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	Facultad de Derecho	26004020
NIVEL	**DENOMINACIÓN CORTA**	
Máster	Ciberdelincuencia	
DENOMINACIÓN ESPECÍFICA		
Máster Universitario en Ciberdelincuencia por la Universidad Internacional de La Rioja		
NIVEL MECES		
3		
RAMA DE CONOCIMIENTO	**ÁMBITO DE CONOCIMIENTO**	**CONJUNTO**
Ciencias Sociales y Jurídicas	Interdisciplinar	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**	
María Dolores Arranz Madrid	Vicedecana de Desarrollo y Organización Académica de la Facultad	

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		902877037

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.

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 24 de enero de 2024
	Firma: Representante legal de la Universidad

1. DESCRIPCIÓN, OBJETIVOS FORMATIVOS Y JUSTIFICACIÓN DEL TÍTULO

1.1-1.3 DENOMINACIÓN, ÁMBITO, MENCIONES/ESPECIALIDADES Y OTROS DATOS BÁSICOS

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

RAMA
Ciencias Sociales y Jurídicas
ÁMBITO
Interdisciplinar
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		6
CRÉDITOS OPTATIVOS	**CRÉDITOS OBLIGATORIOS**	**CRÉDITOS TRABAJO FIN GRADO/ MÁSTER**
0	42	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**
26004020	Facultad de Derecho	Si	Si

1.4-1.9.2 Facultad de Derecho

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		
		300
NÚMERO TOTAL DE PLAZAS	**NÚMERO DE PLAZAS DE NUEVO INGRESO PARA PRIMER CURSO**	
300	300	
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
El máster tiene **una orientación profesional** y su objetivo principal es la formación de expertos en ciberdelincuencia, capacitados para conocer este fenómeno a nivel global, los problemas de persecución y perfiles criminales, las estrategias de prevención, las medidas de investigación actuales para luchar contra el cibercrimen y los métodos de actuación penal contra estas conductas para descubrirlas y sancionarlas.
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/derecho/master-ciberdelincuencia/1.14%20Perfil%20de%20Egreso_MU_CD.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
CB6 - Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación. TIPO: Conocimientos o contenidos
CB7 - Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio. TIPO: Habilidades o destrezas
CG3 - Analizar el fenómeno de la ciberdelincuencia valorando los riesgos y las amenazas que genera. TIPO: Competencias
CG5 - Seleccionar nuevas estrategias adecuadas de actuación frente a la ciberdelincuencia, en base a sus posibilidades de implementación y gestión. TIPO: Competencias
CG6 - Analizar las singularidades en la casuística de los ciberdelitos y contextualizarlos en el fenómeno criminal en el que se desarrollan. TIPO: Competencias
CG7 - Distinguir las diferentes tipologías delictivas que pueden cometerse en el ámbito tecnológico, tanto en la empresa como a nivel particular o de la sociedad, y establecer la estrategia de actuación correspondiente. TIPO: Habilidades o destrezas
CG8 - Aplicar las normas jurídicas en materia de ciberdelincuencia identificando los diversos ciberdelitos. TIPO: Habilidades o destrezas
CG9 - Analizar los problemas derivados de la ciberdelincuencia y sus repercusiones sociales. TIPO: Competencias
CE4 - Diseñar estrategias empresariales de protección de bienes jurídicos en entornos digitales que garanticen la propiedad industrial e intelectual. TIPO: Habilidades o destrezas
CE5 - Asesorar sobre los peligros existentes para los menores de edad en el uso cotidiano de las TIC. TIPO: Habilidades o destrezas
CT1 - Aplicar las nuevas tecnologías como herramientas para el intercambio comunicacional en el desarrollo de procesos de indagación y de aprendizaje. TIPO: Habilidades o destrezas
CT2 - Desarrollar habilidades de comunicación, para redactar informes y documentos, o realizar eficaces presentaciones de los mismos. TIPO: Habilidades o destrezas

CB9 - Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades. TIPO: Competencias
CG1 - Ser capaz de identificar los diferentes intervinientes a nivel nacional e internacional en la lucha contra la ciberdelincuencia y explorar las vías de cooperación necesarias para el trabajo en un equipo de investigación en ciberdelincuencia. TIPO: Conocimientos o contenidos
CG2 - Analizar e interpretar los problemas que se planteen en el ámbito de los delitos informáticos y el entorno digital relacionados con la ciberdelincuencia. TIPO: Competencias
CG4 - Ser capaz de planificar estrategias comunicativas y de análisis en torno a la temática de la ciberdelincuencia. TIPO: Habilidades o destrezas
CE1 - Diseñar estrategias de detección y prevención de fraudes en comercio electrónico. TIPO: Habilidades o destrezas
CE2 - Analizar los diferentes perfiles de ciberdelicuentes y cibervíctimas, sus rasgos y tipología de interacciones. TIPO: Competencias
CE3 - Identificar en los delitos que se producen en el ámbito de la ciberdelincuencia los principales medios de comisión y los factores sociales, ambientales y personales que explican su ocurrencia, así como las circunstancias penales concurrentes en los mismos. TIPO: Conocimientos o contenidos
CE6 - Identificar las principales acciones preventivas en ciberseguridad desarrolladas en el ámbito empresarial. TIPO: Conocimientos o contenidos
CE7 - Diseñar un programa de compliance a nivel de empresa, adaptado a las necesidades de la organización, evaluando los riesgos en la comisión de ciberdelitos por la persona jurídica. TIPO: Habilidades o destrezas
CE8 - Identificar y desarrollar medidas para prevenir, perseguir y sancionar los ciberdelitos relacionados con los derechos fundamentales, el discurso del odio, la violencia de género y la libertad sexual. TIPO: Competencias
CE9 - Desarrollar estrategias preventivas o de detección temprana de ilícitos digitales dirigidos contra los menores de edad. TIPO: Habilidades o destrezas
CE10 - Identificar conductas que vulneren la legislación reguladora de la protección de datos en el ámbito de ubicación y transferencia de archivos digitales y contenido de datos en la nube. TIPO: Conocimientos o contenidos
CE11 - Diseñar estrategias de investigación en el ámbito del ciberterrorismo para neutralizar conductas peligrosas y perseguirlas incluso cuando tienen un origen o destino extranjero. TIPO: Habilidades o destrezas
CE12 - Identificar las medidas de investigación necesarias para la detección de ciberdelitos y la obtención de pruebas para su sanción penal. TIPO: Conocimientos o contenidos
CE13 - Analizar el marco jurídico procesal en relación con la obtención de pruebas para, evitando nulidades en el proceso penal, poder realizar pericias forenses en delitos relacionados con la ciberdelincuencia. TIPO: Competencias
CE14 - Identificar las conductas delictivas en los ciberdelitos, determinar las distintas participaciones de los ciberdelincuentes y aplicar el ámbito penológico correspondiente a cada caso. TIPO: Habilidades o destrezas
CE15 - Ser capaz de realizar y defender un trabajo original sobre la prevención de la ciberdelincuencia y la identificación de cibercriminales. TIPO: Habilidades o destrezas
CB8 - Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios. TIPO: Competencias
CB10 - Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo. 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 mismo, 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 este máster se requerirá:

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 estudios 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.

Además de ello, y de forma más concreta, se requiere que los estudiantes que accedan al máster cumplan al menos uno de los siguientes requisitos:

1. Estén en posesión de alguno de los títulos considerados necesarios para el acceso directo al título propuesto. Así, las titulaciones específicas que facilitarán el acceso al Máster son únicamente las siguientes: **Derecho y Criminología**.

2. Profesionales cualificados (con nivel equivalente a grado universitario) o funcionarios (que cumplan los requisitos exigidos legalmente para el acceso a un máster) de:

a) las Fuerzas y Cuerpos de Seguridad del Estado, cuyas labores estén relacionadas con el fenómeno de la ciberdelincuencia.

b) cuerpos policiales de ámbito autonómico, cuyas labores estén relacionadas con el fenómeno de la ciberdelincuencia.

c) los servicios de Inteligencia nacionales y/o de las Fuerzas Armadas, cuyas labores estén relacionadas con el fenómeno de la ciberdelincuencia.

d) la Administración de Justicia, relacionados con el ámbito del Derecho Penal, cuyas labores estén relacionadas con el fenómeno de la ciberdelincuencia.

e) así como otros ámbitos de la Administración Civil cuyas labores estén relacionadas con el fenómeno de la ciberdelincuencia.

En todo caso, para concretar las labores relacionadas con el fenómeno de la ciberdelincuencia deberían acreditar que han realizado algunas de las siguientes actividades en su ámbito profesional:

1. Que hayan recibido denuncias relacionadas con la comisión de delitos a través de las nuevas tecnologías o en las que esté implicado, ya sea en el *modus operandi* o en la forma de comisión, o en la comunicación, o en el resultado final, algún dispositivo tecnológico.

2. Que hayan investigado y perseguido hechos que puedan tener el carácter de delictivos cometidos a través de la red, a través del teléfono o cualquier dispositivo informático o tecnológico.

3. Que realicen labores de rastreo a través de la red o de las nuevas tecnologías en busca de posibles ilícitos que se hayan cometido o se prevea su comisión.

4. Que en la investigación de delitos, realicen labores relacionadas con la presentación de cualquier tipo de prueba electrónica o periciales informáticas.

5. Que participen en la identificación del autor del delito o en investigaciones en las que se apliquen las medidas del art. 588 bis LECrim.

6. Que realicen labores de prevención en el ámbito de la comisión de delitos a través de internet o de cualquier dispositivo electrónico.

Es decir, en general, las labores relacionadas con el fenómeno de la ciberdelincuencia se refieren a todo tipo de funciones de recepción, investigación y trámite de denuncias o atestados por ciberdelitos (estafas y fraudes, daños, violencia de género, amenazas, coacciones o acoso cometidas por medios tecnológicos, *sextorsión*, *childgrooming*, provocación al odio en redes sociales, ciberterrorismo, así como cualquier otro delito en el que estén implicadas, como medio de comisión o soporte probatorio, las TIC); investigaciones en el ámbito del ciberespacio sobre comisión de estos ilícitos, pertenencia a operaciones en las que se lleve a cabo investigación tecnológica (informática forense, grabación de comunicaciones orales, intervenciones telefónicas, registro de dispositivos informáticos, técnicas OSIT, etc.); o cualesquiera otras relacionadas con los delitos y su comisión por las nuevas tecnologías.

3. Quienes, 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 de conocimiento**:

- Investigación del cibercrimen mediante el empleo de las medidas procesales vigentes en la lucha contra el ciberdelito.
- Cooperación y colaboración internacional en materia de ciberdelincuencia (asistencia técnica, investigación a nivel internacional y planificación de estrategias de cooperación).
- Gestión e implementación de planes de ciberseguridad.
- Estudio de los perfiles de ciberdelincuentes y análisis y desarrollo de estrategias preventivas y apoyo a las víctimas de ciberdelitos.

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

Satisfechos los requisitos específicos de acceso previamente mencionados, y solo en el caso de que el número de solicitudes de plaza que cumplen con los requisitos recogidos en las vías de acceso exceda al número de plazas ofertadas, en la resolución de las solicitudes de admisión se tendrá en cuenta los siguientes criterios de valoración:

- Nota media del expediente en la titulación que otorga el acceso al máster (100 %).

En caso de empate en puntuaciones, se elegirá al que tenga mayor número de matrículas de honor y, en su caso, sobresalientes y así sucesivamente.

Normativa aplicable:

Anexo: 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 Enseñanzas Superiores Oficiales no Universitarias	
MÍNIMO	**MÁXIMO**
0	0
Adjuntar Convenio	
Reconocimiento de Créditos Cursados en Títulos Propios	
MÍNIMO	**MÁXIMO**
0	9
Adjuntar Título Propio	
Ver Apartado 3: Anexo 2.	
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 ni computará a efectos de baremación de expediente.
- Solo se admitirán aquellos estudios propios o de fornación 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 adquiridos 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 o 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.

En base a 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 aprendizaje que se adquieren con las asignaturas reconocidas, podrán ser objeto de reconocimiento por experiencia profesional y laboral, entre otras, las siguientes:

- Prácticas Académicas Externas (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 experiencia se muestre estrechamente relacionada con los conocimientos, competencias y habilidades propias del título universitario oficial.

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

La experiencia profesional o 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 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 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 (ECTS)	Resultados de aprendizaje Específicos	Justificación
Prácticas Académicas Externas	Prácticas Académicas Externas (6 ECTS)	CE9, CE10, CE11, CE13, CE14	Tipo de entidad: Fuerzas y Cuerpos de Seguridad del Estado, INCIBE o instituciones nacionales relacionadas con ciberseguridad, entidades que desarrollen peritajes informáticos o que desarrollen funciones o investigaciones en ciberinteligencia, ciberseguridad o Ciberdefensa. Duración: periodo mínimo de 6 meses. Tareas desempeñadas: estudio de periciales forenses tecnológicas, auditorías de seguridad, elaboración de perfiles de cibercriminales, análisis y prevención de ciberdelitos, consultoría ante ciberataques o asesoramiento legal sobre ciberdelincuencia.

—

Normativa aplicable:

Anexo: Normativa de reconocimiento y transferencia de créditos de UNIR:

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 Anexo I de la memoria.

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: Cuestiones Criminológicas y Victimológicas

4.1.1.1 Datos Básicos del Nivel 2

CARÁCTER	Obligatoria	
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: Derecho Penal Informático y de la Ciberdelincuencia		
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: Perfilación en Ciberdelincuentes y Cibervíctimas		
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		
CB6 - Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación. TIPO: Conocimientos o contenidos		
CG5 - Seleccionar nuevas estrategias adecuadas de actuación frente a la ciberdelincuencia, en base a sus posibilidades de implementación y gestión. TIPO: Competencias		
CG7 - Distinguir las diferentes tipologías delictivas que pueden cometerse en el ámbito tecnológico, tanto en la empresa como a nivel particular o de la sociedad, y establecer la estrategia de actuación correspondiente. TIPO: Habilidades o destrezas		
CE5 - Asesorar sobre los peligros existentes para los menores de edad en el uso cotidiano de las TIC. TIPO: Habilidades o destrezas		
CT1 - Aplicar las nuevas tecnologías como herramientas para el intercambio comunicacional en el desarrollo de procesos de indagación y de aprendizaje. TIPO: Habilidades o destrezas		
CG1 - Ser capaz de identificar los diferentes intervinientes a nivel nacional e internacional en la lucha contra la ciberdelincuencia y explorar las vías de cooperación necesarias para el trabajo en un equipo de investigación en ciberdelincuencia. TIPO: Conocimientos o contenidos		
CG2 - Analizar e interpretar los problemas que se planteen en el ámbito de los delitos informáticos y el entorno digital relacionados con la ciberdelincuencia. TIPO: Competencias		

CG4 - Ser capaz de planificar estrategias comunicativas y de análisis en torno a la temática de la ciberdelincuencia. TIPO: Habilidades o destrezas		
CE2 - Analizar los diferentes perfiles de ciberdelicuentes y cibervíctimas, sus rasgos y tipología de interacciones. TIPO: Competencias		
CE3 - Identificar en los delitos que se producen en el ámbito de la ciberdelincuencia los principales medios de comisión y los factores sociales, ambientales y personales que explican su ocurrencia, así como las circunstancias penales concurrentes en los mismos. TIPO: Conocimientos o contenidos		
CE8 - Identificar y desarrollar medidas para prevenir, perseguir y sancionar los ciberdelitos relacionados con los derechos fundamentales, el discurso del odio, la violencia de género y la libertad sexual. TIPO: Competencias		
CE9 - Desarrollar estrategias preventivas o de detección temprana de ilícitos digitales dirigidos contra los menores de edad. TIPO: Habilidades o destrezas		
CE14 - Identificar las conductas delictivas en los ciberdelitos, determinar las distintas participaciones de los ciberdelincuentes y aplicar el ámbito penológico correspondiente a cada caso. TIPO: Habilidades o destrezas		
CB8 - Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios. TIPO: Competencias		
NIVEL 2: Tipologías Delictivas. Ciberdelitos		
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: Análisis Avanzado de la Ciberdelincuencia Económica y Empresarial		
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: Ciberdelincuencia Social		
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: Ciberdelincuencia en la Infancia y contra las Libertades		
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		
CB6 - Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación. TIPO: Conocimientos o contenidos		
CB7 - Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio. TIPO: Habilidades o destrezas		
CG5 - Seleccionar nuevas estrategias adecuadas de actuación frente a la ciberdelincuencia, en base a sus posibilidades de implementación y gestión. TIPO: Competencias		
CG6 - Analizar las singularidades en la casuística de los ciberdelitos y contextualizarlos en el fenómeno criminal en el que se desarrollan. TIPO: Competencias		
CG7 - Distinguir las diferentes tipologías delictivas que pueden cometerse en el ámbito tecnológico, tanto en la empresa como a nivel particular o de la sociedad, y establecer la estrategia de actuación correspondiente. TIPO: Habilidades o destrezas		
CG9 - Analizar los problemas derivados de la ciberdelincuencia y sus repercusiones sociales. TIPO: Competencias		
CE4 - Diseñar estrategias empresariales de protección de bienes jurídicos en entornos digitales que garanticen la propiedad industrial e intelectual. TIPO: Habilidades o destrezas		
CE5 - Asesorar sobre los peligros existentes para los menores de edad en el uso cotidiano de las TIC. TIPO: Habilidades o destrezas		
CT1 - Aplicar las nuevas tecnologías como herramientas para el intercambio comunicacional en el desarrollo de procesos de indagación y de aprendizaje. TIPO: Habilidades o destrezas		
CG2 - Analizar e interpretar los problemas que se planteen en el ámbito de los delitos informáticos y el entorno digital relacionados con la ciberdelincuencia. TIPO: Competencias		
CG4 - Ser capaz de planificar estrategias comunicativas y de análisis en torno a la temática de la ciberdelincuencia. TIPO: Habilidades o destrezas		
CE1 - Diseñar estrategias de detección y prevención de fraudes en comercio electrónico. TIPO: Habilidades o destrezas		
CE3 - Identificar en los delitos que se producen en el ámbito de la ciberdelincuencia los principales medios de comisión y los factores sociales, ambientales y personales que explican su ocurrencia, así como las circunstancias penales concurrentes en los mismos. TIPO: Conocimientos o contenidos		
CE6 - Identificar las principales acciones preventivas en ciberseguridad desarrolladas en el ámbito empresarial. TIPO: Conocimientos o contenidos		
CE7 - Diseñar un programa de compliance a nivel de empresa, adaptado a las necesidades de la organización, evaluando los riesgos en la comisión de ciberdelitos por la persona jurídica. TIPO: Habilidades o destrezas		
CE8 - Identificar y desarrollar medidas para prevenir, perseguir y sancionar los ciberdelitos relacionados con los derechos fundamentales, el discurso del odio, la violencia de género y la libertad sexual. TIPO: Competencias		
CE9 - Desarrollar estrategias preventivas o de detección temprana de ilícitos digitales dirigidos contra los menores de edad. TIPO: Habilidades o destrezas		
CE11 - Diseñar estrategias de investigación en el ámbito del ciberterrorismo para neutralizar conductas peligrosas y perseguirlas incluso cuando tienen un origen o destino extranjero. TIPO: Habilidades o destrezas		

CE14 - Identificar las conductas delictivas en los ciberdelitos, determinar las distintas participaciones de los ciberdelincuentes y aplicar el ámbito penológico correspondiente a cada caso. TIPO: Habilidades o destrezas		
CB8 - Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios. TIPO: Competencias		
NIVEL 2: Ciberinvestigación Criminal y Proceso Penal		
4.1.1.1 Datos Básicos del Nivel 2		
CARÁCTER	Obligatoria	
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: Investigación Tecnológica Avanzada: La Prueba Electrónica y la Evidencia Digital		
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: Ámbito Procesal y Punitivo en el Marco de la Ciberdelincuencia		
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		
CB6 - Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación. TIPO: Conocimientos o contenidos		
CB7 - Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio. TIPO: Habilidades o destrezas		
CG3 - Analizar el fenómeno de la ciberdelincuencia valorando los riesgos y las amenazas que genera. TIPO: Competencias		
CG8 - Aplicar las normas jurídicas en materia de ciberdelincuencia identificando los diversos ciberdelitos. TIPO: Habilidades o destrezas		

CG9 - Analizar los problemas derivados de la ciberdelincuencia y sus repercusiones sociales. TIPO: Competencias		
CE5 - Asesorar sobre los peligros existentes para los menores de edad en el uso cotidiano de las TIC. TIPO: Habilidades o destrezas		
CT1 - Aplicar las nuevas tecnologías como herramientas para el intercambio comunicacional en el desarrollo de procesos de indagación y de aprendizaje. TIPO: Habilidades o destrezas		
CT2 - Desarrollar habilidades de comunicación, para redactar informes y documentos, o realizar eficaces presentaciones de los mismos. TIPO: Habilidades o destrezas		
CG1 - Ser capaz de identificar los diferentes intervinientes a nivel nacional e internacional en la lucha contra la ciberdelincuencia y explorar las vías de cooperación necesarias para el trabajo en un equipo de investigación en ciberdelincuencia. TIPO: Conocimientos o contenidos		
CG2 - Analizar e interpretar los problemas que se planteen en el ámbito de los delitos informáticos y el entorno digital relacionados con la ciberdelincuencia. TIPO: Competencias		
CG4 - Ser capaz de planificar estrategias comunicativas y de análisis en torno a la temática de la ciberdelincuencia. TIPO: Habilidades o destrezas		
CE3 - Identificar en los delitos que se producen en el ámbito de la ciberdelincuencia los principales medios de comisión y los factores sociales, ambientales y personales que explican su ocurrencia, así como las circunstancias penales concurrentes en los mismos. TIPO: Conocimientos o contenidos		
CE8 - Identificar y desarrollar medidas para prevenir, perseguir y sancionar los ciberdelitos relacionados con los derechos fundamentales, el discurso del odio, la violencia de género y la libertad sexual. TIPO: Competencias		
CE9 - Desarrollar estrategias preventivas o de detección temprana de ilícitos digitales dirigidos contra los menores de edad. TIPO: Habilidades o destrezas		
CE10 - Identificar conductas que vulneren la legislación reguladora de la protección de datos en el ámbito de ubicación y transferencia de archivos digitales y contenido de datos en la nube. TIPO: Conocimientos o contenidos		
CE11 - Diseñar estrategias de investigación en el ámbito del ciberterrorismo para neutralizar conductas peligrosas y perseguirlas incluso cuando tienen un origen o destino extranjero. TIPO: Habilidades o destrezas		
CE12 - Identificar las medidas de investigación necesarias para la detección de ciberdelitos y la obtención de pruebas para su sanción penal. TIPO: Conocimientos o contenidos		
CE13 - Analizar el marco jurídico procesal en relación con la obtención de pruebas para, evitando nulidades en el proceso penal, poder realizar pericias forenses en delitos relacionados con la ciberdelincuencia. TIPO: Competencias		
CB8 - Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios. TIPO: Competencias		
CB10 - Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo. 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		
CB6 - Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación. TIPO: Conocimientos o contenidos		
CB7 - Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio. TIPO: Habilidades o destrezas		
CG3 - Analizar el fenómeno de la ciberdelincuencia valorando los riesgos y las amenazas que genera. TIPO: Competencias		
CG9 - Analizar los problemas derivados de la ciberdelincuencia y sus repercusiones sociales. TIPO: Competencias		
CT1 - Aplicar las nuevas tecnologías como herramientas para el intercambio comunicacional en el desarrollo de procesos de indagación y de aprendizaje. TIPO: Habilidades o destrezas		
CT2 - Desarrollar habilidades de comunicación, para redactar informes y documentos, o realizar eficaces presentaciones de los mismos. TIPO: Habilidades o destrezas		
CB9 - Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades. TIPO: Competencias		
CG2 - Analizar e interpretar los problemas que se planteen en el ámbito de los delitos informáticos y el entorno digital relacionados con la ciberdelincuencia. TIPO: Competencias		
CE15 - Ser capaz de realizar y defender un trabajo original sobre la prevención de la ciberdelincuencia y la identificación de cibercriminales. TIPO: Habilidades o destrezas		
CB8 - Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios. TIPO: Competencias		
CB10 - Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo. TIPO: Habilidades o destrezas		
NIVEL 2: Prácticas Académicas Externas		
4.1.1.1 Datos Básicos del Nivel 2		
CARÁCTER	Prácticas Externas	
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: Prácticas Académicas Externas		
4.1.1.1.1 Datos Básicos del Nivel 3		
CARÁCTER	**ECTS ASIGNATURA**	**DESPLIEGUE TEMPORAL**
Prácticas Externas	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

CB7 - Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio. TIPO: Habilidades o destrezas

CG3 - Analizar el fenómeno de la ciberdelincuencia valorando los riesgos y las amenazas que genera. TIPO: Competencias

CG8 - Aplicar las normas jurídicas en materia de ciberdelincuencia identificando los diversos ciberdelitos. TIPO: Habilidades o destrezas

CG9 - Analizar los problemas derivados de la ciberdelincuencia y sus repercusiones sociales. TIPO: Competencias

CT1 - Aplicar las nuevas tecnologías como herramientas para el intercambio comunicacional en el desarrollo de procesos de indagación y de aprendizaje. TIPO: Habilidades o destrezas

CT2 - Desarrollar habilidades de comunicación, para redactar informes y documentos, o realizar eficaces presentaciones de los mismos. TIPO: Habilidades o destrezas

CB9 - Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades. TIPO: Competencias

CG1 - Ser capaz de identificar los diferentes intervinientes a nivel nacional e internacional en la lucha contra la ciberdelincuencia y explorar las vías de cooperación necesarias para el trabajo en un equipo de investigación en ciberdelincuencia. TIPO: Conocimientos o contenidos

CG2 - Analizar e interpretar los problemas que se planteen en el ámbito de los delitos informáticos y el entorno digital relacionados con la ciberdelincuencia. TIPO: Competencias

CG4 - Ser capaz de planificar estrategias comunicativas y de análisis en torno a la temática de la ciberdelincuencia. TIPO: Habilidades o destrezas

CE9 - Desarrollar estrategias preventivas o de detección temprana de ilícitos digitales dirigidos contra los menores de edad. TIPO: Habilidades o destrezas

CE10 - Identificar conductas que vulneren la legislación reguladora de la protección de datos en el ámbito de ubicación y transferencia de archivos digitales y contenido de datos en la nube. TIPO: Conocimientos o contenidos

CE11 - Diseñar estrategias de investigación en el ámbito del ciberterrorismo para neutralizar conductas peligrosas y perseguirlas incluso cuando tienen un origen o destino extranjero. TIPO: Habilidades o destrezas

CE13 - Analizar el marco jurídico procesal en relación con la obtención de pruebas para, evitando nulidades en el proceso penal, poder realizar pericias forenses en delitos relacionados con la ciberdelincuencia. TIPO: Competencias

CE14 - Identificar las conductas delictivas en los ciberdelitos, determinar las distintas participaciones de los ciberdelincuentes y aplicar el ámbito penológico correspondiente a cada caso. TIPO: Habilidades o destrezas

CB8 - Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios. TIPO: Competencias

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 presenciales virtuales
Recursos didácticos audiovisuales
Estudio del material básico
Lectura del material complementario
Trabajos, casos prácticos y test de evaluación
Tutorías
Trabajo colaborativo
Examen final
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
Estancia en Centro
Lectura de documentación del centro de prácticas
Redacción de la memoria de prácticas
Tutorías (Prácticas)

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 presenciales virtuales, 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, proyectos y/o casos
Test de evaluación
Examen final
Evaluación de la estructura del Trabajo Fin de Máster
Evaluación del contenido individual del Trabajo Fin de Máster
Evaluación de la exposición del Trabajo Fin de Máster
Evaluación con base en el informe del tutor externo
Memoria de prácticas

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

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	2020
Ver Apartado 7: Anexo 1.	
7.2 PROCEDIMIENTO DE ADAPTACIÓN	
No aplicable	
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	

8.2.1. 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.

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.

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*.

8.2.4. Perfil de ingreso recomendado

Las enseñanzas de los diversos títulos de UNIR se dirigen a cualquier persona que, reuniendo las condiciones de acceso, desea tener una enseñanza a distancia ofrecida en un entorno virtual.

Los motivos que suelen llevar a esa elección están relacionados con algún tipo de dificultad para cursar estudios presenciales. Entre estos destacan los de aquellos que ya desempeñan una ocupación laboral o que ya tienen trabajo, que quieren iniciar o reanudar estudios universitarios.

El **perfil recomendado de ingreso** corresponde al de un estudiante que, cumpliendo los requisitos de acceso establecidos en el apartado 3.1., muestre interés por el campo de la ciberdelincuencia. Además, se recomienda que el estudiante posea unas aptitudes que le permitan integrar y relacionar sus conocimientos previos con los que desarrollará en el título:

- Capacidad de abstracción, análisis, síntesis y razonamiento lógico.
- Poseer capacidad de percepción y atención.
- Disponer de sentido práctico de la organización.

8.3 ANEXOS

Ver Apartado 8: Anexo 1.

PERSONAS ASOCIADAS A LA SOLICITUD

RESPONSABLE DEL TÍTULO			
NIF	**NOMBRE**	**PRIMER APELLIDO**	**SEGUNDO APELLIDO**
51683438T	María Dolores	Arranz	Madrid
DOMICILIO	**CÓDIGO POSTAL**	**PROVINCIA**	**MUNICIPIO**
Avenida de la Paz, 137	26006	La Rioja	Logroño
EMAIL	**MÓVIL**	**FAX**	**CARGO**
virginia.montiel@unir.net	676614276	902877037	Vicedecana de Desarrollo y Organización Académica de la Facultad
REPRESENTANTE LEGAL			
NIF	**NOMBRE**	**PRIMER APELLIDO**	**SEGUNDO APELLIDO**
24236227T	Juan Pablo	Guzmán	Palomino
DOMICILIO	**CÓDIGO POSTAL**	**PROVINCIA**	**MUNICIPIO**
Avenida de la Paz, 137	26006	La Rioja	Logroño
EMAIL	**MÓVIL**	**FAX**	**CARGO**
virginia.montiel@unir.net	676614276	902877037	Secretario General
El Rector de la Universidad no es el Representante Legal			
Ver Personas asociadas a la solicitud: Anexo 1.			
SOLICITANTE			
El responsable del título no es el solicitante			

NIF	NOMBRE	PRIMER APELLIDO	SEGUNDO APELLIDO
16609588T	Virginia	Montiel	Martín
DOMICILIO	**CÓDIGO POSTAL**	**PROVINCIA**	**MUNICIPIO**
Avenida de la Paz, 137	26006	La Rioja	Logroño
EMAIL	**MÓVIL**	**FAX**	**CARGO**
virginia.montiel@unir.net	676614276	902877037	Responsable de programas ANECA

INFORME DEL SIGC

Informe del SIGC: Ver Apartado del SIGC: Anexo 1.

Apartado 1: Anexo 6

Nombre :1.10_completo.pdf

HASH SHA1 :CC8C2D486E75CDB5AB58344E990F88AFA98E560E

Código CSV :712162525765128780590919

Ver Fichero: 1.10_completo.pdf

Apartado 4: Anexo 1

Nombre :4.1.pdf

HASH SHA1 :284BBD67871C111506C2B21A8E0D2BC3C682F16B

Código CSV :712234155256650909762502

Ver Fichero: 4.1.pdf

Apartado 5: Anexo 1

Nombre :5.1.pdf

HASH SHA1 :1696FE98A6C4B6D6541F79DC9A2634ACC08F52FD

Código CSV :712166972425972084265713

Ver Fichero: 5.1.pdf

Apartado 5: Anexo 2

Nombre :5.2 (1).pdf

HASH SHA1 :CE8819A7DE2FC16B329CBFDC620C741115DEBA41

Código CSV :704482161256206200192378

Ver Fichero: 5.2 (1).pdf

Apartado 6: Anexo 1

Nombre :6_compressed.pdf

HASH SHA1 :F801FAF0E3DC22728C139F94EC6AA0C207AE889A

Código CSV :712166785325118357384159

Ver Fichero: 6_compressed.pdf

Apartado 7: Anexo 1

Nombre :7 (1).pdf

HASH SHA1 :959C7EE50E1EB782B08898F77ADB562C8B99D2C5

Código CSV :704484666800912028292356

Ver Fichero: 7 (1).pdf

Apartado 8: Anexo 1

Nombre :8.3 Anexo.pdf

HASH SHA1 :B9786349A16BCA549983A79C0C19704F02AB07F1

Código CSV :704510674112682590477196

Ver Fichero: 8.3 Anexo.pdf

Apartado Personas asociadas a la solicitud: Anexo 1

Nombre : Delegacion_Representante_Legal_PABLO_GUZMAN_18052016.pdf

HASH SHA1 :D4E5A5EF190072FEEEBA7875A27E08D566B87E91

Código CSV :37374700580938171550917 0

Ver Fichero: Delegacion_Representante_Legal_PABLO_GUZMAN_18052016.pdf

Apartado Informe del SIGC: Anexo 1

Nombre : Informe_SGIC_20231121_MU_Ciberdelincuencia.pdf

HASH SHA1 :E61AC73E91171A9345DF5235902D6B67F308A3E4

Código CSV :689865749689349061868268

Ver Fichero: Informe_SGIC_20231121_MU_Ciberdelincuencia.pdf