Inteligencia Artificial Aplicada a la Ciberseguridad por la Universidad Internacional de La Rioja

NIVEL MECES
3

RAMA DE CONOCIMIENTO	CAMPO DE ESTUDIO	CONJUNTO
Ingeniería y Arquitectura	Ingeniería informática y de sistemas	No

SOLICITANTE	
NOMBRE Y APELLIDOS	CARGO
Virginia Montiel Martín	Responsable de programas ANECA

REPRESENTANTE LEGAL	
NOMBRE Y APELLIDOS	CARGO
Juan Pablo Guzmán Palomino	Secretario General

RESPONSABLE DEL TÍTULO	
NOMBRE Y APELLIDOS	CARGO
Óscar Sanjuan Martínez	Director de la Escuela Superior de Ingeniería y Tecnología

2. DIRECCIÓN A EFECTOS DE NOTIFICACIÓN

A los efectos de la práctica de la NOTIFICACIÓN de todos los procedimientos relativos a la presente solicitud, las comunicaciones se dirigirán a la dirección que figure en el presente apartado.

DOMICILIO	CÓDIGO POSTAL	MUNICIPIO	TELÉFONO
Avenida de la Paz, 137	26006	Logroño	676614276
E-MAIL	**PROVINCIA**		**FAX**
virginia.montiel@unir.net	La Rioja		

3. PROTECCIÓN DE DATOS PERSONALES

De acuerdo con lo previsto en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, se informa que los datos solicitados en este impreso son necesarios para la tramitación de la solicitud y podrán ser objeto de tratamiento automatizado. La responsabilidad del fichero automatizado corresponde al Consejo de Universidades. Los solicitantes, como cedentes de los datos podrán ejercer ante el Consejo de Universidades los derechos de información, acceso, rectificación y cancelación a los que se refiere el Título III de la citada Ley Orgánica 3/2018, de 5 de diciembre, sin perjuicio de lo dispuesto en otra normativa que ampare los derechos como cedentes de los datos de carácter personal.

El solicitante declara conocer los términos de la convocatoria y se compromete a cumplir los requisitos de la misma, consintiendo expresamente la notificación por medios telemáticos a los efectos de lo dispuesto en el artículo 43 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

	En: La Rioja, AM 31 de diciembre de 2025
	Firma: Representante legal de la Universidad

CSV: 985778453469842713302612 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

1. DESCRIPCIÓN, OBJETIVOS FORMATIVOS Y JUSTIFICACIÓN DEL TÍTULO

1.1-1.3 DENOMINACIÓN, CAMPO DE ESTUDIO, MENCIONES/ESPECIALIDADES Y OTROS DATOS BÁSICOS

NIVEL	DENOMINACIÓN ESPECIFICA	CONJUNTO	CONVENIO	CONV. ADJUNTO
Máster	Máster Universitario en Inteligencia Artificial Aplicada a la Ciberseguridad por la Universidad Internacional de La Rioja	No		Ver Apartado 1: Anexo 1.

RAMA
Ingeniería y Arquitectura
CAMPO DE ESTUDIO
Ingeniería informática y de sistemas
AGENCIA EVALUADORA
Agencia Nacional de Evaluación de la Calidad y Acreditación
LISTADO DE ESPECIALIDADES
No existen datos
MENCIÓN DUAL
No

1.4-1.9 UNIVERSIDADES, CENTROS, MODALIDADES, CRÉDITOS, IDIOMAS Y PLAZAS

UNIVERSIDAD SOLICITANTE
Universidad Internacional de La Rioja

LISTADO DE UNIVERSIDADES	
CÓDIGO	**UNIVERSIDAD**
077	Universidad Internacional de La Rioja

LISTADO DE UNIVERSIDADES EXTRANJERAS	
CÓDIGO	**UNIVERSIDAD**
No existen datos	

CRÉDITOS TOTALES	CRÉDITOS DE COMPLEMENTOS FORMATIVOS	CRÉDITOS EN PRÁCTICAS EXTERNAS
60	0	0
CRÉDITOS OPTATIVOS	**CRÉDITOS OBLIGATORIOS**	**CRÉDITOS TRABAJO FIN GRADO/ MÁSTER**
0	48	12

1.4-1.9 Universidad Internacional de La Rioja

1.4-1.9.1 CENTROS EN LOS QUE SE IMPARTE

LISTADO DE CENTROS			
CÓDIGO	**CENTRO**	**CENTRO RESPONSABLE**	**CENTRO ACREDITADO INSTITUCIONALMENTE**
26004007	Escuela Superior de Ingeniería y Tecnología	Si	Si

1.4-1.9.2 Escuela Superior de Ingeniería y Tecnología

1.4-1.9.2.1 Datos asociados al centro

MODALIDADES DE ENSEÑANZA EN LAS QUE SE IMPARTE EL TITULO		
PRESENCIAL	**SEMIPRESENCIAL/HÍBRIDA**	**A DISTANCIA/VIRTUAL**
No	No	Sí
PLAZAS POR MODALIDAD		
		600
NÚMERO TOTAL DE PLAZAS	**NÚMERO DE PLAZAS DE NUEVO INGRESO PARA PRIMER CURSO**	

CSV: 985778453469842713302612 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

600	600	
IDIOMAS EN LOS QUE SE IMPARTE		
CASTELLANO	**CATALÁN**	**EUSKERA**
Sí	No	No
GALLEGO	**VALENCIANO**	**INGLÉS**
No	No	No
FRANCÉS	**ALEMÁN**	**PORTUGUÉS**
No	No	No
ITALIANO	**OTRAS**	
No	No	

1.10 JUSTIFICACIÓN

JUSTIFICACIÓN DEL INTERÉS DEL TÍTULO Y CONTEXTUALIZACIÓN
Ver Apartado 1: Anexo 6.

1.11-1.13 OBJETIVOS FORMATIVOS, ESTRUCTURAS CURRICULARES ESPECÍFICAS Y DE INNOVACIÓN DOCENTE

OBJETIVOS FORMATIVOS

1.11.Principales objetivos formativos de la titulación

El Máster tiene una orientación profesional y sus principales objetivos formativos son capacitar al estudiantado para aplicar de forma práctica conocimientos avanzados en el ámbito de la inteligencia artificial aplicada a la ciberseguridad, desarrollando habilidades específicas para la detección, el

análisis y la mitigación de amenazas en entornos digitales complejos. Asimismo, fomenta competencias transversales vinculadas a la toma de decisiones éticas, el trabajo en entornos colaborativos y el uso experto de tecnologías emergentes orientadas al sector de la seguridad digital.

1.11 bis) Objetivos formativos de especialidades

No aplica.

1.12.Estructuras curriculares específicas, justificación de sus objetivos

No aplica.

1.13.Estrategias metodológicas de innovación docente específicas, justificación de sus objetivos

No aplica.

ESTRUCTURAS CURRICULARES ESPECÍFICAS Y ESTRATEGIAS METODOLÓGICAS DE INNOVACIÓN DOCENTE

1.14 PERFILES FUNDAMENTALES DE EGRESO Y PROFESIONES REGULADAS

PERFILES DE EGRESO		
https://static.unir.net/calidad/1.14_Perfil_egreso_MU_CI.pdf		
HABILITA PARA EL EJERCICIO DE PROFESIONES REGULADAS	No	
NO ES CONDICIÓN DE ACCESO PARA TITULO PROFESIONAL		

2. RESULTADOS DEL PROCESO DE FORMACIÓN Y DE APRENDIZAJE

RESULTADOS DEL PROCESO DE FORMACIÓN Y DE APRENDIZAJE
RE1 - Analizar algoritmos de aprendizaje automático aplicados a la detección de amenazas digitales. TIPO: Habilidades o destrezas
RE10 - Aplicar marcos regulatorios como el Reglamento de Inteligencia Artificial (AI Act) y la Directiva NIS2 al diseño de soluciones tecnológicas. TIPO: Competencias
RE11 - Desarrollar soluciones avanzadas mediante modelos generativos y agentes autónomos, incluyendo su aplicación controlada en contextos ofensivos y simulados. TIPO: Habilidades o destrezas
RE12 - Evaluar la resiliencia de infraestructuras críticas frente a ciberataques complejos. TIPO: Competencias
RE13 - Analizar patrones anómalos y reconstrucciones de eventos mediante PLN, minería de logs y correlación multifuente en entornos forenses distribuidos. TIPO: Conocimientos o contenidos

CSV: 985778453469842713302612 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

RE14 - Formular propuestas innovadoras para la mejora de procesos de ciberinteligencia en entornos aplicados de detección y respuesta digital. TIPO: Competencias
RE15 - Elaborar, presentar y defender un trabajo original en el ámbito de la inteligencia artificial aplicada a la ciberseguridad, integrando conocimientos, habilidades y competencias adquiridas. TIPO: Competencias
RE2 - Evaluar la efectividad de arquitecturas defensivas resilientes en entornos distribuidos, integrando mecanismos de respuesta automatizada, aprendizaje supervisado y orquestación híbrida de incidentes. TIPO: Competencias
RE3 - Diseñar estrategias de orquestación inteligente de incidentes, basadas en sistemas SOAR, priorización dinámica y simulación de escenarios críticos en infraestructuras distribuidas. TIPO: Habilidades o destrezas
RE4 - Interpretar métricas de evaluación en modelos predictivos orientados a la detección de amenazas de ciberseguridad. TIPO: Conocimientos o contenidos
RE5 - Integrar técnicas de explicabilidad algorítmica en sistemas de inteligencia artificial aplicados a la seguridad. TIPO: Competencias
RE6 - Desarrollar entornos de simulación para validar sistemas defensivos basados en inteligencia artificial. TIPO: Habilidades o destrezas
RE7 - Evaluar riesgos de privacidad, robustez y trazabilidad en entornos cloud, edge e IoT, aplicando técnicas criptográficas y estándares de cumplimiento normativo. TIPO: Conocimientos o contenidos
RE8 - Diseñar políticas de cumplimiento normativo en contextos de inteligencia artificial y ciberseguridad. TIPO: Competencias
RE9 - Analizar el impacto legal y social del uso de sistemas autónomos digitales en entornos regulados. TIPO: Conocimientos o contenidos
RG1 - Evaluar el impacto de los sistemas de inteligencia artificial en la ciberseguridad, considerando su resiliencia, trazabilidad, riesgos operativos y capacidad de respuesta ante amenazas adversarias. TIPO: Competencias
RG2 - Aplicar metodologías avanzadas de análisis y aprendizaje automático para resolver problemas complejos en entornos digitales distribuidos y regulados dentro del ámbito de la ciberseguridad. TIPO: Competencias
RG3 - Diseñar e integrar soluciones de inteligencia artificial en arquitecturas resilientes, incorporando sistemas de defensa autónoma, respuesta parametrizada y recuperación operativa. TIPO: Habilidades o destrezas
RG4 - Crear entornos virtuales de simulación y pruebas para la detección, análisis y evaluación de ciberamenazas emergentes, mediante técnicas de inteligencia artificial, incluyendo ataques adversarios y extracción de modelos (model extraction). TIPO: Competencias
RG5 - Formular propuestas interdisciplinarias basadas en inteligencia artificial aplicada a la ciberseguridad, alineadas con estándares profesionales, criterios de explicabilidad y políticas de cumplimiento normativo. TIPO: Competencias
RT1 - Aplicar las nuevas tecnologías como herramientas para el intercambio comunicacional en el desarrollo de procesos de indagación y de aprendizaje. (Resultado de aprendizaje transversal relacionado con el modelo pedagógico de la Universidad) TIPO: Habilidades o destrezas
RT2 - Desarrollar habilidades de comunicación, para redactar informes y documentos, así como realizar eficaces presentaciones. (Resultado de aprendizaje transversal relacionado con el modelo pedagógico de la Universidad) TIPO: Habilidades o destrezas

3. ADMISIÓN, RECONOCIMIENTO Y MOVILIDAD

3.1 REQUISITOS DE ACCESO Y PROCEDIMIENTOS DE ADMISIÓN

3.1. Requisitos de acceso y procedimientos de admisión de estudiantes

El órgano encargado de la gestión del proceso de admisión es el Departamento de Admisiones en su vertiente Nacional e Internacional.

La admisión definitiva en el título es competencia de la Comisión de Admisiones del título, que está compuesta por, al menos:

- Responsable del título (que puede delegar en un profesor del título).
- Responsable de Acceso y Verificaciones.

De acuerdo con el artículo 18 del Real Decreto 822/2021, de 28 de septiembre, por el que se establece la organización de las enseñanzas universitarias y del procedimiento de aseguramiento de su calidad, para el acceso a las enseñanzas oficiales de máster se requiere:

1. La posesión de un título universitario oficial de Graduada o Graduado español o equivalente es condición para acceder a un Máster Universitario, o en su caso disponer de otro título de Máster Universitario, o títulos del mismo nivel que el título español de Grado o Máster expedidos por universidades e instituciones de educación superior de un país del EEES que en dicho país permita el acceso a los estudios de Máster.

2. De igual modo, podrán acceder a un Máster Universitario del sistema universitario español personas en posesión de títulos procedentes de sistemas educativos que no formen parte del EEES, que equivalgan al título de Grado, sin necesidad de homologación del título, pero sí de comprobación por parte de la universidad del nivel de formación que implican, siempre y cuando en el país donde se haya expedido dicho título permita acceder a estu-

CSV: 985778453469842713302612 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

dios de nivel de postgrado universitario. En ningún caso el acceso por esta vía implicará la homologación del título previo del que disponía la persona interesada ni su reconocimiento a otros efectos que el de realizar los estudios de Máster.

Requisitos de acceso específicos de este título

~~ACCESO DIRECTO SIN COMPLEMENTOS DE FORMACIÓN~~

Además de cumplir con los requisitos legales de acceso establecidos en la normativa vigente, se requiere que los estudiantes que accedan al máster cumplan alguno de los siguientes criterios:

1. Estén en posesión de alguno de los títulos considerados como afines al título propuesto, es decir, sean titulados universitarios en Ingeniería Informática, Ingeniería de Software, Ingeniería de Computadores, Ciberseguridad, Ciencias de la Computación, Ciencia de Datos o Ingeniería de Telecomunicaciones o titulaciones que puedan ser consideradas equivalentes por la comisión de admisiones; en estos casos el estudiante deberá entregar información que demuestre que se han cursado y superado las materias que permiten adquirir un perfil competencial similar al de las titulaciones mencionadas. La Comisión de Admisiones determinará si el título aportado cumple este requisito.
2. Cumpliendo los requisitos de acceso que indica la legislación, también podrán acceder al máster aquellos estudiantes que, en línea con el perfil de egreso de la titulación, demuestren haber cursado al menos 250 horas lectivas de formación universitaria específica en los ámbitos de la **inteligencia artificial** y/o de la **ciberseguridad**. A partir de la documentación aportada, la comisión de admisiones deberá decidir si la formación recibida tiene la calidad suficiente como para que el estudiante pueda seguir el máster de forma adecuada. Estar en posesión de una titulación universitaria que pueda ser considerada equivalente por la Comisión de Admisiones. En estos casos, el estudiante deberá aportar documentación que justifique que ha cursado y superado asignaturas que garanticen un perfil competencial equivalente al de las titulaciones anteriores. La Comisión de Admisiones determinará si el título presentado se ajusta a los requisitos.
3. Cumpliendo los requisitos de acceso que indica la legislación, acrediten experiencia profesional demostrable, con **no menos de dos años de experiencia con dedicación completa, o tiempo equivalente en el caso de dedicación parcial, realizando tareas relacionadas con el ámbito del título**:
    - Desarrollo o mantenimiento de sistemas de ciberseguridad en entornos distribuidos.
    - Diseño o implementación de arquitecturas seguras.
    - Gestión de incidentes de ciberseguridad con análisis de eventos y registros.
    - Análisis de amenazas mediante técnicas de análisis operativo en entornos de ciberseguridad.
    - Desarrollo de *software*, sistemas distribuidos o soluciones basadas en inteligencia artificial aplicadas a la seguridad.

Se solicitará certificado de empresa/institución que acredite la experiencia profesional descrita.

~~ACCESO CON COMPLEMENTOS DE FORMACIÓN~~

~~Adicionalmente, junto con los candidatos que acceden a través del acceso directo, según los requisitos previamente indicados, podrán acceder cursando complementos de formación los interesados que se detallan a continuación.~~

~~Así, con el objetivo de nivelar la formación de los estudiantes del máster, a aquellos que no puedan acreditar poseer los necesarios conocimientos previos para un normal seguimiento del plan de estudios, es decir, aquellos candidatos que provengan de titulaciones universitarias en:~~

- ~~Ingeniería Industrial, Ingeniería Electrónica, así como otras ingenierías técnicas.~~
- ~~Titulados universitarios en Matemáticas, Física o Estadística.~~

~~se les ofertarán los siguientes complementos de formación que se describen con detalle a continuación:~~

1. ~~**Complemento de formación 1:** Introducción a las Arquitecturas Seguras y Sistemas Distribuidos (6 ECTS).~~
2. ~~**Complemento de formación 2:** Fundamentos de Inteligencia Artificial (6 ECTS).~~

~~En función de la titulación presentada para el acceso, las personas interesadas que no cumplan los requisitos para el acceso directo al máster deberán completar varios de los complementos de formación indicados (según los conocimientos que no puedan acreditar que poseen):~~

- ~~Candidatos con titulaciones universitarias en Matemáticas, Física, Estadística, Ingeniería Industrial, Ingeniería Electrónica, así como otras ingenierías técnicas: cursarían los **complementos de formación 1 y 2**.~~

Una vez satisfechos los requisitos específicos de acceso, y solo en caso de que la demanda de plazas exceda la oferta, la resolución de las solicitudes de admisión se realizará conforme al siguiente criterio de valoración:

- Nota media del expediente académico correspondiente a la titulación que otorga el acceso al máster (100%). En caso de empate, se priorizará en función del mayor número de matrículas de honor, sobresalientes, y así sucesivamente.

~~Datos de los Complementos formativos~~

~~**Complemento de Formación 1:** **Introducción a las Arquitecturas Seguras y Sistemas Distribuidos**~~
~~**Créditos ECTS:** 6~~
~~RESULTADOS DE APRENDIZAJE~~
~~Al finalizar este complemento, el estudiante será capaz de:~~ • ~~Identificar los componentes críticos de una arquitectura distribuida segura.~~ • ~~Conocer las topologías de red y esquemas de control de acceso orientados a la resiliencia organizativa.~~ • ~~Identificar y analizar vulnerabilidades comunes en sistemas distribuidos empresariales.~~ • ~~Conocer principios de diseño seguro en entornos multiusuario y arquitecturas híbridas basadas en la nube.~~
~~CONTENIDOS~~
• ~~Modelos de computación distribuida y virtualización.~~ • ~~Diseño de sistemas seguros: control de acceso, segmentación de red y gestión de registros (*logs*).~~

CSV: 985778453469842713302612 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

- Ide Análisis de vectores de ataque en infraestructuras distribuidas.
- Introducción a *DevSecOps* y seguridad en pipelines de desarrollo.

ACTIVIDADES FORMATIVAS	HORAS	% INTERACCIÓN VIRTUAL SÍNCRONA
Sesiones virtuales síncronas	4	100 %
Recursos didácticos audiovisuales	10	0%
Estudio del material básico	43	0%
Lectura del material complementario	39	0%
Trabajos, casos prácticos	32	0%
Test de evaluación	6	0%
Tutorías	16	0%
Total	**150 horas**	-

SISTEMA DE EVALUACIÓN	PONDERACIÓN MÍN.	PONDERACIÓN MÁX.
Participación del estudiante	1 %	20 %
Trabajos, proyectos y/o casos	50 %	70 %
Test de evaluación	10 %	30 %

Complemento de Formación 2: Fundamentos de Inteligencia Artificial

Créditos ECTS: 6

RESULTADOS DE APRENDIZAJE

Al finalizar este complemento, el estudiante será capaz de:

- Comprender los conceptos fundamentales de la inteligencia artificial necesarios para el análisis y resolución de problemas tecnológicos.
- Modelar problemas mediante representaciones basadas en lógicas, reglas y datos.
- Diseñar e implementar modelos de aprendizaje supervisados y no supervisados.
- Aplicar técnicas de clasificación, regresión y agrupamiento
- Evaluar la eficacia y el comportamiento básico de modelos predictivos mediante métricas estándar y técnicas de validación.

CONTENIDOS

- Fundamentos de la inteligencia artificial.
- Representación del conocimiento y razonamiento.
- Fundamentos del aprendizaje automático: aprendizaje supervisado, no supervisado.
- Técnicas de clasificación, regresión y *clustering*.
- Introducción a redes neuronales y aprendizaje profundo.
- Evaluación y validación de modelos predictivos.

ACTIVIDADES FORMATIVAS	HORAS	% INTERACCIÓN VIRTUAL SÍNCRONA
Sesiones virtuales síncronas	4	100 %
Recursos didácticos audiovisuales	10	0
Estudio del material básico	43	0
Lectura del material complementario	39	0
Trabajos, casos prácticos	32	0
Test de evaluación	6	0
Tutorías	16	0
Total	**150 horas**	-

SISTEMA DE EVALUACIÓN	PONDERACIÓN MÍN.	PONDERACIÓN MÁX.
Participación del estudiante	1 %	20 %
Trabajos, proyectos y/o casos	50 %	70 %
Test de evaluación	10 %	30 %

CSV: 985778453469842713302612 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

REGLAMENTO DE ACCESO Y ADMISIÓN A ESTUDIOS OFICIALES DE LA UNIVERSIDAD INTERNACIONAL DE LA RIOJA

Se aporta el enlace que consta en la página web de la Universidad:

https://static.unir.net/documentos/reglamento_acceso_admision_e_o_unir.pdf

Teniendo en cuenta lo indicado por la normativa vigente respecto a la extensión máxima de las memorias de títulos oficiales, limitada a 10 000 palabras.

3.2 CRITERIOS PARA EL RECONOCIMIENTO Y TRANSFERENCIAS DE CRÉDITOS	
Reconocimiento de Créditos cursados en centros de formación profesional de grado superior	
MÍNIMO	**MÁXIMO**
0	0
Adjuntar Convenio	
Reconocimiento de Créditos Cursados en Títulos Propios	
MÍNIMO	**MÁXIMO**
0	9
Adjuntar Título Propio	
Reconocimiento de Créditos Cursados por Acreditación de Experiencia Laboral y Profesional	
MÍNIMO	**MÁXIMO**
0	6

DESCRIPCIÓN

Reconocimiento de Créditos Cursados en Títulos Propios

De acuerdo con lo establecido en el art. 10.4 del Real Decreto 822/2021, podrán ser objeto de reconocimiento los créditos cursados en enseñanzas universitarias conducentes a la obtención de títulos propios o de formación permanente. No obstante, se fijan, de acuerdo con la Normativa de UNIR de reconocimiento y transferencia de créditos, los siguientes límites y criterios para poder proceder a este reconocimiento:

- El máximo de créditos que podrá ser objeto de reconocimiento, tanto por experiencia profesional o laboral previa, como por haber superado estas enseñanzas universitarias no oficiales, no podrá ser superior, en su conjunto, a 9 créditos, correspondientes, según el artículo 10.5 del RD 822/2021, al 15 % del total de créditos que constituyen el plan de estudios.
- El reconocimiento no incorporará calificación numérica ni computará a efectos de baremación de expediente.
- Solo se admitirán aquellos estudios propios o de formación permanente en los que se garantice una adecuada evaluación del proceso formativo. A tal fin, en ningún caso, la simple asistencia podrá ser medio suficiente para acreditar la adquisición de competencia alguna. Tampoco serán aceptadas las acreditaciones o certificaciones expedidas por Departamentos o unidades universitarias que no tengan claras competencias en materia de títulos no oficiales.
- De no estar específicamente delimitado el perfil competencial del estudio universitario no oficial de origen, solo será posible el reconocimiento en caso de que exista una inequívoca equivalencia entre los conocimientos y competencias adquiridas con alguna o algunas materias concretas del título de destino.

Reconocimiento de Créditos Cursados por Acreditación de Experiencia Laboral y Profesional

1) Parte del plan de estudios afectada por el reconocimiento.

La normativa vigente fija el límite máximo de reconocimiento a partir de experiencia profesional y laboral en el 15 % del total de créditos que constituyen el plan de estudios. En el caso de un máster de 60 ECTS, esto equivale a 9 ECTS.

Con base en lo anterior y teniendo en cuenta que la experiencia laboral y profesional aportada por el estudiante debe proporcionar los mismos resultados del proceso de formación y de aprendizaje que se adquieren con las asignaturas reconocidas, podrán ser objeto de reconocimiento por experiencia profesional y laboral~~, entre otras,~~ las siguientes:

- Gobernanza Algorítmica y Explicabilidad en Sistemas de Inteligencia Artificial (6 ECTS).
- ~~Ciberdefensa Autónoma y Orquestación de Incidentes Críticos (6 ECTS).~~

~~El Departamento de Reconocimiento y Transferencia de Créditos revisará la documentación aportada en cada caso. Asimismo, teniendo en cuenta la diversidad de experiencias profesionales que los estudiantes pueden aportar, se podrán realizar otros reconocimientos siempre que, siguiendo las directrices del Real Decreto 822/2021, dicha expe-~~

CSV: 985778453469842713302612 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

~~riencia se muestre estrechamente relacionada con los conocimientos, competencias y habilidades propias del título universitario oficial.~~

2) Definición del tipo de experiencia profesional y laboral que podrá ser reconocida y 3) Justificación de dicho reconocimiento en términos de resultados del proceso de formación y de aprendizaje ya que el perfil de egresados ha de ser el mismo.

La experiencia profesional y laboral acreditada podrá ser reconocida en forma de créditos que computarán a efectos de la obtención de un título oficial, siempre que dicha experiencia esté relacionada con los resultados del proceso de formación y de aprendizaje inherentes a dicho título.

La documentación aportada incluirá, en su caso, contrato laboral con alta en la Seguridad Social acreditado mediante certificado de vida laboral; credencial de prácticas de inserción profesional; certificados de formación de personal; memoria de actividades desempeñadas y/o cualquier otro documento que permita comprobar o poner de manifiesto la experiencia alegada y su relación con los resultados del proceso de formación y de aprendizaje inherentes al título.

El tipo de experiencia que se precisará para el reconocimiento de las asignaturas mencionadas será el que se describe en la siguiente tabla:

Materia	Asignatura (nº ECTS)	Resultados de aprendizaje Específicos	Justificación
~~Aplicaciones Avanzadas de Inteligencia Artificial en Ciberseguridad y Resiliencia~~	~~Ciberdefensa Autónoma y Orquestación de Incidentes Críticos (6 ECTS)~~	~~RE2, RE3, RE6, RE12~~	~~**Tipo de entidad:** Empresas especializadas en ciberseguridad, centros de operaciones de seguridad (SOC), departamentos de tecnología de organizaciones con infraestructuras digitales críticas, proveedores de servicios *cloud* con funciones de seguridad. **Duración:** Periodo mínimo de 360 horas. **Tareas desempeñadas:** Diseño y análisis de arquitecturas digitales seguras en entornos distribuidos; configuración y evaluación de mecanismos de detección y respuesta ante incidentes de ciberseguridad; análisis de la resiliencia de infraestructuras críticas frente a ciberataques; utilización de técnicas de automatización y apoyo algorítmico para la gestión de incidentes y la recuperación operativa.~~
Gobierno, Evaluación y Transparencia en Entornos Críticos	Gobernanza Algorítmica y Explicabilidad en Sistemas de Inteligencia Artificial (6 ECTS)	RE5, RE9, RE10	**Tipo de entidad:** Consultoras tecnológicas, empresas de desarrollo de sistemas basados en inteligencia artificial, unidades internas de cumplimiento normativo y protección de datos, organizaciones con sistemas automatizados sujetos a regulación. **Duración:** Periodo mínimo de 360 horas. **Tareas desempeñadas:** Análisis y evaluación de sistemas algorítmicos desde la perspectiva de la explicabilidad y la trazabilidad; elaboración de documentación técnica relacionada con el impacto legal y social de sistemas de inteligencia artificial; revisión de sistemas automatizados en entornos regulados; evaluación del cumplimiento normativo aplicable a la inteligencia artificial y la ciberseguridad.

CSV: 985778453469842713302612 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

Se aporta el enlace que consta en la página web de la Universidad: **https://static.unir.net/documentos/normativa-RTC.pdf**

Teniendo en cuenta lo indicado por la normativa vigente respecto a la extensión máxima de las memorias de títulos oficiales, limitada a 10 000 palabras.

3.3 MOVILIDAD DE LOS ESTUDIANTES PROPIOS Y DE ACOGIDA

Información indicada en el apartado de Anexos de la presente memoria; en concreto, en el Anexo I. (apartado 8.3. del aplicativo del Ministerio).

4. PLANIFICACIÓN DE LAS ENSEÑANZAS

4.1 ESTRUCTURA BÁSICA DE LAS ENSEÑANZAS

DESCRIPCIÓN DEL PLAN DE ESTUDIOS

Ver Apartado 4: Anexo 1.

4.1 SIN NIVEL 1

NIVEL 2: Bases Tecnológicas y Entornos Seguros para la Inteligencia Artificial Aplicada

4.1.1.1 Datos Básicos del Nivel 2

CARÁCTER	Obligatoria
ECTS NIVEL 2	18

DESPLIEGUE TEMPORAL: Cuatrimestral

ECTS Cuatrimestral 1	**ECTS Cuatrimestral 2**	**ECTS Cuatrimestral 3**
18		
ECTS Cuatrimestral 4	**ECTS Cuatrimestral 5**	**ECTS Cuatrimestral 6**
ECTS Cuatrimestral 7	**ECTS Cuatrimestral 8**	**ECTS Cuatrimestral 9**
ECTS Cuatrimestral 10	**ECTS Cuatrimestral 11**	**ECTS Cuatrimestral 12**

NIVEL 3: Diseño y Aplicación de Algoritmos de Inteligencia Artificial y Aprendizaje Automático

4.1.1.1.1 Datos Básicos del Nivel 3

CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
Obligatoria	6	Cuatrimestral

DESPLIEGUE TEMPORAL

ECTS Cuatrimestral 1	**ECTS Cuatrimestral 2**	**ECTS Cuatrimestral 3**
6		
ECTS Cuatrimestral 4	**ECTS Cuatrimestral 5**	**ECTS Cuatrimestral 6**
ECTS Cuatrimestral 7	**ECTS Cuatrimestral 8**	**ECTS Cuatrimestral 9**
ECTS Cuatrimestral 10	**ECTS Cuatrimestral 11**	**ECTS Cuatrimestral 12**

NIVEL 3: Criptografía Aplicada y Seguridad en Sistemas Distribuidos

4.1.1.1.1 Datos Básicos del Nivel 3

CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
Obligatoria	6	Cuatrimestral

DESPLIEGUE TEMPORAL

ECTS Cuatrimestral 1	**ECTS Cuatrimestral 2**	**ECTS Cuatrimestral 3**
6		
ECTS Cuatrimestral 4	**ECTS Cuatrimestral 5**	**ECTS Cuatrimestral 6**
ECTS Cuatrimestral 7	**ECTS Cuatrimestral 8**	**ECTS Cuatrimestral 9**
ECTS Cuatrimestral 10	**ECTS Cuatrimestral 11**	**ECTS Cuatrimestral 12**

CSV: 985778453469842713302612 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

NIVEL 3: Marco Ético y Regulatorio de la Inteligencia Artificial Aplicada a la Ciberseguridad		
4.1.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
Obligatoria	6	Cuatrimestral
DESPLIEGUE TEMPORAL		
ECTS Cuatrimestral 1	**ECTS Cuatrimestral 2**	**ECTS Cuatrimestral 3**
6		
ECTS Cuatrimestral 4	**ECTS Cuatrimestral 5**	**ECTS Cuatrimestral 6**
ECTS Cuatrimestral 7	**ECTS Cuatrimestral 8**	**ECTS Cuatrimestral 9**
ECTS Cuatrimestral 10	**ECTS Cuatrimestral 11**	**ECTS Cuatrimestral 12**
4.1.1.2 RESULTADOS DE APRENDIZAJE		
RE1 - Analizar algoritmos de aprendizaje automático aplicados a la detección de amenazas digitales. TIPO: Habilidades o destrezas		
RE10 - Aplicar marcos regulatorios como el Reglamento de Inteligencia Artificial (AI Act) y la Directiva NIS2 al diseño de soluciones tecnológicas. TIPO: Competencias		
RE13 - Analizar patrones anómalos y reconstrucciones de eventos mediante PLN, minería de logs y correlación multifuente en entornos forenses distribuidos. TIPO: Conocimientos o contenidos		
RE2 - Evaluar la efectividad de arquitecturas defensivas resilientes en entornos distribuidos, integrando mecanismos de respuesta automatizada, aprendizaje supervisado y orquestación híbrida de incidentes. TIPO: Competencias		
RE4 - Interpretar métricas de evaluación en modelos predictivos orientados a la detección de amenazas de ciberseguridad. TIPO: Conocimientos o contenidos		
RE5 - Integrar técnicas de explicabilidad algorítmica en sistemas de inteligencia artificial aplicados a la seguridad. TIPO: Competencias		
RE7 - Evaluar riesgos de privacidad, robustez y trazabilidad en entornos cloud, edge e IoT, aplicando técnicas criptográficas y estándares de cumplimiento normativo. TIPO: Conocimientos o contenidos		
RE8 - Diseñar políticas de cumplimiento normativo en contextos de inteligencia artificial y ciberseguridad. TIPO: Competencias		
RE9 - Analizar el impacto legal y social del uso de sistemas autónomos digitales en entornos regulados. TIPO: Conocimientos o contenidos		
RG1 - Evaluar el impacto de los sistemas de inteligencia artificial en la ciberseguridad, considerando su resiliencia, trazabilidad, riesgos operativos y capacidad de respuesta ante amenazas adversarias. TIPO: Competencias		
RG2 - Aplicar metodologías avanzadas de análisis y aprendizaje automático para resolver problemas complejos en entornos digitales distribuidos y regulados dentro del ámbito de la ciberseguridad. TIPO: Competencias		
RG3 - Diseñar e integrar soluciones de inteligencia artificial en arquitecturas resilientes, incorporando sistemas de defensa autónoma, respuesta parametrizada y recuperación operativa. TIPO: Habilidades o destrezas		
RT1 - Aplicar las nuevas tecnologías como herramientas para el intercambio comunicacional en el desarrollo de procesos de indagación y de aprendizaje. (Resultado de aprendizaje transversal relacionado con el modelo pedagógico de la Universidad) TIPO: Habilidades o destrezas		
RT2 - Desarrollar habilidades de comunicación, para redactar informes y documentos, así como realizar eficaces presentaciones. (Resultado de aprendizaje transversal relacionado con el modelo pedagógico de la Universidad) TIPO: Habilidades o destrezas		
NIVEL 2: Aplicaciones Avanzadas de Inteligencia Artificial en Ciberseguridad y Resiliencia		
4.1.1.1 Datos Básicos del Nivel 2		
CARÁCTER	Obligatoria	
ECTS NIVEL 2	24	
DESPLIEGUE TEMPORAL: Cuatrimestral		
ECTS Cuatrimestral 1	**ECTS Cuatrimestral 2**	**ECTS Cuatrimestral 3**
12	12	
ECTS Cuatrimestral 4	**ECTS Cuatrimestral 5**	**ECTS Cuatrimestral 6**
ECTS Cuatrimestral 7	**ECTS Cuatrimestral 8**	**ECTS Cuatrimestral 9**

CSV: 985778453469842713302612 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

ECTS Cuatrimestral 10	**ECTS Cuatrimestral 11**	**ECTS Cuatrimestral 12**
NIVEL 3: Inteligencia Artificial para Predicción de Amenazas y Ciberinteligencia Operativa		
4.1.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
Obligatoria	6	Cuatrimestral
DESPLIEGUE TEMPORAL		
ECTS Cuatrimestral 1	**ECTS Cuatrimestral 2**	**ECTS Cuatrimestral 3**
6		
ECTS Cuatrimestral 4	**ECTS Cuatrimestral 5**	**ECTS Cuatrimestral 6**
ECTS Cuatrimestral 7	**ECTS Cuatrimestral 8**	**ECTS Cuatrimestral 9**
ECTS Cuatrimestral 10	**ECTS Cuatrimestral 11**	**ECTS Cuatrimestral 12**
NIVEL 3: Agentes Autónomos y Técnicas Ofensivas Basadas en Inteligencia Artificial		
4.1.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
Obligatoria	6	Cuatrimestral
DESPLIEGUE TEMPORAL		
ECTS Cuatrimestral 1	**ECTS Cuatrimestral 2**	**ECTS Cuatrimestral 3**
6		
ECTS Cuatrimestral 4	**ECTS Cuatrimestral 5**	**ECTS Cuatrimestral 6**
ECTS Cuatrimestral 7	**ECTS Cuatrimestral 8**	**ECTS Cuatrimestral 9**
ECTS Cuatrimestral 10	**ECTS Cuatrimestral 11**	**ECTS Cuatrimestral 12**
NIVEL 3: Ciberdefensa Autónoma y Orquestación de Incidentes Críticos		
4.1.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
Obligatoria	6	Cuatrimestral
DESPLIEGUE TEMPORAL		
ECTS Cuatrimestral 1	**ECTS Cuatrimestral 2**	**ECTS Cuatrimestral 3**
	6	
ECTS Cuatrimestral 4	**ECTS Cuatrimestral 5**	**ECTS Cuatrimestral 6**
ECTS Cuatrimestral 7	**ECTS Cuatrimestral 8**	**ECTS Cuatrimestral 9**
ECTS Cuatrimestral 10	**ECTS Cuatrimestral 11**	**ECTS Cuatrimestral 12**
NIVEL 3: Análisis Forense Digital Automatizado con Inteligencia Artificial		
4.1.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
Obligatoria	6	Cuatrimestral
DESPLIEGUE TEMPORAL		
ECTS Cuatrimestral 1	**ECTS Cuatrimestral 2**	**ECTS Cuatrimestral 3**
	6	
ECTS Cuatrimestral 4	**ECTS Cuatrimestral 5**	**ECTS Cuatrimestral 6**
ECTS Cuatrimestral 7	**ECTS Cuatrimestral 8**	**ECTS Cuatrimestral 9**
ECTS Cuatrimestral 10	**ECTS Cuatrimestral 11**	**ECTS Cuatrimestral 12**

CSV: 985778453469842713302612 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

4.1.1.2 RESULTADOS DE APRENDIZAJE
RE1 - Analizar algoritmos de aprendizaje automático aplicados a la detección de amenazas digitales. TIPO: Habilidades o destrezas
RE11 - Desarrollar soluciones avanzadas mediante modelos generativos y agentes autónomos, incluyendo su aplicación controlada en contextos ofensivos y simulados. TIPO: Habilidades o destrezas
RE12 - Evaluar la resiliencia de infraestructuras críticas frente a ciberataques complejos. TIPO: Competencias
RE14 - Formular propuestas innovadoras para la mejora de procesos de ciberinteligencia en entornos aplicados de detección y respuesta digital. TIPO: Competencias
RE2 - Evaluar la efectividad de arquitecturas defensivas resilientes en entornos distribuidos, integrando mecanismos de respuesta automatizada, aprendizaje supervisado y orquestación híbrida de incidentes. TIPO: Competencias
RE3 - Diseñar estrategias de orquestación inteligente de incidentes, basadas en sistemas SOAR, priorización dinámica y simulación de escenarios críticos en infraestructuras distribuidas. TIPO: Habilidades o destrezas
RE4 - Interpretar métricas de evaluación en modelos predictivos orientados a la detección de amenazas de ciberseguridad. TIPO: Conocimientos o contenidos
RE5 - Integrar técnicas de explicabilidad algorítmica en sistemas de inteligencia artificial aplicados a la seguridad. TIPO: Competencias
RE6 - Desarrollar entornos de simulación para validar sistemas defensivos basados en inteligencia artificial. TIPO: Habilidades o destrezas
RG1 - Evaluar el impacto de los sistemas de inteligencia artificial en la ciberseguridad, considerando su resiliencia, trazabilidad, riesgos operativos y capacidad de respuesta ante amenazas adversarias. TIPO: Competencias
RG2 - Aplicar metodologías avanzadas de análisis y aprendizaje automático para resolver problemas complejos en entornos digitales distribuidos y regulados dentro del ámbito de la ciberseguridad. TIPO: Competencias
RG3 - Diseñar e integrar soluciones de inteligencia artificial en arquitecturas resilientes, incorporando sistemas de defensa autónoma, respuesta parametrizada y recuperación operativa. TIPO: Habilidades o destrezas
RG4 - Crear entornos virtuales de simulación y pruebas para la detección, análisis y evaluación de ciberamenazas emergentes, mediante técnicas de inteligencia artificial, incluyendo ataques adversarios y extracción de modelos (model extraction). TIPO: Competencias
RT1 - Aplicar las nuevas tecnologías como herramientas para el intercambio comunicacional en el desarrollo de procesos de indagación y de aprendizaje. (Resultado de aprendizaje transversal relacionado con el modelo pedagógico de la Universidad) TIPO: Habilidades o destrezas
RT2 - Desarrollar habilidades de comunicación, para redactar informes y documentos, así como realizar eficaces presentaciones. (Resultado de aprendizaje transversal relacionado con el modelo pedagógico de la Universidad) TIPO: Habilidades o destrezas

NIVEL 2: Gobierno, Evaluación y Transparencia en Entornos Críticos		
4.1.1.1 Datos Básicos del Nivel 2		
CARÁCTER	Obligatoria	
ECTS NIVEL 2	6	
DESPLIEGUE TEMPORAL: Cuatrimestral		
ECTS Cuatrimestral 1	ECTS Cuatrimestral 2	ECTS Cuatrimestral 3
	6	
ECTS Cuatrimestral 4	ECTS Cuatrimestral 5	ECTS Cuatrimestral 6
ECTS Cuatrimestral 7	ECTS Cuatrimestral 8	ECTS Cuatrimestral 9
ECTS Cuatrimestral 10	ECTS Cuatrimestral 11	ECTS Cuatrimestral 12

NIVEL 3: Gobernanza Algorítmica y Explicabilidad en Sistemas de Inteligencia Artificial		
4.1.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	ECTS ASIGNATURA	DESPLIEGUE TEMPORAL
Obligatoria	6	Cuatrimestral
DESPLIEGUE TEMPORAL		
ECTS Cuatrimestral 1	ECTS Cuatrimestral 2	ECTS Cuatrimestral 3
	6	

CSV: 985778453469842713302612 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

ECTS Cuatrimestral 4	**ECTS Cuatrimestral 5**	**ECTS Cuatrimestral 6**
ECTS Cuatrimestral 7	**ECTS Cuatrimestral 8**	**ECTS Cuatrimestral 9**
ECTS Cuatrimestral 10	**ECTS Cuatrimestral 11**	**ECTS Cuatrimestral 12**
4.1.1.2 RESULTADOS DE APRENDIZAJE		
RE10 - Aplicar marcos regulatorios como el Reglamento de Inteligencia Artificial (AI Act) y la Directiva NIS2 al diseño de soluciones tecnológicas. TIPO: Competencias		
RE5 - Integrar técnicas de explicabilidad algorítmica en sistemas de inteligencia artificial aplicados a la seguridad. TIPO: Competencias		
RE9 - Analizar el impacto legal y social del uso de sistemas autónomos digitales en entornos regulados. TIPO: Conocimientos o contenidos		
RG5 - Formular propuestas interdisciplinarias basadas en inteligencia artificial aplicada a la ciberseguridad, alineadas con estándares profesionales, criterios de explicabilidad y políticas de cumplimiento normativo. TIPO: Competencias		
RT1 - Aplicar las nuevas tecnologías como herramientas para el intercambio comunicacional en el desarrollo de procesos de indagación y de aprendizaje. (Resultado de aprendizaje transversal relacionado con el modelo pedagógico de la Universidad) TIPO: Habilidades o destrezas		
RT2 - Desarrollar habilidades de comunicación, para redactar informes y documentos, así como realizar eficaces presentaciones. (Resultado de aprendizaje transversal relacionado con el modelo pedagógico de la Universidad) TIPO: Habilidades o destrezas		
NIVEL 2: Trabajo Fin de Máster		
4.1.1.1 Datos Básicos del Nivel 2		
CARÁCTER	Trabajo Fin de Grado / Máster	
ECTS NIVEL 2	12	
DESPLIEGUE TEMPORAL: Cuatrimestral		
ECTS Cuatrimestral 1	**ECTS Cuatrimestral 2**	**ECTS Cuatrimestral 3**
	12	
ECTS Cuatrimestral 4	**ECTS Cuatrimestral 5**	**ECTS Cuatrimestral 6**
ECTS Cuatrimestral 7	**ECTS Cuatrimestral 8**	**ECTS Cuatrimestral 9**
ECTS Cuatrimestral 10	**ECTS Cuatrimestral 11**	**ECTS Cuatrimestral 12**
NIVEL 3: Trabajo Fin de Máster		
4.1.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
Trabajo Fin de Grado / Máster	12	Cuatrimestral
DESPLIEGUE TEMPORAL		
ECTS Cuatrimestral 1	**ECTS Cuatrimestral 2**	**ECTS Cuatrimestral 3**
	12	
ECTS Cuatrimestral 4	**ECTS Cuatrimestral 5**	**ECTS Cuatrimestral 6**
ECTS Cuatrimestral 7	**ECTS Cuatrimestral 8**	**ECTS Cuatrimestral 9**
ECTS Cuatrimestral 10	**ECTS Cuatrimestral 11**	**ECTS Cuatrimestral 12**
4.1.1.2 RESULTADOS DE APRENDIZAJE		
RE15 - Elaborar, presentar y defender un trabajo original en el ámbito de la inteligencia artificial aplicada a la ciberseguridad, integrando conocimientos, habilidades y competencias adquiridas. TIPO: Competencias		
RG2 - Aplicar metodologías avanzadas de análisis y aprendizaje automático para resolver problemas complejos en entornos digitales distribuidos y regulados dentro del ámbito de la ciberseguridad. TIPO: Competencias		
RG4 - Crear entornos virtuales de simulación y pruebas para la detección, análisis y evaluación de ciberamenazas emergentes, mediante técnicas de inteligencia artificial, incluyendo ataques adversarios y extracción de modelos (model extraction). TIPO: Competencias		

CSV: 985778453469842713302612 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

RG5 - Formular propuestas interdisciplinarias basadas en inteligencia artificial aplicada a la ciberseguridad, alineadas con estándares profesionales, criterios de explicabilidad y políticas de cumplimiento normativo. TIPO: Competencias
RT1 - Aplicar las nuevas tecnologías como herramientas para el intercambio comunicacional en el desarrollo de procesos de indagación y de aprendizaje. (Resultado de aprendizaje transversal relacionado con el modelo pedagógico de la Universidad) TIPO: Habilidades o destrezas
RT2 - Desarrollar habilidades de comunicación, para redactar informes y documentos, así como realizar eficaces presentaciones. (Resultado de aprendizaje transversal relacionado con el modelo pedagógico de la Universidad) TIPO: Habilidades o destrezas
NO CONSTAN ELEMENTOS DE NIVEL 2

4.2 ACTIVIDADES Y METODOLOGÍAS DOCENTES

ACTIVIDADES FORMATIVAS

Denominación de las actividades formativas según las definiciones y datos aportados en el apartado 4.1.
Sesiones virtuales síncronas
Recursos didácticos audiovisuales
Estudio del material básico
Lectura del material complementario
Test de evaluación
Trabajos y casos prácticos
Laboratorios virtuales
Tutorías
Sesión inicial de presentación de Trabajo Fin de Máster
Lectura de material en el aula virtual (TFM)
Tutorías (TFM)
Sesiones grupales de Trabajo Fin de Máster
Elaboración del Trabajo Fin de Máster
Exposición del Trabajo Fin de Máster

Adicionalmente, en el PDF del apartado 4.1. se indican las definiciones de las actividades formativas, así como su asignación en horas y porcentaje de interacción virtual síncrona, o porcentaje de presencialidad física en su caso, en las diferentes materias del título.

METODOLOGÍAS DOCENTES

Metodologías docentes	
MD1	**Métodos de enseñanza magistral con mediación tecnológica:** aquí se incluirían las clases virtuales síncronas, recursos didácticos audiovisuales, seminarios monográficos, etc. Este tipo de actividades promueven el conocimiento por comprensión y, en virtud de la función motivacional que cumplen los múltiples recursos tecnológicos utilizados, superan las limitaciones de la enseñanza meramente transmisiva, creando en el estudiante la necesidad de seguir aprendiendo e involucrándole en su propio proceso de aprendizaje.
MD2	**Métodos activos:** son métodos de enseñanza y aprendizaje basados en la actividad, participación y aprendizaje significativo del alumnado (estudio de casos, aprendizaje cooperativo, método por proyectos, aprendizaje basado en problemas y/o aprendizaje - servicio, etc.). En este tipo de metodologías adquiere protagonismo el trabajo colegiado y cooperativo, sin llegar a prescindir del aprendizaje autónomo de cada estudiante.
MD3	**Métodos fundamentados en el aprendizaje individual:** estudio personal, aprendizaje acompañado a través de lecturas de material complementario, realización de actividades individuales. Dichos métodos permiten que el estudiante establezca un ritmo de estudio, marque sus propios objetivos de aprendizaje, y planifique, organice y autoevalúe su trabajo.

Adicionalmente, en el PDF del apartado 4.1. se indica la asignación de las metodologías docentes a las diferentes materias del título.

4.3 SISTEMAS DE EVALUACIÓN

Denominación de los sistemas de evaluación según las definiciones y datos aportados en el apartado 4.1.
Participación del estudiante
Trabajos~~, laboratorios~~ y/o casos
Evaluación de laboratorios virtuales
~~Test de evaluación~~
Examen final
Evaluación de la estructura del Trabajo Fin de Máster
Evaluación de la exposición del Trabajo Fin de Máster
Evaluación del contenido individual del Trabajo Fin de Máster

CSV: 985778453469842713302612 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

Adicionalmente, en el PDF del apartado 4.1. se indican las definiciones de los sistemas de evaluación, así como su asignación a las diferentes materias del título y sus ponderaciones mínimas y máximas correspondientes.

4.4 ESTRUCTURAS CURRICULARES ESPECÍFICAS

CSV: 985778453469842713302612 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

5. PERSONAL ACADÉMICO Y DE APOYO A LA DOCENCIA

PERSONAL ACADÉMICO
Ver Apartado 5: Anexo 1.
OTROS RECURSOS HUMANOS
Ver Apartado 5: Anexo 2.

6. RECURSOS MATERIALES E INFRAESTRUCTURALES, PRÁCTICAS Y SERVICIOS

Justificación de que los medios materiales disponibles son adecuados: Ver Apartado 6: Anexo 1.

7. CALENDARIO DE IMPLANTACIÓN

7.1 CRONOGRAMA DE IMPLANTACIÓN	
CURSO DE INICIO	2026
Ver Apartado 7: Anexo 1.	
7.2 PROCEDIMIENTO DE ADAPTACIÓN	
No aplica	
7.3 ENSEÑANZAS QUE SE EXTINGUEN	
CÓDIGO	**ESTUDIO - CENTRO**

8. SISTEMA INTERNO DE GARANTÍA DE LA CALIDAD Y ANEXOS

8.1 SISTEMA INTERNO DE GARANTÍA DE LA CALIDAD	
ENLACE	http://www.unir.net/universidad-online/manual-calidad-procedimientos/
8.2 INFORMACIÓN PÚBLICA	

8.2. Medios de información pública relevante

8.2.1. Canales de difusión de la información y su gestión

Para informar tanto al estudiantado, previamente a su matriculación y durante el proceso de formación y aprendizaje, como al profesorado, a los empleadores y a la sociedad en su conjunto se dispone de la **página web oficial de la Universidad Internacional de La Rioja** donde se aporta la información sobre las características del título (resultados de aprendizaje, temporalización del plan de estudios que incluye asignaturas, actividades formativas y sistemas de evaluación), sistemas de acceso y admisión, idioma de impartición, etc.

La Universidad dispone de sistemas para el **control periódico de la información** disponible en la página web. Por ello, se verifica periódicamente que la información disponible en la página web del título es suficientemente completa, adecuada y relevante para el estudiantado. El coordinador académico del título hace constar en el informe anual de la Unidad de Calidad de Titulación (UCT) esta revisión periódica.

Información pública relevante del plan de estudios

UNIR pone a disposición del estudiantado, el profesorado, los empleadores y la sociedad en su conjunto toda la información actualizada del plan de estudios a través de las guías docentes disponibles en la página web de la Universidad. Así, a través de la guía docente de cada una de las asignaturas que forman el plan de estudios, se puede acceder a la siguiente información:

- **Presentación**: describe el objetivo de la asignatura y cómo su contenido es relevante para el desarrollo del plan de estudios.
- **Competencias**: se enumeran y describen las competencias y/o resultados de aprendizaje desarrollados en el título.
- **Contenidos**: se detalla por temas el contenido desarrollado en la asignatura.
- **Metodología**: se describen las actividades formativas de la asignatura especificando las horas de dedicación indicadas en la memoria para cada actividad formativa, así como su presencialidad.

Además, se incluye la distribución temporal prevista para la asignatura.

- **Bibliografía**: se detalla la bibliografía básica, considerada imprescindible para el estudio de la asignatura, así como, en su caso, la bibliografía complementaria, para ayudar a profundizar más en los temas de mayor interés.
- **Evaluación y calificación**: se detallan los sistemas de evaluación y sus porcentajes de evaluación, así como los requisitos específicos, en su caso, para aprobar la asignatura.
- **Profesorado**: se presentan los datos básicos del profesor encargado de impartir la asignatura.
- **Orientaciones para el estudio**: se dan orientaciones al estudiante de cómo organizar el estudio de la asignatura, así como diferentes consejos para un adecuado seguimiento de la asignatura.

8.2.2. Sistemas de información previa: información transparente y accesible

Con carácter general, por parte de UNIR se pondrá a disposición de los potenciales estudiantes toda la información necesaria para que puedan realizar la elección de su titulación con los mayores elementos de juicio posibles. **Se garantiza una información transparente y accesible sobre los requisitos de acceso específicos para el título y los procedimientos de admisión, descritos en la presente memoria**, estando disponibles a través de la página web de la Universidad para todos los grupos de interés del título.

En las condiciones de matrícula, disponibles en el apartado normativa de la página web de la universidad, se alude a los requisitos tecnológicos e informáticos precisos para seguir el curso adecuadamente, dichas condiciones son conocidas y firmadas por el estudiante al matricularse de sus estudios.

CSV: 985778453469842713302612 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

En relación a las competencias y conocimientos digitales para seguir la actividad docente programada:

Las competencias digitales que los estudiantes de UNIR precisarán tener para el manejo del campus y correcto desarrollo en la plataforma, serán conocimientos a nivel de usuario de distintos programas (esencialmente del paquete Office), así como nociones básicas sobre navegación por internet.

El estudiante que se matricula en UNIR además cuenta con un período de adecuación a la metodología virtual con apoyo del personal no docente de asistencia.

Por último, desde UNIR se ofrecerá a todos los estudiantes los programas adicionales necesarios que sean específicos para cada titulación que podrán descargar fácilmente desde su campus virtual o a través de cualquier otro enlace accesible o usarse desde las máquinas virtuales habilitadas para tal fin.

Teniendo en cuenta que la rápida evolución en los requisitos de las aplicaciones puede variar rápidamente, una configuración mínima recomendada podría ser:

- 8 GB de RAM.
- Conexión a Internet superior a 6 Mbit/s (>1Mbit/s de subida).
- 250 GB de disco duro.
- Procesador equivalente o superior a Intel i5 / AMD Ryzen 5
- Tarjeta gráfica y monitor básico (1024x768 o superior).
- Tarjeta de sonido y altavoces o auriculares para poder utilizar el material multimedia.
- Webcam y micrófono si se desea participar en conversaciones *face-to-face* con el profesor u otros estudiantes.
- Sistema operativo Windows, Mac OS o Linux.
- Acceso de administrador al sistema.
- Navegador web Chrome, Safari, Microsoft Edge o Firefox actualizado.

8.2.3. Procedimientos de orientación para la admisión y matriculación de estudiantes de nuevo ingreso

UNIR cuenta con una oficina de Atención al Estudiante que centraliza y contesta todas las solicitudes de información (llamadas y correos electrónicos) y un Servicio Técnico de Orientación (*contact center*) que gestiona y soluciona todas las preguntas y posibles dudas de los futuros estudiantes referidas a:

- Descripción de la metodología de UNIR. Para ello, los estudiantes tendrán acceso a una demo donde se explica paso por paso.
- Niveles de dificultad y horas de estudio estimadas para poder llevar a cabo un itinerario formativo ajustado a las posibilidades reales del estudiante para poder planificar adecuadamente su matrícula.
- Descripción de los estudios.
- Convalidaciones de las antiguas titulaciones.
- Preguntas sobre el Espacio Europeo de Educación Superior.

Finalmente, el personal de gestión y administración (PGA) a través del Servicio de Admisiones proporcionará al estudiante todo el apoyo administrativo necesario para realizar de manera óptima todo el proceso de admisión y matriculación por medio de atención telefónica o por correo electrónico, con información guiada en la web para la realización de la matrícula *online*.

8.3 ANEXOS
Ver Apartado 8: Anexo 1.

PERSONAS ASOCIADAS A LA SOLICITUD

RESPONSABLE DEL TÍTULO			
CARGO	**NOMBRE**	**PRIMER APELLIDO**	**SEGUNDO APELLIDO**
Director de la Escuela Superior de Ingeniería y Tecnología	Óscar	Sanjuan	Martínez
DOMICILIO	**CÓDIGO POSTAL**	**PROVINCIA**	**MUNICIPIO**
Avenida de la Paz, 137	26006	La Rioja	Logroño
EMAIL	**FAX**		
virginia.montiel@unir.net			

REPRESENTANTE LEGAL			
CARGO	**NOMBRE**	**PRIMER APELLIDO**	**SEGUNDO APELLIDO**
Secretario General	Juan Pablo	Guzmán	Palomino
DOMICILIO	**CÓDIGO POSTAL**	**PROVINCIA**	**MUNICIPIO**
Avenida de la Paz, 137	26006	La Rioja	Logroño
EMAIL	**FAX**		
virginia.montiel@unir.net			

El Rector de la Universidad no es el Representante Legal
Ver Personas asociadas a la solicitud: Anexo 1.

CSV: 985778453469842713302612 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

SOLICITANTE			
El responsable del título no es el solicitante			
CARGO	**NOMBRE**	**PRIMER APELLIDO**	**SEGUNDO APELLIDO**
Responsable de programas ANECA	Virginia	Montiel	Martín
DOMICILIO	**CÓDIGO POSTAL**	**PROVINCIA**	**MUNICIPIO**
Avenida de la Paz, 137	26006	La Rioja	Logroño
EMAIL	**FAX**		
virginia.montiel@unir.net			

INFORME PREVIO DE LA COMUNIDAD AUTÓNOMA

Informe previo de la Comunidad Autónoma: Ver Apartado Informe previo de la Comunidad Autónoma: Anexo 1.

CSV: 985778453469842713302612 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

Apartado 1: Anexo 6

Nombre : Alegaciones_Justificacion (11).pdf

HASH SHA1 :29B52BDED32F8FA3B25D5483792B1E07B68EA805

Código CSV :98531553570106721274572 5

Ver Fichero: Alegaciones_Justificacion (11).pdf

CSV: 985778453469842713302612 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

Apartado 4: Anexo 1

Nombre :4.1. Planificación de las enseñanzas (16).pdf

HASH SHA1 :5A96BE37EA7D81F6B690B5E5558C86AEA086B8E8

Código CSV :985301036252122116654596

Ver Fichero: 4.1. Planificación de las enseñanzas (16).pdf

CSV: 985778453469842713302612 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

Apartado 5: Anexo 1

Nombre :5.1. Personal académico (10).pdf

HASH SHA1 :4502C8F23A8D9E224DF7411F1CF937E768E05042

Código CSV :98529365286105459361213 3

Ver Fichero: 5.1. Personal académico (10).pdf

CSV: 985778453469842713302612 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

Apartado 5: Anexo 2

Nombre :5.2. Otros recursos humanos.pdf

HASH SHA1 :0B09DA7E7BF6F29E328F6123EDAF00AE0D2908C7

Código CSV :985045754183222893548721

Ver Fichero: 5.2. Otros recursos humanos.pdf

CSV: 985778453469842713302612 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

Apartado 6: Anexo 1

Nombre :6. Recursos materiales.pdf

HASH SHA1 :81663E96B958F79BFAD8F5C95992543DE2E7ADF9

Código CSV :98504584389597335920644O

Ver Fichero: 6. Recursos materiales.pdf

CSV: 985778453469842713302612 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

Apartado 7: Anexo 1

Nombre :7.pdf

HASH SHA1 :6ED7548EDDAEF56855D5563ACBDC616E2E5D54CC

Código CSV :955011187198767173601148

Ver Fichero: 7.pdf

CSV: 985778453469842713302612 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

Apartado 8: Anexo 1

Nombre :8.3.pdf

HASH SHA1 :4720971050F73ED4C3FA4BCA3183D41E6C47BE49

Código CSV :95501140747082514134319 4

Ver Fichero: 8.3.pdf

CSV: 985778453469842713302612 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

Apartado Personas asociadas a la solicitud: Anexo 1

Nombre : Delegacion_Representante_Legal_PABLO_GUZMAN_18052016.pdf

HASH SHA1 :1E53A88EBC8422AC49E10BE3782E07823D3DA297

Código CSV :955011768553711432636727

Ver Fichero: Delegacion_Representante_Legal_PABLO_GUZMAN_18052016.pdf

CSV: 985778453469842713302612 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

Apartado Informe previo de la Comunidad Autónoma: Anexo 1

Nombre : Informe previo MU en Inteligencia Artificial aplicada a la Ciberseguridad.pdf

HASH SHA1 :FA22D78D5BF72767F1A48209E18FA44CFEA0B5A9

Código CSV :95153701791131520829382 2

Ver Fichero: Informe previo MU en Inteligencia Artificial aplicada a la Ciberseguridad.pdf

CSV: 985778453469842713302612 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es

CSV: 985778453469842713302612 - Verificable en https://sede.educacion.gob.es/cid y Carpeta Ciudadana https://sede.administracion.gob.es